(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 766 802**

(51) Int. CI.:

H04L 29/12	(2006.01)
H04L 29/06	(2006.01)
H04L 12/18	(2006.01)
H04W 8/00	(2009.01)
H04W 12/04	(2009.01)
H04W 12/06	(2009.01)
H04W 76/14	(2008.01)
H04W 64/00	(2009.01)
H04W 92/18	(2009.01)
H04W 88/02	(2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **23.01.2014 PCT/EP2014/051318**

(87) Fecha y número de publicación internacional: **31.07.2014 WO14114711**

(96) Fecha de presentación y número de la solicitud europea: **23.01.2014 E 14701517 (6)**

(97) Fecha y número de publicación de la concesión europea: **20.11.2019 EP 2826223**

(54) Título: **Descubrimiento de proximidad, autenticación y establecimiento de enlace entre dispositivos móviles de comunicación en LTE 3GPP**

(30) Prioridad:

25.01.2013 EP 13152725

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.06.2020

(73) Titular/es:

KONINKLIJKE KPN N.V. (50.0%)
Wilhelminakade 123
3072 AP Rotterdam, NL y
NEDERLANDSE ORGANISATIE VOOR TOEGEPAST-NATUURWETENSCHAPPELIJK ONDERZOEK TNO (50.0%)

(72) Inventor/es:

FRANSEN, FRANK;
VEUGEN, PETER;
DE KIEVIT, SANDER y
EVERTS, MAARTEN

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Descubrimiento de proximidad, autenticación y establecimiento de enlace entre dispositivos móviles de comunicación en LTE 3GPP

Campo de la invención

La presente invención está relacionada con el descubrimiento de proximidad de dispositivos de comunicación. Más específicamente, la invención está relacionada con el descubrimiento de proximidad de dispositivos que puede dar como resultado el establecimiento de una sesión de comunicación dispositivo a dispositivo entre los dispositivos.

Antecedentes

Algunos desarrollos recientes en el estándar de 3GPP están relacionados con redes y dispositivos de la Evolución a Largo Plazo (LTE). LTE, también conocida como estándar de comunicaciones móviles 4G (esto es, de cuarta generación), es un estándar para la comunicación inalámbrica de datos a alta velocidad para teléfonos móviles y terminales de datos. Es el sucesor de las tecnologías de red GSM/EDGE (también conocida como 2G o 2.5G) y UMTS/HSPA (también conocida como 3G), que incrementa la capacidad y velocidad utilizando una interfaz radio diferente junto con mejoras de la red troncal. Algunas extensiones recientes de LTE permiten las comunicaciones dispositivo a dispositivo (D2D), bien directamente o bien utilizando una estación base próxima como retransmisor, como paso siguiente a las comunicaciones tradicionales exclusivamente entre estaciones base y dispositivos móviles. En LTE, la comunicación dispositivo a dispositivo también se conoce como comunicación LTE Directa.

El informe técnico TR 22.803 del 3GPP da a conocer algunos casos de uso de comunicación LTE Directa. En un primer caso de uso, Alice se encuentra en una conferencia y desearía detectar la proximidad de su amigo Bob. Alice activa el descubrimiento en modo directo para su amigo Bob. A tal fin, el teléfono de Alice le envía un mensaje a su operadora de telefonía móvil para hacerle saber que desearía hacer uso del modo directo y, en particular, que Bob pueda descubrirla. El servidor de modo directo de la operadora móvil registra a Alice y Bob como par. A partir de ahí, si la red detecta que Bob y Alice se encuentran próximos (por ejemplo, se encuentran en la misma celda de la red o por algún otro medio), se lo notifica a Alice y Bob y les envía información con la que pueden identificarse de manera segura entre sí sin revelar su privacidad. Un segundo caso de uso está relacionado con servicios públicos de seguridad, como por ejemplo el cuerpo de bomberos, la policía y servicios de ambulancia. Por ejemplo, un bombero que entra en un edificio sin cobertura desearía poder hablar con sus compañeros. En este ejemplo, los dispositivos pueden descubrirse mutuamente y establecer una conexión segura y autenticada.

Cuando unos dispositivos fijos y/o móviles, como por ejemplo teléfonos y dispositivos de comunicación tipo máquina (MTC), se encuentran próximos entre sí, se puede establecer una sesión de comunicación dispositivo a dispositivo entre dichos dispositivos, por ejemplo utilizando LTE Directa en el caso de dispositivos móviles LTE o cualquier otro estándar de comunicación dispositivo a dispositivo, por ejemplo, basado en IEEE 802.11, IEEE 802.16, IEEE 802.20, Bluetooth, Wi-Fi o WiMAX. En este caso típicamente los dispositivos detectan la presencia de los otros y le notifican al usuario la proximidad de otro dispositivo. La versión 4.0 de las especificaciones de Seguridad Bluetooth en particular divulgan cómo establecer un emparejamiento simple seguro, SSP, entre dos dispositivos, basado en un conjunto de parámetros de autenticación.

El documento WO 2013/009288 A1 describe métodos, sistemas y programas de ordenador para una comunicación segura entre dispositivos móviles. En algunos aspectos, la información se transmite de forma inalámbrica desde un primer dispositivo móvil a un segundo dispositivo móvil. La información permite que el segundo dispositivo móvil detecte la proximidad del primer dispositivo móvil. En algunas implementaciones, la información se puede transmitir de forma inalámbrica mediante una interfaz inalámbrica activada por proximidad, como, por ejemplo, una interfaz de Comunicación de Campo Cercano (NFC). En respuesta a dicha información, el primer dispositivo móvil recibe un mensaje y un primer valor de autenticación transmitido de forma inalámbrica desde el segundo dispositivo móvil al primer dispositivo móvil. En el primer dispositivo móvil se genera un segundo valor de autenticación a partir del mensaje y un valor secreto compartido. Para establecer el valor secreto compartido, los dispositivos se pueden configurar para comunicarse con una autoridad de certificación sobre un enlace de comunicación. La integridad del mensaje se verifica mediante la comparación del primer valor de autenticación y el segundo valor de autenticación.

El documento US 20120284517 A1 describe sistemas, métodos y otros modos de realización asociados con la autenticación inalámbrica utilizando mensajes de baliza. De acuerdo con un modo de realización, un controlador de punto de acceso incluye un transmisor configurado para transmitir de forma inalámbrica un mensaje baliza. El mensaje baliza está configurado para anunciarle a un dispositivo remoto que hay un punto de acceso inalámbrico disponible que proporciona acceso a una red. El mensaje baliza incluye un identificador de seguridad que identifica una clave pública para el punto de acceso inalámbrico.

El documento US 2006/0101280 A1 está relacionado con un método de autenticación para realizar la autenticación entre equipos de procesamiento de datos mediante la utilización de información de autenticación del primer equipo. Una vez establecida la comunicación con un equipo de procesamiento de datos, un primer equipo determina si es

necesario o no generar información de autenticación basada en información de identificación acerca del equipo de procesamiento de datos. Si se determina que es necesario generar la información de autenticación, el primer equipo genera la información de autenticación y la almacena en una memoria. Si se determina que es necesario generar la información de autenticación, el primer equipo le envía la información de autenticación generada al equipo de procesamiento de datos con el que se ha establecido la comunicación. Si se determina que es innecesario generar la información de autenticación, el primer equipo le envía la información de autenticación almacenada en la memoria al equipo de procesamiento de datos con el que se ha establecido la comunicación.

El documento US 2012/282922 A1 está relacionado con un equipo de usuario y un nodo de red, así como con métodos relacionados de soporte de redes ad hoc eficientes de recursos entre equipos de usuario (UE) de una red celular. Esto se aborda mediante una solución en la que el nodo de red soporta la red ad hoc entre los UE. El nodo de red es capaz de acceder a una base de datos de capacidad de los equipos de usuario y recibe mensajes de actualización desde los UE con información sobre las capacidades de los equipos de usuario, tales como las bandas de frecuencia que soportan, las RAT (tecnologías de acceso radio) y los modos de antena. El nodo de red actualiza la base de datos de capacidad de los equipos de usuario con la información contenida en el mensaje de actualización recibido y determina, en función de la información almacenada en la base de datos de capacidad de equipos de usuario y un algoritmo de coincidencia, que las capacidades del UE1 y el UE2 coinciden y pueden comunicarse de forma inalámbrica. A continuación, el nodo de red difunde un mensaje ad hoc de "paging" (radiobúsqueda) que incluye las identidades del UE1 y el UE2. El mensaje de "paging" es recibido por los UE1 y UE2 identificados en el mensaje de "paging" y, a continuación, el UE1 puede, por ejemplo, establecer una red ad hoc con el UE2.

El documento US 2011/0098043 A1 está relacionado con el descubrimiento asistido por la red y el establecimiento de comunicaciones dispositivo a dispositivo, D2D, por medio de una asignación de identificadores temporales de dispositivo, que son difundidos por los dispositivos con el fin de realizar la detección de proximidad y el establecimiento de la conexión.

En general, una red puede asistir al descubrimiento de la proximidad de dispositivos. A tal fin, la red determina que es probable que dos dispositivos se encuentren cerca uno del otro e informa a los dispositivos respectivos de la probable proximidad del otro. La red puede no ser capaz de determinar que los dispositivos se encuentran también dentro del alcance, en cuyo caso los dispositivos deben realizar un test de proximidad adicional, por ejemplo difundiendo un identificador para ser reconocido por otros dispositivos cercanos.

Alternativamente, el descubrimiento de proximidad lo realizan directamente los dispositivos. En este caso, los dispositivos normalmente difunden identificadores y descubren otros dispositivos mediante los identificadores difundidos. Es conocido que los dispositivos Bluetooth disponen de semejantes capacidades de descubrimiento de proximidad.

En cualquiera de las soluciones (descubrimiento de proximidad asistido por red o directo), los identificadores de los respectivos dispositivos son difundidos, o en todo caso transmitidos, por los respectivos dispositivos. Típicamente los identificadores son estáticos, lo que hace posible rastrear un dispositivo individual simplemente escuchando el identificador difundido a intervalos regulares. Dicha brecha en la privacidad del usuario es altamente indeseable.

Otro inconveniente de las soluciones de descubrimiento de proximidad conocidas es que se utilizan para el descubrimiento de dispositivos individuales. Se necesita una solución de capacidad de descubrimiento selectiva que permita tanto el descubrimiento de proximidad de un dispositivo individual como el descubrimiento de proximidad de un grupo de dispositivos. En ese caso, por ejemplo, un usuario podría ajustar la capacidad de su dispositivo para ser descubierto de tal modo que solo se identifique a un número limitado de dispositivos, por ejemplo, en una conferencia solo a los dispositivos de colegas, o en un concierto pop solo a los dispositivos de amigos. Preferiblemente, otros dispositivos que se encuentren dentro del alcance para una comunicación dispositivo a dispositivo, no deberían ser capaces de detectar la proximidad de los dispositivos en el grupo.

Se necesita una solución que permita el descubrimiento de proximidad de dispositivos en una red de radio controlada que respete la privacidad, permita la capacidad de descubrimiento selectiva y, preferiblemente, tenga un perfil bajo en términos de la carga de red y la potencia de procesamiento requerida.

Resumen de la invención

Un objetivo de la invención es proporcionar una solución que permita el descubrimiento de proximidad de dispositivos en una red de radio controlada que respete la privacidad, permita la capacidad de descubrimiento selectiva y, preferiblemente, tenga un perfil bajo en términos de la carga de red y la potencia de procesamiento requerida. La invención es particularmente útil, pero no se limita a, dispositivos que sean capaces de comunicación dispositivo a dispositivo y deseen descubrir dispositivos cercanos para una sesión de comunicación dispositivo a dispositivo.

