(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 734 989**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **18.04.2013 PCT/US2013/037108**

(87) Fecha y número de publicación internacional: **07.11.2013 WO13165695**

(96) Fecha de presentación y número de la solicitud europea: **18.04.2013 E 13721830 (1)**

(97) Fecha y número de publicación de la concesión europea: **05.06.2019 EP 2845362**

(54) Título: **Comunicaciones seguras para dispositivos informáticos que utilizan servicios de proximidad**

(30) Prioridad:

30.04.2012 US 201213460035

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.12.2019

(73) Titular/es:

ALCATEL LUCENT (100.0%)
Site Nokia Paris Saclay, Route de Villejust
91620 Nozay, FR

(72) Inventor/es:

BROUSTIS, IOANNIS y
CAKULEV, VIOLETA

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Comunicaciones seguras para dispositivos informáticos que utilizan servicios de proximidad

Campo

El campo se refiere a la seguridad de comunicación asociada con dispositivos informáticos que utilizan servicios de proximidad.

Antecedentes de la invención

El diseño de redes de comunicación de banda ancha tradicionales se ha enfocado en permitir servicios de comunicación entre los usuarios, de modo que el tráfico de usuario siempre atraviese la infraestructura nuclear de la red (es decir, el núcleo de la red o CN). Véase, por ejemplo, 3GPP TS 23.401, Proyecto de Asociación para la Tercera Generación, Grupo de Especificación Técnica de Aspectos de Servicios y Sistemas; mejoras del Servicio General de Paquetes de Radio (GPRS) para el acceso a la Red de Acceso Terrestre por Radio Universal Evolucionada (E-UTRAN) (Edición 11).

Dicho planteamiento de diseño ofrece algunos beneficios de gestión de los usuarios a los operadores de la red, tales como la capacidad para autenticar al equipo de usuario (UE) y para seguir el comportamiento del usuario en términos de utilización de recursos (por ejemplo, tales como el consumo de ancho de banda en la interfaz por aire y cantidad de tráfico de datos subidos/descargados a lo largo del tiempo).

Además forzar al tráfico a atravesar el núcleo de la red de banda ancha permite el soporte de la Intercepción Legal (LI) de datos y/o de llamadas de voz por las autoridades legales. Esto es debido a que el CN tiene acceso explícito al tráfico del usuario (dado que dicho tráfico va a través del núcleo) y por ello puede proporcionar mecanismos a las entidades de LI para obtener el tráfico intercambiado entre usuarios específicos, bajo demanda. Véase, por ejemplo 3GPP TS 33.107, Proyecto de Asociación para la Tercera Generación; Grupo de Especificación Técnica de Aspectos de Servicios y Sistemas; Seguridad 3G; arquitectura y funciones de Intercepción Legal (Edición 11); y 3GPP TS 33.108, Proyecto de Asociación para la Tercera Generación; Grupo de Especificación Técnica de Aspectos de Servicios y Sistemas; Seguridad 3G; interfaz de Traspaso para Intercepción Legal (LI) (Edición 11).

Sumario

Realizaciones de la invención proporcionan técnicas para establecer comunicaciones seguras entre dispositivos informáticos que utilizan servicios de proximidad en un sistema de comunicación.

La invención se divulga mediante métodos para proporcionar comunicaciones seguras en un sistema de comunicaciones de acuerdo con las reivindicaciones 1 y 9 y aparatos correspondientes de acuerdo con las reivindicaciones 8 y 10, las realizaciones adicionales se definen en las reivindicaciones dependientes.

Ventajosamente, técnicas de la invención proporcionan comunicaciones seguras entre dispositivos de proximidad (es decir, dispositivos informáticos que utilizan servicios de proximidad) en un sistema de comunicaciones.

Estos y otros objetivos, características y ventajas de la presente invención se harán evidentes a partir de la descripción detallada que sigue de realizaciones ilustrativas de la misma, que ha de leerse en conexión con los dibujos adjuntos.

La solicitud de patente US 2011/170694 divulga gestión de claves jerárquica para comunicaciones seguras en un sistema de comunicaciones multimedia.

La solicitud de patente US 2011/0055567 divulga gestión de claves seguras en un sistema de comunicaciones multimedia.

La patente de Estados Unidos 6.137.885 divulga un método para permitir la comunicación encriptada directa entre dos terminales de la red de radio móvil e instalaciones de estación y terminal correspondientes.

Breve descripción de los dibujos

La FIG. 1A ilustra el paso de tráfico en el plano de usuario en un sistema de comunicaciones de banda ancha en un escenario de base tradicional.
La FIG. 1B ilustra el paso de tráfico en el plano de usuario en un sistema de comunicaciones de banda ancha en un escenario basado en servicios de proximidad.
La FIG. 2A ilustra un protocolo de deducción y distribución de claves basado en servicios de proximidad, de acuerdo con una realización de la invención.
La FIG. 2B ilustra un protocolo de deducción y distribución de claves basado en servicios de proximidad, de

acuerdo con otra realización de la invención.
La FIG. 3 ilustra una metodología de comunicaciones seguras basadas en servicios de proximidad de acuerdo con la presencia de operaciones de intercepción legal, de acuerdo con una realización de la invención.
La FIG. 4 ilustra una arquitectura de hardware de una parte de un sistema de comunicaciones y dispositivos informáticos adecuados para implementar una o más de las metodologías y protocolos de acuerdo con una o más realizaciones de la invención.

Descripción detallada

Se describirán a continuación realizaciones de la invención en el contexto de protocolos de comunicaciones ilustrativos. Sin embargo, ha de apreciarse que las realizaciones de la invención no están limitadas a ningún protocolo de comunicaciones particular. Por el contrario, las realizaciones de la invención son aplicables a cualquier entorno de comunicación adecuado en el que sea deseable proporcionar comunicaciones seguras entre dispositivos informáticos que utilizan servicios de proximidad.

El término “clave” tal como se usa en el presente documento se define en general como una entrada a un protocolo criptográfico, para finalidades tales como, pero sin limitación, autenticación de la entidad, privacidad, integridad del mensaje, etc.

La expresión “asociación de seguridad” tal como se usa en el presente documento se refiere en general a una definición de seguridad en un entorno de comunicación a través del que comunican dos o más partes y/o dispositivos. En un ejemplo, la definición de seguridad puede incluir, pero sin limitación, una clave de sesión.

La expresión “servicios de proximidad” tal como se usa en el presente documento se define en general como descubrimiento y comunicaciones controladas en la red entre dispositivos informáticos que están en proximidad entre sí de modo que el tráfico de usuario fluya entre los dispositivos en lugar de a través de la red. Estar en una proximidad entre sí se refiere en general a los dispositivos que están a una distancia de alcance entre sí dentro de la que es posible la comunicación entre los dispositivos (es decir, dentro del alcance de cobertura del otro) sin que las comunicaciones vayan a través de la red.

Se ha comprendido que forzar el tráfico de usuario a pasar siempre a través del CN, en un planteamiento de base tradicional, introduce limitaciones y sobrecargas significativas en ciertos escenarios de despliegue. La FIG. 1A ilustra el paso del tráfico en el plano de usuario en un sistema de comunicaciones de banda ancha en dicho escenario de base tradicional. El sistema de comunicación de banda ancha representado en la figura es una red de la Evolución a Largo Término (LTE). Como es conocido, LTE es una red de la Cuarta Generación (4G) desplegada por el Proyecto de Asociación para la Tercera Generación (3GPP).

Consideremos el caso en el que dos dispositivos de abonado de la misma red de la Evolución a Largo Término (LTE) 100, concretamente Alicia 102-A y Bob 102-B, que están adscritos a la misma estación base eNB (e-NodoB) 104, desean establecer una sesión de comunicación de datos de modo que puedan iniciar una llamada de vídeo a través de la red LTE. Obsérvese que los números de referencia 102-A y 102-B pueden referirse alternativamente en el presente documento a dispositivos, dispositivos informáticos, dispositivos de comunicación, dispositivos de abonado, dispositivos de usuario final, equipos de usuario (UE) y similares. A modo de ejemplo solamente, los dispositivos 102-A y 102-B pueden ser dispositivos de usuario final móviles tales como, pero sin limitación, teléfonos celulares, ordenadores portátiles, tabletas y similares.

En una configuración LTE tradicional, los paquetes para Alicia (dispositivos 102-A) y los paquetes para Bob (dispositivo 102-B) se intercambiarían a través del núcleo de la red (CN) LTE 105, es decir atravesarían la pasarela en servicio (SGW) 106 y la pasarela de la red de datos en paquetes (PDN) (PGW) 108, como se muestra en la FIG. 1A. Obsérvese que mientras que Alicia (dispositivo 102-A) y Bob (dispositivo 102-B) están dentro del alcance de transmisión del otro, los paquetes de Alicia viajan a través del eNB 104 (normalmente hasta la PGW 108) y desde ahí vuelven al mismo eNB 104 y se entregan a Bob. Dado que pueden tener lugar simultáneamente una multiplicidad de dichas comunicaciones (entre usuarios vecinos), forzar a que dicho tráfico pase a través del núcleo incrementa la utilización tanto de las entidades de la red de acceso por radio (RAN) (por ejemplo, eNB) como las entidades del CN (por ejemplo, SGW y PGW) y consume adicionalmente excesivas cantidades tanto de enlace como de ancho de banda inalámbrico.

