(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 712 960**

(51) Int. CI.:

H04W 12/04 (2009.01)
H04L 29/06 (2006.01)
H04W 76/14 (2008.01)
H04W 84/12 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.08.2013 PCT/EP2013/067868**

(87) Fecha y número de publicación internacional: **06.03.2014 WO14033199**

(96) Fecha de presentación y número de la solicitud europea: **29.08.2013 E 13756120 (5)**

(97) Fecha y número de publicación de la concesión europea: **05.12.2018 EP 2891352**

(54) Título: **Método y dispositivos para emparejamiento dentro de un grupo de dispositivos inalámbricos**

(30) Prioridad:

30.08.2012 EP 12182285
30.08.2012 US 201261695022 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.05.2019

(73) Titular/es:

KONINKLIJKE PHILIPS N.V. (100.0%)
High Tech Campus 5
5656 AE Eindhoven, NL

(72) Inventor/es:

DEES, WALTER y
BERNSEN, JOHANNES ARNOLDUS CORNELIS

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Método y dispositivos para emparejamiento dentro de un grupo de dispositivos inalámbricos

Campo de la invención

La invención se relaciona con un sistema de acuerdo con la reivindicación 1 para comunicación inalámbrica que comprende un grupo de dispositivos inalámbricos y un dispositivo portátil, comprendiendo cada dispositivo un transceptor de radio para intercambiar datos de forma inalámbrica con los otros dispositivos,

- un primer dispositivo inalámbrico del grupo con capacidad para una primera función de servidor y un segundo dispositivo inalámbrico del grupo con capacidad para una segunda función de servidor, siendo el primer y segundo dispositivos inalámbricos el mismo dispositivo inalámbrico o diferentes dispositivos inalámbricos;

- el grupo de dispositivos inalámbricos que comparten los primeros datos secretos y están configurados para la comunicación inalámbrica con el primer dispositivo inalámbrico con capacidad para la primera función de servidor a través de las primeras conexiones seguras respectivas con base en los primeros datos secretos.

La invención se relaciona además con un dispositivo portátil de acuerdo con la reivindicación 2, un dispositivo central de acuerdo con la reivindicación 6, un dispositivo inalámbrico de acuerdo con la reivindicación 11, un método de acuerdo con la reivindicación 14 y un producto de programa informático de acuerdo con la reivindicación 15 para uso en el sistema anterior para la comunicación inalámbrica.

La invención se relaciona con el campo de la comunicación inalámbrica segura, por ejemplo, a través de Wi-Fi, y más específicamente con una configuración segura para un sistema de acoplamiento inalámbrico.

Antecedentes de la invención

En la comunicación inalámbrica, tal como la conexión Wi-Fi conocida de los documentos IEEE 802.11, los dispositivos deben estar emparejados para establecer una conexión segura, por ejemplo, como se describe en el documento "Wi-Fi Protected Access (WPA), Enhances Security Implementation Based on IEEE P802.11i standard, versión 3.1, agosto de 2004, por la alianza Wi-Fi" disponible a través de www.wi-fi.org. Aunque la invención se aclara más con el uso del sistema Wi-Fi, se observa que la invención se puede aplicar de manera similar en otros sistemas de comunicación inalámbrica, como Bluetooth (ver, por ejemplo, BLUETOOTH SPECIFICATION, Core Package version 2.1 + EDR, publicado el 26 de julio de 2007).

Las conexiones Wi-Fi están protegidas por confidencialidad e integridad por medios criptográficos, utilizando tecnologías tales como WPA2. La seguridad en WPA2 puede basarse en dos sistemas. El primero es el modo de clave previamente compartida (PSK, también conocido como modo personal) y está diseñado para redes domésticas y de pequeñas oficinas. El segundo se basa en el uso de un servidor de autenticación 802.1X y está diseñado para redes empresariales.

En el modo PSK, todos los dispositivos que se comunican entre sí comparten una clave de 256 bits, que también se denomina "Frase de contraseña". La configuración simple de Wi-Fi (también conocida como configuración protegida Wi-Fi), conocida en el documento " Wi-Fi Simple Configuration, Technical Specification , versión 2.0.2, 2011", también de la Alianza Wi-Fi, es un estándar que permite un primer dispositivo que conoce la frase de contraseña, por ejemplo, un punto de acceso de LAN inalámbrica, para enviarlo a un segundo dispositivo de forma segura, sin que el usuario tenga que ingresar la frase de contraseña en el segundo dispositivo. En cambio, el usuario puede, por ejemplo, presionar un botón en ambos dispositivos dentro de un tiempo limitado, o ingresar un PIN de 8 dígitos que aparece en el primer dispositivo en el segundo dispositivo, con el fin de recibir una frase de contraseña. Normalmente, esto implica una acción del usuario, es decir, una llamada acción de emparejamiento del usuario.

El documento de los Estados Unidos US2010/0153727 describe una seguridad mejorada para comunicaciones de enlace directo entre múltiples dispositivos inalámbricos, que intercambian hápax que se utilizan para generar un hápax común. Un elemento de información de identificación de grupo se genera al menos a partir del hápax común y se reenvía a un servidor de autenticación. El servidor de autenticación genera una clave maestra de enlace directo de grupo a partir del elemento de información de identificación de grupo para que coincida con los dispositivos como parte de una clave de grupo de acuerdo. Las claves de grupo también se generan con base en el hápax común. Así se crea un grupo seguro de dispositivos para la comunicación de enlace directo.

Resumen de la invención

En la infraestructura de Wi-Fi, un punto de acceso (AP), o más bien su registrador, almacena y administra las credenciales de la red de la que es responsable. Un dispositivo de Wi-Fi que desea acceder a la red de infraestructura de Wi-Fi de un AP necesita obtener las credenciales de la red en una operación de emparejamiento con el AP. Una vez que se establece la conexión segura con el AP, el dispositivo Wi-Fi puede comunicarse con otros dispositivos Wi-

Fi asociados con el AP. La infraestructura tradicional tiene la desventaja de que las conexiones son indirectas, ya que todas las comunicaciones deben pasar por el punto de acceso. Sin embargo, en muchos casos es beneficioso (por ejemplo, para reducir la latencia, mejorar la velocidad de conexión) que los dispositivos puedan establecer un enlace directo entre ellos sin tener que retransmitir el tráfico a través del punto de acceso. Se han creado dos tecnologías Wi-Fi directo y Configuración de Enlace Directo Tunelizado (TDLS) para poder configurar dicho enlace de Wi-Fi directo entre dispositivos.

Wi-Fi directo (también conocido como Wi-Fi Punto a Punto), conocido en el documento "Wi-Fi Wi-Fi Peer-to-Peer (P2P) Technical Specification, versión 1.1, 2010", también de Alianza Wi-Fi es un estándar que permite que los dispositivos Wi-Fi se conecten entre sí sin necesidad de un punto de acceso inalámbrico. Wi-Fi directo juega un papel importante en la conexión de dispositivos inalámbricos y periféricos independientes, como dispositivos/periféricos de pantalla compatibles con Visualización Wi-Fi, y dispositivos/periféricos de E/S compatibles con Bus en Serie Wi-Fi (por ejemplo, ratón inalámbrico, teclado, impresora, Concentrador USB). Por lo tanto, es una tecnología importante para el acoplamiento inalámbrico, una tecnología para permitir que un dispositivo portátil se conecte a una multitud de periféricos inalámbricos. En Wi-Fi directo, una etapa de emparejamiento del usuario normalmente se debe realizar para cada nueva conexión Wi-Fi directo que se crea. Cuando dos dispositivos Wi-Fi directo desean comunicarse, uno de ellos se convierte en el llamado Propietario del Grupo (GO). El otro dispositivo asume el rol de cliente. Juntos forman un grupo llamado P2P. Un GO tiene muchas similitudes con un AP. Por ejemplo, puede permitir que otros dispositivos se unan al grupo P2P y ofrecer posibilidades para distribuir el tráfico entre los diferentes dispositivos en el grupo P2P. Sin embargo, como se mencionó anteriormente, es beneficioso que los dispositivos puedan comunicarse directamente entre sí sin tener que retransmitir el tráfico. En el caso de Wi-Fi directo, esto significaría que tendría que conectarse y emparejarse con cada uno de los otros dispositivos individualmente. Esto es engorroso, especialmente si hay diversos dispositivos involucrados. Por ejemplo, para el acoplamiento inalámbrico de un dispositivo portátil con una multitud de periféricos inalámbricos, sería muy hostil si el usuario tuviera que realizar una etapa de emparejamiento de usuarios con cada periférico inalámbrico individualmente. Por lo tanto, es muy importante mantener la cantidad de acciones de emparejamiento al mínimo.

