(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 728 468**

(51) Int. CI.:

H04B 5/00	(2006.01)	***H04W 80/10***	(2009.01)
H04B 17/318	(2015.01)	***H04W 88/02***	(2009.01)
H04L 1/18	(2006.01)	***H04W 92/18***	(2009.01)
H04L 29/08	(2006.01)		
H04W 12/06	(2009.01)		
H04W 28/16	(2009.01)		
H04W 40/24	(2009.01)		
H04W 48/16	(2009.01)		
H04W 72/00	(2009.01)		
H04W 74/00	(2009.01)		

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **24.09.2013 PCT/US2013/061379**

(87) Fecha y número de publicación internacional: **03.04.2014 WO14052303**

(96) Fecha de presentación y número de la solicitud europea: **24.09.2013 E 13840542 (8)**

(97) Fecha y número de publicación de la concesión europea: **10.04.2019 EP 2901811**

(54) Título: **Sistemas y métodos para comunicación de dispositivo a dispositivo en ausencia de cobertura de red**

(30) Prioridad:

28.09.2012 US 201261707784 P
28.06.2013 US 201313930669

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.10.2019

(73) Titular/es:

INTEL CORPORATION (100.0%)
2200 Mission College Boulevard
Santa Clara, CA 95054, US

(72) Inventor/es:

STOJANOVSKI, ALEXANDRE SASO;
LUFT, ACHIM y
VENKATACHALAM, MUTHAIAH

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Sistemas y métodos para comunicación de dispositivo a dispositivo en ausencia de cobertura de red

Campo técnico

Las realizaciones pertenecen a la electrónica. Algunas realizaciones pertenecen a productos de comunicación electrónica.

Antecedentes de la técnica

En ajustes de comunicaciones típicos, un teléfono celular u otro tipo de dispositivo de comunicación móvil se comunica con otros dispositivos a través del uso de una red. En muchas situaciones, sería deseable que un dispositivo de comunicación móvil se comunicara directamente con uno o más otros dispositivos de comunicación móvil de una manera segura, con o sin una red.

El documento US 2012/155643 A1 muestra un dispositivo informático inalámbrico que opera como un controlador de un grupo entre pares configurado para generar claves maestras únicas para cada dispositivo que se une al grupo. El dispositivo informático inalámbrico puede usar las claves maestras únicas para eliminar de manera selectiva dispositivos remotos del grupo de manera que el dispositivo remoto no puede volverse a unir más tarde al grupo. Otros dispositivos remotos, cada uno con una clave maestra que permanece válida, pueden desconectarse del grupo y reconectarse más tarde al grupo sin acción concreta del usuario.

La publicación internacional WO 2005/008939 A2 proporciona un sistema de comunicación que usa arquitectura de cliente-servidor acoplada de manera holgada para mejorar la eficacia de las comunicaciones. El sistema de comunicación mejora la eficacia de comunicaciones de voz permitiendo a los usuarios del dispositivo de comunicación gestionar dinámicamente cómo y cuándo tienen lugar las llamadas móviles, detectar de manera inteligente llamadas basándose en la identidad del llamante, urgencia y materia, determinar qué contactos están disponibles en un directorio para hablar y cuáles elegir para que no se les interrumpa, y aumentar la accesibilidad de información de contacto empresarial y personal de teléfonos móviles.

El documento US 2011/0026504 A1 proporciona un método que incluye participar en una red de comunicaciones inalámbricas entre pares que incluye un controlador de grupo para crear y finalizar la red y controlar el acceso a la red por estaciones inalámbricas. Un miembro de la red recibe un indicador de estado del controlador de grupo que indica que el propietario de grupo está o ya no estará sirviendo como propietario de grupo.

El documento GB 2 419 067 A proporciona un método para posibilitar a respectivos usuarios de primer y segundo dispositivos de una red de confianza para realizar una transacción segura entre ellos. Se establece un canal de comunicaciones, tal como una conversación por teléfono entre los usuarios. Se comunica un identificador de verificación para la transacción entre los usuarios que usan el canal de comunicaciones. El identificador de verificación se almacena en el primer dispositivo como un identificador de referencia para la transacción. Se abre una conexión segura entre los dos dispositivos a través de la red de confianza, siendo la conexión segura diferente al canal de comunicaciones entre los usuarios. El identificador de verificación se envía desde el segundo dispositivo al primer dispositivo a través de la conexión segura. El identificador de verificación recibido a través de la conexión segura se compara con el identificador de referencia en el primer dispositivo. La transacción segura se realiza a través de la conexión segura dependiendo de la comparación.

El documento US 2011/116415 A1 se refiere a una primera estación para comunicarse con una segunda estación. La primera estación incluye una unidad de almacenamiento configurada para almacenar información de relación que define una relación de comunicación entre la primera estación y la segunda estación. La primera estación también incluye una unidad de comunicación configurada para comunicarse con la segunda estación y con un punto de acceso. La relación de comunicación se mantiene cuando la unidad de comunicación empieza a comunicarse con el punto de acceso.

El documento US 2004/0039906 A1 se refiere a un método para realizar limitación de acceso fiable en comunicación mediante una red. En comunicación entre dispositivos de procesamiento de comunicación mediante una red de comunicación, un servidor de retransmisión, tal como un servidor doméstico, verifica y examina un certificado de atributo de la fuente de acceso, y determina si la fuente de acceso es o no un miembro permitido del destino de acceso. Únicamente cuando está permitida la fuente de acceso por el destino de acceso, se realiza un proceso de resolución de nombre, y la información de dirección del destino de acceso se notifica a la fuente de acceso. Se usa un certificado de atributo de grupo en el que se describe el nombre de dominio y el nombre de anfitrión de la fuente de acceso, y se actualiza la dirección que corresponde al nombre de dominio y al nombre de anfitrión.

El documento US 2003/0056093 A1 muestra un método para asegurar la formación de grupo entre pares segura, adición de miembro de grupo, expulsión de miembro de grupo, distribución de información de grupo, etc. Tal funcionalidad puede distribuirse a los pares individuales en el grupo para mejorar adicionalmente la seguridad global del grupo mientras se mejora la flexibilidad. La seguridad de grupo P2P permite que cada par que es un miembro válido del grupo invite a nuevos miembros. Los receptores de estas invitaciones pueden a continuación contactar

con cualquier miembro del grupo para unirse al grupo, no únicamente el invitador. Además, los grupos pueden funcionar cuando el creador del grupo no está en línea.

Compendio

La invención se define por la materia de las reivindicaciones independientes. Realizaciones ventajosas están sujetas a las reivindicaciones dependientes.

Breve descripción de los dibujos

En los dibujos, que no están necesariamente dibujados a escala, números de referencia similares pueden describir componentes similares en diferentes vistas. Números de referencia similares que tienen diferentes sufijos de letra pueden representar diferentes instancias de componentes similares. Se ilustran algunas realizaciones a modo de ejemplo, y no como limitación, en las figuras de los dibujos adjuntos en los que:

Las Figuras 1A y 1B presentan vistas generales de comunicación 1:1 y comunicación de grupo;

La Figura 2 presenta una arquitectura de sistema ejemplar para comunicación 1:1;

La Figura 3 es un diagrama de flujo que ilustra la operación de una realización para comunicación 1:1;

La Figura 4 presenta una arquitectura de sistema ejemplar para la comunicación de grupo;

La Figura 5 presenta un diagrama de flujo de la operación de una realización para comunicación de grupo;

La Figura 6 es un diagrama de bloques que ilustra una máquina de ejemplo que puede ejecutar una realización.

Descripción de las realizaciones

La siguiente descripción y los dibujos ilustran de manera suficiente realizaciones específicas para posibilitar a los expertos en la técnica ponerlas en práctica. Otras realizaciones pueden incorporar cambios estructurales, lógicos, eléctricos, de proceso y otros. Los ejemplos simplemente tipifican posibles variaciones. Los componentes individuales y funciones son opcionales a menos que se requieran explícitamente, y la secuencia de operaciones puede variar. Pueden incluirse porciones y características de algunas realizaciones en, o sustituirse por, aquellas de otras realizaciones. Se exponen realizaciones en las reivindicaciones que abarcan todos los equivalentes de estas reivindicaciones.

En la siguiente descripción detallada, se exponen numerosos detalles específicos para proporcionar un entendimiento minucioso de la invención. Sin embargo, se entenderá por los expertos en la técnica que la presente invención puede ponerse en práctica sin estos detalles específicos. En otras instancias, métodos bien conocidos, procedimientos, componentes, y circuitos no se han descrito en detalle para no dificultar ensombrecer la presente invención.