La invención se recoge en las reivindicaciones adjuntas, y está relacionada con un método para el descubrimiento de proximidad entre un dispositivo origen y uno o más dispositivos objetivo, y además reivindica un dispositivo origen, un dispositivo objetivo y una red.

De acuerdo con un aspecto de la invención, se propone un método para el descubrimiento de proximidad entre un dispositivo origen y uno o más dispositivos objetivo. El método comprende recibir en el dispositivo origen unos primeros datos que incluyen un identificador. El método comprende, además, recibir en el dispositivo objetivo unos segundos datos que incluyen una primera representación del identificador. El método comprende, además, difundir por parte del dispositivo origen una señal que comprende una segunda representación del identificador. El método comprende, además, recibir la señal en el dispositivo objetivo. El método comprende, además, comparar en el dispositivo objetivo la primera representación del identificador con la segunda representación del identificador para obtener un resultado de la comparación con el fin de establecer un descubrimiento de proximidad exitoso.

El resultado de la comparación así obtenido indica típicamente si coinciden o no los identificadores en la primera y segunda representación de los identificadores. Si es así, se puede concluir que el descubrimiento de proximidad es exitoso.

En lugar del identificador, resulta ventajoso que el dispositivo origen difunda un valor derivado del identificador que únicamente pueden relacionar con el dispositivo origen un dispositivo objetivo o un grupo de dispositivos objetivo específicos. De ese modo, el dispositivo objetivo puede reconocer quién está haciendo la difusión y, por ejemplo, concluir que el dispositivo origen se encuentra a corta distancia, por ejemplo dentro del alcance para una sesión de comunicación dispositivo a dispositivo, o desencadenar cualquier acción basada en que el dispositivo origen se encuentre a corta distancia, por ejemplo cobrando en una garita de peaje. Mientras tanto, la identidad del dispositivo origen no es rastreable.

En un modo de realización de la invención el método puede comprender, además, transmitir desde el dispositivo objetivo al dispositivo origen un mensaje de confirmación en función del resultado de la comparación. Esto tiene la ventaja de permitir que el dispositivo origen sepa que el dispositivo objetivo se encuentra a corta distancia.

En otro modo de realización, el identificador puede ser un identificador temporal de difusión que identifica de forma unívoca al dispositivo objetivo, y el identificador se puede asociar al dispositivo origen por parte del dispositivo objetivo. Esto tiene la ventaja de permitir que el dispositivo origen transmita un identificador que para alguien que lo intente interceptar parezca no estar vinculado con el dispositivo origen, consiguiendo que el dispositivo origen no pueda ser rastreado. El dispositivo objetivo es capaz de asociar el identificador al dispositivo de origen.

En otro modo de realización, el dispositivo origen y el uno o más dispositivos objetivo pueden formar un grupo de dispositivos y el identificador puede identificar al grupo de dispositivos. Esto tiene la ventaja de permitir el descubrimiento de proximidad de un grupo de dispositivos objetivo en lugar de tan solo un dispositivo objetivo.

En otro modo de realización, el dispositivo origen y el uno o más dispositivos objetivo se pueden configurar para conectarse en comunicación a una red, y los primeros datos y los segundos datos se pueden recibir desde un servidor en la red. Alternativamente, los primeros datos y los segundos datos se pueden recibir desde el dispositivo origen. Esto tiene la ventaja de permitir que intervenga la red u operen de forma autónoma sin la red.

En otro modo de realización de la invención, el método puede comprender, además, recibir en el dispositivo objetivo unos terceros datos que incluyen una tercera representación del identificador. La primera representación del identificador puede ser un valor derivado del identificador obtenido mediante una primera función matemática que utiliza el identificador y un número aleatorio como argumentos para calcular el valor derivado del identificador. La tercera representación del identificador puede ser el número aleatorio. El paso de comparación puede comprender calcular el valor derivado del identificador utilizando una segunda función matemática idéntica a la primera función matemática, que utiliza como argumentos la segunda representación del identificador y la tercera representación del identificador. El paso de comparación puede comprender, además, comparar el valor derivado calculado del identificador con la primera representación del identificador. El número aleatorio puede ser un número aleatorio generado por el servidor o por el dispositivo origen. Alternativamente, el número aleatorio puede ser una sal generada por el servidor o por el dispositivo origen. Alternativamente, el número aleatorio puede ser un valor derivado a partir de un número aleatorio adicional obtenido en el servidor o en el dispositivo origen mediante una tercera función matemática que utiliza, como argumentos para calcular el valor derivado del número aleatorio, el número aleatorio adicional y un identificador origen que identifica al dispositivo origen.

Esto tiene la ventaja de añadir un nivel de ocultación a los identificadores intercambiados, haciendo más difícil rastrear los dispositivos.

En otro modo de realización, los segundos datos pueden comprender, además, un identificador de boleto (ticket). El método puede comprender, además, recibir en el dispositivo origen desde el servidor datos del boleto que comprenden el identificador del boleto, los primeros datos y unos cuartos datos. El método puede comprender, además, transmitir el identificador del boleto desde el dispositivo objetivo al servidor para obtener una copia de los

cuartos datos asociados con el identificador del boleto. El método puede comprender, además, recibir en el dispositivo objetivo la copia de los cuartos datos desde el servidor. El mensaje de confirmación puede comprender la copia de los cuartos datos para su verificación con los cuartos datos del dispositivo origen.

La utilización del boleto hace posible, de forma ventajosa, rastrear los intentos de descubrimiento de proximidad. El rastreo puede, por ejemplo, utilizarse para registrar o aplicar una tarifa por los intentos de descubrimiento de proximidad.

En otro modo de realización, el método puede comprender, además, la aplicación de una tarifa por parte de un operador del servidor a la solicitud de los primeros datos, los segundos datos y/o los datos del boleto por parte del dispositivo origen o el dispositivo objetivo. Esto tiene la ventaja de permitir aplicar una tarifa por los intentos de descubrimiento de proximidad, posiblemente solo a los intentos de descubrimiento de proximidad realizados con éxito.

En otro modo de realización, el método puede comprender, además, recibir en el dispositivo objetivo unos primeros datos de reto desde el dispositivo origen. El método puede comprender, además, calcular en el dispositivo objetivo unos primeros datos de reto derivados mediante una cuarta función matemática, por ejemplo, una función hash(función de aleatorización), con los primeros datos de reto. El mensaje de reconocimiento puede comprender, además de los primeros datos de reto derivados, unos segundos datos de reto. El método puede comprender, además, calcular en el dispositivo origen los primeros datos de reto derivados mediante una quinta función matemática idéntica a la cuarta función matemática con los primeros datos de reto para compararlos con los primeros datos de reto derivados recibidos. El método puede comprender, además, calcular en el dispositivo origen los segundos datos de reto derivados utilizando una sexta función matemática con los segundos datos de reto. El método puede comprender, además, transmitirle al dispositivo objetivo los segundos datos de reto derivados. El método puede comprender, además, calcular en el dispositivo objetivo los segundos datos de reto derivados mediante una séptima función matemática idéntica a la sexta función matemática con los segundos datos de reto para compararlos con los segundos datos de reto derivados recibidos.

Esto tiene la ventaja de añadir un nivel de seguridad al intercambio de identificadores en forma de una autenticación de reto-respuesta.

En otro modo de realización, los datos del boleto pueden comprender además una clave de cifrado. El método puede comprender, además, recibir en el dispositivo objetivo desde el servidor la clave de cifrado asociada en el servidor al identificador del boleto. La cuarta, quinta, sexta y séptima funciones matemáticas pueden comprender una función criptográfica que utiliza la clave de cifrado.

Esto tiene la ventaja de añadir un nivel de seguridad al intercambio de identificadores.

De acuerdo con un aspecto de la invención, se propone un dispositivo origen configurado para llevar a cabo un procedimiento de descubrimiento de proximidad con uno o más dispositivos objetivo utilizando uno o más pasos del método descrito más arriba.

De acuerdo con un aspecto de la invención, se propone un dispositivo objetivo configurado para llevar a cabo un procedimiento de descubrimiento de proximidad con un dispositivo origen utilizando uno o más pasos del método descrito más arriba.

De acuerdo con un aspecto de la invención, se propone una red que comprende un dispositivo origen tal como se ha descrito más arriba y uno o más dispositivos objetivo tal como se ha descrito más arriba.

De aquí en adelante se describirán de forma más detallada algunos modos de realización de la invención. No obstante, se debe entender que estos modos de realización no se pueden interpretar como limitantes del alcance de protección para la presente invención.

Breve descripción de los dibujos

Los aspectos de la invención se explicarán con mayor detalle haciendo referencia a algunos ejemplos de modos de realización que se ilustran en los dibujos, en los que:

las Fig. 1-6 son procedimientos de descubrimiento de proximidad de acuerdo con algunos ejemplos de modos de realización de la invención, representados en forma de diagramas de secuencia temporal, entre un dispositivo origen, un dispositivo objetivo y opcionalmente un servidor.

Descripción detallada de los dibujos

En la descripción que se hace a continuación, los términos "dispositivo", "terminal" y "equipo de usuario (UE)" se deben entender como sinónimos de un dispositivo fijo o móvil de usuario final o MTC. Un "par (peer)" se debe

entender como cualquier dispositivo fijo o móvil de usuario final que puede participar en una comunicación dispositivo a dispositivo.

En el modo de comunicación dispositivo a dispositivo los dispositivos se comunican directamente, es decir, sin utilizar una red fija o inalámbrica. Los enlaces de comunicación dispositivo a dispositivo pueden utilizar una estación base para retransmitir las señales entre los dispositivos, pero sin utilizar ninguna funcionalidad de red adicional perteneciente a la red de la estación base. Los pares pueden estar conectados a una red inalámbrica o fija además del modo de comunicación dispositivo a dispositivo.

La invención le permite a un dispositivo descubrir uno o más otros dispositivos dentro del alcance del modo de comunicación dispositivo a dispositivo. Este descubrimiento de proximidad puede hacer que un dispositivo objetivo, por ejemplo, empiece a escuchar señales de un dispositivo origen o realice cualquier otra acción basada en el descubrimiento de proximidad, como por ejemplo el cobro en una garita de peaje. El descubrimiento de proximidad puede dar lugar al establecimiento de una comunicación dispositivo a dispositivo entre el dispositivo origen y el dispositivo objetivo.

Para permitir el descubrimiento de proximidad se intercambian las identidades de los dispositivos o las representaciones de las identidades. El intercambio de identificadores se realiza de tal modo que los dispositivos no se puedan rastrear escuchando o tratando de interceptar las transmisiones de los dispositivos y capturando los identificadores transmitidos. Al no ser rastreable, se incrementa la privacidad de los usuarios de los dispositivos.

Para establecer una sesión de comunicación dispositivo a dispositivo entre dos o más dispositivos que disponen de una conexión fija o inalámbrica a una red, uno de los dispositivos puede activar opcionalmente otros dispositivos antes de comenzar el procedimiento de descubrimiento de proximidad indicándole a un servidor de la red que desearía ser descubierto o descubrir un cierto (conjunto de) par(es). Antes del procedimiento de descubrimiento de proximidad, una red, un tercero (por ejemplo, un proveedor over-the-top (por encima de la red) o cualquier otro tercero) o los propios dispositivos detectan generalmente que algunos pares se encuentran próximos.