Configuración de Enlace Directo en Túnel (TDLS), conocido por el documento "IEEE Std 802.11z-2010 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 7: Extensions to Direct-Link Setup (DLS), publicado por IEEE el 14 de octubre de 2010 ", es una opción en Wi-Fi que permite configurar un enlace directo entre dos dispositivos que están conectados al mismo punto de acceso Wi-Fi, sin necesidad de emparejarse de nuevo para configurar una conexión directa segura. Esto se hace de la siguiente manera. Una vez que un dispositivo Wi-Fi habilitado para TDLS se conecta al punto de acceso, puede enviar una solicitud a otro dispositivo habilitado para TDLS que esté conectado al mismo punto de acceso para configurar una conexión directa. Después de intercambiar información, como las credenciales de seguridad y la información sobre qué canal Wi-Fi utilizar, los dos dispositivos pueden iniciar un enlace directo seguro privado entre los dos dispositivos.

Sin embargo, TDLS tiene diversos inconvenientes: todos los dispositivos involucrados deben admitir operaciones simultáneas (para mantener un enlace directo al otro dispositivo y un enlace al AP simultáneamente, incluido el funcionamiento en dos frecuencias diferentes), a la vez que muchos dispositivos periféricos inalámbricos y portátiles solo son capaces de configurar y mantener una única conexión Wi-Fi y/o conexiones de una sola frecuencia Wi-Fi.

TDLS tiene diversos problemas de compatibilidad cuando se usa en una red Wi-Fi Directa (por ejemplo, TDLS a través de Wi-Fi directo GO para configurar un enlace directo entre diferentes dispositivos dentro de un grupo Wi-Fi directo P2P). Por ejemplo, los mecanismos de ahorro de energía de Wi-Fi directo y TDLS no son compatibles y pueden causar conflictos.

El intercambio de credenciales de seguridad para el enlace directo de TDLS se realiza a través de una negociación de clave de igual TDLS (TPK). El problema es que esta negociación entre los dos dispositivos TDLS se realiza a través del AP. Dado que el AP puede descifrar los mensajes de los dispositivos TDLS involucrados, significa que el AP puede escuchar esta negociación y es capaz de recuperar la clave con la que los dispositivos TDLS aceptan la conexión directa. Cuando se usa el modo PSK, también otros dispositivos asociados con el mismo AP podrán escuchar este tráfico, por ejemplo, de la siguiente manera: cuando un dispositivo Wi-Fi se asocia con un AP que usa PSK, usa la frase de contraseña y otra información en una llamada negociación de cuatro vías para generar/derivar una clave de enlace llamada clave transitoria por pares (PTK). El PTK se utiliza para el cifrado y la autenticación del tráfico entre ese dispositivo Wi-Fi y el AP. El tráfico destinado a otro dispositivo es re cifrado por el AP con la clave de enlace (PTK) que el AP y el otro dispositivo han derivado de la frase de contraseña. Aunque el AP tiene un PTK diferente para cada dispositivo Wi-Fi asociado, cualquier dispositivo asociado con el AP, en posesión de la frase de contraseña, puede calcular el PTK que se usa al escuchar la negociación de cuatro vías entre el otro dispositivo y el AP. Dado que al usar este PTK, el dispositivo puede descifrar la comunicación entre el otro dispositivo y el AP, esto significa que también puede escuchar la negociación de clave de igual TDLS y calcular la clave que se usa para proteger el enlace directo de TDLS entre los dos dispositivos TDLS. Por lo tanto, TDLS por defecto no proporciona comunicación privada segura a través del enlace directo.

El emparejamiento de un dispositivo inalámbrico y la configuración de la conexión siempre tiene que pasar por el punto de acceso al que deben conectarse todos los dispositivos del grupo. No puede conectarse directamente con ninguno

de los clientes/estaciones (por ejemplo, la pantalla) en el grupo a menos que primero configure una conexión con el propietario del punto de acceso/grupo. Esto significa que es posible que deba estar físicamente cerca del propietario del punto de acceso/grupo para realizar las etapas de emparejamiento, ya que no puede conectarse con el grupo a través de uno de los otros dispositivos del grupo.

Un objeto de la invención es proporcionar un sistema para la comunicación segura que mantenga el número de etapas de emparejamiento del usuario al mínimo, impedir la interceptación de los enlaces directos entre los dispositivos y proporcionar flexibilidad para conectarse al grupo.

Para este propósito, en el sistema para la comunicación inalámbrica como se describe en el párrafo inicial, el dispositivo portátil comprende un procesador de comunicaciones del dispositivo para

- configurar una segunda conexión segura con el segundo dispositivo inalámbrico que se acomoda a la segunda función de servidor mediante un procedimiento de emparejamiento con base en segundos datos secretos diferentes de los primeros datos secretos,

- recibir una segunda instrucción a través de la segunda conexión segura y, de acuerdo con la segunda instrucción,

- configurar una conexión segura inalámbrica directa respectiva con al menos un dispositivo inalámbrico del grupo usando un procedimiento de emparejamiento respectivo con base en terceros datos secretos, los terceros datos secretos difieren de los primeros datos secretos;

el segundo dispositivo inalámbrico con capacidad para la segunda función de servidor comprende un procesador de comunicaciones servidor para

- configurar la segunda conexión segura con el dispositivo portátil mediante el procedimiento de emparejamiento con base en los segundos datos secretos,

- transferir a al menos un dispositivo inalámbrico a través de la primera conexión segura una primera instrucción para aplicar los terceros datos secretos transferidos en la primera instrucción para configurar una conexión segura inalámbrica directa con el dispositivo portátil, y

- transferir al dispositivo portátil a través de la segunda conexión segura una segunda instrucción para aplicar los terceros datos secretos transferidos en la segunda instrucción para configurar la conexión segura inalámbrica directa con al menos un dispositivo inalámbrico con base en los terceros datos secretos;

el al menos un dispositivo inalámbrico comprende un procesador de comunicaciones para

- recibir la primera instrucción a través de la primera conexión segura y, de acuerdo con la primera instrucción,

- configurar la conexión segura inalámbrica directa respectiva con el dispositivo portátil mediante un procedimiento de emparejamiento respectivo con base en los terceros datos secretos.

Para este propósito, de acuerdo con un aspecto adicional de la invención, el método de comunicación inalámbrica en el sistema de dispositivos inalámbricos como se describe en el párrafo inicial comprende

- configurar una segunda conexión segura entre el dispositivo portátil y el segundo dispositivo inalámbrico con capacidad para la segunda función de servidor mediante un procedimiento de emparejamiento con base en segundos datos secretos diferentes de los primeros datos secretos;

- transferir a al menos un dispositivo inalámbrico del grupo a través de la primera conexión segura una primera instrucción para aplicar unos terceros datos secretos transferidos en la primera instrucción para configurar una conexión segura inalámbrica directa con el dispositivo portátil, los terceros datos secretos difieren de los primeros datos (240) secretos, y

- transferir al dispositivo portátil a través de la segunda conexión segura una segunda instrucción para aplicar los terceros datos secretos transferidos en la segunda instrucción para configurar la conexión segura inalámbrica directa con al menos un dispositivo inalámbrico con base en los terceros datos secreto;

- configurar una conexión segura inalámbrica directa respectiva entre el dispositivo portátil y al menos un dispositivo inalámbrico utilizando un procedimiento de emparejamiento respectivo con base en los terceros datos secretos.