Aunque las realizaciones de la invención no están limitadas en este sentido, los términos “pluralidad” y “una pluralidad” como se usan en la presente memoria pueden incluir, por ejemplo, “múltiples” o “dos o más”. Los términos “pluralidad” o “una pluralidad” pueden usarse a través de toda la memoria descriptiva para describir dos o más componentes, dispositivos, elementos, unidades, parámetros y similares. Por ejemplo, “una pluralidad de dispositivos” puede incluir dos o más dispositivos.

El Proyecto de Asociación para la 3ª Generación (3GPP) es un acuerdo de colaboración establecido en diciembre de 1998 para reunir un número de organismos de normas de telecomunicaciones, conocido como “Socios Organizacionales”, que actualmente incluyen la Asociación de Industrias y Negocios de Radio (ARIB), la Asociación de Normas de Comunicaciones China (CCSA), el Instituto Europeo de Normas de Telecomunicaciones (ETSI), la Alianza para Soluciones de la Industria de las Telecomunicaciones (ATIS), la Asociación de Tecnología de las Telecomunicaciones (TTA), y el Comité de la Tecnología de la Telecomunicación (TTC). El establecimiento del 3GPP se formalizó en diciembre de 1998 por la firma del “El Acuerdo del Proyecto Común de Tecnologías Inalámbricas de la 3ª Generación”.

El 3GPP proporciona normas globalmente aplicables como Especificaciones Técnicas e Informes Técnicos para un Sistema Móvil de la 3ª Generación basándose en unas redes de núcleo GSM evolucionadas y tecnologías de acceso de radio que admiten (p. ej., Acceso de Radio Terrestre Universal (UTRA) para tanto modos de Dúplex por División de Frecuencia (FDD) como de Dúplex por División en el Tiempo (TDD)). El 3GPP también proporciona normas para mantenimiento y despliegue del Sistema Global de Comunicaciones Móviles (GSM) como especificaciones técnicas e informes técnicos que incluyen tecnologías de acceso de radio evolucionadas (p. ej., Servicio General de Paquetes de Radio (GPRS) y tasas de datos mejoradas para la evolución de GSM (EDGE)). Las Especificaciones Técnicas para normas actuales relacionadas con la telefonía móvil están generalmente disponibles al público a partir de la organización 3GPP.
El 3GPP está estudiando actualmente la evolución del Sistema Móvil 3G y considera contribuciones (opiniones y propuestas) dirigidas hacia la evolución de la red UTRA (UTRAN). Se identificó un conjunto de requisitos de alto

nivel por los laboratorios del 3GPP que incluyen: coste reducido por bit; aprovisionamiento de servicio aumentado (es decir, más servicios a coste inferior con mejor calidad); flexibilidad de uso de bandas de frecuencia existentes y nuevas; arquitectura simplificada con interfaces abiertas; y consumo de potencia de terminal reducido/razonable.

Un estudio sobre la Evolución a Largo Plazo de UTRA Y UTRAN (UTRAN-LTE, también conocido como 3GPP-LTE y E-UTRA) se inició en diciembre de 2004 con el objetivo para desarrollar una estructura para la evolución de la tecnología de acceso de radio del 3GPP hacia una tecnología de acceso de radio de tasa de datos alta, baja latencia y de paquetes optimizados. El estudio considera modificaciones a la capa física de interfaz de radio (enlace descendente y enlace ascendente) tal como medios para admitir ancho de banda de transmisión flexible de hasta 20 MHz, la introducción de nuevos esquemas de transmisión, y tecnologías de múltiples antenas avanzadas. El 3GPP-LTE está basado en una interfaz de radio que incorpora técnicas de múltiplex por división de frecuencias ortogonales (OFDM). OFDM es un formato de modulación de múltiples portadoras digital que usa un gran número de subportadoras ortogonales espaciadas de manera cercana para llevar respectivos canales de datos de usuario. Cada subportadora se modula con un esquema de modulación convencional, tal como Modulación por Amplitud en Cuadratura (QAM), a una tasa de símbolos baja (relativamente) en comparación con la tasa de transmisión de frecuencia de radio (RF). En la práctica, las señales de OFDM se generan usando el algoritmo de transformada rápida de Fourier (FFT).

En un escenario de comunicación tradicional, cuando un dispositivo, tal como un equipo de usuario ("UE"), se comunica con otro dispositivo o UE, la comunicación en primer lugar viaja a través de una red. Por ejemplo, en una red del 3GPP-LTE, tales comunicaciones viajarían desde el UE, a través de un Nodo B evolucionado ("eNB"), a otro UE. En una red de WiFi, tales comunicaciones pueden viajar a través de un punto de acceso ("AP"). Los servicios basados en proximidad ("ProSe"), también conocidos como comunicaciones de dispositivo a dispositivo (D2D), permiten que un dispositivo comunique directamente con otro dispositivo, sin la necesidad de que las comunicaciones viajen a través de una red. Un servicio de este tipo puede ser especialmente valioso en el caso de una emergencia que desactiva toda o parte de una red. Una emergencia de este tipo puede incluir desastres naturales, cortes de energía generalizados, ataques terroristas, y similares. Un servicio de este tipo puede ser especialmente útil para equipos de primera respuesta, p. ej., oficiales de policía, bomberos, técnicos médicos de emergencias (EMT), y similares. Hay varias propuestas para establecer una red 3GPP separada para equipos de primera respuesta, tal como la Autoridad de la Primera Red de Respuesta (FirstNet). Debería entenderse, sin embargo, que esta memoria descriptiva no está limitada en este sentido.

Hay dos tipos básicos de comunicaciones ProSe: comunicación ProSe 1:1 y comunicación de grupo ProSe. Con referencia a la Figura 1A, se ilustra una instancia ejemplar de comunicación ProSe 1:1. Un dispositivo 102 y un dispositivo 104 están dispuestos para comunicarse directamente entre sí sin ninguna necesidad de dirigir en primer lugar las comunicaciones a través de una red mediante un eNB, un punto de acceso, una estación base, o similares.

Con referencia a la Figura 1B, se ilustra una instancia ejemplar de comunicación de grupo ProSe. Un dispositivo 152 está dispuesto para comunicarse directamente con el dispositivo 154 y el dispositivo 156, sin la necesidad de dirigir en primer lugar las comunicaciones a través de un eNB, estación base, u otro dispositivo similar. De manera similar, aunque no se ilustra en la Figura 1B, el dispositivo 154 y el dispositivo 156 podrían comunicarse directamente entre sí sin ninguna necesidad de dirigir en primer lugar las comunicaciones a través de una red. Debe entenderse que puede haber dispositivos adicionales en el grupo ProSe. Sin embargo, tales dispositivos no se ilustran en la Figura 1B.

Haciendo referencia de nuevo a la Figura 1A, puede haber una situación donde se desee que el dispositivo 102 y el dispositivo 104 debieran poder descubrirse entre sí y participar en comunicación directa. El sistema debería poder autorizar al dispositivo 102 y 104 a establecer sesiones de datos mediante señalización con la red (si está disponible cobertura de red) o mediante configuración disponible en un Módulo de Identidad de Abonado Universal ("USIM") de cada dispositivo (si no está disponible cobertura de red).

Dos tecnologías posibles para el enlace de comunicación D2D son WiFi (p. ej., WiFi Directa) o una nueva tecnología basada en LTE, denominada en la presente memoria como "LTE Directa". Mientras que porciones de esta memoria descriptiva pueden hacer referencia específicamente a WiFi Directa, debe entenderse que las realizaciones pueden usarse también con LTE Directa u otras tecnologías de enlace de comunicación D2D que existen actualmente o puedan desarrollarse en el futuro.

En WiFi Directa, el canal de multidifusión en el enlace D2D es equivalente a comunicaciones de enlace de capa de 802.11 de multidifusión como se define en las normas 802.11. Para este fin, los miembros de grupo ProSe se unirían en primer lugar al mismo conjunto de servicio básico (BSS) 802.11. El dispositivo de recepción debería poder recibir una transmisión de comunicación de grupo ProSe independientemente de si el dispositivo de transmisión ha descubierto o no el dispositivo de recepción. Por lo tanto, se supone en este punto que la arquitectura de sistema debería proporcionar una manera para proteger datos de plano de usuario que se transmiten en el canal de comunicación de grupo ProSe que permite que el dispositivo de recepción descifre los datos incluso antes de que el dispositivo de recepción haya sido descubierto (es decir, antes de que el dispositivo de recepción se haya unido al grupo ProSe en la capa D2D).