Como parte del procedimiento de descubrimiento de proximidad, un dispositivo origen que desea ser descubierto difunde un mensaje que incluye un identificador o una representación del identificador. Este identificador puede ser un identificador del dispositivo objetivo a contactar, o del dispositivo origen, o un valor derivado del mismo o una asociación de seguridad común utilizada por un conjunto de pares. Preferiblemente, el dispositivo no difunde su propio identificador de forma obvia con el fin de evitar la trazabilidad del dispositivo.

El identificador puede ser un identificador temporal de difusión (T-BID) y puede cambiar a lo largo del tiempo. El T-BID se puede cambiar mediante provisión por parte de un tercero, por ejemplo, por una red que proporciona a los dispositivos nuevos identificadores o por un servicio over-the-top, esto es, un agente externo a la red como Facebook, Google+ o Whatsapp, que proporciona nuevos identificadores. El T-BID se puede cambiar por medio de una sesión de comunicación entre dos dispositivos que tiene lugar sobre la red (es decir, que no utiliza el modo de comunicación dispositivo a dispositivo) o cualquier otra conexión, como por ejemplo WiFi, Bluetooth, NFC o comunicación de cámara y pantalla, por ejemplo mediante el intercambio por parte de los dispositivos de nuevas identidades temporales o un número aleatorio/algoritmo para calcular un nuevo identificador temporal. El T-BID se puede cambiar mediante un algoritmo que incluya, por ejemplo, el tiempo, el número de veces que se ha establecido una conexión dispositivo a dispositivo entre los dos (o más) dispositivos, un número aleatorio o una sal proporcionados por un tercero, como por ejemplo un operador de red o un proveedor de servicios over-the-top, y/o un número aleatorio que se transmite conjuntamente con un identificador cifrado/aleatorizado.

Como parte del procedimiento de descubrimiento de proximidad, un dispositivo objetivo extrae la información necesaria del mensaje de difusión (por ejemplo, descifrándolo, volviendo a aleatorizarlo o simplemente comparándolo con una lista de identidades conocidas). El dispositivo origen difunde su identidad de tal forma que únicamente un dispositivo objetivo específico pueda saber quién está realizando la difusión.

Opcionalmente, el dispositivo objetivo responde enviándole un mensaje de confirmación al dispositivo origen indicando que escuchó al otro dispositivo y que está disponible para una comunicación dispositivo a dispositivo. El mensaje de reconocimiento opcional puede contener una respuesta a un reto que puede haberse incluido en la difusión inicial. El mensaje de reconocimiento opcional puede contener datos a partir de los cuales se puede establecer que un dispositivo origen y un dispositivo objetivo comparten una clave secreta común a efectos de autenticación.

Tras un descubrimiento de proximidad exitoso, se puede establecer una conexión dispositivo a dispositivo entre los dispositivos.

El procedimiento de descubrimiento de proximidad se puede utilizar para establecer una conexión segura dispositivo a dispositivo. Puede ser deseable verificar que los dos dispositivos se pueden autenticar mutuamente (por ejemplo, para evitar un ataque por parte de alguien intermedio) y que la red tiene algún tipo de control sobre cómo se establece la conexión (por ejemplo, para aplicar una tarifa al descubrimiento de proximidad). El descubrimiento de

proximidad puede incorporar en el mismo un procedimiento de reconocimiento de tres vías que se puede implementar del siguiente modo:

1. El dispositivo origen le envía un número aleatorio (el reto) a un dispositivo objetivo en la misma difusión que el T-BID;

2. El dispositivo objetivo calcula el valor de la función hash(reto‖ clave secreta común), en donde la clave secreta común puede ser, por ejemplo, un número aleatorio, una sal o un T-BID común. El dispositivo objetivo genera respuestas aleatorias adicionales con un mensaje que incluye un número aleatorio‖hash(reto‖clave secreta común);

3. El dispositivo origen puede verificar el valor de la función hash(reto‖clave secreta común) y responde con un mensaje que incluye el valor de la función hash(nuevo número aleatorio‖clave secreta común);

4. El dispositivo objetivo puede verificar el valor de la función hash(nuevo número aleatorio‖clave secreta común) y ahora tanto el dispositivo origen como el dispositivo objetivo saben que ambos tienen la misma clave secreta común y se han autenticado mutuamente.

En los siguientes ejemplos de modos de realización de la invención se explicará de forma más detallada el procedimiento de descubrimiento de proximidad que se ha esquematizado más arriba.

En el procedimiento de descubrimiento de proximidad se pueden utilizar diferentes tipos de identificadores, ejemplos de los cuales son un identificador de difusión (BID), un identificador temporal de difusión (T-BID), un identificador de difusión específico de grupo (G T-BID), un identificador de difusión (temporal) específico de amigo (F (T)-BID) y un identificador de difusión (temporal) de asociación de seguridad (SA(T)-BID). Un identificador de difusión es un identificador globalmente único que se difunde sobre un medio compartido para anunciar la propia presencia o llamar a alguien. Un dispositivo puede difundir, bien su valor derivado del BID o el BID del "amigo"/otro dispositivo al que desea llamar. Un identificador temporal de difusión es un identificador de difusión que se utiliza únicamente para un período de tiempo, utilización o ubicación geográfica limitados. Una excepción a esta regla consiste en que un "T-BID de un solo uso" se deriva del T-BID y se difunde en su lugar. Un (T-)BID específico de grupo es un identificador de difusión que se refiere a un grupo. Esto significa que todos los dispositivos del grupo escuchan por si llega este BID. Un (T)-BID específico de amigo es un identificador de difusión que se comparte únicamente entre dos amigos/dispositivos. Un (T-)BID de asociación de seguridad es un identificador de difusión que se refiere a una asociación de seguridad. Esto significa que si dos dispositivos comparten una asociación de seguridad, están a la escucha del mismo identificador de difusión.

Típicamente, al procedimiento de descubrimiento de proximidad le precede una detección de proximidad. En la fase de detección de proximidad, los dispositivos reciben información que les indica que se encuentran próximos. En el procedimiento de descubrimiento de proximidad, uno o más de los dispositivos que han recibido la información de que se encuentran cerca determinan si es posible o no una comunicación dispositivo a dispositivo. Existen múltiples formas de llevar a cabo una detección de proximidad. Por ejemplo, una red puede detectar y notificar que dos pares se encuentran próximos. Esto puede ser una ventaja, en primer lugar porque el dispositivo solo tiene que difundir un identificador una vez que ha sido notificado por la red, lo que conduce a un menor consumo de batería y una menor utilización del canal de difusión, y en segundo lugar porque la red puede proporcionar (en el mismo mensaje) unos identificadores y (opcionalmente) material criptográfico. Adicional o alternativamente, un proveedor de servicios over-the-top o un tercero les notifica a los pares que se encuentran próximos. Adicional o alternativamente, los usuarios pueden activar dispositivos que se encuentren próximos entre sí. Esto puede resultar ventajoso en aquellas situaciones en las que no hay cobertura de red y uno quisiera establecer una conexión dispositivo a dispositivo. En caso de que sí haya cobertura de red, este método aún puede ser ventajoso, por ejemplo para pares que todavía no se conocen entre sí, por ejemplo, en caso de que se conozca a una nueva persona y se desee intercambiar los números de teléfono.

Las Fig. 1-6 ilustran ejemplos de modos de realización de la invención, en donde los procedimientos de descubrimiento de proximidad se representan en forma de diagramas de secuencia temporal entre un dispositivo origen 1, un dispositivo objetivo 2 y opcionalmente un servidor 3 en una red. Se debe entender que puede haber múltiples dispositivos objetivo 2. Las flechas indican los flujos de datos. Los puntos negros indican las acciones que se llevan a cabo en un dispositivo. Los números de referencia entre llaves "{}" indican elementos de datos. Las líneas discontinuas indican pasos opcionales.

En la Fig. 1, en el dispositivo origen 1 se reciben 101 unos primeros datos 11 que contienen un identificador 12. Los primeros datos 11 se pueden haber originado en un servidor externo o en el propio dispositivo origen 1. En este último caso, el dispositivo origen 1 genera el identificador 12. En el dispositivo objetivo 2 se reciben 102 unos segundos datos 20 que contienen una primera representación 21 del identificador 12. Los segundos datos 20 se pueden haber originado en el servidor externo o en el dispositivo origen 1. A continuación, el dispositivo origen 1 difunde 103 una señal 103 que contiene una segunda representación 31 del identificador 12, la cual se recibe 104 en el dispositivo objetivo 2. El dispositivo objetivo 2 compara 105 la primera representación 21 del identificador 12 con la segunda representación 31 del identificador 12. El resultado de la comparación obtenido de este modo indica si

coinciden o no los identificadores en la primera y segunda representaciones de los identificadores. En el primer caso, se puede concluir que el descubrimiento de proximidad ha sido exitoso, lo que opcionalmente se le puede notificar 106 al dispositivo origen 1 en un mensaje de reconocimiento 40.

La Fig. 2 muestra un modo de realización basado en boletos y asistido por la red que permite de forma ventajosa aplicar, por parte de un operador de red, una tarifa de descubrimiento de proximidad mediante la detección de la utilización de los boletos.

Antes del descubrimiento de proximidad, el dispositivo origen 1 le informa 201 a un servidor 3 de la red, o de un tercero, que desea descubrir uno o más dispositivos objetivo 2. La red o el tercero pueden saber cuáles de estos dispositivos objetivo 2 indicados pueden ser descubiertos o ser capaces de descubrir, y relacionarlos como pares, por ejemplo porque los dispositivos son abonados de la red o del tercero y están siendo rastreados o porque los dispositivos se lo han notificado a la red o al tercero.

El servidor 3 le proporciona 101 al dispositivo origen 1 un boleto en forma de datos del boleto 10, en los que al dispositivo origen 1 se le proporciona un identificador 12 para difundir 103 con el fin de contactar con cada uno de sus pares 2. La red 3 también les notifica a los pares 2 el identificador 21 del dispositivo origen 1 que deberían escuchar. El identificador 21 puede ser idéntico al identificador 12 o a una primera representación 21 del identificador 12.

La red puede incluir opcionalmente en el boleto 10 una asociación de seguridad 14, por ejemplo, una clave criptográfica, que el dispositivo origen 1 puede utilizar para establecer de forma segura la conexión a uno de sus pares 2. De modo análogo, la red 3 también puede enviarle la asociación de seguridad 14 al dispositivo objetivo 2, aunque desde la perspectiva de la tarificación puede ser deseable enviarle el boleto completo una vez que el dispositivo objetivo 2 lo haya solicitado. La razón es que, en ese caso, la red puede estar segura de que se ha producido un descubrimiento exitoso, lo cual significa que se puede aplicar la tarifa. Alternativamente, la red puede enviar las claves 14 cuando la red 3 detecte que dos pares 1, 2 se encuentran próximos. En este caso, la red 3 participa en la detección de proximidad o en el establecimiento de la conexión. Esto es ventajoso para la renovación de las claves. Por otro lado, la red 3 no tiene que mantener un registro con claves para todos los dispositivos pares.

La red 3 puede enviar los identificadores 12 y/o el valor derivado 21 del identificador 12 en el punto de detección de proximidad.

Para cada uno de sus pares 2, el dispositivo origen 1 tiene ahora un boleto 10 que contiene la siguiente información: un identificador 22 del boleto; opcionalmente un clave secreta común o un número aleatorio para ser utilizado en un sistema opcional de respuesta al reto; un identificador 12, 21, por ejemplo un T-BID, que el primer dispositivo 1 puede utilizar para contactar con el dispositivo objetivo 2; opcionalmente, un identificador adicional 13, por ejemplo un T-BID, que el dispositivo objetivo 2 puede utilizar en su respuesta para contactar con el primer dispositivo 1. En los ejemplos de modos de realización, el identificador adicional 13 también recibe el nombre de cuartos datos.