Para escenarios de despliegue en donde Alicia (dispositivo 102-A) y Bob (dispositivo 102-B) son “vecinos” (es decir, dentro del alcance de cobertura del otro), los servicios de proximidad (ProSe), tales como los descritos en 3GPP TR 22.803, Proyecto de Asociación para la Tercera Generación; Grupo de Especificación Técnica SA; Estudio de Factibilidad para Servicios de Proximidad (ProSe) (Edición 12), incrementan la capacidad del canal para permitir el establecimiento de sesiones de tráfico de dispositivo a dispositivo (D2D) directa e intercambio de datos entre Alicia y Bob (o incluso entre un grupo de más de dos usuarios). La FIG. 1B ilustra el paso del tráfico en el plano de usuario en una red LTE 100 en un escenario basado en servicios de proximidad. Obsérvese que los dispositivos 102-A y 102-B también se denominan como “dispositivos de proximidad” cuando se conectan en funciones basadas en servicios de proximidad (ProSe).

Como se puede observar con ProSe, Alicia (dispositivo 102-A) envía paquetes directamente a Bob (dispositivo 102-B) a través de la interfaz por aire, sin necesidad de implicar ni la RAN ni la infraestructura del CN. Esto ofrece dos ventajas principales: (i) descarga la red en términos de operaciones de gestión de tráfico de datos y (ii) puede incrementar el rendimiento del usuario final cuando el enlace de datos directos entre Alicia y Bob sostiene una relación de entrega de paquetes (PDR) más alta que los enlaces Alicia-eNB y/o Bob-eNB. ProSe permite por tanto aplicaciones de Internet móvil a alta velocidad tales como, pero sin limitación, flujo de vídeo en tiempo real y juegos en línea.

Sin embargo, se comprueba que las comunicaciones ProSe introducen algunas consideraciones de seguridad críticas, que no existen con los despliegues en la red de banda ancha tradicionales;

i. En las configuraciones tradicionales, la red celular realiza autenticación mutua con Alicia (dispositivo 102-A) y Bob (dispositivo 102-B) individualmente y establece adicionalmente credenciales de seguridad separadas, únicas (es decir claves de sesión) con cada uno de ellos. Véase, por ejemplo 3GPP TS 33.102, Proyecto de Asociación para la Tercera Generación; Grupo de Especificación Técnica de Aspectos de Servicios y Sistemas; Seguridad 3G; Arquitectura de Seguridad (Edición 11); y 3GPP TS 33.401, Proyecto de Asociación para la Tercera Generación; Grupo de Especificación Técnica de Aspectos de Servicios y Sistemas; Evolución de la Arquitectura del Sistema 3GPP (SAE); arquitectura de Seguridad (edición 11), cuyas divulgaciones se incorporan por referencia en el presente documento en sus totalidades. Las claves establecidas se usan para proteger la señalización de control (por ejemplo, señalización en el estrato no de acceso (NAS)) y pueden usarse opcionalmente para proteger el tráfico a través de la interfaz por aire, entre el eNB y cada UE. Dado que las credenciales de seguridad establecidas son separadas y únicas Alicia y Bob no conocen las claves de sesión del otro. Sin embargo, como se ha indicado anteriormente con ProSe, Alicia y Bob comunican directamente y no a través de la red. Por lo tanto, se comprueba que se necesita un método con el que la comunicación directa entre Alicia y Bob sea segura usando claves de sesión que sean conocidas tanto para Alicia como para Bob. De lo contrario, Alicia y Bob no pueden realizar operaciones criptográficas tales como cifrado y descifrado de sus paquetes de datos intercambiados.

ii. Las normas de red 3G y 4G (véase, por ejemplo 3GPP TS 33.102 y 3GPP TS 33.401, como se ha citado anteriormente) especifican funciones con las que la RAN puede verificar el origen (UE adscrito) del tráfico de enlace ascendente, a través del uso de claves de sesión establecidas durante la autenticación entre el UE y la red. Con esto, la red puede asegurarse de que solo los UE autenticados están autorizados a usar el ancho de banda inalámbrico acreditado. Sin embargo con ProSe, el tráfico en el plano de usuario (UP) fluye a través del enlace inalámbrico directo entre los UE. En consecuencia, aunque cada UE puede autenticarse aún por la red, esta última no tiene forma de determinar si los UE que se conectan en comunicaciones ProSe están realmente autorizados para hacerlo. Esto es debido a que con ProSe, la red no puede seguir explícitamente el tráfico de usuario dado que el tráfico no fluye a través de la RAN o entidades del núcleo.

iii. Llevando más allá la observación anterior, dado que con ProSe, Alicia (dispositivo 102-A) y Bob (dispositivo 102-B) intercambian directamente tráfico, la red es ahora incapaz de realizar funcionalidades que permitan la intercepción legal (LI). Sin embargo, como se ha explicado anteriormente, este no es un problema con las redes 3G y 4G tradicionales, dado que el tráfico de usuario atraviesa el CN, permitiendo de ese modo las interfaces apropiadas para finalidades de LI. Por lo tanto, dado que las comunicaciones ProSe están sometidas a LI, se comprueba que es necesario un mecanismo de modo que sea factible la LI en configuraciones ProSe.

En consecuencia, una o más de las realizaciones de la invención proporcionan servicios de proximidad seguros. En una realización ilustrativa, se proporciona una metodología ProSe segura (SeProSe) que establece asociaciones de seguridad entre los UE con capacidad ProSe (dispositivos informáticos tales como Alicia y Bob a los que se ha hecho referencia anteriormente) de forma tal que acomete los problemas de seguridad anteriores y otros. La metodología proporciona las siguientes funciones:

a. Autorización y establecimiento de seguridad ProSe para enlaces ProSe. Con SeProSe, cada UE realiza autenticación y acuerdo de claves con la red de acceso en la misma forma que ya se ha especificado. Más aún, siempre que Alicia (dispositivo 102-A) desea establecer un enlace ProSe con su vecino Bob (dispositivo 102-B) la red asociada verifica que Alicia y Bob están autorizados por ProSe y, si lo están, entonces la red suministra con seguridad una clave secreta común tanto a Alicia como a Bob. Llamamos a esta clave “PK”. El suministro seguro de esta clave hace uso del material clave que es esencial durante la autenticación precedente y el procedimiento de acuerdo de claves entre cada UE y su red afiliada. Alicia y Bob usan esta clave común para asegurar su comunicación directa. Obsérvese que cada usuario recibe la clave común de forma encriptada por la red de adscripción (y autenticada). Por ello, Alicia está segura de que Bob ha sido también autenticado por su red afiliada y autorizado a usar ProSe, dado que está en posesión de la misma clave PK.

b. Verificación y supervisión de usuario. El uso de PK proporciona la forma para que la red verifique que el UE con capacidad ProSe está autorizado a hacer uso del espectro inalámbrico acreditado. Sin embargo, para que la red sea capaz de realizar dicha verificación, el tráfico en el UP (plano de usuario o directo) del UE debe ser alcanzable por la red. SeProSe incluye un mecanismo según el que los UE con capacidad ProSe transmiten el tráfico usando un nivel de potencia de transmisión y una tasa de bits de la capa física (PHY) tales que la red asociada pueda escuchar con éxito el tráfico ProSe. Obsérvese que dicho modo de transmisión permite

claramente el soporte de LI, dado que la red tiene ahora la capacidad para acceder a los datos intercambiados directamente entre los UE. Obsérvese que en los escenarios de despliegue en los que no es necesario el soporte de LI, no se necesita usar este mecanismo.

Aunque realizaciones alternativas de la invención no están limitadas a la misma, el siguiente conjunto de suposiciones se realiza de acuerdo con las realizaciones ilustrativas a ser descritas a continuación. Obsérvese también que dichas suposiciones definen un modelo de riesgo. Se supone que:

i. Cada UE con capacidad ProSe tiene la posibilidad de mantener trayectorias de tráfico separadas con al menos una estación base en todo momento (por ejemplo, el eNodoB para el caso de LTE). Cada UE tiene la capacidad de ajustar su potencia de transmisión y la tasa de bits PHY para compensar la interferencia inalámbrica.
ii. Previamente al inicio del tráfico ProSe, los UE están dentro del alcance de cobertura de al menos una estación base operada por el proveedor de servicios de red con el que están asociados. Cada UE con capacidad ProSe puede adscribirse a una estación base diferente.
iii. Las infraestructuras de redes de banda ancha asociadas (RAN y CN) no están comprometidas en términos de cálculo, almacenamiento y suministro de credenciales secretas con seguridad, tales como claves permanentes y de sesión. De modo similar, los UE no están comprometidos en términos de cálculo, deducción o divulgación de credenciales secretas permanentes o temporales.
iv. Un UE que se ha autenticado mutuamente con una red y ha deducido/obtenido material clave basándose en dicha autenticación y proceso de acuerdo de claves, confía que cualquier información de seguridad enviada al UE por la red es auténtica y verdadera. De modo similar, en tal caso, la red confía que el UE autenticado siempre envía información relacionada con ProSe precisa y verdadera a la red.

De acuerdo con realizaciones ilustrativas, se describirán a continuación protocolos y metodologías para deducir y distribuir el contexto de seguridad ProSe, seguido por una descripción de cómo está soportada la Intercepción Legal (LI) cuando los UE funcionan en el modo ProSe.

Se debe apreciar que aunque las realizaciones ilustrativas descritas en el presente documento se enfocan en el caso en el que tienen lugar comunicaciones ProSe en el contexto de LTE (es decir, se supone que la infraestructura de la red de soporte se basa en LTE), muchas de las funcionalidades de SeProSe son aplicables a otros tipos de redes tales como, pero sin limitación, el Sistema Universal de Telecomunicaciones Móviles (UMTS) y Paquetes de Radio a Alta Velocidad (HRPD).