Con referencia a la Figura 2, se presenta una arquitectura de sistema ejemplar para comunicación ProSe 1:1. En este punto, el dispositivo 202 y el dispositivo 204 están acoplados entre sí mediante tanto un enlace D2D 210 como una sesión de comunicación de capa de aplicación 220. El enlace D2D puede realizarse como un enlace WiFi-Directa. La sesión de comunicación puede establecerse usando un cliente entre pares (P2P) basado en SIP en la capa de aplicación para establecer y liberar sesiones de voz y datos P2P.

Con referencia a la Figura 3, se presenta un diagrama de flujo ejemplar que ilustra el establecimiento de una sesión de comunicación 1:1. Un primer dispositivo y un segundo dispositivo se descubren entre sí usando una diversidad de técnicas actualmente conocidas en la técnica o desarrolladas en el futuro (302). Posteriormente, el primer dispositivo y el segundo dispositivo negocian entre sí para determinar qué estación será el propietario de grupo y cuál será el cliente (304).

Las comunicaciones mediante WiFi Directa son asimétricas en que uno de los dispositivos actúa en un papel similar al de un punto de acceso 802.11 y se denomina como el propietario de grupo de P2P (“GO”). El otro dispositivo toma el papel de un cliente P2P. Haciendo referencia de nuevo a la Figura 2, el dispositivo 202 es el cliente P2P y el dispositivo 204 es el P2P GO. La determinación de cuál dispositivo se hace el cliente P2P y cuál se hace el P2P GO puede tener lugar en una de varias diferentes maneras que existen actualmente o puedan desarrollarse en el futuro. Por ejemplo, puede haber un valor de intención de GO asociado con cada dispositivo. En un caso de este tipo, el dispositivo con el valor de intención GO más alto puede convertirse en el GO. En caso de un empate de valor de intención GO, pueden usarse otros criterios para determinar el GO.

Posteriormente, el cliente comenzará un procedimiento de autenticación mutua con el GO (306). Esta autenticación tiene lugar de una manera similar a la manera que una estación (STA) 802.11 usaría para autenticarse con un punto de acceso (AP) 802.11. El fin del proceso de autenticación es para que cada dispositivo confirme que el otro dispositivo es un miembro autorizado de la red. Pueden usarse diversos tipos de credenciales como parte del proceso de autenticación. Por ejemplo, los dispositivos autorizados pueden tener un certificado emitido por una Autoridad de Certificado (CA) común. En un caso de uso que implica una red privada que es accesible únicamente por los equipos de primera respuesta, la CA puede emitir certificados a todos los dispositivos propiedad de los equipos de primera respuesta. Posteriormente, si un dispositivo se vuelve comprometido (p. ej., el dispositivo se pierde o es robado), la CA puede revocar el certificado a ese dispositivo de modo que el dispositivo comprometido ya no estaría autorizado.

El certificado puede ser específico de usuario o especifico de dispositivo o ambos. En una realización, el certificado puede incluir el identificador global del usuario en la capa de aplicación y el identificador de enlace del dispositivo en la capa de enlace D2D. Aunque pueden usarse muchos identificadores globales de usuario diferentes, en una realización, el certificado incluye el Identificador de Recurso Uniforme (URI) del Protocolo de Iniciación de Sesión (SIP) del usuario. Aunque pueden usarse muchos identificadores de enlace diferentes para el dispositivo, en una realización, el certificado incluye la dirección de control de acceso al medio (MAC) del dispositivo. Como parte del procedimiento de autenticación 802.1x basado en certificado, se deriva una Clave Maestra por Pares (PMK1) común. El procedimiento de autenticación puede usar uno de una diversidad de diferentes métodos. En una realización, puede usarse la seguridad de capa de transporte del protocolo de autenticación extensible (EAP-TLS) para generar la PMK1. La PMK1 puede usarse posteriormente para protección de confidencialidad e integridad de tramas de datos durante la duración de la sesión. Como alternativa, puede generarse otra clave maestra por pares durante la sesión. Haciendo referencia de nuevo a la Figura 2, se muestra la PMK1 compartiéndose entre el dispositivo 202 y el dispositivo 204 en el enlace 215.

En la capa de aplicación, la señalización de SIP también está protegida. Esto puede tener lugar a través del uso de otra Clave Maestra por Pares (PMK2) que puede derivarse de la PMK1. La derivación puede hacerse con una Función de Derivación de Clave (KDF). Ejemplos de las KDF incluyen la función de derivación de clave basada en contraseña (PBKDF2) y guiones. La razón para usar un cliente P2P basado en SIP cuando se está sin cobertura es que la comunicación puede estar también basada en SIP cuando se establece mediante la infraestructura de red (p. ej., reutilizando el Subsistema Multimedia de IP definido por el 3GPP). Además, los URI de SIP pueden usarse como identificadores de usuario globales para ambos casos de uso (tanto con como sin cobertura). Haciendo referencia de nuevo a la Figura 2, se muestra la PMK2 compartiéndose entre el dispositivo 202 y el dispositivo 204 en el enlace 225.

Haciendo referencia de vuelta a la Figura 1B, se muestra cómo se transmiten tramas de multidifusión en un grupo P2P en WiFi Directa. Presentes en el grupo P2P 150 se encuentran un dispositivo 152, un dispositivo 154, y un dispositivo 156. En la Figura 1B, se ha asignado al dispositivo 154 el papel del P2P GO y tanto el dispositivo 152 como el dispositivo 156 sirven como clientes P2P.

El dispositivo 152 envía una trama de multidifusión (es decir, una trama cuya dirección de destino es una dirección de MAC de multidifusión) como una trama de unidifusión al P2P GO (dispositivo 154). Esta trama está protegida con claves transitorias por pares (PTK) generadas a partir de una clave maestra por pares (PMK3) que se comparte entre el dispositivo 152 y el dispositivo 154.

El dispositivo 154 a continuación retransmite la trama como una trama de multidifusión que puede recibirse y descifrarse por todos los miembros del grupo P2P, incluyendo el dispositivo 156 y cualesquiera otros dispositivos que pueden existir en la red pero que no se ilustran en la Figura 1B. Esta trama está protegida con claves temporales de grupo (GTK) que se generan a partir de la clave maestra de grupo (GMK) que se genera típicamente por el P2P GO y se distribuye a todos los miembros de grupo P2P.

Con referencia a la Figura 4, se presenta una arquitectura de sistema ejemplar para su uso en comunicación de grupo ProSe. Aunque las comunicaciones de grupo ProSe típicamente implican más de dos dispositivos en comunicación directa entre sí, únicamente se muestran dos de tales dispositivos en la Figura 4. Debe entenderse que pueden conectarse dispositivos adicionales, pero que no se muestran para evitar saturar la Figura 4. La porción por debajo de la línea discontinua 450 hace referencia a comunicaciones de grupo ProSe en ausencia de cobertura de red. La porción por encima de la línea discontinua 450 hace referencia a comunicaciones de grupo ProSe en la presencia de cobertura de red y se describirá en detalle adicional a continuación, después del análisis de la Figura 5.

En la Figura 4, se muestra una conexión entre un dispositivo 460 y un dispositivo 470. El dispositivo 470 es el P2P GO, mientras que el dispositivo 460 es un cliente P2P. Se realiza un enlace D2D 480 como un enlace de WiFi Directa. El enlace D2D 480 acopla juntos el cliente de enlace D2D 462, que se ejecuta en el dispositivo 460, con el cliente de enlace D2D 472, que se ejecuta en el dispositivo 470. Se usa un cliente basado en Pulsar para Hablar sobre Celular (PoC) de la Alianza Móvil Abierta (OMA) 464 en la capa de aplicación para establecer y liberar sesiones de voz y datos de P2P en los dispositivos que toman el papel del cliente P2P. Se usa un software de servidor basado en PoC de OMA 474 en el dispositivo que toma el papel de P2P GO (dispositivo 470). Este software de servidor PoC de OMA aloja la funcionalidad de una Función de Control de PoC de OMA y la función de participación de PoC de OMA, como se define en la especificación de la versión 2.1 de PoC de OMA. El cliente de PoC 464 y el servidor de PoC 474 se comunican entre sí mediante la conexión de PoC 496.

En la capa de aplicación, se supone que cada cliente es un miembro de una sesión de grupo de PoC de OMA que se identifica mediante un identificador de sesión de grupo de PoC de OMA (p. ej., un URI de SIP). En la capa de enlace D2D, a la sesión de grupo de PoC de OMA se le proporciona un identificador de grupo D2D especial. En el caso de WiFi Directa, este identificador de grupo D2D puede ser la dirección de multidifusión que se usa para distribución de tramas de datos que pertenecen a este grupo de PoC de OMA.