Opcionalmente, en los datos del boleto 10 se puede incluir una clave criptográfica maestra a partir de la cual se pueden derivar otras claves o un conjunto de claves (claves de cifrado y claves de protección de integridad).

Cada uno de los pares 1, 2 ahora tiene la siguiente información en la memoria: los T-BID 12, 21 (o una representación de los mismos) a escuchar y relacionar con el dispositivo origen 1; opcionalmente, la misma clave secreta común o número aleatorio; el identificador 22 del boleto; opcionalmente, una clave criptográfica maestra a partir de cual se pueden derivar otras claves o un conjunto de claves (claves de cifrado y claves de protección de integridad).

En algún instante posterior, la red o un tercero/proveedor over-the-top puede detectar que el dispositivo origen y el dispositivo objetivo se encuentran próximos (e incluso se pueden descubrir entre sí, esto es, que ninguno de los usuarios ha cambiado su configuración). La red o el tercero le notifican al primer dispositivo que se encuentran próximos.

Aquí la ventaja del sistema basado en boletos resulta evidente: no tiene que ser la red la que realice la detección de proximidad, lo que significa que una vez que la red ha emitido el boleto 10 que incluye las claves 14, solo tiene que proporcionarle las claves 14 al dispositivo objetivo 2 y facturar al dispositivo origen 1.

El primer dispositivo 1 difunde 103 una señal 30 que contiene el identificador temporal de difusión recibido previamente o una segunda representación 31 del mismo, que recibe 104 el dispositivo objetivo 2.

Opcionalmente, se puede ampliar el mecanismo con un sistema de respuesta al reto. En este caso, la difusión 103 del identificador 31 se podría realizar junto con un reto 32 (también denominado primeros datos de reto 32 en los ejemplos de los modos de realización), al cual el dispositivo objetivo 2 puede proporcionar la respuesta correcta.

Después de que el dispositivo objetivo 2 haya recibido la transmisión, opcionalmente le responde al dispositivo objetivo 1 que ha recibido el mensaje mediante un mensaje 106 de confirmación. Opcionalmente, como se ha indicado más arriba, al recibir el mensaje de difusión 103 el dispositivo objetivo 2 recupera el boleto completo (incluidas las claves) de la red. Opcionalmente, el dispositivo objetivo 2 calcula 114 su respuesta al reto 32, opcionalmente lo encripta y le envía la respuesta 106 al primer dispositivo 1.

La respuesta 106 al reto 32 puede ser de la forma hash(reto 32‖clave secreta común). Al recibirla, el dispositivo origen 1 puede realizar el mismo cálculo y comprobar 115 si la respuesta es la misma. La ventaja de encriptar también la respuesta es que ésta no es vulnerable a un ataque de fuerza bruta o de tabla arco iris sobre la función hash. Aunque la solución sigue siendo segura incluso sin cifrado.

El dispositivo objetivo 2 también puede incluir un reto 43 (también denominado segundos datos de reto 43 en los ejemplos de los modos de realización) en su respuesta. Éste puede ser otro número aleatorio generado por el dispositivo objetivo 2.

El dispositivo origen opcionalmente calcula 116 la función hash(reto 43‖clave secreta común) y responde 117 al dispositivo objetivo 2 con este valor 33 derivado de los segundos datos de reto, que a su vez puede verificar si el dispositivo origen 1 ha calculado correctamente la función hash(reto 43‖ clave secreta común). En este momento, a partir de la asociación de seguridad existente entre ambos se puede establecer opcionalmente una conexión 202 segura y autenticada.

Un solo boleto 10 se puede utilizar varias veces, aunque se recomienda limitar su utilización a un número bajo de ocasiones con el fin de dificultar el rastreo de los T-BID difundidos. Esto quiere decir que incluso tras la difusión fallida de un T-BID (por ejemplo, no se pudo contactar con el par), es posible que se deba emitir un nuevo boleto 10.

Es concebible que se pueda desear reutilizar el mismo boleto sin que éste pueda ser rastreado. En este caso, además de la Fig. 2 se pueden utilizar las soluciones que se ilustran en la Fig. 4 y la Fig. 6 y la solución que se describe más abajo para dirigirse a grupos.

En los modos de realización asistidos por la red que se ilustran en la Fig. 3 y la Fig. 4, los identificadores se han cargado previamente en los pares 1, 2 y se le notifica a la red con antelación que el dispositivo origen 1 y el/(los) dispositivo(s) objetivo 2 son pares.

Haciendo referencia a la Fig. 2, antes del descubrimiento de proximidad el dispositivo origen 1 le notifica a la red 3 que desearía descubrir uno o más dispositivos objetivo 2. La red 3 sabe cuáles de esos dispositivos objetivo 2 indicados son detectables o son capaces de descubrir y los relaciona como pares. De este modo la red puede detectar que un dispositivo origen 1 y un dispositivo objetivo 2 se encuentran próximos e informarles a ambos.

Estos pasos anteriores al descubrimiento de proximidad se indican en el bloque 203.

En algún intervalo especificado (por ejemplo, durante la noche o cualquier otro intervalo de tiempo), los pares 1, 2 reciben 101, 102 un conjunto de T-BID 12, 21 (u otros identificadores 12, 21) que se pueden utilizar en el descubrimiento de proximidad para cada uno de los dispositivos 1, 2. Aquí, los identificadores 12 se reciben 101 en los primeros datos 11 procedentes de la red en el dispositivo origen 1, y los identificadores 21 se reciben 102 en los segundos datos procedentes de la red en el/(los) dispositivo(s) objetivo 2. En este ejemplo, los T-BID 12, 21 son T-BID específicos de los pares. Asimismo, a los pares 1, 2 se les proporcionan 101, 102 los T-BID 12, 21 que utilizará el otro dispositivo. Opcionalmente, los pares 1, 2 también reciben 101, 102 un T-BID General 12, 21 (Gen T-BID) que se puede utilizar para el descubrimiento de un grupo de dispositivos. Dicho Gen T-BID 12, 21 también se le distribuye a cada uno de los dispositivos emparejados. Cada par 1, 2 ahora tiene un registro que puede parecerse a la siguiente tabla (este ejemplo es válido para el dispositivo origen 1):

	Difunde	Recibe	
	T-BID	Gen T-BID	T-BID
T-BID General	a		
T-BID para el dispositivo objetivo 1	b	f	j
T-BID para el dispositivo objetivo 2	c	g	k
T-BID para el dispositivo objetivo 3	d	h	m

	Difunde	Recibe	
	T-BID	Gen T-BID	T-BID
T-BID para el dispositivo objetivo 4	e	i	n

En la parte Difunde de la tabla están los T-BID 31 (esto es, "b", "c", "d" y "e") que se difundirán 103 en una señal 30 desde el dispositivo origen 1 y se recibirán 104 en un dispositivo objetivo 2 en caso de que el dispositivo origen 1 deseara ponerse en contacto con cualquiera de los dispositivos objetivo 2 específicos o ser descubierto por cualquiera que utilice el T-BID General 31 (esto es, "a"). En la parte Recibe de la tabla están las difusiones que el dispositivo origen 1 debería escuchar en caso de descubrimiento entre pares. Así, si el dispositivo origen 1 deseara contactar con el primer dispositivo objetivo 2 debería difundir 103 "b". Alternativamente, si el dispositivo origen 1 deseara poder ser descubierto por cualquiera que tenga su T-BID general, difunde 103 "a". En la parte Recibe, el dispositivo origen 1 debería escuchar las dos últimas columnas. Si se difunde alguno de los valores que aparecen en la última columna ("j", "k", "m", "n"), puede concluir 105 que uno de sus pares 2 está próximo y está tratando de ponerse en contacto con el dispositivo origen 1. Si se difunde cualquiera de los valores que aparecen en la columna central ("f", "g", "h", "i"), el dispositivo origen 1 sabe que uno de sus pares 2 se encuentra próximo y que están difundiendo su T-BID general solo para hacer saber que están presentes.

Se debe entender que la forma de almacenar el registro es arbitraria. El formato de tabla es tan solo un ejemplo, y se puede utilizar cualquier otra forma de almacenar los valores. Los identificadores 12, 21 se muestran como letras del alfabeto. Se debe entender que los identificadores pueden tener cualquier valor binario, valor decimal, valor hexadecimal, valor word (una palabra), valor dword (doble palabra), valor de cadena de caracteres, etcétera, de cualquier longitud.

El modo de realización de la Fig. 3 permite difundir simplemente un T-BID Gen 31 o una serie de T-BID 31 específicos sin tener un conocimiento previo acerca de quién se encuentra próximo. Esto también funcionará si un par 1, 2 no se encuentra actualmente bajo cobertura o control de la red, por ejemplo, cuando se encuentra operando (posiblemente de forma temporal) en modo ad-hoc.

Si al establecerse una conexión dispositivo a dispositivo 206 no se conoce una asociación de seguridad y se desea dicha asociación de seguridad 204, la red 3 puede proporcionarles opcionalmente unas claves criptográficas 14 a los dispositivos 1, 2, preferiblemente a través de una línea segura. En tal caso, y de forma ventajosa, también se le notifica 205 a la red que el descubrimiento ha funcionado, lo cual tiene la ventaja de que permite aplicarle la tarifa.

Puede ser deseable disponer de un mecanismo para cambiar el BID General 12, 21 o el T-BID 12, 21 específico de un par. Por ejemplo, una vez que se ha difundido 103 un T-BID 31 (e independientemente de si se ha conseguido establecer con éxito una sesión 206 dispositivo a dispositivo) es posible que un usuario malicioso almacene ese T-BID y permanezca buscándolo en el futuro. Si en algún instante se vuelve a difundir el mismo T-BID, el usuario malicioso podría concluir que un dispositivo en particular se encuentra próximo. En consecuencia, es posible opcionalmente que un dispositivo origen 1 le solicite 101a a la red 3 que actualice su T-BID 12. A continuación, la red 3 le asigna un nuevo T-BID 12 y les notifica 101b, 102a a los pares 1, 2 el nuevo T-BID 12, 21.

Es posible que la red reasigne los T-BID 12, 21 para cada ocasión en la que se utiliza un T-BID 12, 21 en la difusión y los redistribuya 101b, 102a a todos los pares 1, 2.

Junto con el BID y el T-BID específico de los pares, la red puede proporcionar opcionalmente un T-BID específico que únicamente puede ser descubierto por un grupo específico de amigos/dispositivos. Así, se puede definir un T-BID específico de grupo cerrado de usuarios (CUG T-BID) para los grupos más grandes. Esos identificadores CUG T-BID también se les proporcionan preferiblemente a todos los miembros del grupo. Esto tiene la ventaja de aquellos grupos que sean estáticos, como por ejemplo colegas o servicios públicos de seguridad tales como la policía y los bomberos.

Durante una conexión dispositivo a dispositivo se puede actualizar opcionalmente el T-BID específico de los pares sin involucrar o notificárselo a la red. Esto proporciona un mayor grado de privacidad (la red incluso ni siquiera conoce las identidades 12, 21), lo cual libera a la red de la tarea de generar los T-BID.

En el modo de realización de la Fig. 4, los identificadores 12 se han cargado previamente y son estáticos. Sin embargo, los T-BID 31 de difusión pueden ser cambiados, por ejemplo, por la red 3 (antes de producirse la difusión) proporcionando al dispositivo origen 1 y al dispositivo objetivo 2 un número aleatorio 51 que el dispositivo origen 1 utiliza para calcular 103a un valor derivado del identificador, por ejemplo, encriptando o aleatorizando el identificador 12, y el dispositivo objetivo 2 puede utilizar para descifrar y verificar 109 el identificador.