Las realizaciones ilustrativas de la invención proporcionan una solución que asegura que la comunicación directa entre dos UE con capacidad ProSe es segura. Esto incluye métodos para: (i) generar y distribuir claves de sesión usadas para asegurar la comunicación directa entre dos UE con capacidad ProSe; y (ii) verificación de que ambos UE con capacidad ProSe implicados en comunicaciones ProSe están autenticados por sus redes respectivas y autorizados para el uso de ProSe.

Consideremos un escenario en el que dos abonados a la misma red LTE, concretamente Alicia y Bob (dispositivos 102-A y 102-B, respectivamente, tal como se muestra en las FIGS. 1A y 1B), desean establecer una comunicación ProSe. Como en las configuraciones tradicionales, en algún punto previo a la comunicación ProSe, la red celular ha realizado autenticación mutua con Alicia y con Bob individualmente y establecido credenciales de seguridad separadas, únicas (por ejemplo, claves de sesión) con cada uno de ellos. Posteriormente, usando las características de descubrimiento ProSe, Alicia descubre que Bob está en su proximidad y desea establecer comunicación ProSe con él. Para establecer la comunicación ProSe el UE de Alicia envía una solicitud a la red de acceso por radio (RAN) indicando que desea establecer comunicación ProSe con Bob. Tras verificar que Alicia es un abonado autenticado, la red RAN de Alicia verifica que Alicia está autorizada para servicios ProSe. Si ambas verificaciones tienen éxito, la red RAN verifica adicionalmente que Bob es un usuario autenticado autorizado para comunicación ProSe. Si este es el caso, la RAN deduce la clave de sesión PK usando el contexto de seguridad de Alicia (es decir, K_{Alicia}) como sigue:

$$PK = KDF(K_{Alicia}, S),$$

en la que S es una cadena construida usando parámetros de entrada predeterminados y KDF es una Función de Deducción de Clave (véase, por ejemplo SHA-256, Standards for Efficient Cryptography Group, "Secure Hash Standard", Federal Information Processing Standards Publication 180-2, agosto de 2002, con la nota de cambio 1, febrero de 2004). Una vez la RAN deduce la PK, la envía con seguridad a Alicia y a Bob.

La FIG. 2A ilustra un protocolo de deducción y distribución de clave basado en servicios de proximidad, de acuerdo con una realización de la invención. En particular, la FIG. 2A representa el caso en el que los UE con capacidad ProSe están adscritos al mismo eNB. Esto es, tal como se muestra, Alicia (dispositivo 102-A) y Bob (dispositivo 102-B) están en el alcance de cobertura del mismo eNB 104.

Como se ha descrito anteriormente, Alicia y Bob son usuarios autenticados de una red del operador. Dichas operaciones de autenticación se representan como 210-A y 210-B en la FIG. 2A. Además, en el ejemplo de la FIG.

2A, Alicia y Bob están en el alcance de cobertura del mismo eNB (es decir están adscritos al mismo eNB). El descubrimiento ProSe se realiza en la etapa 212.

Con SeProSe (ProSe seguro), una vez que Alicia y Bob reciben un anuncio de que están dentro del alcance relativo entre ellos (representado como las etapas 214 y 216 en la FIG. 2A), Alicia determina si desea iniciar una comunicación ProSe con Bob. Si es este el caso, Alicia (dispositivo 102-A) envía una solicitud ProSe (en la etapa 218 de la FIG. 2A) al eNB 104 indicando que desea iniciar la comunicación ProSe con Bob (dispositivo 102-B). El eNB adscrito verifica (en la etapa 220 de la FIG. 2A) que tanto Alicia como Bob están autenticados y autorizados para usar ProSe.

Para que Alicia y Bob se impliquen en una comunicación ProSe, necesitan estar primero autenticados (por ejemplo, según el procedimiento AKA (Autenticación y Acuerdo de Claves) en el caso de LTE, véase 3GPP TS 33.102, Proyecto de Asociación para la Tercera Generación; Grupo de Especificación Técnica de Aspectos de Servicios y Sistemas; Seguridad 3G; Arquitectura de Seguridad (Edición 11); y 3GPP TS 33.401, Proyecto de Asociación para la Tercera Generación; Grupo de Especificación Técnica de Aspectos de Servicios y Sistemas; Evolución de la Arquitectura de Sistemas (SAE) 3GPP; Arquitectura de Seguridad (Edición 11)). La autenticación entre Alicia y la red se representa como la etapa 210-A y la autenticación entre Bob y la red se representa como la etapa 210-B en la FIG. 2A. Obsérvese que una entidad de gestión de la movilidad (MME) 202 en la RAN se usa para ayudar con la autenticación.

Tras la autenticación exitosa, el eNB 104 mantiene un contexto de seguridad activo para cada UE adscrito y por ello, tras la recepción de una solicitud ProSe enviada por Alicia (etapa 218), el eNB 104 puede determinar si ya está autenticada examinando el contexto de seguridad (que se mantiene localmente en el eNB) del servidor de autenticación (AS no expresamente mostrado) correspondiente. Obsérvese que, usando material clave de este contexto de seguridad, Alicia puede cifrar y/o proteger la integridad de la solicitud ProSe, por ejemplo, o bien usando su clave K_{RRCint}/K_{RRCenc} si la solicitud ProSe es un mensaje del control de recursos de radio (RRC) o la clave K_{UPint}/K_{UPenc} si es un mensaje en el plano de usuario (UP), o K_{NASint}/K_{NASenc} si es un mensaje NAS (estrato no de acceso). En este último caso, la autenticidad de la solicitud ProSe se verifica por el MME 202 en la RAN usando la solicitud de seguridad NAS correspondiente (válida), que se mantiene localmente en el MME 202.

Tras la verificación de que Alicia y Bob están autenticados, el eNB 104 determina si están autorizados para implicarse en una comunicación ProSe. La verificación de la autorización puede realizarse usando información de autorización que se mantiene localmente en el eNB 104 (en la etapa 220). Dicha información puede obtenerse proactivamente por el eNB tras el registro del UE con éxito con la red, junto con otros parámetros de registro.

Si la verificación tiene éxito, el eNB 104 genera la PK (en la etapa 222 de la FIG. 2A) como se ha definido anteriormente. K_{Alicia} en el cálculo de PK puede ser: (i) cualquiera de las otras claves mantenidas por el eNB (por ejemplo, K_{eNB}, K_{RRCenc}, K_{RRCint}, K_{UPenc}, K_{UPint}); (ii) combinación de dos o más claves; (iii) un valor aleatoriamente deducido; o (iv) una clave ProSe (K_{ProSe}) deducida y proporcionada por el MME al eNB tras la autenticación con éxito del UE autorizado para ProSe. Posteriormente, el eNB 104 envía la PK a Alicia y Bob (en las etapas 226 y 228, respectivamente, en la FIG. 2A). Para asegurar la comunicación RRC segura entre eNB-Alicia y eNB-Bob, se usa el contexto de seguridad deducido de la autenticación con éxito (es decir, K_{RRCint}, y K_{RRCenc}). En este instante, Alicia y Bob pueden comenzar la comunicación ProSe, que se asegura usando PK.

Obsérvese que al recibir la PK, Alicia y Bob se aseguran de que la otra parte está autorizada a usar ProSe, es decir, el eNB envía la PK a Alicia y Bob solamente después de la verificación de que ambos están autorizados a implicarse en una comunicación ProSe. Por ello, la recepción de la PK sirve como prueba para Alicia de que Bob está también autorizado.

Obsérvese que mediante la verificación mutua de la posesión de la PK, Alicia y Bob se aseguran de que están en comunicación entre sí.

Alicia y Bob pueden usar la PK para asegurar su comunicación ProSe, o deducciones de clave de PK para una seguridad y autorización ProSe de grano fino. Recuérdese que la PK se usa solamente para asegurar que el tráfico se intercambia directamente entre Alicia y Bob. Cualquier comunicación entre Alicia-eNB y Bob-eNB se protege (opcionalmente) usando el contexto de seguridad AS correspondiente a cada UE. La clave PK puede usarse para asegurar la comunicación ProSe entre Alicia y Bob en una o más de las siguientes formas ilustrativas:

a. Uso de clave única para todo el tráfico ProSe. Con esta opción, Alicia y Bob usan la PK directamente para cifrar y/o proteger la integridad del tráfico que fluye en su enlace de comunicación directo.
b. El uso de claves separadas deducidas para cifrado y protección de integridad. El SeProSe proporciona la capacidad de que Alicia y Bob usen la PK para deducir claves separadas para el cifrado (PK_{enc}) y protección de integridad (PK_{int}). Para ello, pueden usarse dos KDF diferentes tal como sigue:

$$PK_{enc} = KDF_1(PK, S),$$

y

$$PK_{int} = KDF_2(PK, S),$$

en la que S es una cadena construida usando parámetros de entrada predeterminados. De hecho, cada UE puede deducir PK_{enc} y PK_{int} mediante la utilización de funciones de deducción de clave que ya están implementadas y usadas para deducción de otras claves, tales como K_{RRCenc}, K_{RRCint}, K_{UPint} y K_{UPenc}.