Los mensajes de SIP entre el cliente de PoC de OMA y el servidor de PoC de OMA pueden protegerse, si fuera necesario, con una clave maestra por pares (PMK4) 492 que puede derivarse a partir de la PMK3 490.

Para establecer la relación de confianza en el enlace D2D, los miembros de grupo de P2P poseen ciertos parámetros. Por ejemplo, el P2P GO puede tener los identificadores de capa de enlace D2D de todos los participantes de grupo de multidifusión activos. Además, el P2P GO puede tener, para cada miembro, una Clave Maestra por Pares (PMK3) que se comparte con ese miembro de grupo. De manera similar, todos los clientes P2P en el grupo de P2P pueden tener el identificador de capa de enlace D2D del P2P GO y su correspondiente PMK3. Todos los dispositivos en el grupo (tanto el P2P GO como los clientes P2P) pueden tener el identificador de capa de enlace D2D del canal PoC de multidifusión (denominado en este punto como el Grupo D2D_ID) usado por la función de PoC de participación en el grupo de propietario de P2P para distribución de tramas de datos a todos los miembros de grupo de PoC de OMA. Además, todos los dispositivos en el grupo pueden tener la clave maestra de grupo (GMK) 494 que se usó para generar claves temporales de grupo (GTK) para protección del canal D2D de multidifusión. Los dispositivos pueden derivar en cualquier momento de manera autónoma la GTK actual. Esto puede realizarse en una diversidad de diferentes maneras, tal como basándose en una indicación de tiempo. Esto puede usarse de modo que los dispositivos en el grupo pueden desencriptar tramas D2D incluso antes de ser descubiertas por el P2P GO.

Toda esta información podría estar configurada por los dispositivos individuales. Sin embargo, una solución de este tipo puede no escalarse bien. Un sistema de autenticación basado en certificado puede ser más escalable. En autenticación basada en certificado, el certificado puede ser tanto específico de usuario como específico de dispositivo e incluir los siguientes parámetros; 1) el identificador global del usuario en la capa de aplicación (p. ej., URI de SIP); 2) el identificador de enlace del dispositivo en la capa D2D (p. ej., dirección de MAC administrada globalmente del “sub-dispositivo” de WLAN en el dispositivo y/o un identificador de hardware inmodificable similar); 3) el identificador de sesión de grupo PoC predispuesto (URI de SIP) al que pertenece el usuario (opcional); 4) el correspondiente identificador de canal de multidifusión D2D (Grupo de D2D_ID = dirección de MAC de multidifusión); y 5) la clave maestra de grupo (GMK) usada para protección del canal D2D de multidifusión.

Con referencia a la Figura 5, se presenta un diagrama de flujo que ilustra el establecimiento general de comunicación de grupo ProSe. Para los fines de la Figura 5, debe suponerse que ya hay un propietario de grupo P2P en el grupo ProSe. La manera en la que el propietario de grupo de P2P se estableció puede tener lugar en una de una diversidad de diferentes maneras, tanto conocidas ahora como desarrolladas en el futuro.

El cliente P2P descubre el P2P GO (502). Posteriormente al descubrimiento del descubrimiento de P2P GO por un cliente P2P, el cliente P2P activa un procedimiento de autenticación 802.1X basado en certificado (504). Esto puede tener lugar en una de una diversidad de diferentes maneras, tanto conocidas ahora (tal como mediante EAP-TLS) o

desarrolladas en el futuro. Durante el procedimiento de autenticación, se deriva (506) una clave maestra por pares (PMK3). Posteriormente, se deriva una clave maestra por pares (PMK4) a partir de la PMK3 (508). Como se ha descrito anteriormente, se usa la PMK4 para encriptar mensajes de señalización de SIP entre el cliente PoC de OMA y el servidor PoC de OMA.

Durante la autenticación basada en certificado, el cliente P2P evalúa su identidad de capa de enlace D2D (ID de D2D) y su identidad de capa de aplicación (tal como un URI de SIP), así como el hecho de que pertenece a la sesión de grupo de PoC de OMA que se identifica tanto con un URI de SIP como con un identificador de canal de multidifusión D2D (dirección de MAC de multidifusión) en la capa de aplicación y en la capa de enlace D2D, respectivamente.

Durante la autenticación basada en certificado, el cliente P2P también evalúa el conocimiento de la clave maestra de grupo (GMK) que se usará para generar claves temporales de grupo (GTK) para protección del canal D2D de multidifusión. En cualquier punto en el tiempo, los miembros de grupo P2P pueden derivar de manera autónoma la GTK actualmente válida a partir de la GMK de manera algorítmica (p. ej., usando la hora del día actual). Después de que se han derivado la PMK3 y PMK4, el dispositivo puede comenzar a enviar y recibir señales en el grupo ProSe (510).

La porción de la Figura 4 que incluye la línea discontinua anterior 450 es un ejemplo de una arquitectura de sistema para comunicación de grupo ProSe para Seguridad Pública, cuando se establece un enlace de comunicación D2D bajo cobertura de red. Por debajo de la línea discontinua 450 se encuentra el caso de uso cuando no está disponible cobertura de red, descrito en detalle anteriormente. En contraste al caso sin cobertura por debajo de la línea discontinua 450, por encima de la línea discontinua 450, los dispositivos pueden comunicarse entre sí (tanto señalización como datos de usuario) a través de la infraestructura de red. Tales comunicaciones se usan en arquitectura de PoC de OMA. Los dispositivos 460 y 470 pueden cada uno comunicarse con el servidor de PoC de OMA 440.

Supóngase que los dispositivos que pertenecen al mismo grupo de PoC de OMA han establecido una sesión de grupo de PoC de OMA con un servidor de PoC de OMA central 440. En algún punto, un miembro de grupo y/o la red pueden decidir que todos los miembros de grupo están en proximidad y deberían poder comunicarse con los otros miembros de grupo sobre un enlace de comunicación D2D. En una realización de WiFi Directa, uno de los miembros de grupo se vuelve un P2P GO. Los otros miembros de grupo toman el papel de un cliente P2P y establecen individualmente un enlace D2D seguro con el P2P GO en una de las siguientes maneras.

En un método, cada cliente P2P realiza autenticación basada en certificado con el propietario de grupo de P2P como se ha descrito con referencia a la Figura 5. En otras palabras, el mismo mecanismo para establecimiento de enlace D2D seguro puede usarse independientemente de si los dispositivos están con cobertura de red o sin cobertura de red.

Como alternativa, una entidad centralizada en la red (tal como la entidad de PoC 440) distribuye la información (detallada adicionalmente a continuación) a cada dispositivo en la red. La información distribuida permite que cada cliente P2P establezca un enlace seguro con el P2P GO. Para esta opción, la información distribuida por la red consiste en varios parámetros. El propietario de grupo de P2P recibe los identificadores de capa de enlace D2D de todos los participantes de grupo de multidifusión activos (D2D_ID (A) en la Figura 4). Además, para cada miembro de grupo, el P2P GO recibe una clave maestra por pares (PMK3 (A)) que se comparte con ese miembro de grupo. Los clientes P2P reciben el identificador de capa de enlace D2D del propietario de grupo de P2P (D2D_ID (GO) en la Figura 4) y su correspondiente PMK3 (PMK3 (A) en la Figura 4).

Cada uno de los dispositivos (es decir, tanto el propietario de grupo de P2P como los clientes P2P) reciben el identificador de capa de enlace D2D del canal PoC de multidifusión (Grupo de D2D_ID en la Figura 4) usado por la función PoC de participación en el propietario de grupo de P2P para distribución de tramas de datos a todos los miembros de grupo de PoC de OMA. Además, cada uno de los dispositivos recibe la GMK—la clave maestra de grupo usada para generar claves temporales de grupo (las GTK) para protección del canal D2D de multidifusión. Como se ha descrito anteriormente, los dispositivos deberían poder derivar de manera autónoma en cualquier momento la GTK actual en uno de una diversidad de diferentes métodos. Por ejemplo, la GTK actual puede derivarse basándose en una indicación de tiempo.

La solución de red para establecimiento de comunicación ProSe 1:1 bajo cobertura de red (no ilustrada) es incluso más sencilla para ayudar al establecimiento de un enlace D2D seguro, la información de asistencia de red proporcionada a cualquier dispositivo incluye el D2D_ID del dispositivo al que se desea conexión, así como la clave maestra por pares (PMK1). Esta información puede proporcionarse mediante SIP o mediante una diversidad de otras entidades diferentes, tanto aquellas que existen ahora como aquellas que pueden existir en el futuro.