Los elementos principales del sistema y método seguro permiten que un dispositivo portátil A (por ejemplo, compatible con Wi-Fi directo) se conecte a un grupo G de dispositivos inalámbricos. El grupo G está configurado previamente para actuar como un grupo conectado a un dispositivo inalámbrico con capacidad para una primera función de servidor y comparte un secreto S1 común utilizado para asegurar la comunicación dentro del grupo. El grupo puede, por

ejemplo, comprender un servidor de acoplamiento inalámbrico y periféricos inalámbricos. El dispositivo A se conecta a uno de los dispositivos inalámbricos, que funciona como un segundo dispositivo servidor al acomodar una segunda función de servidor, en el grupo que utiliza el secreto S2 para asegurar la comunicación a través de la segunda conexión segura. Posteriormente, los dispositivos del grupo y el dispositivo A reciben instrucciones sobre otro secreto, seguido por el dispositivo A para comenzar a escuchar las conexiones entrantes, seguido por uno o más dispositivos que configuran una conexión inalámbrica segura directa con el dispositivo A mediante el uso del secreto S3 para emparejamiento con el dispositivo A, por ejemplo de una manera que sea compatible con Wi-Fi Directo. Opcionalmente, el segundo dispositivo servidor es el mismo dispositivo que el dispositivo inalámbrico con capacidad para la primera función de servidor. Por lo tanto, la primera y la segunda función de servidor pueden implementarse en un solo dispositivo inalámbrico. Además, el grupo G puede contener dispositivos que solo son capaces de admitir un cliente P2P o una función de estación Wi-Fi (STA), y no un propietario de grupo P2P o una función de punto de acceso Wi-Fi (AP).

Las medidas tienen el efecto de que se proporcionan un sistema de comunicación seguro inalámbrico y un protocolo seguro para distribuir los secretos utilizados para establecer enlaces directos seguros con pasos mínimos de emparejamiento de usuarios, de manera que se impida la interceptación de enlaces directos entre dispositivos, y que además ofrece flexibilidad adicional al permitir que cualquier dispositivo capaz de realizar la función del segundo servidor sea el punto de entrada al grupo de dispositivos inalámbricos que realizan una función. Por ejemplo, el grupo de dispositivos puede proporcionar un entorno de acoplamiento para un dispositivo portátil como un teléfono inteligente (también conocido como acoplado). En particular, el acoplado no siempre tiene que usar el mismo dispositivo en el sistema de acoplamiento (por ejemplo, un AP o GO) para conectarse con el grupo, sino que puede conectarse a cualquier dispositivo del grupo que acomode dicha segunda función de servidor.

La invención también se basa en el siguiente reconocimiento (utilizando el entorno Wi-Fi como ejemplo). Cuando un grupo de dispositivos Wi-Fi directo realiza juntos funciones para otro dispositivo inalámbrico (como el acoplamiento inalámbrico), es deseable que el otro dispositivo inalámbrico pueda configurar uno o más enlaces de igual a igual con cualquiera de los dispositivos inalámbricos. Los dispositivos en el grupo sin tener que realizar una acción de emparejamiento de usuario con cada uno de estos dispositivos del grupo individualmente.

Wi-Fi directo tiene el concepto de un propietario de un grupo (GO). Si todos los dispositivos Wi-Fi directo del grupo se conectaran al mismo GO, y el GO es compatible con la llamada función de distribución Intra-BSS de Wi-Fi directo, entonces es suficiente que el otro dispositivo inalámbrico se conecte a este GO para poder comunicarse con todos los dispositivos del grupo. Un campo de distribución Intra-BSS indica si el dispositivo P2P aloja, o pretende hospedar, un grupo P2P que proporciona un servicio de distribución de datos entre clientes en el grupo P2P. Sin embargo, toda la comunicación tendría que pasar por el GO. Esto es muy ineficiente, y aumenta la latencia de la comunicación. Para funciones como el acoplamiento inalámbrico, la latencia es un tema importante. La conexión con la pantalla inalámbrica, el ratón, el teclado, etc., debe tener la menor latencia posible. Por lo tanto, es importante poder configurar conexiones directas (es decir, punto-a-punto) con múltiples o incluso con todos los miembros del grupo. Sin embargo, eso requeriría que se realizaran diversas etapas de emparejamiento de usuarios para cada acoplado inalámbrico que quisiera conectarse a este grupo de periféricos. Por las razones mencionadas en la sección anterior, el uso de TDLS no es una opción para superar este problema.

Otro problema es que Wi-Fi directo impone ciertas restricciones en los dispositivos, como la restricción de que un dispositivo P2P solo se puede conectar a un solo GO. Una vez conectado a un GO, el dispositivo P2P cambia los roles, es decir, el dispositivo se convierte en un cliente P2P. Wi-Fi directo define diversas restricciones para los clientes P2P, tales como las restricciones en el descubrimiento y la comunicación entre los clientes P2P. Además, el número de instancias de cliente P2P simultáneas que normalmente pueden ejecutarse en un solo dispositivo también es muy limitado. Se espera que diversos periféricos inalámbricos de gama baja (como un ratón o un teclado Wi-Fi) tengan incluso más restricciones debido a sus limitaciones de recursos, como la función de cliente P2P y un solo enlace Wi-Fi.

Los inventores han visto que los problemas anteriores son superados por el protocolo seguro que genera, a través del segundo servidor, los datos secretos del tercer orden e instruye al dispositivo portátil (acoplado) y dispositivos inalámbricos del grupo para aplicar los terceros datos secretos para conectar el primer dispositivo a los dispositivos inalámbricos seleccionados del grupo, por ejemplo, constituyendo un entorno de acoplamiento previamente configurado.

Opcionalmente, en el dispositivo portátil, el procesador de comunicaciones del dispositivo está dispuesto además para controlar la comunicación a través de dichas conexiones inalámbricas directas como propietario del grupo. En general, en un sistema de red inalámbrica, un dispositivo puede controlar un grupo de dispositivos como propietario de un grupo, por ejemplo, en WLAN ejecutando el rol de AP. En un ejemplo en Wi-Fi, el primer dispositivo toma un rol de propietario de grupo de Wi-Fi directo cuando configura las conexiones Wi-Fi directo P2P entre los dispositivos en un subconjunto G' de otros dispositivos inalámbricos y el primer dispositivo.

Opcionalmente, en el dispositivo portátil, el procesador de comunicaciones del dispositivo está además dispuesto para configurar las respectivas conexiones seguras inalámbricas directas respectivas con los respectivos dispositivos

inalámbricos de los respectivos subconjuntos diferentes utilizando un procedimiento de emparejamiento respectivo con base en los respectivos terceros datos secretos diferentes. Ventajosamente, múltiples subconjuntos se acomodan para comunicarse con el primer dispositivo a través de diferentes instancias de los terceros datos secretos.

Opcionalmente, en el dispositivo portátil, el procesador de comunicaciones del dispositivo está dispuesto además para recibir la segunda instrucción que incluye los respectivos terceros datos secretos para múltiples subconjuntos. Ventajosamente, múltiples subconjuntos se acomodan para comunicarse con el dispositivo portátil a través de una sola instrucción.

Opcionalmente, en el dispositivo portátil, el procesador de comunicaciones del dispositivo está dispuesto además para generar los terceros datos secretos y transferir los terceros datos secretos al dispositivo con capacidad para la segunda función de servidor. Ventajosamente, el dispositivo portátil controla la seguridad al controlar la generación de los terceros datos secretos.

Opcionalmente, en el dispositivo portátil, el procesador de comunicaciones del dispositivo está dispuesto para desconectar la segunda conexión segura antes de iniciar la configuración de la conexión segura inalámbrica directa respectiva con un dispositivo inalámbrico respectivo del subconjunto. Ventajosamente, se requiere menos capacidad de transceptor de radio y se usa menos capacidad del medio inalámbrico.

Opcionalmente, en el dispositivo portátil, el procesador de comunicaciones del dispositivo está dispuesto para proporcionar una agrupación persistente y, de acuerdo con esto para, después de desconectar la conexión segura inalámbrica directa respectiva con base en dichos terceros datos secretos, establecer una conexión segura inalámbrica directa respectiva con base nuevamente en dichos terceros datos secretos. Ventajosamente, cuando un dispositivo portátil, por ejemplo, un acoplado, se vuelve a conectar, la comunicación segura se restaura más rápido.

Opcionalmente, en el dispositivo portátil, el procesador de comunicaciones del dispositivo está dispuesto para utilizar los segundos datos secretos o los terceros datos secretos adquiridos durante el emparejamiento anterior cuando, después de desconectar la conexión segura inalámbrica directa respectiva con base en dichos terceros datos secretos, se vuelve a conectar con el dispositivo inalámbrico respectivo del subconjunto para configurar una conexión segura inalámbrica directa respectiva. Ventajosamente, cuando un dispositivo portátil, por ejemplo, un acoplado, se vuelve a conectar, la comunicación segura se restaura más rápido.

Opcionalmente, la segunda conexión segura comprende una conexión Wi-Fi directo P2P. En la práctica, la conexión puede ser una conexión Wi-Fi directo P2P y donde los segundos datos secretos (S2) es una frase de contraseña de Wi-Fi, por ejemplo, la clave maestra de Wi-Fi por pares (PMK) o la clave previamente compartida de Wi-Fi (PSK).