c. Usar deducciones de claves específicas de la aplicación ProSe. Cuando los UE se aprovisionan con más de una aplicación ProSe, el operador puede desear realizar una autorización específica de la aplicación para acceder a servicios de proximidad. Por ejemplo, puede permitirse que Alicia acceda a ProSe solamente para aplicaciones específicas (es decir, Alicia puede no estar autorizada para acceder a ProSe para todas las aplicaciones). En dicho caso, suponiendo que el UE con capacidad ProSe puede restringir fiablemente el uso de claves de aplicación a las aplicaciones correspondientes, el SeProSe permite la deducción y uso de claves específicas de la aplicación usando PK. Más específicamente, el eNB envía la PK a cada UE con capacidad ProSe, junto con una lista de aplicaciones que el UE está autorizado a usar. Cada UE puede usar la PK para deducir una clave específica de la aplicación PK_A, usando la fórmula siguiente:

$$PK_A = KDF(PK, S),$$

en la que S es una cadena construida usando parámetros de entrada predeterminados, incluyendo potencialmente el identificador de aplicación particular. Obsérvese que, alternativamente, el eNB puede deducir una PK por aplicación ProSe y enviarla a cada UE. En otras palabras, en lugar de una única PK, pueden enviarse múltiples claves PK (una por aplicación) a cada UE.

d. Uso híbrido de PK. El SeProSe también permite la deducción de claves para cifrado y protección de integridad por aplicación ProSe tal como sigue:

$$PK_{Aenc} = KDF_1(PK_A, S),$$

y

$$PK_{Aint} = KDF_2(PK_A, S).$$

La FIG. 2B ilustra un protocolo de deducción y distribución de claves basado en servicios de proximidad, de acuerdo con otra realización de la invención. En particular, la FIG. 2B representa un caso en el que los UE con capacidad ProSe se adscriben a diferentes eNB. Esto es, tal como se muestra, Alicia (dispositivo 102-A) y Bob (dispositivo 102-B) están dentro de la cobertura de dos eNB diferentes 104-1 y 104-2. De modo similar al escenario representado en la FIG. 2A, en este escenario, Alicia y Bob son usuarios autenticados de una red del operador. Sin embargo, en este caso Alicia y Bob están en el alcance de cobertura de dos eNB diferentes. Obsérvese que se usan los mismos números de referencia en la FIG. 2B que los usados en la FIG. 2A para las etapas/operaciones que son las mismas o sustancialmente similares. Se añaden nuevos números de referencia para indicar etapas adicionales y/o un cambio en el orden de las etapas.

Así, una vez que Alicia y Bob reciben los anuncios de que están dentro del alcance del otro (etapas 214 y 216), Alicia determina si desea iniciar una comunicación ProSe con Bob. En dicho caso, Alicia envía (etapa 218) una solicitud ProSe al eNB1 (104-1) indicando que desea iniciar la comunicación ProSe con Bob. El eNB1 determina (etapa 220) si Alicia está autenticada y autorizada a usar ProSe, tal como se ha descrito anteriormente. Si la verificación tiene éxito, el eNB1 genera la PK (etapa 222) tal como se ha descrito anteriormente.

Posteriormente, en la etapa 224, el eNB1 (104-1) envía la PK al eNB2 (104-2) sobre la interfaz X2, junto con la identidad de Alicia y Bob. Una vez que el eNB2 recibe este mensaje, se asegura implícitamente que Alicia ha sido autenticada por el eNB1. Adicionalmente, el eNB2 determina (etapa 220) si Bob está autenticado y autorizado a usar ProSe. Si la verificación tiene éxito, el eNB2 realiza lo siguiente:

a. El eNB2, en la etapa 230, envía con seguridad la PK (que se ha deducido y enviado por el eNB1) a Bob usando un contexto de seguridad válido deducido de la autenticación con éxito.
b. El eNB2, en la etapa 232, responde al eNB1 con un mensaje verificando que Bob está también autenticado y autorizado para ProSe.

Tras la recepción de la respuesta del eNB2 sobre la interfaz X2, el eNB1 se asegura de que Bob está también autenticado y por ello, el eNB1 suministra adicionalmente (con seguridad) la PK a Alicia (en la etapa 234).

En este punto, Alicia y Bob pueden comenzar la comunicación ProSe segura usando la PK. Lo mismo que en el caso de un único eNB, al recibir la PK, Alicia y Bob se aseguran de que la otra parte está autorizada a usar ProSe, mientras se prueben entre ellos que están en posesión de la PK, Alicia y Bob se aseguran de que están en comunicación entre sí. Similarmente en este caso, la PK puede usarse por Alicia y Bob o bien como una clave única usada para cifrado y protección de integridad del tráfico ProSe directo o puede usarse para deducción de claves

adicionales, como se ha descrito anteriormente.

Obsérvese que las descripciones ilustrativas anteriores se han enfocado sobre escenarios que implican dos UE con capacidad ProSe. Claramente sin embargo, los procedimientos descritos son aplicables directamente a casos en los que más de dos UE con capacidad ProSe desean implicarse en una comunicación en grupo. En dicho caso, todos los miembros del grupo recibirán la misma PK desde su eNB de adscripción. De nuevo, en dicho caso, la posesión de la PK implícitamente autentica a un UE para todos los otros miembros del grupo y también permite que todos los otros miembros del grupo verifiquen que un UE particular está autorizado a participar en la comunicación ProSe en grupo.

Adicionalmente, los protocolos y metodologías de seguridad descritos en el presente documento pueden estar en escenarios en los que los UE con capacidad ProSe se asocian con diferentes dominios de la Red Móvil Terrestre Pública (PLMN). En particular, supóngase que Alicia (dispositivo 102-A) y Bob (dispositivo 102-B) están dentro de la cobertura de dos eNB diferentes que pertenecen a dos dominios PLMN diferentes. Se ha de entender que los métodos descritos anteriormente son aplicables en este escenario siempre que haya una forma de comunicación (por ejemplo, la interfaz X2 o a través de la MME) entre los eNB que pertenecen a estos dos dominios PLMN.

Se comprueba adicionalmente que cuando los UE con capacidad ProSe comunican entre sí, pueden ajustar sus parámetros de transmisión basándose en sus características del canal. Como un ejemplo, si dos de dichos UE, digamos Alicia y Bob, están en cercanía entre sí, entonces Alicia puede usar una alta velocidad de bits PHY y una baja potencia de transmisión para enviar el tráfico a Bob. Con dichos parámetros de transmisión, sin embargo, las señales de Alicia pueden ser suficientemente débiles de modo que el eNB asociado no pueda decodificarlas con éxito. Como resultado, el eNB puede no ser capaz de seguir a Alicia y a Bob. Más aún, la intercepción legal (LI) es un desafío en dichos casos.

Para realizar el seguimiento del usuario por el eNB así como posibilitar la LI, realizaciones de la invención proporcionan un mecanismo de realimentación del canal con el que las señales de Alicia y Bob se transmiten suficientemente intensas de modo que puedan decodificarse por el (los) eNB al (a los) que están adscritos. Este mecanismo se ilustra en la metodología de la FIG. 3.

Más específicamente, como se muestra en la FIG. 3, Alicia (dispositivo 102-A) y Bob (dispositivo 102-B) no intercambian información del canal (y otros controles) directamente, sino a través de la infraestructura de la red. En otras palabras, para que Bob informe a Alicia acerca de sus propiedades observadas del enlace, no usa la comunicación ProSe. En su lugar, Bob envía esta información (302 en la FIG. 3) a su eNB de adscripción (104), que retransmite adicionalmente la información a Alicia (tanto directamente cuando Alicia está adscrita al mismo eNB (304 la FIG. 3) como a través del eNB de Alicia a través de la interfaz X2). De modo similar, Alicia informa a Bob acerca de sus propiedades observadas del canal a través de la infraestructura de red (ruta 304 a 302). La transmisión de dicha información usando la red ofrece las siguientes ventajas:

a. Permite que el operador de la red controle la duración de la sesión entre Alicia y Bob (por ejemplo, con finalidad de realizar los cargos). En particular, a menos que Alicia y Bob reciban información y parámetros del canal desde su eNB, no pueden ajustar los parámetros de comunicación (transmisión y recepción) y por lo tanto no pueden intercambiar tráfico. Con esto, la red obtiene una forma para controlar la duración de la sesión ProSe, es decir, la sesión se finaliza tan pronto como el eNB detiene el envío de información de parámetros de canal a Alicia y a Bob. Un ejemplo de dicha información de parámetros podía ser la potencia de transmisión y la tasa de bits PHY para transmisión. En dichos casos, el eNB informa a Alicia de que debería usar una potencia de transmisión específica y una tasa de bits PHY específica para la transmisión de paquetes a Bob. Claramente, otros parámetros de comunicación críticos podrían enviarse en su lugar/adicionalmente.

b. Permite que el operador de la red suministre los parámetros de comunicación ProSe a Alicia y a Bob, de modo que el eNB sea capaz de escuchar las comunicaciones ProSe. Específicamente, cuando el eNB informa a Alicia acerca de la información de realimentación del canal de Bob, el eNB puede transmitir parámetros de comunicación ProSe de modo que: (a) Alicia y Bob puedan usar los parámetros para establecer con éxito y mantener una comunicación ProSe; y (b) el eNB es también capaz de escuchar la comunicación entre Alicia y Bob. En otras palabras, aunque Bob pueda transmitir parámetros del canal que ofrecen potencialmente altas ganancias de rendimiento en el enlace Alicia-Bob, el eNB puede proporcionar parámetros diferentes a Alicia, lo que puede no ser tan propicio para un alto rendimiento (por ejemplo, alto rendimiento en el enlace Alicia-Bob), pero que permite al eNB escuchar el tráfico de Alicia y de Bob. Obsérvese que basándose en la política de la red, el eNB puede decidir que solo Alicia o solo Bob deberían transmitir de modo que el eNB pueda escuchar los mensajes transmitidos. En dicho caso, el eNB proporciona los parámetros apropiados en consecuencia a cada uno de ellos, dependiendo de qué dispositivo desee seguir el eNB.