Transiciones entre con cobertura y sin cobertura

Independientemente de cómo se estableció el enlace de comunicación D2D bajo cobertura de red, los dispositivos en cualquiera de una 1:1 o un grupo de comunicaciones pueden seguir usando la misma clave maestra por pares incluso cuando pasan a sin cobertura de red. De manera similar, para un enlace D2D que se estableció sin cobertura

usando autenticación basada en certificado, si los dispositivos vuelven bajo cobertura de red con comunicación establecida, pueden seguir usando la misma clave maestra por pares.

Sin embargo, si la validez de la clave maestra por pares actual caduca después de que los dispositivos han dejado el contexto original (es decir, cuando un dispositivo deja la cobertura de red, a continuación, entra en cobertura de red de nuevo) no habrá necesidad de replegarse a la opción u opciones para la renovación de clave que es/son válidas para su entorno actual. Una situación ejemplar es que un dispositivo se vuelve vulnerable durante un periodo sin cobertura de red. La persona que usa el dispositivo informa este hecho a la autoridad de certificado, que revoca el certificado para el dispositivo. Sin embargo, hasta que los otros dispositivos entran en cobertura de red, pueden no tener conocimiento del certificado revocado. Por lo tanto, puede ser deseable comprobar el certificado tan pronto como un dispositivo vuelve a entrar en cobertura de red.

Aplicabilidad a otras tecnologías D2D

El enlace D2D basándose en la tecnología WiFi Directa (que se usó hasta ahora como una base para la descripción de la presente propuesta) es intrínsecamente asimétrico, en que designa un “dispositivo con privilegios” especial, es decir, el dispositivo que toma el papel del P2P GO.

Con referencia a la arquitectura ProSe 1:1 de comunicación representada en la Figura 2, esta designación de un dispositivo con privilegio (el GO) es específica a la operación de WiFi Directa; una realización que no usa WiFi Directa para la tecnología D2D puede tener o no un dispositivo con privilegio de este tipo. Sea cual sea la tecnología D2D alternativa, una tecnología de este tipo probablemente también esté basada en identificadores de capa de enlace D2D (similar a las direcciones de MAC en WiFi Directa) y un secreto pre-compartido para asegurar el enlace D2D. Como consecuencia, se aplica aún tanto una solución basada en certificado como una solución asistida por red.

En referencia a la arquitectura de comunicación de grupo ProSe representada en la Figura 4, el dispositivo con privilegio (es decir, el propietario de grupo P2P) tiene funcionalidades con privilegio adicionales en las capas superiores, tal como la funcionalidad de servidor PoC de OMA. Esperamos que cualquier tecnología D2D alternativa que admita comunicación de grupo ProSe necesite aún estar basada en un dispositivo con privilegio similar, caso en el que las soluciones para la comunicación de grupo ProSe anteriormente descritas aún aplican.

Ejemplos, como se describe en la presente memoria, pueden incluir, o pueden operar en, lógica o un número de componentes, módulos, o mecanismos. Los módulos son entidades tangibles (p. ej., hardware) que pueden realizar operaciones especificadas y pueden estar configurados o dispuestos en una cierta manera. En un ejemplo, pueden estar dispuestos circuitos (p. ej., de manera interna o con respecto a entidades externas tales como otros circuitos) de una manera especificada como un módulo. En un ejemplo, la totalidad o parte de uno o más sistemas informáticos (p. ej., un sistema informático independiente, de cliente o servidor) o uno o más procesadores de hardware pueden estar configurados por firmware o software (p. ej., instrucciones, una porción de aplicación, o una aplicación) como un módulo que opera para realizar operaciones especificadas. En un ejemplo, el software puede residir en un medio legible por máquina. En un ejemplo, el software, cuando se ejecuta por el hardware subyacente del módulo, provoca que el hardware realice las operaciones especificadas.

Por consiguiente, el término “módulo” se entiende que abarca una entidad tangible, que es una entidad que está físicamente construida, específicamente configurada (p. ej., alámbrica), o temporalmente (p. ej., transitoriamente) configurada (p. ej., programada) para operar en una manera específica o para realizar parte de cualquier operación descrita en la presente memoria. Considerando ejemplos en los que los módulos están temporalmente configurados, cada uno de los módulos no necesita instanciarse en un momento cualquiera en el tiempo. Por ejemplo, cuando los módulos comprenden un procesador de hardware de fin general configurado usando software, el procesador de hardware de fin general puede estar configurado como respectivos módulos diferentes en diferentes tiempos. El software puede configurar, por consiguiente, un procesador de hardware, por ejemplo, para constituir un módulo particular en una instancia de tiempo y para constituir un módulo diferente en una instancia diferente de tiempo.

La Figura 6 es un diagrama de bloques que ilustra una máquina de ejemplo 600 en la que puede realizarse una cualquiera o más de las técnicas (p. ej., metodologías) analizadas en la presente memoria. En realizaciones alternativas, la máquina 600 puede operar como un dispositivo independiente o puede estar conectada (p. ej., en red) a otras máquinas. En un despliegue en red, la máquina 600 puede operar en la capacidad de una máquina de servidor, una máquina cliente, o tanto en entornos de red de servidor-cliente. En un ejemplo, la máquina 600 puede actuar como una máquina de pares en entorno de red entre pares (P2P) (u otro distribuido). La máquina 600 puede ser un ordenador personal (PC), un PC de tableta, un decodificador de salón (STB), un Asistente Digital Personal (PDA), un teléfono inteligente, un aparato web, un encaminador de red, conmutador o puente, un dispositivo de navegación especializado, ordenadores portátiles, una televisión, o cualquier máquina que pueda ejecutar instrucciones (secuencial o de otra manera) que especifiquen acciones a tomarse por esa máquina. Además, aunque únicamente se ilustra una única máquina, el término “máquina” deberá tomarse también para incluir cualquier colección de máquinas que ejecuten de manera individual o conjunta un conjunto (o múltiples conjuntos) de instrucciones para realizar una cualquiera o más de las metodologías analizadas en la presente memoria, tales como informática en la nube, software como un servicio (SaaS), otras configuraciones de agrupación informática.

La máquina (p. ej., el sistema informático) 600 puede incluir un procesador de hardware 602 (p. ej., una unidad de procesamiento central (CPU), una unidad de procesamiento de gráficos (GPU), un núcleo de procesador de hardware, o cualquier combinación de los mismos), una memoria principal 604, y una memoria estática 606, algunos o todos los cuales pueden comunicarse entre sí mediante un inter-enlace (p. ej., bus) 608. La máquina 600 puede incluir adicionalmente un dispositivo de visualización 610, un dispositivo de entrada alfanumérica 612 (p. ej., un teclado), y un dispositivo de navegación de interfaz de usuario (UI) 614 (p. ej., un ratón o almohadilla táctil). En un ejemplo, el dispositivo de visualización 610, dispositivo de entrada 612 y el dispositivo de navegación de UI 614 pueden ser una pantalla táctil que consigue todas las tres tareas. La máquina 600 puede incluir adicionalmente un dispositivo de almacenamiento masivo (p. ej., memoria flash) 616, un dispositivo de generación de señal 618 (p. ej., un altavoz), un dispositivo de interfaz de red 620, y uno o más sensores 621, tales como un sensor de sistema de posicionamiento global (GPS), brújula, acelerómetro u otro sensor. La máquina 600 puede incluir un controlador de salida 628, tal como una conexión en serie (p. ej., bus serie universal (USB), paralela u otra alámbrica o inalámbrica (p. ej., de infrarrojos (IR), Bluetooth, o de comunicación de campo cercano) para comunicarse o controlar uno o más dispositivos periféricos (p. ej., una impresora, lector de tarjetas, etc.).

El dispositivo de almacenamiento masivo 616 puede incluir un medio legible por máquina 622, en el que se almacena uno o más conjuntos de estructuras de datos o instrucciones 624 (p. ej., software) que incorporan o se utilizan por una cualquiera o más de las técnicas o funciones descritas en la presente memoria. Las instrucciones 624 pueden residir también, completa o al menos parcialmente, en la memoria principal 604, en memoria estática 606, o en el procesador de hardware 602 durante la ejecución de las mismas por la máquina 600. En un ejemplo, uno o cualquier combinación del procesador de hardware 602, la memoria principal 604, la memoria estática 606, o el dispositivo de almacenamiento masivo 616 pueden constituir medios legibles por máquina.

Aunque el medio legible por máquina 622 se ilustra como un único medio, la expresión “medio legible por máquina” puede incluir un único medio o múltiples medios (p. ej., una base de datos centralizada o distribuida, y/o cachés y servidores asociados) que están dispuestos para almacenar la una o más instrucciones 624.