Opcionalmente, la respectiva conexión segura inalámbrica directa comprende una conexión Wi-Fi directo punto a punto, o la respectiva conexión segura inalámbrica directa comprende una conexión Configuración de Enlace Directo en Túnel (TDLS). En la práctica, las conexiones directas entre los dispositivos en el subconjunto G' y el primer dispositivo pueden ser conexiones Wi-Fi directo P2P y donde los terceros datos secretos es una frase de contraseña de Wi-Fi, por ejemplo, la clave maestra de Wi-Fi por pares (PMK) o la clave previamente compartida de Wi-Fi (PSK). Alternativamente, las conexiones directas entre los dispositivos en el subconjunto G' y el primer dispositivo son conexiones TDLS. Además, el procedimiento de emparejamiento puede comprender un acceso protegido a Wi-Fi (WPA/WPA2) o un procedimiento de configuración simple de Wi-Fi. Ventajosamente, dicho procedimiento de emparejamiento conocido ya puede estar disponible en el dispositivo inalámbrico y puede compartirse.

Opcionalmente, una etapa de configuración previa implica designar el dispositivo para que la segunda función de servidor sea un propietario de grupo de P2P de Wi-Fi directo de un grupo de P2P que consiste en el segundo dispositivo servidor y los dispositivos en el grupo G, y emparejando cada uno de los dispositivos en grupo con el segundo dispositivo servidor para obtener el secreto S1 común del segundo dispositivo servidor y donde S1 es la frase de contraseña (la clave maestra por pares de Wi-Fi (PMK) o la clave previamente compartida de Wi-Fi (PSK).

Opcionalmente, en el dispositivo servidor, el procesador de comunicaciones servidor está dispuesto para generar los terceros datos secretos. Ventajosamente, el dispositivo servidor controla la seguridad al controlar la generación de los terceros datos secretos.

Opcionalmente, en el dispositivo servidor, el procesador de comunicaciones servidor está dispuesto para generar un conjunto respectivo y diferente de los terceros datos secretos para las respectivas instancias diferentes del primer dispositivo. Ventajosamente, se impide la audición de la comunicación entre diferentes primeros dispositivos.

Opcionalmente, en el dispositivo servidor, el procesador de comunicaciones servidor está dispuesto para generar un conjunto diferente y respectivo de los terceros datos secretos cuando el dispositivo (A), después de haber desconectado la segunda conexión segura, está configurando la segunda conexión segura un tiempo respectivo, adicional. Ventajosamente, los ataques de repetición se impiden al generar diferentes conjuntos de terceros datos secretos.

Opcionalmente, en el dispositivo servidor, el procesador de comunicaciones servidor está dispuesto para generar un conjunto diferente, respectivo, de los terceros datos secretos para un subconjunto diferente, respectivo de los dispositivos inalámbricos en el grupo. Ventajosamente, múltiples subconjuntos se acomodan para comunicarse con el primer dispositivo a través de diferentes instancias de los terceros datos secretos.

Opcionalmente, en el dispositivo servidor, el procesador de comunicaciones servidor está dispuesto para generar los terceros datos secretos con base o iguales a los segundos datos secretos. Básicamente, los terceros datos secretos se pueden elegir para que sean diferentes de los segundos datos secretos, lo que mejora la seguridad. Ventajosamente, los terceros datos secretos pueden generarse con base en los segundos datos secretos, lo que mejora la eficiencia. Además, los terceros datos secretos se pueden elegir para que sean iguales a los segundos datos secretos, lo que mejora la velocidad a medida que se necesita transferir menos datos.

Opcionalmente, en el dispositivo servidor, el procesador de comunicaciones servidor está dispuesto para asignar una vida útil limitada a los terceros datos secretos, y/o asignar una vida útil a los terceros datos secretos en función de un nivel de autorización del dispositivo (A). Ventajosamente, el acceso al sistema seguro está limitado en el tiempo, o a un invitado o propietario se le pueden asignar diferentes derechos.

Opcionalmente, en el dispositivo servidor, el procesador de comunicaciones servidor está dispuesto para transferir una tercera instrucción al dispositivo inalámbrico respectivo del subconjunto para desconectar la primera conexión segura antes de configurar la conexión segura inalámbrica directa respectiva al dispositivo. Ventajosamente, se requiere menos capacidad de transceptor de radio y se usa menos capacidad del medio inalámbrico.

Opcionalmente, el dispositivo servidor es un servidor de acoplamiento inalámbrico o una estación de acoplamiento inalámbrica. En la práctica, el dispositivo servidor puede ser el mismo dispositivo que el primer dispositivo servidor inalámbrico y/o el segundo dispositivo servidor inalámbrico. Por lo tanto, la primera y la segunda función de servidor pueden implementarse en un solo servidor de acoplamiento o estación de acoplamiento inalámbrica.

Opcionalmente, en el dispositivo inalámbrico, el procesador de comunicaciones respectivo está dispuesto para iniciar la configuración de la conexión segura inalámbrica directa respectiva al dispositivo portátil. Ventajosamente, el dispositivo inalámbrico controla la configuración.

Opcionalmente, en el dispositivo inalámbrico, el procesador de comunicaciones respectivo está dispuesto para desconectar la primera conexión segura antes de configurar la conexión segura inalámbrica directa respectiva al dispositivo portátil. Ventajosamente, se requiere menos capacidad de transceptor de radio y se usa menos capacidad del medio inalámbrico.

Opcionalmente, en el dispositivo inalámbrico, el procesador de comunicaciones respectivo está dispuesto para restaurar la primera conexión segura después de desconectar la conexión segura inalámbrica directa respectiva al dispositivo portátil. Ventajosamente, el grupo previamente configurado se vuelve a conectar automáticamente después de que el primer dispositivo se haya desconectado.

Opcionalmente, el dispositivo servidor puede ser parte de dos grupos independientes de Wi-Fi directo P2P, un grupo que consiste en los dispositivos del grupo G y otro que consiste en que el dispositivo portátil tiene una conexión P2P con el dispositivo servidor.

Opcionalmente, el dispositivo servidor informa a otros dispositivos en el grupo G del secreto S3 antes de que el dispositivo portátil A se conecte. Ventajosamente, la conexión del dispositivo portátil al grupo, por ejemplo, el procedimiento de acoplamiento se realiza más rápido.

Opcionalmente, el dispositivo servidor admite la operación de grupo persistente directo de Wi-Fi. Opcionalmente, el dispositivo servidor invita a los dispositivos del grupo G a conectarse al dispositivo servidor mediante el procedimiento de invitación a Wi-Fi directo P2P. Opcionalmente, el procedimiento de emparejamiento automatizado se basa en el acceso protegido a Wi-Fi (por ejemplo, WPA o WPA2). Opcionalmente, el procedimiento de emparejamiento automatizado se basa en la configuración simple de Wi-Fi. Opcionalmente, el dispositivo portátil es compatible con la distribución Wi-Fi directo intra-BSS, de modo que los dispositivos inalámbricos en el grupo G aún pueden comunicarse entre sí para realizar una función juntos, sin necesidad de una red troncal. Opcionalmente, el dispositivo portátil es compatible con la operación de agrupación persistente directa de Wi-Fi y utiliza los terceros datos secretos recuperados durante una primera conexión con el grupo a través del segundo dispositivo servidor para conectarse a los dispositivos del subconjunto G' en una conexión posterior. Ventajosamente, estas opciones son extensiones de elementos existentes de dispositivos habilitados para Wi-Fi.

Otras realizaciones preferidas del dispositivo y el método de acuerdo con la invención se dan en las reivindicaciones adjuntas, cuya divulgación se incorpora aquí como referencia.

Breve descripción de los dibujos

Estos y otros aspectos de la invención serán evidentes y se explicarán con más detalle con referencia a las realizaciones descritas a modo de ejemplo en la siguiente descripción y con referencia a los dibujos adjuntos, en los cuales

La Figura 1 muestra un sistema de acoplamiento inalámbrico durante la configuración previa,

La Figura 2 muestra un dispositivo inalámbrico que establece una conexión a un servidor,

La Figura 3 muestra un servidor inalámbrico que da instrucciones a los dispositivos inalámbricos conectados, y

La Figura 4 muestra un dispositivo inalámbrico conectado directamente a otros dispositivos inalámbricos.