Dado esto, una realización del esquema SeProSe incluye un proceso por el que el eNB envía parámetros de comunicación ProSe a cada UE con capacidad ProSe (rutas 302 y 304 en la FIG. 3), de modo que el eNB sea capaz de escuchar el tráfico de usuario con finalidades de supervisión y LI. El suministro de dichos parámetros puede hacer uso de los mismos procedimientos de intercambio de mensajes que los ya normalizados para comunicación entre el UE y el eNB (por ejemplo, los mismos formatos de paquete usados para la transmisión de Información de

Mejora Continua de la Calidad (CQI) entre el UE y el eNB).

Siempre que el eNB pueda escuchar el tráfico ProSe, dicho tráfico puede enviarse adicionalmente a entidades de LI (por ejemplo, el servidor de LI 310 de la FIG. 3) que están interrelacionadas con la infraestructura de red. Se ha de observar lo siguiente:

a. El tráfico ProSe escuchado puede enviarse continuamente hacia arriba hasta la GW de PDN 108 para procesamiento adicional fuera de línea y actualización de los registros de sesión de usuario, en caso de que el operador desee utilizar los registros de usuario del PGW para supervisión del usuario ProSe.

b. La escucha de la comunicación ProSe no requiere ninguna modificación de los valores del UE notificados por el eNB. Este sería normalmente el caso cuando el enlace directo entre los UE (por ejemplo el enlace Alicia-Bob) tiene una calidad más pobre que el enlace entre cada UE y el eNB. En dicho caso, el eNB sería capaz de escuchar la comunicación ProSe por omisión, dado que los parámetros de comunicación serían suficientes para que el eNB escuchara el tráfico ProSe.

c. Claramente, cuando el tráfico de usuario no necesita ser seguido o escuchado por la red, no es necesaria ninguna modificación en los parámetros de comunicación por parte del eNB.

d. Cuando Alicia transmite información de canal a su eNB asociado, es posible que Bob reciba la misma información, dado que la transmisión de Alicia se decodifica con éxito por Bob. Si los UE no son confiables, entonces Alicia podría ignorar las recomendaciones del eNB para el ajuste de sus parámetros de transmisión y podría hacer uso en su lugar de la realimentación de escucha que se envió originalmente por Bob. Para evitar dicho comportamiento con SeProSe, el eNB puede solicitar a Alicia y a Bob cifrar su información de control antes de enviarla al eNB, usando el material de clave (K_{RRCenc}) que se dedujo durante la autenticación más reciente y el procedimiento de acuerdo de claves entre el UE y el eNB.

e. En escenarios en los que el rendimiento de la comunicación ProSe no es de gran importancia, las comunicaciones ProSe pueden tener lugar usando los mismos parámetros exactos de canal de comunicación que los del enlace UE-eNB, suponiendo que el enlace UE-eNB tiene una calidad más pobre que el enlace UE-UE (lo que será normalmente el caso; claramente, si el enlace UE-eNB tiene una mejor calidad que el enlace UE-UE, el eNB siempre tendrá capacidad de escuchar la comunicación ProSe). Como un ejemplo, puede haber aplicaciones ProSe que no requieran comunicaciones rápidas entre los UE, tales como mensajería de texto y aplicaciones de voz de baja velocidad. Dichas aplicaciones pueden funcionar en enlaces que no necesitan usar altas tasas de bits. Dicho enlace se ilustra en la FIG. 3 como 312. En otras palabras, el uso de parámetros de transmisión subóptimos (que sin embargo son suficientes para una escucha con éxito de la comunicación ProSe) no afectará al rendimiento de dichas aplicaciones. En tales escenarios el uso de parámetros de canal subóptimos para ProSe se produce sin coste para la comunicación, mientras que permite a la red escuchar la comunicación.

Finalmente, la FIG. 4 ilustra una arquitectura de hardware generalizada de una parte de un sistema de comunicación 400 adecuado para implementar comunicaciones seguras entre dispositivos de proximidad (es decir, dispositivos informáticos que utilizan servicios de proximidad) en un sistema de comunicación de acuerdo con realizaciones de la invención.

Como se muestra, el dispositivo informático A 410 (por ejemplo, correspondiente a Alicia o dispositivo 102-A) y el dispositivo informático B 420 (por ejemplo, correspondiente a Bob o dispositivo 102-B) y el elemento de red 430 (por ejemplo, correspondiente al eNB 104, eNB1 104-1, eNB2 104-2, GW de SAE 106, GW de PDN 108 o MME 202) se conectan operativamente a través del medio de comunicación 440. El medio de red puede ser cualquier medio de red a través del que los dispositivos de cálculo y el elemento de red se configuran para comunicar. A modo de ejemplo, el medio de red puede transportar paquetes del protocolo de Internet (IP) y puede implicar cualquiera de las redes de comunicación anteriormente mencionadas. Sin embargo, las realizaciones de la invención no están limitadas a un tipo particular de medio de red.

Como será fácilmente evidente para un experto en la materia, los elementos pueden implementarse como ordenadores programados funcionando bajo el control de un código de programa informático. El código de programa informático se almacenaría en un medio de almacenamiento legible por ordenador (o procesador) (por ejemplo, una memoria) y el código se ejecutaría por un procesador del ordenador. Dada la divulgación de realizaciones de la invención, un experto en la materia podría producir fácilmente el código de programa informático apropiado para implementar los protocolos y metodologías descritas en el presente documento.

En cualquier caso la FIG. 4 ilustra en general una arquitectura de ejemplo para cada dispositivo en comunicación a través del medio de comunicación. Tal como se muestra, el dispositivo informático A 410 comprende dispositivos de E/S 412, procesador 414 y memoria 416. El dispositivo informático B 420 comprende dispositivos de E/S 422, procesador 424 y memoria 426. El elemento de red 430 comprende dispositivos de E/S 432, procesador 434 y memoria 436.

Debería entenderse que el término “procesador” tal como se usa en el presente documento se pretende que incluya uno o más dispositivos de procesamiento, incluyendo una unidad de procesamiento central (CPU) u otros circuitos de procesamiento, incluyendo pero sin limitación uno o más procesadores de señal, uno o más circuitos integrados y similares. También, el término “memoria” tal como se usa en el presente documento se pretende que incluya

memoria asociada con un procesador o CPU, tal como RAM, ROM, un dispositivo de memoria fija (por ejemplo disco duro) o un dispositivo de memoria extraíble (por ejemplo disquete o CD-ROM). Además, la expresión “dispositivos de E/S” tal como se usa en el presente documento se pretende que incluya uno o más dispositivos de entrada (por ejemplo, teclado, ratón) para introducir datos a la unidad de procesamiento, así como uno o más dispositivos de salida (por ejemplo, pantalla CRT) para proporcionar los resultados asociados con la unidad de procesamiento. Los dispositivos de E/S también representan transceptores (inalámbricos y/o cableados) que permiten las comunicaciones entre los dispositivos mostrados.

En consecuencia, las instrucciones de software o código para realizar las metodologías descritas en el presente documento pueden almacenarse en uno o más dispositivos de memoria asociados, por ejemplo, ROM, memoria fija o extraíble y, cuando están listos para ser utilizados, cargarse en la RAM y ejecutarse por la CPU. Dichos dispositivos de memoria pueden considerarse cada uno un medio de almacenamiento legible por ordenador o un medio de almacenamiento no transitorio. Cada dispositivo (410, 420 y 430) mostrado en la FIG. 4 puede programarse individualmente para realizar sus etapas respectivas de los protocolos y funciones representadas en las FIGS. 1A a 3. También, ha de entenderse que cada uno de los bloques 410, bloque 420 y bloque 430 pueden implementarse a través de más de un nodo discreto o dispositivo informático.

Ventajosamente, como se ha descrito en el presente documento de acuerdo con realizaciones ilustrativas, se proporciona un método para asegurar descubrimiento y comunicaciones ProSe en el contexto de redes de banda ancha inalámbricas. El SeProSe hace uso de la autenticación y procedimientos de acuerdo de claves realizado entre cada UE y la red, para deducir asociaciones de seguridad entre los UE que deseen comunicar directamente. Dicha asociación de seguridad permite a los UE con capacidad ProSe autenticarse entre sí. Por su lado, el SeProSe proporciona una forma para que el operador autentique a los UE con capacidad ProSe así como autorice a los UE para acceder a ProSe. Adicionalmente, con SeProSe el operador es capaz de verificar si los UE con capacidad ProSe que usan ProSe están realmente autorizados a hacerlo y también soporta procedimientos de intercepción legal (LI) cuando los UE funcionan en el modo ProSe. Además, el SeProSe proporciona granularidad a nivel de aplicación para sesiones seguras entre los UE, deduciendo claves de sesión para aplicaciones SeProSe individuales que se ofrecen potencialmente por el operador de la red o por entidades afiliadas.

Aunque se han descrito realizaciones ilustrativas de la presente invención en el presente documento con referencia a los dibujos adjuntos, se ha de entender que la invención no está limitada a estas realizaciones precisas.