La expresión “medio legible por máquina” puede incluir cualquier medio que pueda almacenar, codificar o llevar instrucciones para su ejecución por la máquina 600 y que provoque que la máquina 600 realice una cualquiera o más de las técnicas de la presente descripción, o que pueda almacenar, codificar o llevar estructuras de datos usadas por o asociadas con tales instrucciones. Ejemplos de medio legible por máquina no limitantes pueden incluir memorias de estado sólido y medios ópticos y magnéticos. En un ejemplo, un medio legible por máquina masivo comprende un medio legible por máquina con una pluralidad de partículas que tienen masa en reposo. Ejemplos específicos de medios legibles por máquina masivos pueden incluir: memoria no volátil, tal como dispositivos de memoria de semiconductores (p. ej., Memoria de Sólo Lectura Eléctricamente Programable (EPROM), Memoria de Sólo Lectura Eléctricamente Programable Borrable (EEPROM)) y dispositivos de memoria flash; discos magnéticos, tales como discos duros internos y discos extraíbles; discos magneto-ópticos; y discos CD-ROM, DVD-ROM, y Blu-Ray.

Las instrucciones 624 pueden transmitirse o recibirse adicionalmente a través de una red de comunicaciones 626 usando un medio de transmisión mediante el dispositivo de interfaz de red 620 que utiliza uno cualquiera de un número de protocolos de transferencia (p. ej., retransmisión de tramas, protocolo de Internet (IP), protocolo de control de transmisión (TCP), protocolo de datagrama de usuario (UDP), protocolo de transferencia de hipertexto (HTTP), etc.). Redes de comunicación de ejemplo pueden incluir una red de área local (LAN), una red de área extensa (WAN), una red de datos de paquetes (p. ej., la Internet), redes de telefonía móvil (p. ej., redes celulares), redes de Servicio Telefónico Básico (POTS), y redes de datos inalámbricas (p. ej., la familia de normas 802.11 del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) conocidas como Wi-Fi®, la familia de normas del IEEE 802.16 conocidas como WiMAX®), redes entre pares (P2P), entre otras. En un ejemplo, el dispositivo de interfaz de red 620 puede incluir uno o más conectores físicos (p. ej., Ethernet, coaxial, o conectores de teléfono) o una o más antenas para conectar a la red de comunicaciones 626. En un ejemplo, el dispositivo de interfaz de red 620 puede incluir una pluralidad de antenas para comunicarse inalámbricamente usando al menos una de las técnicas de única-entrada múltiple-salida (SIMO), múltiple-entrada múltiple-salida (MIMO), o múltiple-entrada única-salida (MISO). La expresión “medio de transmisión” deberá tomarse para incluir cualquier medio intangible que pueda almacenar, codificar o llevar instrucciones para ejecución por la máquina 600, e incluye señales de comunicaciones digitales o analógicas u otro medio intangible para facilitar la comunicación de tal software.

La descripción detallada anterior incluye referencias a dibujos adjuntos, que forman una parte de la descripción detallada. Los dibujos muestran, por medio de ilustración, realizaciones específicas que pueden realizarse. A estas realizaciones también se hace referencia en la presente memoria como “ejemplos”. Tales ejemplos pueden incluir elementos además de aquellos mostrados o descritos. Sin embargo, también se contemplan ejemplos que incluyen los elementos mostrados o descritos. Además, también se contemplan ejemplos usando cualquier combinación o permutación de aquellos elementos mostrados o descritos (o uno o más aspectos de los mismos), ya sea con respecto a un ejemplo particular (o uno o más aspectos del mismo), o con respecto a otros ejemplos (o uno o más aspectos de los mismos) mostrados o descritos en la presente memoria.

En este documento, los términos “un”, “una” se usan, como es común en los documentos de patentes, para incluir uno o más de uno, independientemente de cualesquiera otras instancias o usos de “al menos uno” o “uno o más”.

En este documento, el término “o” se usa para hacer referencia a un o no exclusivo, de manera que “A o B” incluye “A pero no B”, “B pero no A”, y “A y B”, a menos que se indique de lo contrario. En las reivindicaciones adjuntas, las expresiones “que incluye” y “en que” se usan como las equivalentes de inglés sencillo de las respectivas expresiones “que comprende” y “en donde”. También, en las siguientes reivindicaciones, las expresiones “que incluye” y “que comprende” son abiertas, es decir, un sistema, dispositivo, artículo o proceso que incluye elementos además de aquellos enumerados después de un término de este tipo en una reivindicación aún se considera que cae dentro del el alcance de esa reivindicación. Además, en las siguientes reivindicaciones, los términos “primero”, “segundo” y “tercero”, etc., se usan principalmente como etiquetas, y no se pretende que sugieran un orden numérico para sus objetos.

En la descripción detallada anterior, diversas características pueden agruparse juntas para simplificar la descripción. Sin embargo, las reivindicaciones pueden no exponer cada característica descrita en la presente memoria ya que las realizaciones pueden presentar un subconjunto de dichas características. Además, las realizaciones pueden incluir menos características que las descritas en un ejemplo particular.

La invención se define por las reivindicaciones independientes. Se proporcionan realizaciones preferidas por las reivindicaciones dependientes.

REIVINDICACIONES

1. Un método para acoplar un primer dispositivo móvil (102, 202) con un segundo dispositivo móvil (104, 204) en una sesión de comunicación de servicios basados en proximidad, ProSe, 1:1, comprendiendo el método:

descubrir el primer dispositivo móvil (102, 202) la presencia del segundo dispositivo móvil (104, 204);

negociar entre el primer dispositivo móvil (102, 202) y el segundo dispositivo móvil (104, 204) para determinar que el segundo dispositivo móvil (104, 204) será un propietario de grupo (306) de la sesión de comunicación y el primer dispositivo móvil (102, 202) será un cliente de la sesión de comunicación; y

realizar una autenticación mutua con el propietario de grupo (306);

el primer dispositivo móvil (102, 202) y el segundo dispositivo móvil (104, 204) se comunican entre sí mediante un enlace de dispositivo a dispositivo (210);

caracterizado por que

realizar la autenticación mutua comprende adicionalmente:

verificar el segundo dispositivo móvil (104, 204) un primer certificado propiedad del primer dispositivo móvil (102, 202); y

verificar el primer dispositivo móvil (102, 202) un segundo certificado propiedad del segundo dispositivo móvil (104, 204); en donde,

el primer certificado incluye un primer identificador de enlace que identifica el primer dispositivo móvil (102, 202);

el segundo certificado incluye un segundo identificador de enlace que identifica el segundo dispositivo móvil (104, 204);

el primer certificado está dispuesto para confirmar que el primer dispositivo móvil (102, 202) está autorizado; y

el segundo certificado está dispuesto para confirmar que el segundo dispositivo móvil (104, 204) está autorizado.

2. El método de la reivindicación 1, en donde realizar autenticación mutua comprende adicionalmente:

generar una clave maestra por pares; y en donde el método comprende adicionalmente:

usar la clave maestra por pares para proteger las transmisiones entre el primer dispositivo móvil (102, 202) y el segundo dispositivo móvil (104, 204) que viajan mediante el enlace D2D.

3. El método de la reivindicación 1 o 2 que comprende adicionalmente:

establecer una sesión de comunicación de capa de aplicación entre el primer dispositivo móvil (102, 202) y el segundo dispositivo móvil (104, 204).

4. El método de la reivindicación 1, en donde:

el primer identificador de enlace es una dirección de MAC del primer dispositivo móvil (102, 202) en la capa del enlace de dispositivo a dispositivo (210); y

el segundo identificador de enlace comprende una dirección de MAC del segundo dispositivo móvil (104, 204) en la capa del enlace de dispositivo a dispositivo (210).

5. El método de una de las reivindicaciones 1 o 4, en donde:

el primer certificado incluye adicionalmente un identificador global que pertenece a un usuario del primer dispositivo móvil (102, 202);

el segundo certificado incluye adicionalmente un identificador global que pertenece a un usuario del segundo dispositivo móvil (104, 204).

6. El método de la reivindicación 1, en donde el enlace de dispositivo a dispositivo (210) es una conexión de WiFi directa o una conexión de LTE directa.

7. El método de la reivindicación 1, en donde el primer dispositivo móvil (102, 202) está dispuesto para comunicarse al segundo dispositivo móvil (104, 204) en ausencia de cobertura de una red.