El modo de realización de la Fig. 4 resulta particularmente ventajoso en el caso de grupos que cambian rápidamente, en los que los miembros del grupo tienen los identificadores de cada uno de los demás, pero no todos reciben las mismas claves aleatorias.

En el siguiente primer ejemplo que hace referencia a la Fig. 4, antes del descubrimiento de proximidad se les asignan 207 a los pares 1, 2 unos T-BID denominado p_i (p_1 para el dispositivo origen 1, p_2 para un primer dispositivo objetivo 2, p_3 para un segundo dispositivo objetivo 2, etc.).

El operador 3 recibe un mensaje 101c desde el dispositivo origen 1 indicando que desearía descubrir un primero, segundo, tercero y cuarto dispositivos objetivo 2. El operador 3 detecta que el primero, segundo y cuarto dispositivos objetivo 2 se encuentran próximos. Unos quinto y sexto dispositivos objetivo también pueden estar próximos, pero no en la lista del dispositivo origen 1. Por lo tanto, los dispositivos objetivo quinto y sexto no deben ser descubiertos.

El operador 3 utiliza un número aleatorio x, cuya longitud es p_i^2 y calcula para el primer dispositivo objetivo 2: $x_2=x \bmod p_2$ para p_2; y lo mismo para el tercer dispositivo objetivo 2 (no para el segundo y cuarto dispositivos objetivo, porque en este ejemplo no se encuentran próximos). Alternativamente, el dispositivo origen 1 le proporciona al operador 3 el número aleatorio x.

El operador 3 le envía 102b el valor x al dispositivo origen 1. El operador 3 envía 102 el valor x_2 al primer dispositivo objetivo 2 y el valor x_4 al tercer dispositivo objetivo 2. Aquí x_2 y x_4 son representaciones 21 del identificador 12.

El dispositivo origen 1 difunde 103 el número aleatorio x 31 y todos los pares 2 dentro de su alcance (incluyendo probablemente el primer dispositivo objetivo 2 y el tercer dispositivo objetivo 2) pueden verificar 109 si $x_i==x \bmod p_i$. El valor x 31 funciona ahora como un segundo representante del identificador, por lo que se puede utilizar para verificar la identidad en el dispositivo objetivo 2.

El primer y tercer dispositivos objetivo 2 pueden responder 106 que han recibido el mensaje y que los dispositivos pueden establecer una sesión de comunicación dispositivo a dispositivo, posiblemente utilizando una asociación de seguridad recibida desde el servidor 3.

Los quinto y sexto dispositivos objetivo también habrán recibido el número aleatorio x 31, pero su información es demasiado limitada (no han recibido los valores x_i del operador 3) para saber quién está llamando o usarlo para rastreo y seguimiento.

Es posible que, para una próxima difusión 103, el dispositivo origen 1 vuelva a utilizar una versión modificada de r 31. Esto es posible si el primer dispositivo 1 conoce los valores de p_i de los dispositivos objetivo 2. Si los conoce, puede utilizar (un múltiplo de) el mínimo común múltiplo (MCM) de ambos para obtener un nuevo valor x para el cual todavía se cumple que $x_i==x \bmod p_i$, esto es, $x'= x + k\ MCM(p_2,p_3,etc.)$. En la presente solicitud, k no debe ser primo y debe ser preferiblemente un producto de primos con el fin de evitar proporcionar demasiada información sobre el MCM de los identificadores utilizados. El beneficio de esta solución es que no cambia nada para los dispositivos objetivo, por lo que su respuesta sigue siendo la misma.

En el siguiente segundo ejemplo que hace referencia a la Fig. 4, antes del descubrimiento de proximidad se les asignan 207 a los pares 1, 2 unos T-BID denominados p_i (p_1 para el dispositivo origen 1, p_2 para un primer dispositivo objetivo 2, p_3 para un segundo dispositivo objetivo 2, etc.). A los pares 1, 2 se les notifica la identidad de cada uno de los otros, de modo que, por ejemplo, el dispositivo origen 1 conoce el T-BID del primer dispositivo objetivo 2 y el segundo dispositivo objetivo 2 conoce el T-BID del dispositivo origen 1.

El operador 3 recibe un mensaje 101c desde el dispositivo origen 1 indicando que desea descubrir un primer, segundo, tercero y cuarto dispositivos objetivo 2. El operador 3 detecta que el primer, segundo y cuarto dispositivos objetivo 2 se encuentran próximos. Un quinto y sexto dispositivos objetivo también pueden estar próximos, pero no en la lista del dispositivo origen 1. Por lo tanto, los dispositivos objetivo quinto y sexto no deben ser descubiertos.

El operador 3 utiliza un número aleatorio r y calcula $x=hash(T\text{-}BID_{dispositivo\ origen\ 1}||r)$ y de nuevo $x_i=x \bmod p_i$ para el segundo y cuarto dispositivos objetivo 2. Alternativamente, el dispositivo origen 1 le proporciona al operador 3 el número aleatorio r.

El operador 3 le envía 102b el número aleatorio r al dispositivo origen 1. El operador 3 le envía 102 (x_2,r) al primer dispositivo objetivo 2 y (x_4,r) al tercer dispositivo objetivo 2. Aquí x_2 y x_4 son representaciones 21 del identificador 12.

El dispositivo origen 1 difunde 103 el valor x 31 y todos los pares 2 dentro su alcance (incluyendo probablemente el primer dispositivo objetivo 2 y el tercer dispositivo objetivo 2) pueden verificar 109 si $x_i==x \bmod p_i$. El valor x 31 funciona ahora como un segundo representante del identificador, por lo que se puede utilizar para verificar la identidad en el dispositivo objetivo 2.

El primer y tercer dispositivos objetivo 2 pueden responder 106 que han recibido el mensaje y confirmar su autenticidad devolviendo un valor_hash(p_i||r) calculado 108 en el dispositivo objetivo 2.

Al igual que en los modos de realización anteriores, la red 3 puede estar implicada en el intercambio de unas claves criptográficas 14 que proporcionan seguridad adicional y permiten aplicar una tarifa a una detección de proximidad exitosa.

Los ejemplos de la Fig. 4 también funcionan en el caso de que un dispositivo 1, 2 desee descubrir solo otro dispositivo 1, 2. En tal caso, la red 3 se lo notifica únicamente a esos pares específicos.

A continuación se describen algunos ejemplos de modos de realización de procedimientos de descubrimiento de proximidad autónomos, en los que los propios dispositivos 1, 2 deciden qué difundir para descubrimiento. La red 3 o un tercero aún pueden estar involucrados en notificarles a los dispositivos 1, 2 sobre una probable proximidad, esto es, pueden estar involucrados en la detección de proximidad. En los procedimientos de descubrimiento de proximidad autónomos, se supone que en cualquier instante anterior, ha habido un contacto o se han intercambiado identificadores por otros medios, como por ejemplo la utilización de un chip de campo cercano en el dispositivo origen 1 y el dispositivo objetivo 2 (por ejemplo, activado acercando los dispositivos 1, 2 y agitándolos), escaneando un código de barras o una etiqueta en la pantalla del otro dispositivo, introduciendo manualmente por parte del usuario un identificador, utilizando WiFi, utilizando una aplicación de un tercero como Facebook o cualquier otro medio.

La Fig. 5 ilustra un procedimiento de descubrimiento de proximidad autónomo que se basa en una pila de hash inversa con una opción automática de olvido. El ejemplo de la Fig. 5 resulta particularmente útil en entornos con muchos pares 1, 2 que tengan una alta probabilidad de volverse a encontrar. Los propios pares 1, 2 deciden qué difundir 103 y cómo encriptar u oscurecer la segunda representación 31 del identificador 12 en la señal difundida. La representación 31 del T-BID que se difunde puede cambiar en el tiempo, de tal modo que el rastreo y el seguimiento se vuelven muy difíciles.

Un dispositivo origen 1 y un dispositivo objetivo 2 que se encuentran en una sesión de comunicación dispositivo a dispositivo pueden generar 101 ambos un T-BID 12 aleatorio y una sal 51. Ambos dispositivos 1, 2 calculan de forma recursiva un n-ésimo valor_hash 21 utilizando cualquier función hash que utilice como argumentos el hash anterior y la sal 51. El primer valor_hash se calcula entonces como $hash_1$=hash(T-BID, sal) y todos los valores hash posteriores se calculan como hash(hash_anterior, sal). Para calcular el n-ésimo valor_hash 21 se puede utilizar, por ejemplo, el siguiente código:

$valor\_hash_1$=hash(T-BID, sal);
i=2; while i<=n do {
$valor\_hash_i$=hash($valor\_hash_{i-1}$, sal);
}

En la presente solicitud, el T-BID 12 es un identificador 12, el n-ésimo valor_hash del T-BID es una primera representación 21 del identificador 12 y la sal es una tercera representación 51 del identificador 12.

Los dispositivos 1, 2 intercambian su n-ésimo valor_hash y la sal en los pasos 102 y 107.

En esta etapa, el dispositivo origen 1 y el dispositivo objetivo 2 tienen suficiente información para ponerse en contacto entre sí en una etapa posterior sin tener que ponerse en contacto con la red 3 o cualquier otro tercero.

La próxima vez que se encuentren próximos, lo cual se representa en el bloque 209, el dispositivo origen 1 puede difundir como segunda representación 31 del T-BID el n-1-ésimo valor_hash 31 del T-BID. A continuación, el dispositivo objetivo 2 puede calcular 108 la función hash($valor\_hash_{n-1}$, sal) = valor_hash anterior. Una persona que intercepte y conozca la función hash no conocerá la sal 51 y, por consiguiente, no podrá saber a quién se llama.

Opcionalmente, los dispositivos cercanos 1, 2 podrían ser informados por la red 3 sobre su proximidad en un procedimiento de detección de proximidad previo al procedimiento de descubrimiento de proximidad. De este modo se podrían evitar la necesidad de una monitorización constante de la señal de difundida y el gasto de batería relacionado.

Como ambos dispositivos 1,2 poseen muchos valores hash, pueden decidir utilizar un valor_hash diferente, por ejemplo, cada día o cada vez que se encuentren próximos. Si a continuación difunden 103 como hash la segunda representación 31 del T-BID, pueden incluir, por ejemplo, en la señal difundida 30 un valor k contador que indica qué hash han difundido. El valor k puede indicar, por ejemplo, que se incluye el valor_hash(n-k)-ésimo (valor_hash n menos k ésimo) como segunda representación 31 del identificador en la señal difundida 30.

Opcionalmente, k se proporciona mediante un temporizador, por ejemplo, en función de la cantidad de días u horas que han transcurrido desde la última sesión de comunicación dispositivo a dispositivo. Esto se puede utilizar para introducir un criterio de expiración que vaciará la pila de valores hash a tiempo y romperá eventualmente el "emparejamiento" de los dos dispositivos 1, 2. Si, por ejemplo, los dispositivos 1, 2 se vuelven a encontrar nuevamente después de que haya expirado su asociación de seguridad inicial, tendrán que volver a pasar por el procedimiento inicial de descubrimiento de proximidad.

El modo de realización que se ilustra en la Fig. 5 se puede ampliar computacionalmente si un dispositivo objetivo 2 tiene que calcular 108 el hash sobre cada T-BID 31 aleatorizado que recibe. Esto se puede reducir confiando en que la red 3 indique cuándo esperar para escuchar las transmisiones. Alternativamente, esto se puede reducir concatenando el número del valor_hash difundido (esto es, agregando n-k a la difusión). De este modo, el dispositivo objetivo 2 puede verificar si espera un (n-k)-ésimo valor_hash de uno de sus pares y a continuación decidir calcular 108 el/(los) valor(es) hash(es) recursivo(s) para la difusión recibida.