REIVINDICACIONES

1. Un método en un elemento de red (430) para proporcionar comunicaciones seguras en un sistema de comunicación (400), que comprende:

enviar al menos una clave a un primer dispositivo informático (410) y a al menos un segundo dispositivo informático (420), en donde el primer dispositivo informático y el segundo dispositivo informático utilizan una red de acceso para acceder al sistema de comunicación y son autenticados por la red de acceso previamente a que se envíe al menos una clave y en donde adicionalmente la al menos una clave es utilizable por el primer dispositivo informático y el segundo dispositivo informático para comunicar con seguridad entre sí sin que las comunicaciones entre el primer dispositivo informático y el segundo dispositivo informático vayan a través de la red de acceso,
caracterizado por que,
el descubrimiento de proximidad, entre el primer dispositivo informático y el segundo dispositivo informático, está controlado por la red de acceso, mediante el anuncio (214 216) desde el elemento de red de la red de acceso al primer y segundo dispositivos informáticos y,
la al menos una clave es generada por (222) y proporcionada (226 228 234 230) desde al menos el elemento de red de la red de acceso al primer dispositivo informático (410) y a al menos el segundo dispositivo informático (420).

2. El método de la reivindicación 1, en el que la clave enviada por el elemento de red al primer dispositivo informático y al segundo dispositivo informático se genera basándose en una de entre: (i) un contexto de seguridad establecido durante la autenticación de uno de entre el primer dispositivo informático y el segundo dispositivo informático por la red de acceso; (ii) una clave mantenida en el elemento de red; (iii) una combinación de dos o más claves; (iv) un valor deducido aleatoriamente; y (v) una clave basada en el servicio de proximidad deducida y entregada por una entidad de gestión de la movilidad al elemento de red tras la autenticación de al menos uno de entre el primer dispositivo informático y el segundo dispositivo informático.

3. El método de la reivindicación 1, que comprende adicionalmente que el elemento de red, previamente a enviar la clave al primer dispositivo informático y al segundo dispositivo informático, verifica que el primer dispositivo informático y el segundo dispositivo informático están autorizados a comunicar entre sí cuando se descubre que están en proximidad entre sí sin que sus comunicaciones vayan a través de la red de acceso.

4. El método de la reivindicación 1, que comprende adicionalmente que el elemento de red, previamente a enviar la clave al primer dispositivo informático y al segundo dispositivo informático, determina si el primer dispositivo informático y el segundo dispositivo informático se ha descubierto que están en proximidad entre sí de modo que puedan comunicar con seguridad sin que sus comunicaciones vayan a través de la red de acceso.

5. El método de la reivindicación 1, que comprende adicionalmente la obtención por el elemento de red de al menos una parte de las comunicaciones entre el primer dispositivo informático y el segundo dispositivo informático que no van a través de la red de acceso.

6. El método de la reivindicación 5, que comprende adicionalmente realizar operaciones de intercepción legal sobre las comunicaciones obtenidas.

7. El método de la reivindicación 5, que comprende adicionalmente el envío por el elemento de red de uno o más parámetros de comunicación al primer dispositivo informático y al segundo dispositivo informático para permitir que el elemento de red obtenga las comunicaciones entre el primer dispositivo informático y el segundo dispositivo informático que no van a través de la red de acceso.

8. Un aparato para proporcionar comunicaciones seguras en un sistema de comunicación (400), que comprende:

una memoria (416; 426; 436); y
un procesador (414; 424; 434) acoplado a la memoria formando al menos una parte de un elemento de red de una red de acceso, configurados el procesador y la memoria del elemento de red para:

enviar al menos una clave a un primer dispositivo informático (410) y a al menos un segundo dispositivo informático (420), en donde el primer dispositivo informático y el segundo dispositivo informático utilizan la red de acceso para acceder al sistema de comunicaciones y están autenticados por la red de acceso previamente a que se envíe la al menos una clave y adicionalmente en donde la al menos una clave es utilizable por el primer dispositivo informático y el segundo dispositivo informático para comunicar con seguridad entre sí cuando se descubre que están en proximidad entre sí sin que las comunicaciones entre el primer dispositivo informático y el segundo dispositivo informático vayan a través de la red de acceso,
caracterizado por que
el descubrimiento de la proximidad, entre el primer dispositivo informático y el segundo dispositivo informático, está controlado por la red de acceso, mediante el anuncio (214 216) desde el elemento de red de

la red de acceso al primer y segundo dispositivos informáticos, y
la al menos una clave es generada por (222) y proporcionada (226 228 234 230) desde al menos el elemento de red de la red de acceso al primer dispositivo informático (410) y a al menos el segundo dispositivo informático (420).

9. Un método en un primer dispositivo informático (410) para proporcionar comunicaciones seguras en un sistema de comunicación (400), que comprende:

recibir, en un primer dispositivo informático (410), al menos una clave desde al menos un elemento de red de una red de acceso enviada al primer dispositivo informático y a al menos un segundo dispositivo informático (420), en donde el primer dispositivo informático y el segundo dispositivo informático utilizan la red de acceso para acceder al sistema de comunicación y son autenticados por la red de acceso previamente a que se envíe la clave; y
utilizar la clave en el primer dispositivo informático para comunicar con seguridad con el segundo dispositivo informático, cuando se descubre que el primer dispositivo informático y el segundo dispositivo informático están en proximidad entre sí, mediante la recepción de un anuncio (214 216) desde la red de acceso y sin que las comunicaciones entre el primer dispositivo informático y el segundo dispositivo informático vayan a través de la red de acceso.

10. Un aparato para proporcionar comunicaciones seguras en un sistema de comunicación (400), que comprende:

una memoria (416; 426; 436); y
un procesador (414; 424; 434) acoplado a la memoria formando un primer dispositivo informático (410), configurados el procesador y la memoria del primer dispositivo informático para:

recibir al menos una clave desde al menos un elemento de red en una red de acceso, enviada al primer dispositivo informático y a al menos un segundo dispositivo informático (420), en el que el primer dispositivo informático y el segundo dispositivo informático utilizan la red de acceso para acceder al sistema de comunicación y son autenticados por la red de acceso previamente a que se envíe la al menos una clave; y
utilizar la al menos una clave para comunicar con seguridad con el segundo dispositivo informático, cuando se descubre que el primer dispositivo informático y el segundo dispositivo informático están en proximidad entre sí, mediante la recepción de un anuncio (214 216) desde la red de acceso y sin que las comunicaciones entre el primer dispositivo informático y el segundo dispositivo informático vayan a través de la red de acceso.