8. Un dispositivo móvil (102, 202) para comunicarse en una sesión de comunicación 1:1 de servicios basados en proximidad (ProSe), comprendiendo el dispositivo móvil (102, 202):

medios para procesar;

medios para transmitir y recibir señales acoplados a los medios para procesar y dispuestos para transmitir y recibir señales mediante un conjunto de antenas;

en donde los medios para procesar están dispuestos para:

descubrir la presencia de un segundo dispositivo móvil (104, 204);

negociar con el segundo dispositivo móvil (104, 204) para determinar que el segundo dispositivo móvil (104, 204) será un propietario de grupo (306) de la sesión de comunicación y el dispositivo móvil (102, 202) será un cliente de la sesión de comunicación; y

realizar una autenticación mutua con el segundo dispositivo móvil (104, 204) que es el propietario de grupo (306);

en donde el dispositivo móvil (102, 202) y el segundo dispositivo móvil (104, 204) están dispuestos para comunicarse entre sí mediante un enlace de dispositivo a dispositivo (210);

caracterizado por que

los medios para procesar están dispuestos adicionalmente para:

verificar un certificado propiedad del segundo dispositivo móvil (104, 204);

el certificado incluye un identificador de enlace que identifica el segundo dispositivo móvil (104, 204) y está dispuesto para confirmar que el segundo dispositivo móvil (104, 204) está autorizado.

9. El dispositivo móvil de la reivindicación 8, en donde el dispositivo móvil es un equipo de usuario dispuesto para transmitir y recibir señales mediante señalización de 3GPP-LTE.

10. El dispositivo móvil de la reivindicación 8, en donde el enlace de dispositivo a dispositivo (210) es mediante una conexión de WiFi directa.

11. El dispositivo móvil de la reivindicación 8, en donde el enlace de dispositivo a dispositivo (210) es mediante una conexión de LTE directa.

12. Un medio legible por máquina que incluye instrucciones para acoplar un primer dispositivo móvil (102, 202) con un segundo dispositivo móvil (104, 204) en una sesión de comunicación 1:1 de servicios basados en proximidad (ProSe), en donde las instrucciones, cuando se ejecutan por el primer dispositivo móvil (102, 202), provocan al primer dispositivo móvil (102, 202):

descubrir la presencia de un segundo dispositivo móvil (104, 204);

negociar con el segundo dispositivo informático que el segundo dispositivo móvil (104, 204) será un propietario de grupo (306) de la sesión de comunicación y el primer dispositivo móvil (102, 202) será un cliente de la sesión de comunicación; e

iniciar una autenticación mutua con el segundo dispositivo móvil (104, 204);

y

acoplar el primer dispositivo móvil (102, 202) y el segundo dispositivo móvil (104, 204) entre sí en una sesión de comunicación de servicios basados en proximidad, ProSe, 1:1, y para comunicarse con el segundo dispositivo móvil (104, 204) mediante un enlace de dispositivo a dispositivo (210); y

caracterizado por que

las instrucciones, cuando se ejecutan, provocan que el primer dispositivo móvil (102, 202) verifique un certificado propiedad del segundo dispositivo móvil (104, 204);

en donde el certificado incluye un identificador de enlace que identifica el segundo dispositivo móvil (104, 204) y está dispuesto para confirmar que el segundo dispositivo móvil (104, 204) está autorizado.

13. El medio legible por máquina de la reivindicación 12, en donde el medio comprende adicionalmente instrucciones que, cuando se ejecutan, provocan al primer dispositivo móvil (102, 204):

establecer una sesión de comunicación entre el primer dispositivo móvil y el segundo dispositivo móvil.

14. El medio legible por máquina de la reivindicación 13, en donde el medio comprende adicionalmente instrucciones que, cuando se ejecutan, provocan al primer dispositivo móvil (102, 204):

generar una clave maestra por pares; y

usar la clave maestra por pares para proteger las transmisiones entre el primer dispositivo móvil y el segundo dispositivo móvil que viajan mediante el enlace de dispositivo a dispositivo (210).

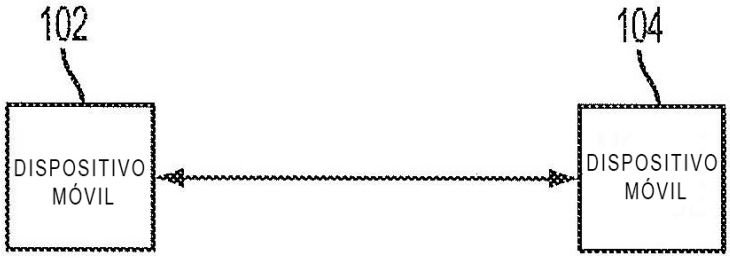
102
104
DISPOSITIVO MÓVIL
DISPOSITIVO MÓVIL

FIG. 1A

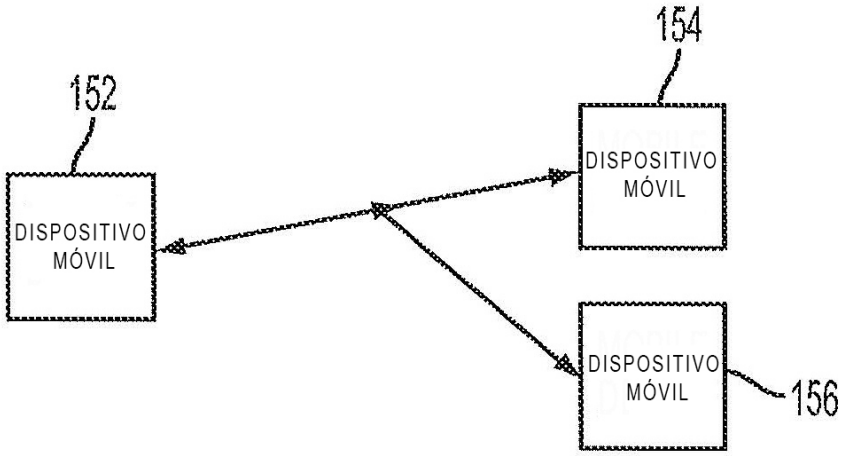
154
152
DISPOSITIVO MÓVIL
DISPOSITIVO MÓVIL
DISPOSITIVO MÓVIL
156

FIG. 1B

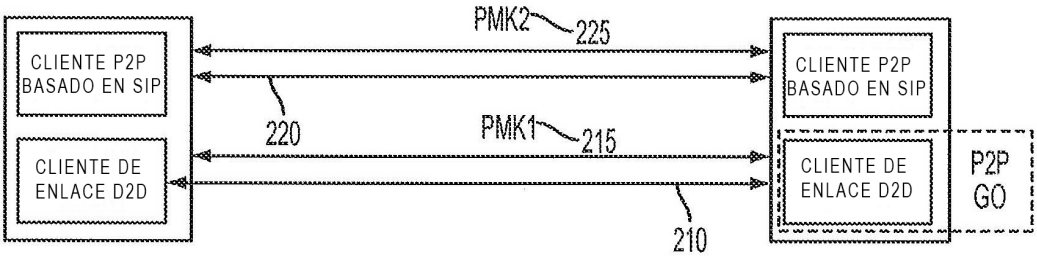
PMK2
225
CLIENTE P2P BASADO EN SIP
CLIENTE DE ENLACE D2D
220
PMK1
215
210
CLIENTE P2P BASADO EN SIP
CLIENTE DE ENLACE D2D
P2P GO

FIG. 2

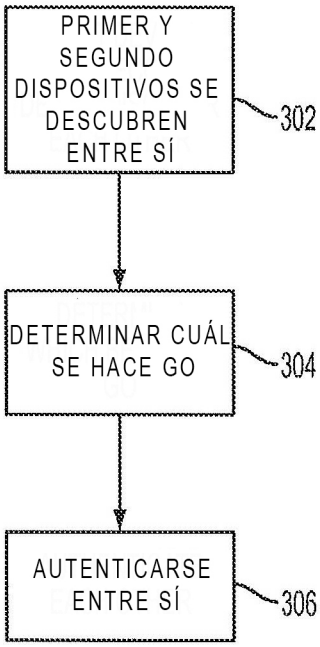
PRIMER Y SEGUNDO DISPOSITIVOS SE DESCUBREN ENTRE SÍ
302
DETERMINAR CUÁL SE HACE GO
304
AUTENTICARSE ENTRE SÍ
306