El procedimiento de descubrimiento de proximidad de la Fig. 5 funciona de forma ventajosa incluso cuando no existe cobertura por parte de la red (la red no tiene por qué estar involucrada). Aún más, dispone de un mecanismo para olvidar los pares transcurrido algún tiempo, lo cual se puede utilizar con fines de tarificación o suscripción, y permite un mecanismo para reducir la carga computacional de calcular valores hash recursivos en todas las difusiones 103 que se reciben.

Como variante del ejemplo de la Fig. 5, es posible que los propios dispositivos 1, 2 decidan qué número aleatorio utilizar para encriptar el identificador 12. Cuando los identificadores se han intercambiado, por ejemplo, en un procedimiento de detección de proximidad previo o proporcionados por la red, la red o un tercero no tienen por qué estar involucrados en el establecimiento de la sesión de comunicación dispositivo a dispositivo. Este procedimiento alternativo puede funcionar del siguiente modo.

En primer lugar, un dispositivo origen 1 calcula un número aleatorio 51 y calcula la función hash(R‖T-BID), en donde R es el número aleatorio 51 y T-BID es un identificador 12. El T-BID puede ser, por ejemplo, un T-BID específico de un par (por ejemplo, b ó j, tal como se muestra en la tabla del ejemplo de la Fig. 2), lo que indica que puede especificar quién llama o quién es llamado. El T-BID puede ser, por ejemplo, un T-BID de Asociación de Seguridad (SA-T-BID) si se ha especificado uno.

A continuación, el dispositivo origen 1 difunde el valor R‖hash(R‖T-BID). El/(los) dispositivo(s) objetivo 2 que recibe(n) esta difusión calcula(n) la función hash(R‖T-BID) con los T-BID almacenados en su memoria (incluyendo posiblemente los propios) y determina(n) si coinciden. Si se encuentra una coincidencia, la conclusión que se puede obtener depende de qué T-BID se ha difundido. Si el dispositivo origen 1 difunde un T-BID que representa su propia identidad, el dispositivo objetivo 2 puede concluir que el dispositivo origen 1 se encuentra dentro de su alcance. Si el dispositivo origen 1 difunde un T-BID que representa la identidad del dispositivo objetivo 2, entonces solo el dispositivo objetivo 2, que es la parte llamada, encontrará una coincidencia con su propia identidad. A pesar de todo, los usuarios maliciosos aún pueden descubrir que se está llamando al dispositivo objetivo 2, pero no pueden saber quién está llamando. Si el dispositivo origen 1 difunde los T-BID a partir de una asociación de seguridad común (que puede incluir los T-BID del dispositivo origen 1 y/o del/(de los) dispositivo(s) objetivo 2 y/o un T-SA-BID), entonces el dispositivo objetivo 2 puede determinar que está siendo llamado.

Una ventaja de esta variante de la ventaja de la Fig. 5 es que el dispositivo origen 1 puede determinar por sí mismo cómo darse a conocer y proporciona un alto grado de privacidad, permitiendo al mismo tiempo que la red descubra quién está realizando la difusión. Esto último resulta ventajoso, por ejemplo, por razones de tarificación o intercepción legal. Una ventaja adicional es que la red no necesita estar involucrada y, por lo tanto, el procedimiento también funciona sin cobertura de red.

El ejemplo de la Fig. 6 ilustra una solución híbrida, en donde la red o un tercero proporciona una sal para ser utilizada en las funciones hash. El ejemplo de la Fig. 6 es una variante de los ejemplos de la Fig. 4 y la Fig. 5, y resulta particularmente ventajoso en caso de que haya muchos pares 1, 2 con una alta probabilidad de volverse a encontrar. Los pares 1, 2 mantienen información acerca del resto como, por ejemplo, el identificador 12, que pueden utilizar en sesiones posteriores para identificarse entre sí o para encontrar un siguiente T-BID.

En el ejemplo de la Fig. 6, dos dispositivos 1, 2 que se encuentran en una sesión dispositivo a dispositivo generan un T-BID aleatorio. Se notifican 101 entre sí los T-BID 12 escogidos. En ciertos instantes de tiempo preestablecidos, por ejemplo, cada noche o a intervalos de tiempo predefinidos, la red 3 (o cualquier otro tercero) distribuye 107 sales 51 a los dispositivos 1, 2. Opcional o alternativamente, la red 3 (o un tercero) puede proporcionar 107 la sal al detectar que dos dispositivos 1, 2 se encuentran próximos y desean conversar (chat). El/(los) dispositivo(s) objetivo 2 obtiene(n) 102 una primera representación 21 de los T-BID 12 conocidos de los dispositivos 1, 2, esto es, los que se han recibido en el paso 101 de notificación, calculando la función hash(T-BID, sal) para todos los T-BID 12. El dispositivo origen realiza el mismo cálculo 210 con su propio T-BID 12 calculando una segunda representación 31 del T-BID 31 utilizado por el dispositivo origen 1. La segunda representación 31 del T-BID se difunde 103 y es

recibida por el/(los) dispositivo(s) objetivo 2. El/(los) dispositivo(s) objetivo 2 compara(n) 105, 108 la primera representación 21 calculada de los T-BID con la segunda representación 31 del T-BID 12 recibida y verifica(n) 109 si hay alguna coincidencia.

Una ventaja del ejemplo de la Fig. 6 es que, desde el punto de vista computacional, es menos intensivo que los ejemplos que dependen de parámetros que cambian rápidamente como, por ejemplo, el número aleatorio recibido, y el cálculo de la función hash cada vez que se recibe el número aleatorio. A pesar de todo, aún proporciona una privacidad suficiente para el difusor 1 de los identificadores 12.

Las Fig. 1-6 ilustran diferentes ejemplos de modos de realización ilustrativos de la invención. La invención no se limita a los ejemplos que se han ilustrado. Por ejemplo, los pasos que se ilustran en un ejemplo se pueden utilizar en otros ejemplos, aunque no se muestra. Algunos ejemplos de esto son la aleatorización de los identificadores, la utilización de boletos, la verificación adicional de reto-respuesta, y el cifrado de datos mediante una clave de cifrado 14. Algunos otros de los pasos que se ilustran pueden ser opcionales como, por ejemplo, la transmisión 106 del mensaje de reconocimiento y el establecimiento de una sesión 206 de comunicación dispositivo a dispositivo.

En algunos de los ejemplos, las funciones hash se utilizan para calcular valores derivados 21, 31 del identificador 12. Se debe entender que, en su lugar, se puede utilizar cualquier otra función matemática que utilice un número aleatorio 51 para crear los valores derivados 21, 31. El número aleatorio 51 puede ser, por ejemplo, un número aleatorio o un valor derivado del mismo generado en el servidor 3 o en el dispositivo origen 1, una sal generada en el servidor 3 o en el dispositivo origen 1.

Los identificadores 12 se pueden utilizar para identificación de un grupo. Por ejemplo, se puede utilizar un T-BID para indicar que se está llamando a un determinado grupo de dispositivos 1, 2. Los dispositivos 1, 2 que pertenecen a un grupo reciben un identificador 12 que representa al grupo. Para descubrir otros dispositivos, los dispositivos calculan un valor derivado del identificador 12, por ejemplo, en función de la fecha y/u hora actual o cualquier otro número aleatorio 51 que pueda ser conocido por los dispositivos 1, 2 sin necesidad de intercambiar el número aleatorio 51. El segundo valor derivado 31 del identificador se puede calcular entonces como x=hash(fecha||IdentificadorDeGrupo). El dispositivo origen 1 difunde 103 el valor x y el/(los) dispositivo(s) objetivo 2 del grupo recibe(n) el valor x y calcula(n) un primer valor derivado 21 del identificador realizando el cálculo de la misma función hash(fecha||IdentificadorDeGrupo). Si un primer valor derivado 21 coincide con el tercer valor derivado 31, el descubrimiento de proximidad se ha realizado con éxito.

En general, si el número aleatorio 51 es un parámetro que varía en función del tiempo, el número aleatorio 51 se puede elegir de modo que cambie lentamente, por ejemplo, una vez al día en caso de que el número aleatorio 51 sea la fecha actual. En tal caso, el cálculo de la función hash(fecha||IdentificadorDeGrupo) o hash(fecha||identificador) se puede realizar solo una vez al día. Una vez realizado dicho cálculo, solo es necesario llevar a cabo las comparaciones 109. En los ejemplos de la Fig. 5 y la Fig. 6, esto puede resultar ventajoso al tener que realizar menos cálculos, ya que las funciones hash de los otros dispositivos solo tienen que calcularse una vez al día.

Un modo de realización de la invención se puede implementar como un producto de software para ser utilizado con un sistema informático. El/(los) programa(s) del producto de software define(n) funciones de los modos de realización (incluyendo los métodos descritos en la presente solicitud) y puede(n) estar almacenado(s) en una variedad de medios de almacenamiento no transitorios legibles por un ordenador. Algunos medios de almacenamiento ilustrativos legibles por un ordenador incluyen, pero no se limitan a: (i) medios de almacenamiento no grabables (por ejemplo, dispositivos de memoria de solo lectura dentro de un ordenador, tales como discos CD-ROM legibles por una unidad de CD-ROM, chips ROM o cualquier tipo de memoria de semiconductor no volátil de estado sólido) en los que la información se almacena de forma permanente; y (ii) medios de almacenamiento grabables (por ejemplo, una memoria flash, unos discos flexibles en una unidad de disquete o una unidad de disco duro o cualquier tipo de memoria de semiconductor de acceso aleatorio de estado sólido) en los que se almacena la información que se puede modificar.

REIVINDICACIONES

1. Un método para el descubrimiento de proximidad entre un dispositivo origen (1) y uno o más dispositivos objetivo (2) en donde el dispositivo origen (1) y el uno o más dispositivos objetivo (2) están configurados para conectarse en comunicación a una red, comprendiendo dicho método los pasos de:

recibir (101) en el dispositivo origen (1) desde un servidor (3) en la red unos primeros datos (11) que comprenden un identificador (12), en donde el identificador (12) es un identificador temporal de difusión que identifica de forma unívoca al dispositivo origen (1);

recibir (102) en el dispositivo objetivo (2) desde el servidor (3) unos segundos datos (20) que comprenden una primera representación (21) del identificador (12) del dispositivo origen (1) con el fin de permitir que el dispositivo objetivo (2) asocie el identificador (12) al dispositivo origen (1);

difundir (103) por parte del dispositivo origen (1) una señal (30) que comprende una segunda representación del identificador (31) del dispositivo origen (1);

recibir (104) en el dispositivo objetivo (2) la señal (30); y

comparar (105) en el dispositivo objetivo la primera representación (21) del identificador (12) con la segunda representación (31) del identificador (12) para obtener un resultado de la comparación con el fin de establecer un descubrimiento de proximidad exitoso.

2. El método de acuerdo con la reivindicación 1, que comprende, además, transmitir (106) desde el dispositivo objetivo (2) al dispositivo origen (1) un mensaje (40) de confirmación en función del resultado de la comparación.