FIG. 1B

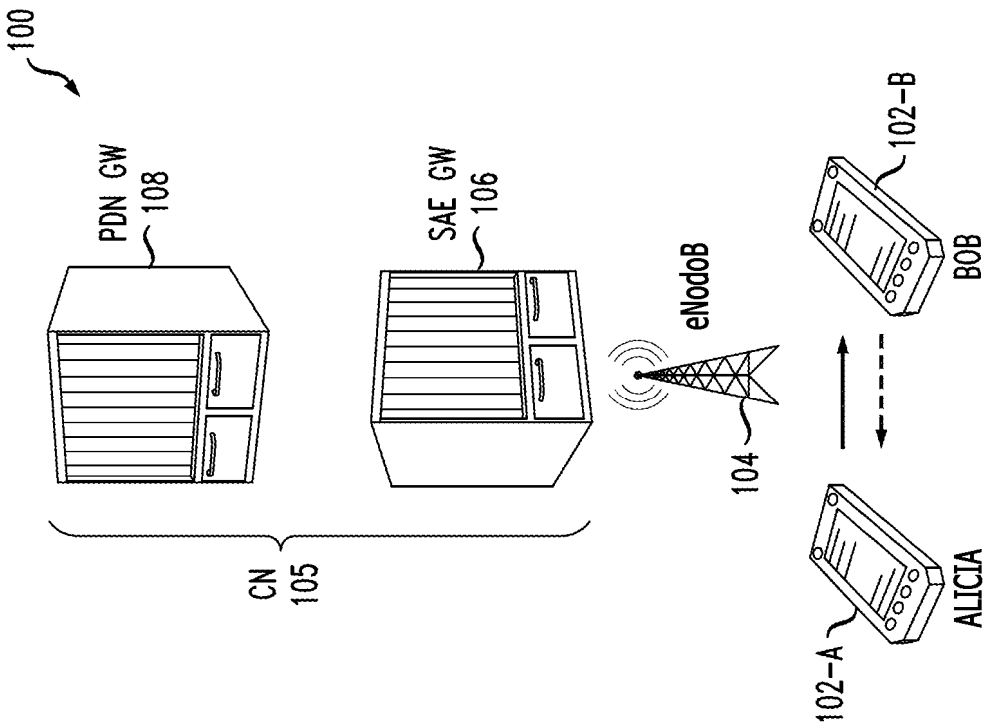

100
PDN GW
108
SAE GW
106
eNodoB
104
102-B
BOB
102-A
ALICIA
CN
105

FIG. 1A

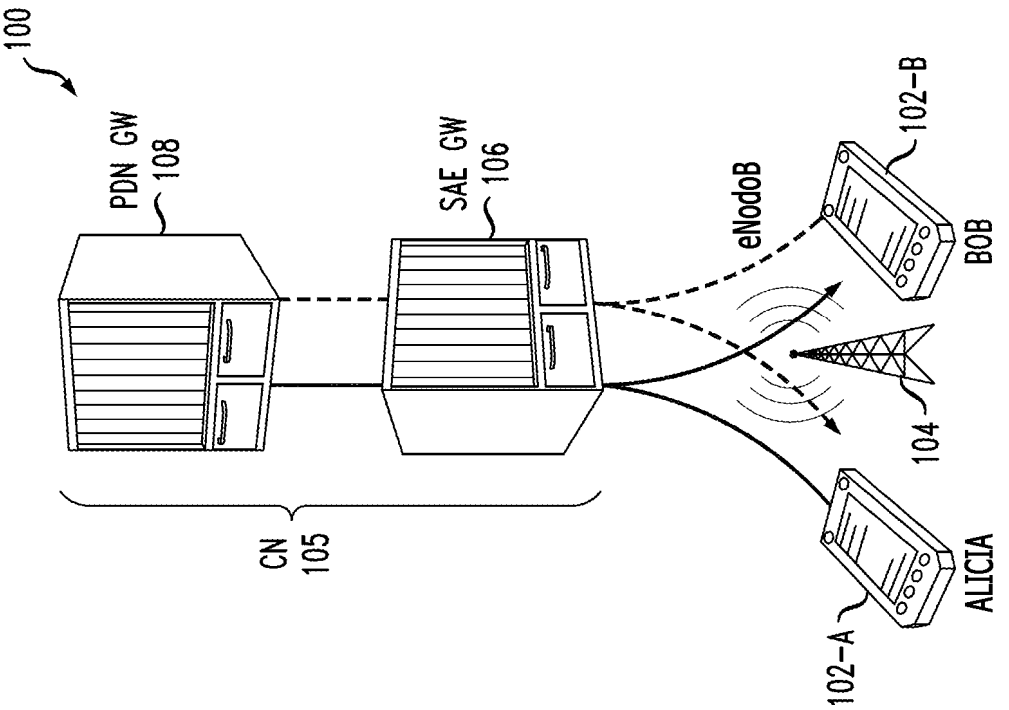

100
PDN GW
108
SAE GW
106
eNodoB
102-B
BOB
104
102-A
ALICIA
CN
105

FIG. 2A

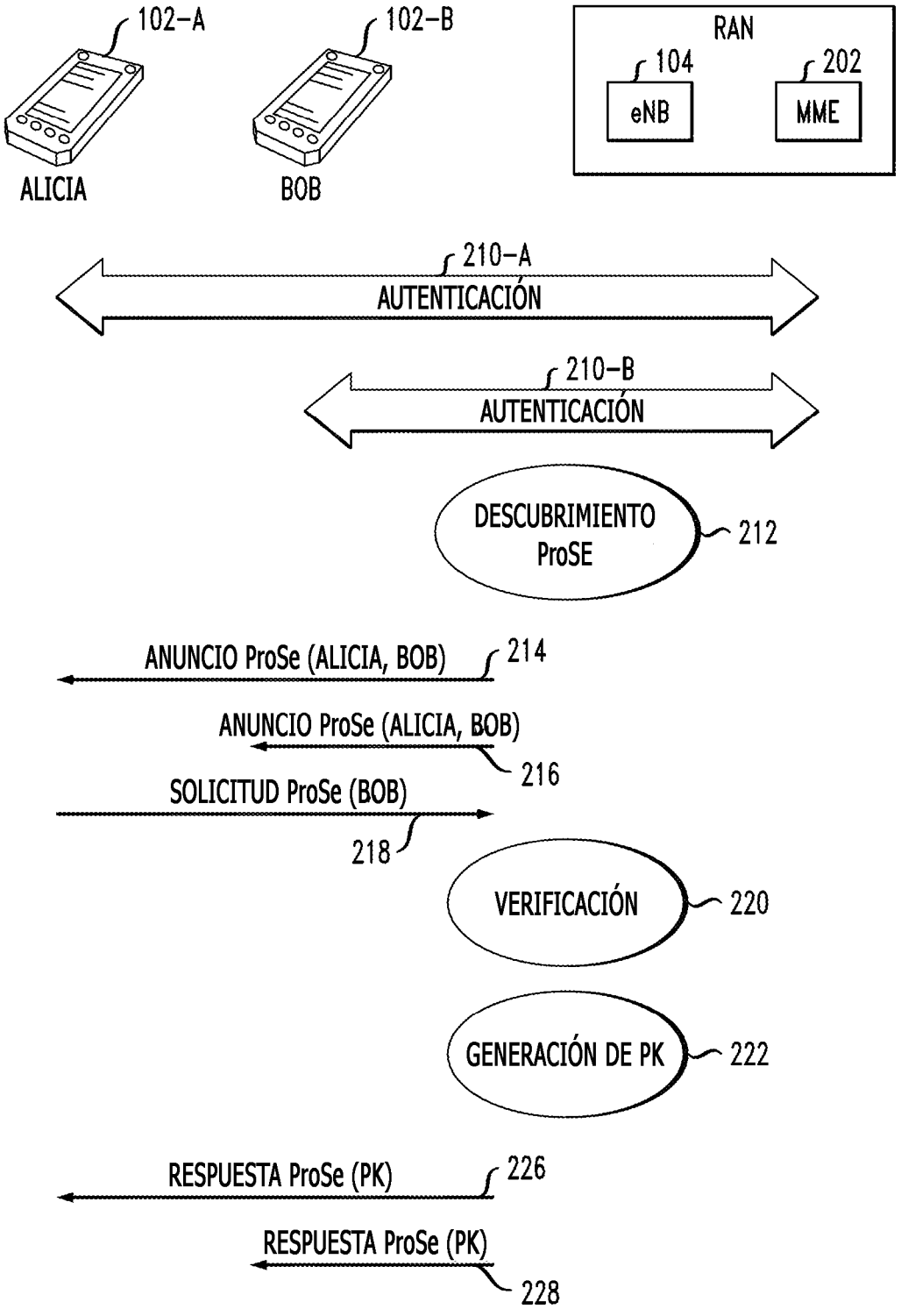

102-A
102-B
RAN
104
202
eNB
MME
ALICIA
BOB
210-A
AUTENTICACIÓN
210-B
AUTENTICACIÓN
DESCUBRIMIENTO ProSE
212
ANUNCIO ProSe (ALICIA, BOB)
214
ANUNCIO ProSe (ALICIA, BOB)
216
SOLICITUD ProSe (BOB)
218
VERIFICACIÓN
220
GENERACIÓN DE PK
222
RESPUESTA ProSe (PK)
226
RESPUESTA ProSe (PK)
228

FIG. 2B

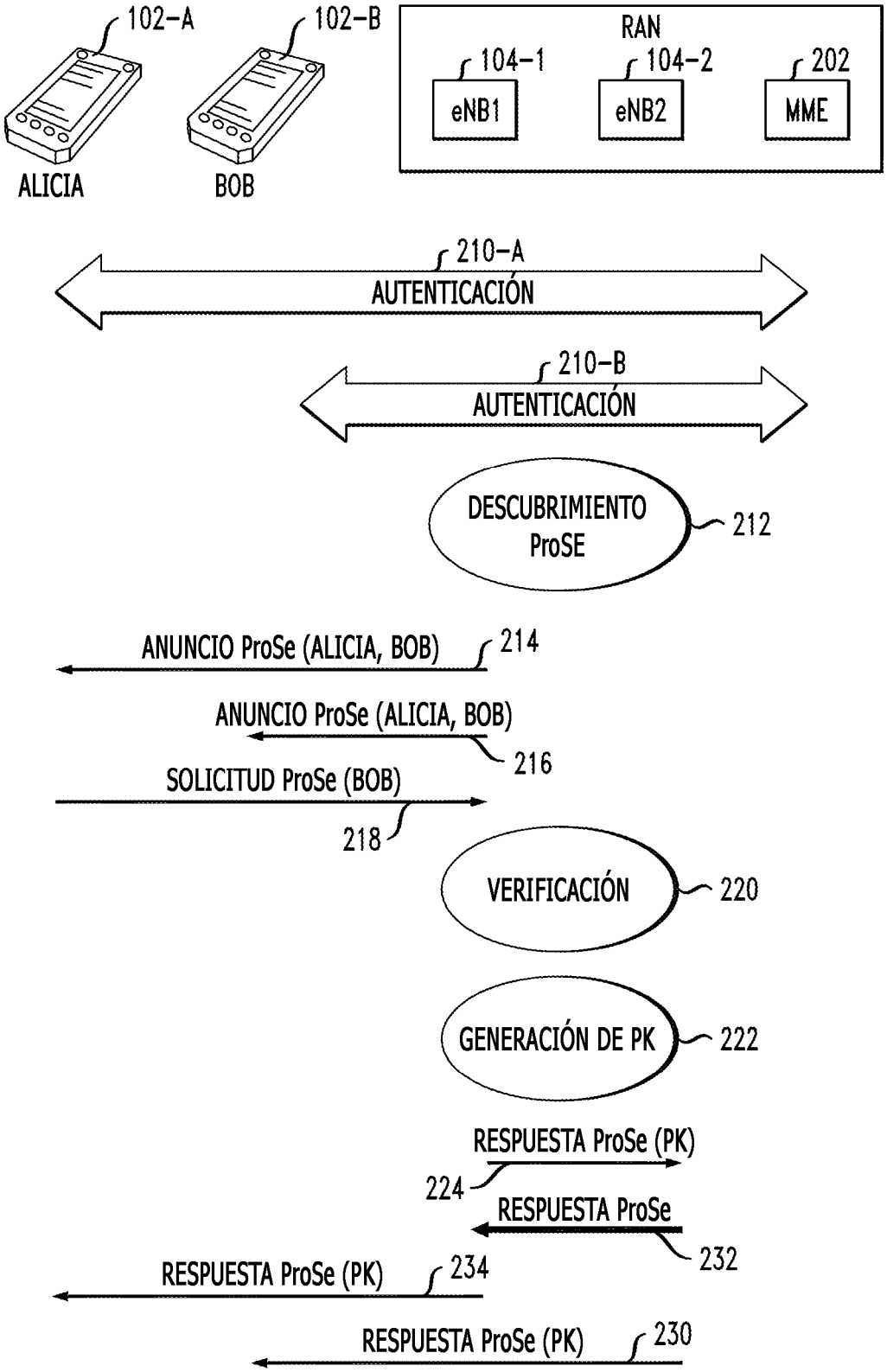

102-A
102-B
RAN
104-1
104-2
202
eNB1
eNB2
MME
ALICIA
BOB
210-A
AUTENTICACIÓN
210-B
AUTENTICACIÓN
DESCUBRIMIENTO ProSE
212
ANUNCIO ProSe (ALICIA, BOB)
214
ANUNCIO ProSe (ALICIA, BOB)
216
SOLICITUD ProSe (BOB)
218
VERIFICACIÓN
220
GENERACIÓN DE PK
222
RESPUESTA ProSe (PK)
224
RESPUESTA ProSe
232
RESPUESTA ProSe (PK)
234
RESPUESTA ProSe (PK)
230