FIG. 3

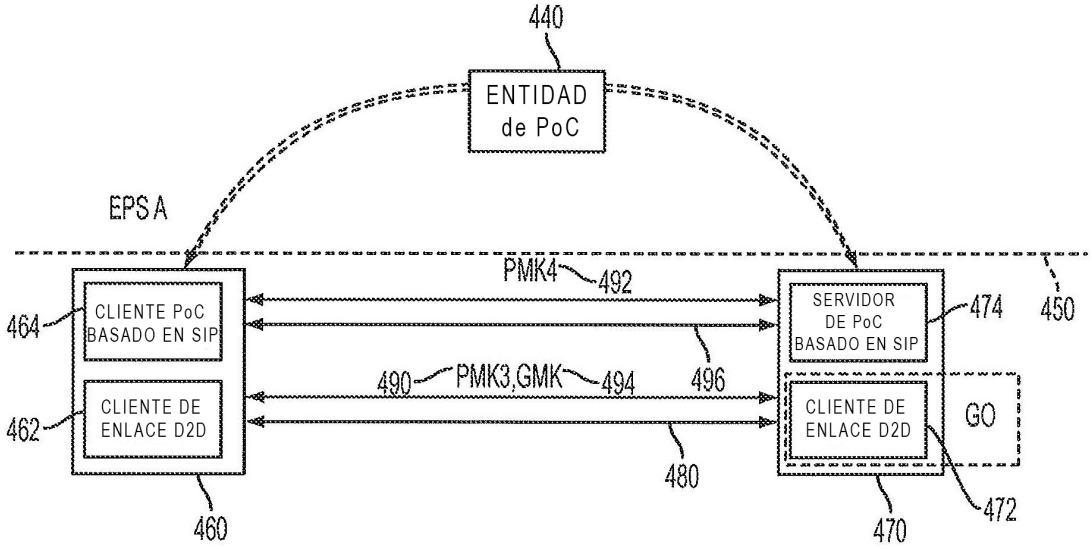
440
ENTIDAD de PoC
EPS A
PMK4
492
450
464
CLIENTE PoC BASADO EN SIP
SERVIDOR DE PoC BASADO EN SIP
474
490
PMK3,GMK
494
496
462
CLIENTE DE ENLACE D2D
GO
480
460
470
472

FIG. 4

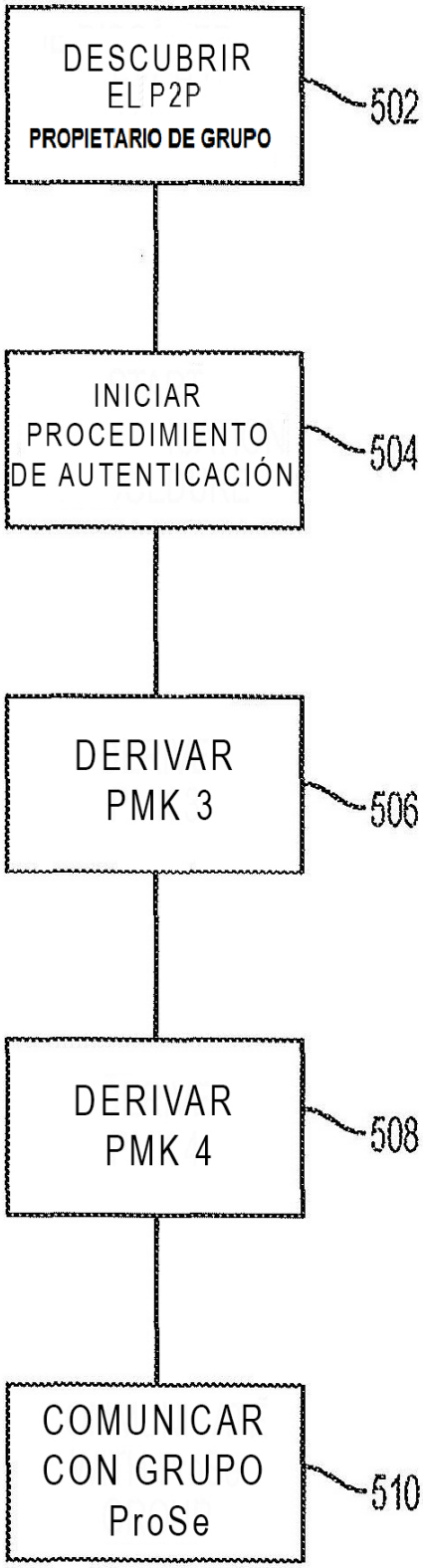
DESCUBRIR
EL P2P
PROPIETARIO DE GRUPO
502
INICIAR
PROCEDIMIENTO
DE AUTENTICACIÓN
504
DERIVAR
PMK 3
506
DERIVAR
PMK 4
508
COMUNICAR
CON GRUPO
ProSe
510

FIG. 5

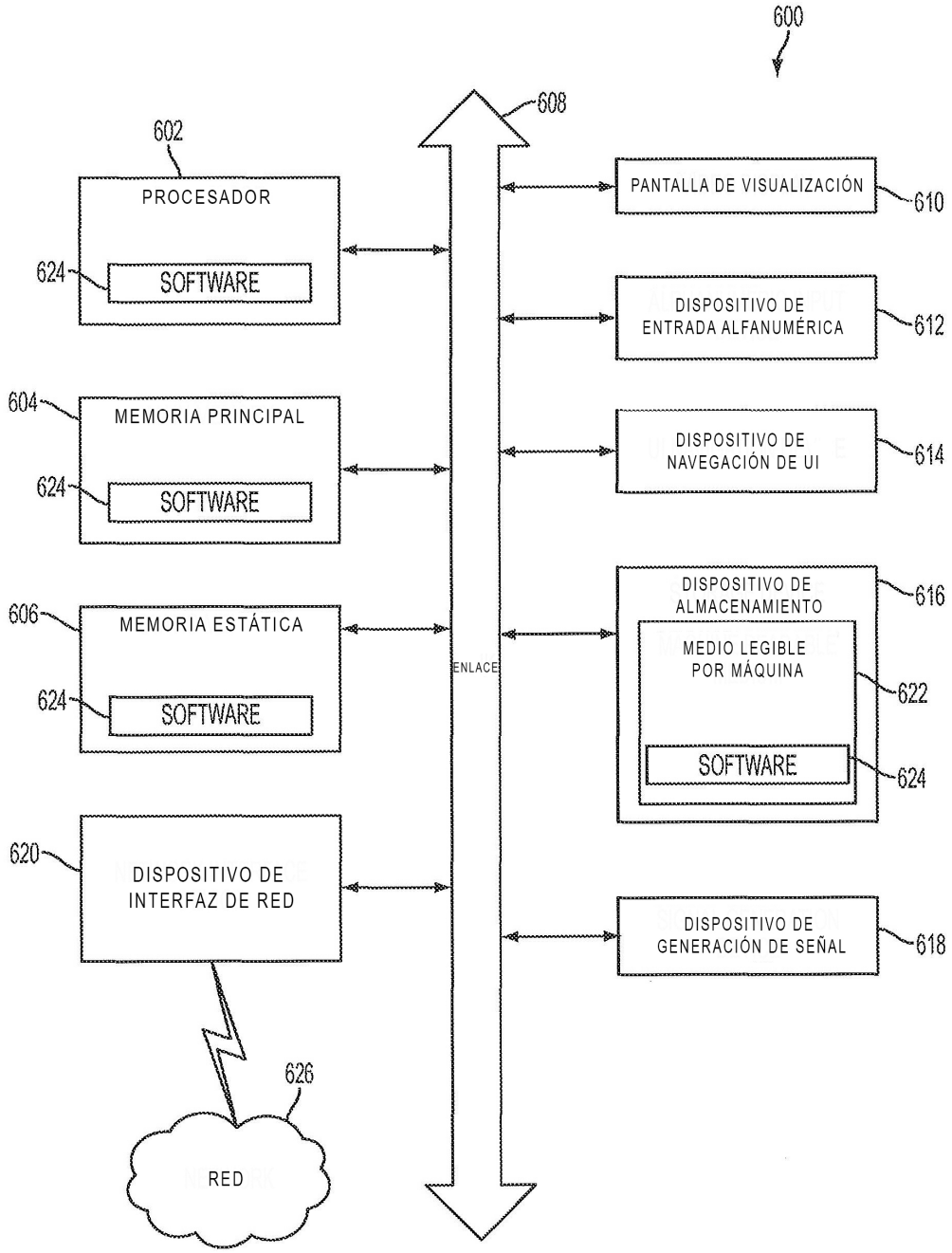
600
608
602
PROCESADOR
624
SOFTWARE
604
MEMORIA PRINCIPAL
624
SOFTWARE
606
MEMORIA ESTÁTICA
624
SOFTWARE
620
DISPOSITIVO DE INTERFAZ DE RED
626
RED
ENLACE
PANTALLA DE VISUALIZACIÓN
610
DISPOSITIVO DE ENTRADA ALFANUMÉRICA
612
DISPOSITIVO DE NAVEGACIÓN DE UI
614
DISPOSITIVO DE ALMACENAMIENTO
616
MEDIO LEGIBLE POR MÁQUINA
622
SOFTWARE
624
DISPOSITIVO DE GENERACIÓN DE SEÑAL
618

FIG. 6