3. El método de acuerdo con una cualquiera de las reivindicaciones 1-2, que comprende, además, recibir (107) en el dispositivo objetivo (2) unos terceros datos (50) que comprenden una tercera representación (51) del identificador (12), en donde la primera representación del identificador (21) es un valor derivado del identificador obtenido mediante una primera función matemática que utiliza el identificador (12) y un número aleatorio como argumentos para calcular el valor derivado del identificador, en donde la tercera representación (51) del identificador (12) es el número aleatorio,

y en donde la etapa de comparación (105) comprende:

calcular (108) el valor derivado del identificador utilizando una segunda función matemática idéntica a la primera función matemática que utiliza como argumentos la segunda representación (31) del identificador (12) y la tercera representación (51) del identificador (12); y

comparar (109) el valor derivado calculado del identificador con la primera representación (21) del identificador (12),

en donde el número aleatorio es uno de:

un número aleatorio generado en el servidor o en el dispositivo origen (1);

una sal generada en el servidor (3) o en el dispositivo origen (1);

un valor derivado de un número aleatorio adicional obtenido en el servidor (3) o en el dispositivo origen (1) mediante una tercera función matemática que utiliza como argumentos el número aleatorio adicional y un identificador de origen que identifica el dispositivo origen (1) para calcular el valor derivado del número aleatorio.

4. El método de acuerdo con la reivindicación 2 o con las reivindicaciones 2 y 3, en donde los segundos datos (20) comprenden además un identificador (22) de boleto (ticket), comprendiendo el método además:

recibir (110) en el dispositivo origen (1) desde el servidor (3) los datos (10) del boleto que comprenden el identificador (22) del boleto, los primeros datos (11) y unos cuartos datos (13);

transmitir (111) desde el dispositivo objetivo (2) al servidor (3) el identificador (22) del boleto con el fin de obtener una copia (41) de los cuartos datos (13) asociados con el identificador (22) del boleto; y

recibir (112) en el dispositivo objetivo (2) desde el servidor (3) la copia (41) de los cuartos datos (13),

en donde el mensaje (40) de confirmación comprende la copia (41) de los cuartos datos (13) para su verificación con los cuartos datos (13) en el dispositivo origen (1).

5. El método de acuerdo con una cualquiera de las reivindicaciones 1-4, que comprende además aplicar una tarifa por parte de un operador del servidor (3) a una solicitud de los primeros datos (11), los segundos datos (20) y/o los datos (10) del boleto desde el dispositivo origen (1) o el dispositivo objetivo (2).

6. El método de acuerdo con la reivindicación 4 o la reivindicación 5, que comprende, además:

recibir (113) en el dispositivo objetivo (2) desde el dispositivo origen (1) los primeros datos (32) de reto; y

calcular (114) en el dispositivo objetivo (2) unos primeros datos (42) de reto derivados utilizando una cuarta función matemática, por ejemplo, una función hash(de aleatorización), con los primeros datos (32) de reto,

en donde el mensaje (40) de confirmación comprende, además, los primeros datos (42) de reto derivados y unos segundos datos (43) de reto, comprendiendo además el método:

calcular (115) en el dispositivo origen (1) los primeros datos (42) de reto derivados utilizando una quinta función matemática idéntica a la cuarta función matemática con los primeros datos (32) de reto con el fin de comparar con los primeros datos (42) de reto derivados recibidos;

calcular (116) en el dispositivo origen (1) unos segundos datos (33) de reto derivados utilizando una sexta función matemática con los segundos datos (43) de reto;

transmitirle (117) los segundos datos (33) de reto derivados al dispositivo objetivo (1);

calcular (118) en el dispositivo objetivo (2) los segundos datos (33) de reto derivados utilizando una séptima función matemática idéntica a la sexta función matemática con los segundos datos (43) de reto para compararlos con los segundos datos (33) de reto derivados recibidos.

7. El método de acuerdo con la reivindicación 6, en donde los datos (10) del boleto comprenden, además, una clave (14) de cifrado, en donde el método comprende, además, recibir (119) en el dispositivo objetivo (1) desde el servidor (3) la clave (14) de cifrado asociada en el servidor (3) al identificador (22) del boleto, y en donde la cuarta, quinta, sexta y séptima funciones matemáticas comprenden una función criptográfica que utiliza la clave (14) de cifrado.

8. Un dispositivo origen (1) configurado para realizar un procedimiento de descubrimiento de proximidad con uno o más dispositivos objetivo (2) utilizando el método de acuerdo con una cualquiera de las reivindicaciones 4 a 7.

9. Un dispositivo objetivo (2) configurado para realizar un procedimiento de descubrimiento de proximidad con un dispositivo origen (1) en donde el dispositivo origen (1) y el dispositivo objetivo (2) están configurados para conectarse en comunicación a una red y el dispositivo origen (1) está configurado para recibir desde un servidor (3) en la red unos primeros datos (11) que comprenden un identificador (12), en donde el identificador (12) es un identificador temporal de difusión que identifica al dispositivo origen (1), caracterizado por que el dispositivo objetivo está configurado para:

recibir desde el servidor (3) en la red unos segundos datos (20) que comprenden una primera representación (21) del identificador (12) del dispositivo origen (1) que permite que el dispositivo objetivo (2) asocie el identificador (12) al dispositivo origen (1);

recibir desde el dispositivo origen (1) una señal de difusión (30) que comprende una segunda representación (31) del identificador (12) del dispositivo origen (1); y

comparar la primera representación (21) del identificador (12) con la segunda representación (31) del identificador (12) para obtener un resultado de la comparación con el fin de establecer un descubrimiento de proximidad exitoso.

10. Una red que comprende un dispositivo origen (1) de acuerdo con la reivindicación 8 y uno o más dispositivos objetivo (2) de acuerdo con la reivindicación 9.

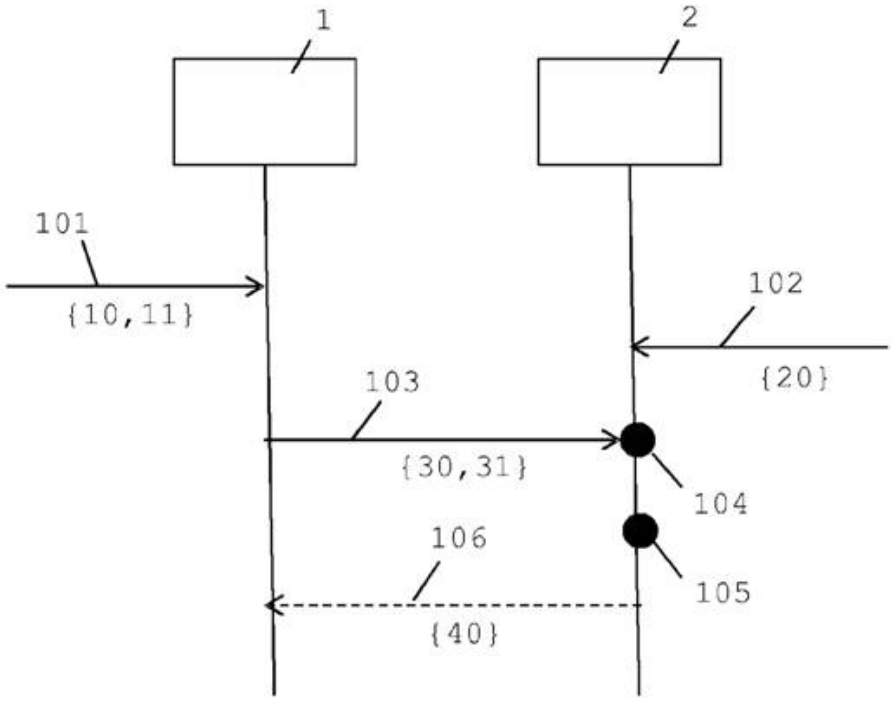

Fig.1

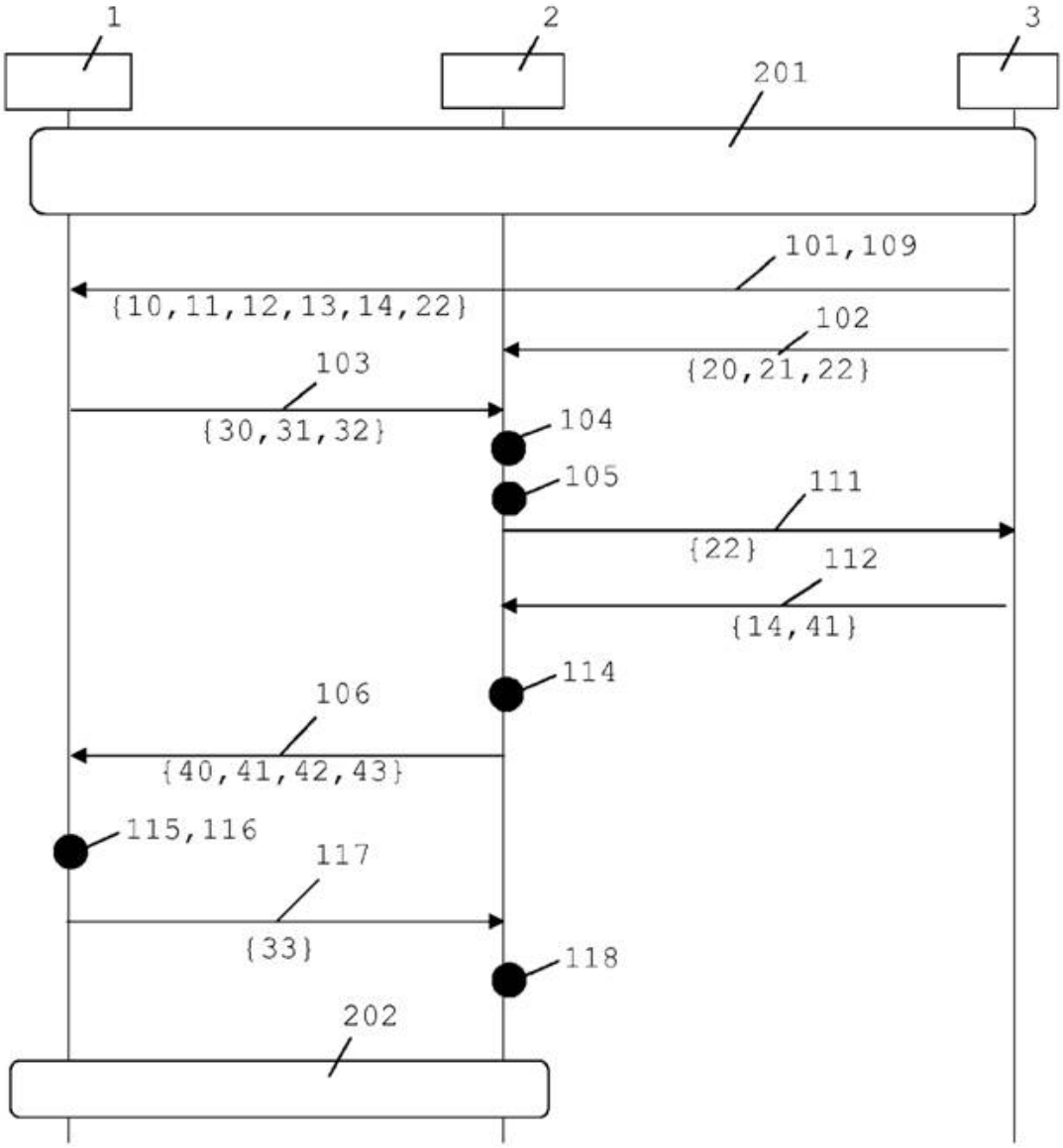
1
2
3
201
101,109
{10,11,12,13,14,22}
102
{20,21,22}
103
{30,31,32}
104
105
111
{22}
112
{14,41}
114
106
{40,41,42,43}
115,116
117
{33}
118
202