Las figuras son puramente diagramáticas y no están dibujadas a escala. En las figuras, los elementos que corresponden a elementos ya descritos pueden tener los mismos números de referencia.

Descripción detallada de realizaciones

Se discute ahora un ejemplo de implementación detallada para un sistema de acoplamiento inalámbrico. El acoplamiento inalámbrico consiste en permitir que los dispositivos portátiles (también llamados acoplados inalámbricos o WDs) se conecten de manera inalámbrica a un grupo de periféricos inalámbricos, de modo que las aplicaciones en el dispositivo portátil puedan hacer uso de estos periféricos para mejorar la experiencia y la productividad de trabajar/interactuar con estas aplicaciones La agrupación de periféricos, el descubrimiento de grupos de periféricos, la gestión de las conexiones a grupos de periféricos, se realiza mediante un denominado servidor de acoplamiento inalámbrico (WDH).

Los posibles acoplados inalámbricos incluyen (pero no se limitan a) teléfonos móviles, ordenadores portátiles, tabletas, reproductores de medios portátiles, cámaras. Los WDHs posibles incluyen (pero no se limitan a) dispositivos de estación de acoplamiento inalámbricos dedicados, dispositivos de visualización, dispositivos de audio, impresoras, PCs. Los posibles periféricos incluyen (pero no se limitan a) ratones inalámbricos, teclados, dispositivos de visualización, dispositivos de audio, cámaras web, impresoras, dispositivos de almacenamiento, concentradores USB. Se considera que estos periféricos son compatibles con estándares tales como Bus en Serie Wi-Fi y Pantalla Wi-Fi para que su funcionalidad esté disponible a través de la red inalámbrica para otros dispositivos tales como acoplados y WDHs. Los periféricos cableados pueden conectarse a la red inalámbrica conectándolos a un dispositivo intermedio a través de cables, y el dispositivo intermedio se puede conectar de forma inalámbrica como se define en este documento, por ejemplo, un dispositivo concentrador USB que admite Bus en Serie Wi-Fi. Los periféricos y acoplados también pueden ser WDHs por sí mismos.

La Figura 1 muestra un sistema de acoplamiento inalámbrico durante la configuración previa. El sistema de acoplamiento inalámbrico tiene un dispositivo H 100 servidor de acoplamiento inalámbrico, y diversos dispositivos periféricos PI... Pn 110, 120, 130, 140 inalámbricos. Todos los dispositivos tienen un transceptor 101, 111 de radio Wi-Fi y soporte para participar en un grupo Wi-Fi P2P directo. Es posible que algunos dispositivos periféricos estén restringidos solo para admitir que actúan como un cliente P2P o un cliente heredado.

La Figura 1 ilustra una situación inicial de configuración previa de un conjunto de periféricos para acoplamiento inalámbrico. Los dispositivos periféricos forman un grupo 190 de dispositivos inalámbricos que están conectados a un dispositivo H 100 servidor a través de conexiones 150 directas Wi-Fi SC1... SCn, que actúa como propietario del grupo (P2P GO) del grupo P2P formado por H y los periféricos PI... Pn actuando como clientes P2P. Para ello, los dispositivos inalámbricos tienen un procesador 112 de comunicaciones respectivo, que se muestra con la función del Cliente P2P. En la práctica, el procesador de comunicaciones de dichos dispositivos inalámbricos y/o dispositivos servidor se conoce como tal y puede implementarse en un circuito integrado dedicado, en un circuito programable y/o en un firmware que se ejecuta en un microcontrolador o un procesador dedicado. Los procesadores de comunicación están dispuestos para ejecutar el proceso de comunicación como se explica a continuación.

La configuración de las conexiones directas Wi-Fi SC1... SCn requiere una etapa de emparejamiento, por ejemplo, utilizando la configuración simple de Wi-Fi (WSC). Durante la etapa de emparejamiento, un secreto S1 común se proporciona por H para establecer una conexión segura con base en el acceso protegido Wi-Fi (WPA/WPA2). El secreto S1 puede ser la frase de contraseña (la clave maestra por pares de Wi-Fi (PMK) o la clave previamente compartida de Wi-Fi (PSK), que se usa en la negociación de cuatro vías para configurar el acceso protegido de Wi-Fi (WPA/WPA2).

Hay diversas posibilidades para distribuir el secreto S1, por ejemplo, el secreto S1 puede distribuirse mediante la configuración simple de Wi-Fi o el secreto S1 puede configurarse previamente en todos los dispositivos relevantes. El dispositivo H servidor de acoplamiento inalámbrico también tiene un procesador 102 de comunicaciones servidor (también denominado administración de acoplamiento inalámbrico) para almacenar la información sobre los

periféricos, hacer un seguimiento de las conexiones, establecer secretos, instruir a otros dispositivos, configurar qué periféricos forman un entorno de acoplamiento inalámbrico.

La Figura 2 muestra un dispositivo inalámbrico que establece una conexión a un servidor. El dispositivo 200 inalámbrico se llama un acoplado D y se muestra en un sistema de acoplamiento inalámbrico similar al de la Figura 1 anterior. El dispositivo inalámbrico tiene un transceptor 201 de radio Wi-Fi y un procesador PROC 202 de comunicaciones para controlar el proceso de comunicación.

En el sistema, el acoplado D inalámbrico establece una conexión C 250 Wi-Fi directo con un servidor H 210 inalámbrico de acoplamiento para acoplarse con un conjunto de periféricos. Este ejemplo de implementación en particular solo muestra la solución mediante la cual el acoplado configura una conexión de acoplamiento inicial (llamada conexión piloto) al servidor H de acoplamiento inalámbrico y no a ninguno de los dispositivos PI... Pn. Se observa que, de manera similar, el acoplado puede configurar la conexión inicial con cualquiera de los dispositivos PI... Pn inalámbricos adicionales, cuando dicho dispositivo inalámbrico está dispuesto para realizar la función de servidor para configurar la conexión inicial. Por lo tanto, las funciones de servidor pueden ser realizadas por un solo dispositivo, o pueden ser distribuidas entre diferentes dispositivos.

Durante la etapa de emparejamiento entre D y H para configurar la conexión C, H se asegura de que, por razones de seguridad, S proporcione un secreto S2 diferente al S1 para establecer una conexión segura con base en el acceso protegido Wi-Fi (WPA/WPA2). Similar a la conexión SC1... SCn con base en los datos S1 secretos como lo indican las líneas 240 de conexión, el secreto S2 es la frase de acceso (la clave maestra por pares de Wi-Fi (PMK) o la clave previamente compartida de Wi-Fi (PSK), que se utiliza en la negociación de cuatro vías para configurar el acceso protegido a Wi-Fi (WPA/WPA2). Existen muchas posibilidades para distribuir el secreto S2, por ejemplo, el secreto S2 puede distribuirse usando la configuración simple de Wi-Fi o el secreto S2 puede ser previamente configurado en todos los dispositivos relevantes. En este ejemplo de implementación, D se conecta al P2P GO de H, por lo que D se convierte automáticamente en cliente P2P. Alternativamente, D y H forman un nuevo grupo P2P, independiente del grupo P2P establecido entre H y los periféricos, por lo que D o H pueden convertirse en P2P GO.

La Figura 3 muestra un servidor inalámbrico que da instrucciones a los dispositivos inalámbricos conectados. Se muestra un servidor H 310 inalámbrico en el sistema de acoplamiento inalámbrico similar a la Figura 1 y la Figura 2 anteriores. La figura ilustra el acoplado D 200 y los periféricos PI... Pn 110,120 que reciben instrucciones del servidor H 310 de acoplamiento inalámbrico.

La figura muestra que H instruye a uno o más periféricos a través de las instrucciones I1... In 320, y también al acoplado a través de la instrucción DI 330, sobre el uso del secreto S3 durante una etapa de emparejamiento automático entre los periféricos y D. Estas instrucciones y mensajes pueden tomar cualquier formato utilizando diversos protocolos de comunicación diferentes, a partir de instrucciones codificadas en binario en cuadros MAC hasta instrucciones codificadas en XML a través de HTTP.