FIG. 3

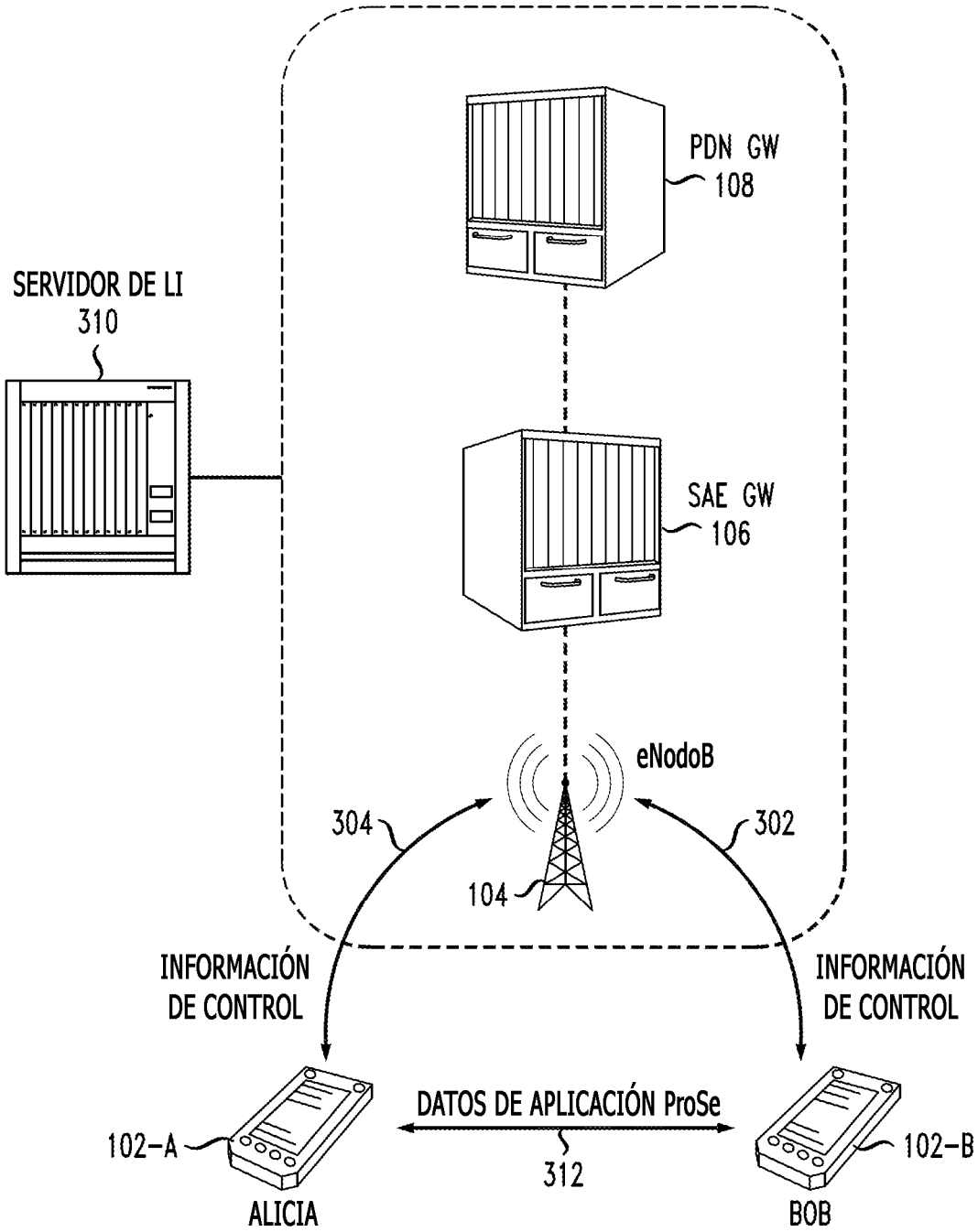
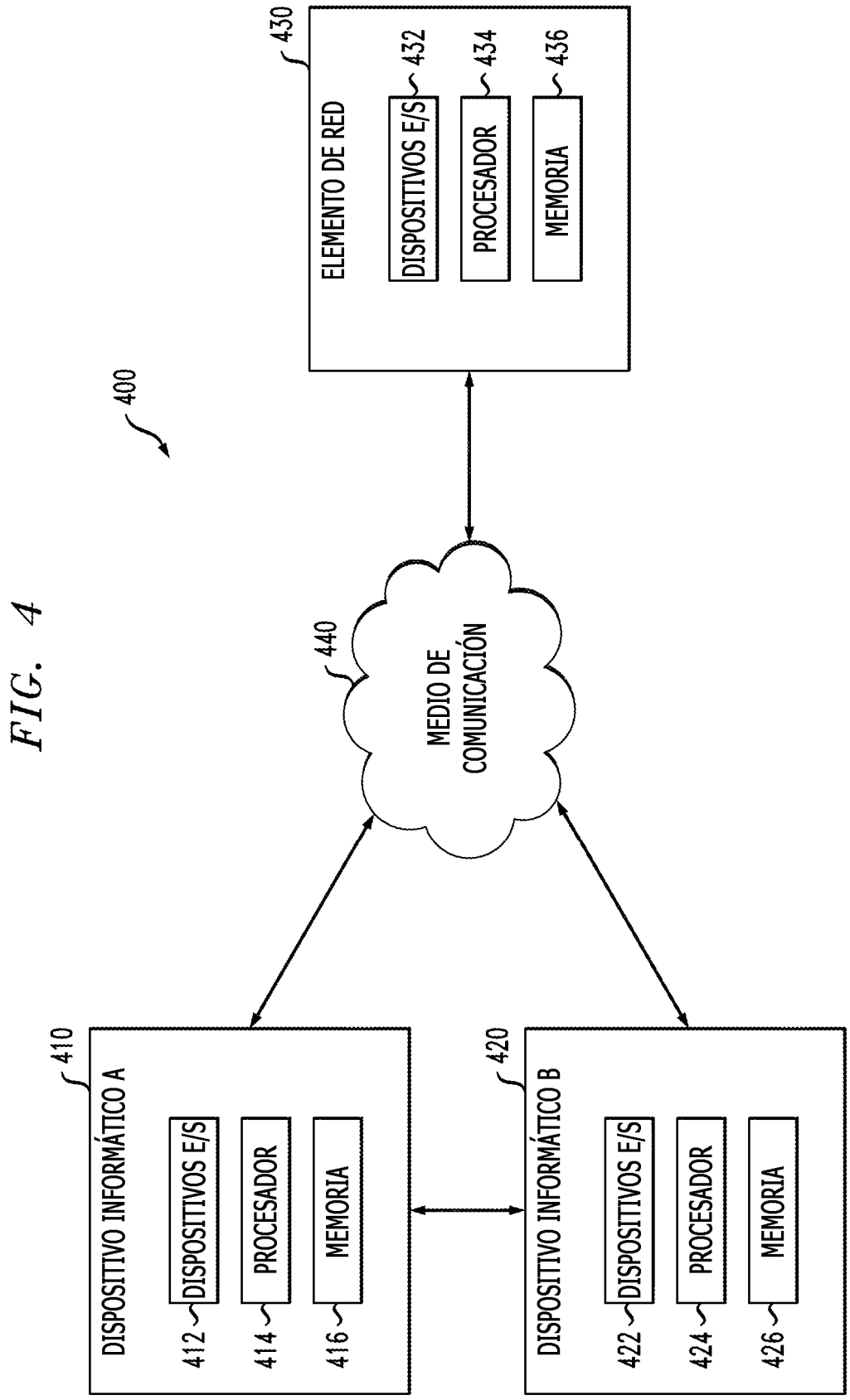

PDN GW
108
SERVIDOR DE LI
310
SAE GW
106
eNodoB
304
302
104
INFORMACIÓN
DE CONTROL
INFORMACIÓN
DE CONTROL
DATOS DE APLICACIÓN ProSe
312
102-A
102-B
ALICIA
BOB

FIG. 4


400
430
ELEMENTO DE RED
432
DISPOSITIVOS E/S
434
PROCESADOR
436
MEMORIA
440
MEDIO DE COMUNICACIÓN
410
DISPOSITIVO INFORMÁTICO A
412
DISPOSITIVOS E/S
414
PROCESADOR
416
MEMORIA
420
DISPOSITIVO INFORMÁTICO B
422
DISPOSITIVOS E/S
424
PROCESADOR
426
MEMORIA