Fig.2

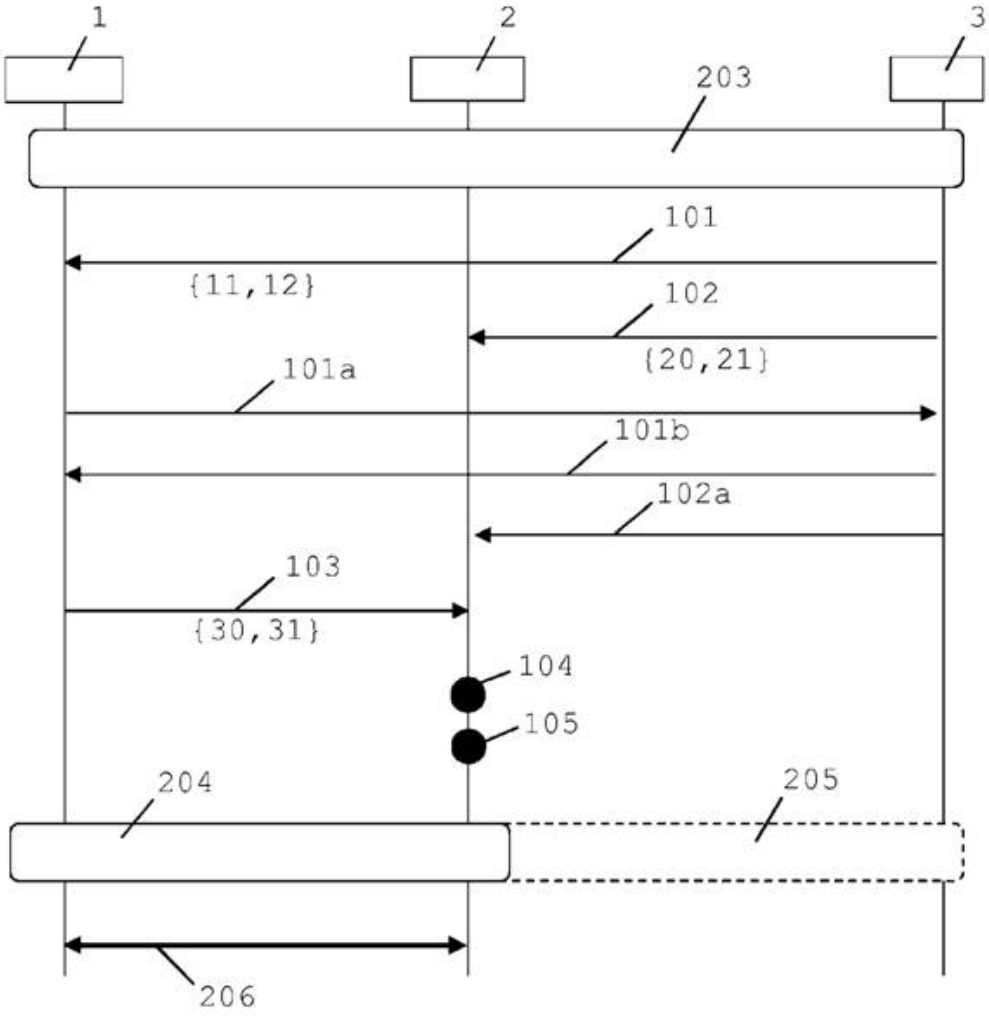
1
2
3
203
101
{11,12}
102
{20,21}
101a
101b
102a
103
{30,31}
104
105
204
205
206

Fig.3

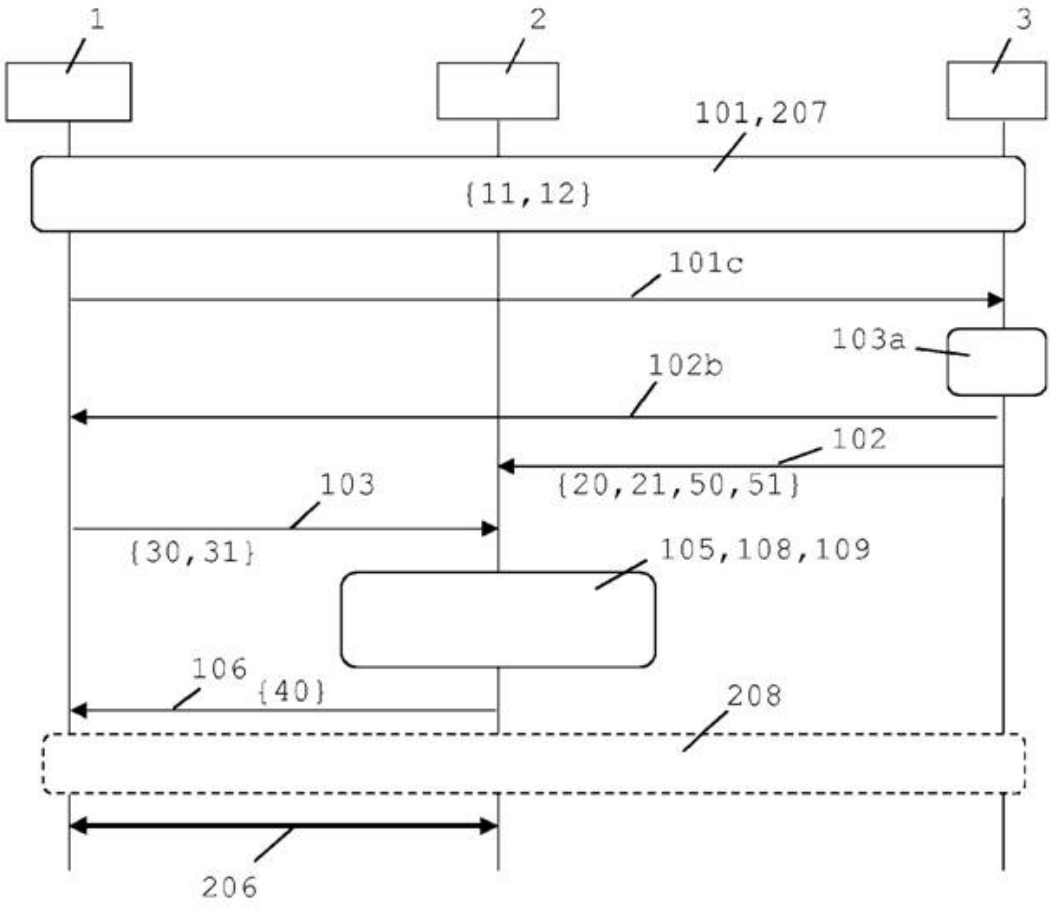
1
2
3
101,207
{11,12}
101c
103a
102b
102
{20,21,50,51}
103
{30,31}
105,108,109
106
{40}
208
206

Fig.4

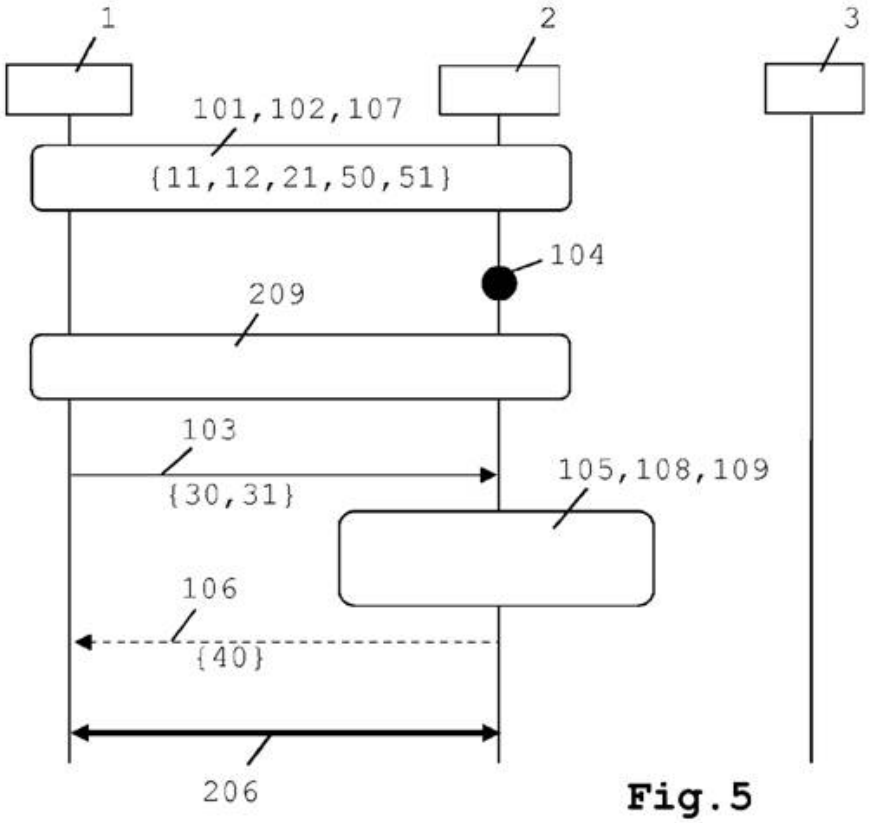
1
2
3
101,102,107
{11,12,21,50,51}
104
209
103
{30,31}
105,108,109
106
{40}
206

Fig.5

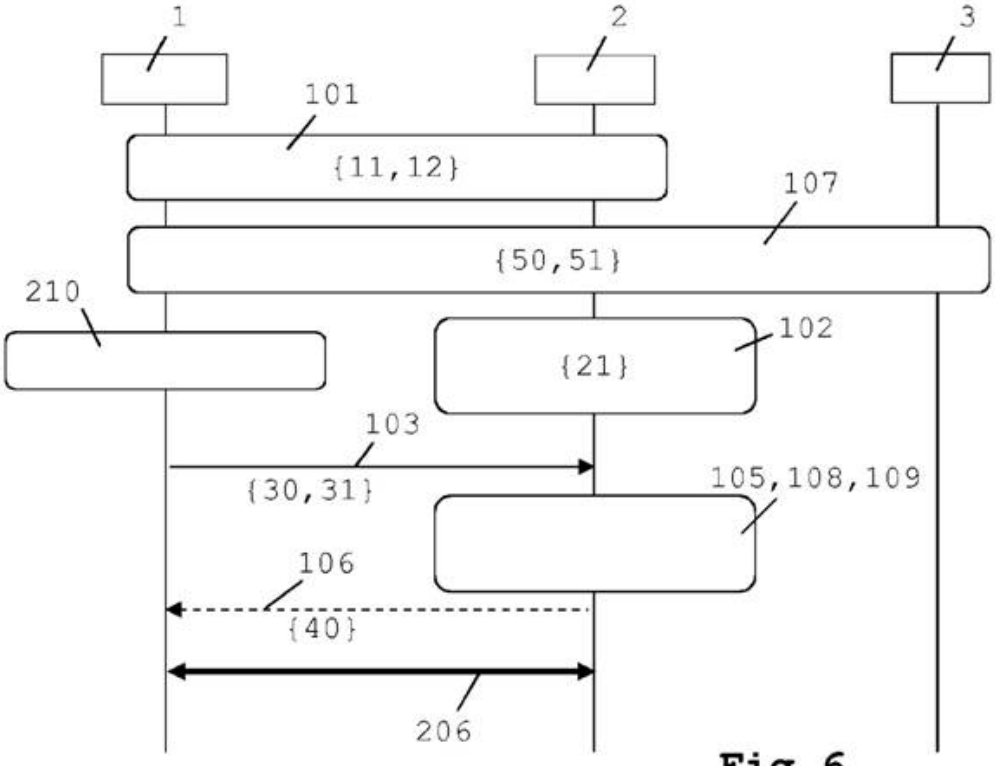
1
2
3
101
{11,12}
107
{50,51}
210
102
{21}
103
{30,31}
105,108,109
106
{40}
206

Fig.6