Además de los datos S3 secretos, las instrucciones también pueden incluir información sobre qué acciones deben realizar los dispositivos después de recibirlos, como romper la conexión con H y establecer una conexión con D. Es posible que los periféricos deban proporcionárseles información sobre el identificador de conjunto de servicios SSID que D usará para publicitar sus capacidades de Wi-Fi directo, y es posible que D deba recibir información como identificadores únicos de los periféricos que establecerán una conexión. Uno o más dispositivos periféricos Pi también pueden permanecer conectados a H. Estos dispositivos pueden recibir una instrucción para permanecer conectados a H o desconectarse de H. En la Figura 3, se asume que los dispositivos P3... Pn-1 reciben una instrucción de permanecer conectados a H.

Al usar el canal C, protegido por una clave derivada de los datos S2 secretos, los datos S3 secretos también se envían al acoplado D. Esto significa que D y los uno o más periféricos pueden configurar conexiones protegidas WPA/WPA2 directamente utilizando la negociación de cuatro vías y que no se requiera la ejecución de un procedimiento de configuración simple de Wi-Fi, que implique la posible interacción del usuario para ingresar códigos PIN. No tener que ejecutar el procedimiento de configuración simple de Wi-Fi también acelera el procedimiento de acoplamiento.

La Figura 4 muestra un dispositivo inalámbrico conectado directamente a otros dispositivos inalámbricos. Se muestra un dispositivo D 400 inalámbrico en el sistema de acoplamiento inalámbrico similar a la Figura 1, 2 y 3 anteriores. La Figura ilustra el acoplado D 400 y un subconjunto, por ejemplo, tres periféricos 110, 120, 140, de los periféricos P1... Pn que están directamente conectados, y opcionalmente desconectados, se indican mediante líneas 430 discontinuas a partir del servidor H 100 de acoplamiento inalámbrico. En la Figura 1, un periférico 130 no está conectado al acoplado D y solo permanece conectado al servidor 100 de acoplamiento inalámbrico.

La figura muestra la situación en donde los dispositivos P1, P2 y Pn tienen conexiones SP1, SP2 y SPn directas de configuración con el dispositivo D acoplado, utilizando los datos S3 secretos (frase S3 de contraseña) indicados por 420. D actúa como un propietario de grupo Wi-Fi directo (indicado por la unidad P2P GO 403 en la figura) para SD1, SD2 y SDn. Las conexiones SC1, SC2 y SCn con H pueden liberarse o pueden permanecer activas. Las líneas discontinuas en la Figura 4 reflejan eso. El acoplamiento implica que el acoplado D cambie roles y se convierta en un

P2P GO para el subconjunto de periféricos inalámbricos. Durante la negociación de cuatro vías WPA/WPA2, S3 se puede usar como un secreto común (clave maestra Wi-Fi por pares (PMK) o la clave Wi-Fi previamente compartida (PSK)) para derivar la clave de enlace (clave transitoria por pares). Alternativamente, S3 se usa en el procedimiento de emparejamiento de la configuración protegida de Wi-Fi, donde en lugar de que el usuario ingrese, por ejemplo, un código PIN, el PIN se deriva de S3.

En la práctica, el sistema de acoplamiento inalámbrico anterior se puede aplicar para conectar un acoplado D inalámbrico directamente a un dispositivo de visualización o un ratón/teclado (USB) para reducir la latencia. Los dispositivos pueden recibir instrucciones para utilizar un conjunto de configuración predefinido. Los dispositivos desconectados pueden suspenderse. Opcionalmente, el servidor inalámbrico puede indicarles que se despierten a un intervalo regular en particular para poder descubrirlos y conectarse con ellos nuevamente.

En un sistema de ejemplo, un dispositivo P periférico inalámbrico (por ejemplo, una pantalla Wi-Fi) puede conectarse inicialmente a un servidor H inalámbrico a través de un canal C seguro con base en una clave de enlace (clave transitoria por pares) con base en una frase S1 de contraseña. El servidor actúa como propietario del grupo (GO) y P actúa como cliente. Tanto H como P son compatibles con la agrupación P2P de Wi-Fi directo persistente. A ello, P almacena la frase S1 de contraseña en su memoria. El acoplado D se conecta inicialmente con el servidor H a través de Wi-Fi directo a través de un canal D seguro con una clave de enlace (Clave transitoria por pares) que se basa en la frase S2 de contraseña. A través de un protocolo de configuración de acoplamiento, H le indica al acoplado D que una conexión de carga útil a través de Wi-Fi debe ser aceptada. La conexión directamente con el periférico P se efectúa a través de una unidad de propietario del grupo en D, a la vez que se usa una frase S3 de contraseña para generar una clave de enlace (Clave transitorio por pares) M de acuerdo con lo acordado con el periférico P. H también le indica a P que debe conectarse a los periféricos Ds. GO a la vez que usa la clave de enlace (clave transitoria por pares) M de acuerdo con lo acordado con D. A continuación, P puede desconectar la conexión con H y establecer un enlace con D con la clave de enlace (clave transitoria por pares) M. Si la conexión se interrumpe entre P y D (por ejemplo, si D se desacopla), P puede reconectarse con H usando la frase S1 de contraseña original.

En una realización práctica, el sistema de acoplamiento inalámbrico mejorado tal como se describe anteriormente puede implementarse como sigue. En el ejemplo del sistema de acoplamiento inalámbrico, hay un servidor inalámbrico WDH a través del cual puede acoplarse un dispositivo WD inalámbrico. El WDH está conectado a los periféricos PF a través de interfaces por cable e inalámbricas y también puede tener PFs incorporados. Además, se supone que algunos de los PFs inalámbricos tienen una funcionalidad adicional incorporada para que se les pueda indicar que se conecten directamente a un WD acoplado, o que estén equipados para realizar las funciones de servidor inalámbrico.

Las siguientes ventajas se consiguen mediante el sistema de acoplamiento inalámbrico mejorado. Los PFs se pueden conectar rápidamente a un WD (sin necesidad de ejecutar el protocolo WSC de configuración simple de Wi-Fi) y sin la intervención del usuario. Un WD al que solo se puede acoplar una vez, después de desacoplarlo, ya no está habilitado para volver a conectarse automáticamente con los PFs o WDH con los que se acopló. La comunicación de Wi-Fi entre un WD y el WDH con el que está acoplado está protegida por su privacidad e integridad. Además, otros WDs que pueden haberse acoplado previamente con ese WDH no pueden descifrar esta comunicación o manipularla sin ser detectados. La comunicación Wi-Fi entre un WD y los PFs con los que se conecta directamente durante el acoplamiento está protegida por su privacidad e integridad. Además, otros WDs que se hayan conectado previamente con estos PFs no pueden descifrar esta comunicación o manipularla sin ser detectados. La comunicación entre un WDH y un PF conectado a Wi-Fi está protegida por la privacidad y la integridad. Además, los WDs no pueden descifrar esta comunicación o manipularla sin detección, aunque el WD que está acoplado con este WDH recibirá parte de esta comunicación del WDH y parte de esta comunicación se originó en el WD que está acoplado con este WDH. Un WD que se puede acoplar más de una vez debe realizar WSC solo una vez cuando se acopla por primera vez y puede acoplarse sin usar WSC cuando se acopla de nuevo. Tanto un WD como un WDH pueden configurarse previamente de modo que el WD siempre pueda acoplarse automáticamente.

En el ejemplo del sistema de acoplamiento inalámbrico mejorado, se definen las siguientes fases: fase de preparación (o configuración), modo no acoplado, fase de acoplamiento y fase de desacoplamiento, ya sea controlada o no controlada.

En una fase de configuración, un WDH se configura a sí mismo como un P2P GO para un grupo G1 P2P con SSID SSID1 y frase PP1 de contraseña. El WDH acepta solo PFs para unirse a G1. Diversos PFs se unen a G1 utilizando PBC o WSC-PIN para obtener PP1. Los PFs también pueden configurarse previamente para SSID1 y PP1.

En el modo no acoplado, el WDH se configura a sí mismo como un P2P GO para un grupo G2 P2P con SSID SSID2, pero aún no decide una frase de contraseña para G2. El WDH puede enviar cuadros baliza para G2. El WDH responde a los cuadros de solicitud de sonda. El WDH da información de que es un WDH, en sus PFs, en sus WDEs, etc. en los elementos de información relevantes. El WDH acepta solo WDs para unirse a G2.

En una fase de acoplamiento, un WD que ha descubierto G2 solicita unirse a G2. Esto activa la acción de acoplamiento. Si no se permite el acoplamiento de WD, se rechaza la acción de acoplamiento solicitada. Si el WD ha acoplado antes y si ese WD puede acoplarse nuevamente, el WDH establece como frase PP2 de contraseña para G2 la frase de

contraseña que ha usado antes con ese WD. En todos los demás casos (de manera cuando el WD nunca se acopló antes, o cuando se acopló antes pero solo se pudo acoplar una vez), el WDH genera un nuevo PP2 aleatorio como frase de contraseña para G2. El WDH envía SSID2, PP2, la dirección de WD y el ID de WD a todos los PFs que utilizan el grupo G1 P2P (encriptado con una clave derivada de PP1 y, por lo tanto, se mantiene privado para todos los WDs y todos los demás dispositivos). Si el WD está previamente configurado con una frase de contraseña para este WDH o aún posee una frase de contraseña de una sesión de acoplamiento anterior, puede intentar usar esa frase de contraseña en una negociación de cuatro vías. De lo contrario, o cuando se usa la frase de contraseña antigua, el WD realiza WSC para el grupo G2 P2P con el WDH para obtener PP2. WSC puede usar PBS o WSC-PIN usando el PIN de WD o WDH.

Si después de unirse a G2, no se va a conectar ningún PF directamente al WDH, el WD y el WDH configuran una conexión de carga útil a través del WDH a los PFs y el WD está acoplado.

Si uno o más PFs se van a conectar directamente al WD, el WD intercambia el rol GO con el WDH. El WDH envía las direcciones/IDs de todos los PFs que admiten la configuración de una conexión Wi-Fi directa al WD. Puede excluir las direcciones de PFs para las cuales la conexión de carga útil se encamina mejor a través del WDH por alguna razón. Los llamamos los PFs 'directos'. Todos los demás PFs se denominan PF 'indirectos'. Usando el grupo G1 P2P como medio de comunicación, el WDH le pide a los PFs directos que se unan al grupo G2 P2P usando la frase PP2 de contraseña. Efectivamente, en este ejemplo, los segundos datos secretos son iguales a los terceros datos secretos. Como los PFs directos ya conocen el PP2, no necesitan realizar WSC para unirse a G2, lo que ahorra un tiempo considerable, incluso si, por ejemplo, los PINs son pre-provisionados. Estos PFs simplemente ejecutan la negociación de cuatro vías con el WD utilizando la frase de contraseña que conocen (PP2). El WD ha obtenido las direcciones de los PFs directos involucrados para saber cuáles esperar para la conexión. Tanto el WD, a través de G2, como los PFs, a través de G1, pueden indicar al WDH que las uniones de grupo G2 de P2P han tenido éxito o han fallado. Un PF puede fallar al unirse al grupo G2 P2P, por ejemplo, si la distancia entre el PF y el WD es demasiado grande. Los PFs directos para los cuales falló la unión se convierten en PFs indirectos y permanecen conectados al WDH. El WD configura las conexiones de carga útil directa para los PFs que se han unido con éxito a G2 (es decir, los PFs directos). Estas conexiones de carga útil están protegidas mediante una clave derivada de PP2. El WD y el WDH configuran una conexión de carga útil a través del WDH a los otros PFs (es decir, los PFs indirectos), y el WD está acoplado. Si el WDH admite más de un WD simultáneamente, puede configurar un nuevo SSID para aceptar un nuevo WD para acoplamiento.

En una fase de desacoplamiento, el desacoplamiento se puede realizar de forma controlada o no controlada. El acoplamiento controlado es por el cual el WD le indica al WDH que se desea desacoplar. El desacoplamiento no controlado se produce cuando el WDH detecta de alguna manera que el WD se ha dejado o se ha vuelto inalcanzable sin haber recibido una indicación del WD de que desea desacoplarlo.

Durante el desacoplamiento controlado, cuando un WD quiere desacoplarse, envía un mensaje al WDH utilizando el grupo G2 P2P como medio de comunicación que quiere desacoplar. El WDH reconoce la recepción exitosa de este mensaje. Después de la entrega exitosa de ese mensaje, el WD finalizará la sesión del grupo G2 P2P enviando el WDH y los PFs en los cuadros de desautenticación G2 con el código 3 de razón. Al recibir el cuadro de desautenticación, los PFs eliminan las conexiones de carga útil. Al utilizar el grupo G2 P2P como medio de comunicación, el WDH le indica a los PFs directos que eliminen el PP2 utilizado. Alternativamente, solo puede hacer esto si el WD no puede acoplarse nuevamente. En este caso, los PFs tienen que almacenar las combinaciones de frase de contraseña y WD ID para su uso posterior de los WDs que pueden acoplarse nuevamente. Esto puede ahorrar algo de tiempo durante la operación de acoplamiento. El WDH tiene que hacer un seguimiento de qué PF ha recibido qué frases de contraseña. El WDH instruye a los PFs indirectos para que destruyan las conexiones de carga útil. El WDH asume nuevamente el rol GO del grupo G2 P2P y establece la frase de contraseña como no decidida. El WDH ahora puede anunciar el estado desacoplado de nuevo.

Durante el desacoplamiento no controlado, el WDH de alguna manera decide que el WD se ha ido o se ha vuelto inalcanzable sin haber recibido una indicación del WD de que desea desacoplarlo. El WDH informa a todos los PFs para que destruyan las conexiones de carga útil (directa o indirecta). Al utilizar el grupo G1 P2P como medio de comunicación, el WDH le indica a los PFs directos que eliminen el PP2 utilizado. Alternativamente, solo puede hacer esto si el WD no puede acoplarse nuevamente. En este caso, los PFs tienen que almacenar las combinaciones de frase de contraseña y WD ID para su uso posterior de los WDs que pueden acoplarse nuevamente. Esto puede ahorrar algo de tiempo durante la operación de acoplamiento. El WDH tiene que hacer un seguimiento de qué PF ha recibido qué frases de contraseña. El WDH asume nuevamente el rol GO del grupo G2 P2P y establece la frase de contraseña como no decidida. El WDH ahora puede anunciar el estado desacoplado de nuevo.

Aunque la invención se ha explicado principalmente mediante realizaciones que usan acoplamiento inalámbrico, la invención también es adecuada para cualquier sistema inalámbrico en donde un dispositivo inalámbrico no conectado necesite conectarse a un grupo de dispositivos. La invención es relevante para dispositivos habilitados para acoplamiento de Wi-Fi, dispositivos de bus en serie Wi-Fi, dispositivos con pantalla Wi-Fi y cualquier otro dispositivo compatible con Wi-Fi directo, a partir de dispositivos de audio portátiles, teléfonos móviles, ordenadores portátiles y tabletas hasta Wi-Fi, ratones, teclados, dispositivos de visualización, impresoras, cámaras.

Debe observarse que la invención puede implementarse en hardware y/o software, utilizando componentes programables. Un método para implementar la invención tiene las etapas correspondientes a las funciones definidas para el sistema como se describe con referencia a la Figura 1.

Se apreciará que la descripción anterior para mayor claridad ha descrito realizaciones de la invención con referencia a diferentes unidades y procesadores funcionales. Sin embargo, será evidente que se puede usar cualquier distribución adecuada de funcionalidad entre diferentes unidades o procesadores funcionales sin desviarse de la invención. Por ejemplo, la funcionalidad ilustrada para ser realizada por unidades separadas, procesadores o controladores puede ser realizada por el mismo procesador o controladores. Por lo tanto, las referencias a unidades funcionales específicas solo deben verse como referencias a medios adecuados para proporcionar la funcionalidad descrita en lugar de ser indicativas de una estructura u organización lógica o física estricta. La invención se puede implementar en cualquier forma adecuada que incluya hardware, software, firmware o cualquier combinación de estos.

Se observa que, en este documento, la palabra "que comprende" no excluye la presencia de otros elementos o etapas distintas a las enumerados y la palabra "un" o "una" que precede a un elemento no excluye la presencia de una pluralidad de tales elementos, que cualquier signo de referencia no limite el alcance de las reivindicaciones, que la invención pueda implementarse a través de hardware y software, y que diversos "medios" o "unidades" pueden estar representados por el mismo elemento de hardware o software, y un procesador puede cumplir la función de una o más unidades, posiblemente en cooperación con elementos de hardware. Además, la invención no está limitada a las realizaciones, y la invención está definida por el alcance de las siguientes reivindicaciones.

REIVINDICACIONES

1. Sistema para comunicación inalámbrica que comprende un grupo de dispositivos (110, 120, 130, 140) inalámbricos y un dispositivo (200) portátil, cada dispositivo comprende un transceptor de radio para intercambiar datos de forma inalámbrica con los otros dispositivos,

- un primer dispositivo inalámbrico del grupo con capacidad para una primera función de servidor y un segundo dispositivo inalámbrico del grupo con capacidad para una segunda función de servidor, siendo el primer y segundo dispositivos inalámbricos el mismo dispositivo inalámbrico o diferentes dispositivos inalámbricos;

- el grupo de dispositivos (110, 120, 130, 140) inalámbricos que comparten los primeros datos (240) secretos y están configurados para la comunicación inalámbrica con el primer dispositivo (100) inalámbrico con capacidad para la primera función de servidor a través de las primeras conexiones seguras respectivas con base en los primeros datos (240) secretos;

el dispositivo (200) portátil que comprende un procesador (202) de comunicaciones de dispositivo para

- configurar una segunda conexión segura con el segundo dispositivo (210) inalámbrico que se acomoda a la segunda función de servidor mediante un procedimiento de emparejamiento con base en los segundos datos (250) secretos diferente de los primeros datos (240) secretos,

- recibir una segunda instrucción a través de la segunda conexión segura y, de acuerdo con la segunda instrucción,

- configurar una conexión segura inalámbrica directa respectiva con al menos un dispositivo (110, 120, 140) inalámbrico del grupo usando un procedimiento de emparejamiento respectivo con base en terceros datos (420) secretos, los terceros datos secretos que difieren de los primeros datos (240) secretos;

el segundo dispositivo (210) inalámbrico que aloja la segunda función de servidor que comprende un procesador (102) de comunicaciones de servidor para

- configurar la segunda conexión segura con el dispositivo (200) portátil utilizando el procedimiento de emparejamiento con base en los segundos datos (250) secretos,

- transferir a al menos un dispositivo inalámbrico a través de la primera conexión segura una primera instrucción para aplicar los terceros datos (420) secretos transferidos en la primera instrucción para configurar una conexión segura inalámbrica directa con el dispositivo (200) portátil, y

- transferir al dispositivo (200) portátil a través de la segunda conexión segura (SC) una segunda instrucción para aplicar los terceros datos (420) transferida en la segunda instrucción para configurar la conexión segura inalámbrica directa con al menos un dispositivo inalámbrico con base en el tercer dato (420) secreto;

el al menos un dispositivo inalámbrico que comprende un procesador (112) de comunicaciones para

- recibir la primera instrucción a través de la primera conexión segura y, de acuerdo con la primera instrucción,

- configurar la conexión segura inalámbrica directa respectiva con el dispositivo (200) portátil usando un procedimiento de emparejamiento respectivo con base en los terceros datos (420) secretos.

2. Dispositivo (200) portátil para comunicación inalámbrica para uso en el sistema de acuerdo con la reivindicación 1, el dispositivo comprende un transceptor de radio para intercambiar datos de forma inalámbrica con otros dispositivos inalámbricos,

el dispositivo (200) portátil que comprende un procesador (202) de comunicaciones de dispositivo para

- configurar una segunda conexión segura con un segundo dispositivo (210) inalámbrico con capacidad para una segunda función de servidor utilizando un procedimiento de emparejamiento con base en los segundos datos (250) secretos diferente de los primeros datos (240) secretos;

- recibir una segunda instrucción a través de la segunda conexión segura y, de acuerdo con la segunda instrucción,

- configurar una conexión segura inalámbrica directa respectiva con al menos un dispositivo (110, 120, 140) inalámbrico de un grupo de dispositivos inalámbricos usando un procedimiento de emparejamiento respectivo con base en terceros datos (420) secretos, los terceros datos secretos que difieren de los primeros datos (240) secretos, los terceros datos secretos transferidos en la segunda instrucción.

3. Dispositivo de acuerdo con la reivindicación 2, en donde el procesador (202) de comunicaciones del dispositivo está además dispuesto

- para controlar la comunicación a través de dichas conexiones inalámbricas directas como propietario de un grupo; y/o

- configurar las diferentes conexiones seguras inalámbricas directas respectivas con los respectivos dispositivos inalámbricos de los respectivos subconjuntos diferentes del grupo de dispositivos inalámbricos utilizando un procedimiento de emparejamiento respectivo con base en los respectivos terceros datos secretos, y/o

- generar los terceros datos secretos y transferir los terceros datos secretos al dispositivo con capacidad para la segunda función de servidor.

4. Dispositivo de acuerdo con la reivindicación 2, en donde el procesador (202) de comunicaciones del dispositivo está dispuesto para

- desconectar la segunda conexión segura antes de iniciar la configuración de la conexión segura inalámbrica directa respectiva con al menos un dispositivo inalámbrico; y/o

- proporcionar una agrupación persistente, y en consecuencia para, después de desconectar la conexión segura inalámbrica directa respectiva con base en dichos terceros datos (420) secretos, configurar otra conexión segura inalámbrica directa respectiva con base nuevamente en dichos terceros datos (420) secretos, y/o

- utilizar los segundos datos secretos o los terceros datos secretos adquiridos durante el emparejamiento anterior cuando, después de desconectar la conexión segura inalámbrica directa respectiva con base en dichos terceros datos (420) secretos, volver a conectarse con el al menos un dispositivo inalámbrico para configurar una respectiva conexión segura inalámbrica directa.

5. Dispositivo de acuerdo con la reivindicación 2, en donde

- la segunda conexión segura comprende una conexión Wi-Fi directo P2P, y/o

- la respectiva conexión segura inalámbrica directa comprende una conexión Wi-Fi directo punto a punto, o

- la respectiva conexión segura inalámbrica directa comprende una conexión de configuración de enlace directo tunelizado, y/o

- el procedimiento de emparejamiento comprende un procedimiento de acceso protegido por Wi-Fi o un procedimiento de configuración simple de Wi-Fi.

6. Dispositivo servidor para comunicación inalámbrica para uso en el sistema de acuerdo con la reivindicación 1, comprendiendo el dispositivo

un procesador (102) de comunicaciones servidor para alojar una segunda función de servidor, y

un transceptor de radio para intercambiar datos de forma inalámbrica con otros dispositivos inalámbricos a través de

- configurar una segunda conexión segura con un dispositivo (200) portátil mediante un procedimiento de emparejamiento con base en segundos datos (250) secretos,

- transferir a al menos un dispositivo inalámbrico a través de una primera conexión segura una primera instrucción para aplicar los terceros datos (420) secretos transferidos en la primera instrucción para configurar una conexión segura inalámbrica directa con el dispositivo (200) portátil, y

- transferir al dispositivo (200) portátil a través de la segunda conexión segura una segunda instrucción para aplicar los terceros datos (420) secretos transferidos en la segunda instrucción para configurar la conexión segura inalámbrica directa con al menos un dispositivo inalámbrico con base en los terceros datos (420) secretos.

7. Dispositivo servidor de acuerdo con la reivindicación 6, en donde el procesador (102) de comunicaciones del servidor está dispuesto para

- generar los terceros datos secretos, y/o

- generar un conjunto diferente, respectivo, de los terceros datos secretos para instancias diferentes, respectivas del dispositivo (200) portátil, y/o

- generar un conjunto diferente, respectivo, de los terceros datos secretos cuando el dispositivo (200) portátil, después de haber desconectado la segunda conexión segura, está configurando la segunda conexión segura en un tiempo respectivo, adicional, y/o

- generar un conjunto diferente, respectivo, de los terceros datos secretos para un subconjunto diferente, respectivo de los dispositivos inalámbricos, y/o

- generar los terceros datos secretos con base en, o igual a, los segundos datos secretos.

8. Dispositivo servidor de acuerdo con la reivindicación 6, en donde el procesador de comunicaciones servidor (102) está dispuesto para

- asignar una duración limitada a los terceros datos secretos, y/o

- asignar una vida útil a los terceros datos secretos de acuerdo con el nivel de autorización del dispositivo (200).

9. Dispositivo servidor de acuerdo con la reivindicación 6, en donde el procesador (102) de comunicaciones del servidor está dispuesto para

- transferir una tercera instrucción a al menos un dispositivo inalámbrico para desconectar la primera conexión segura antes de configurar la conexión segura inalámbrica directa respectiva al dispositivo (200) portátil.

10. Dispositivo servidor de acuerdo con la reivindicación 6, en donde el dispositivo servidor es un servidor de acoplamiento inalámbrico o una estación de acoplamiento inalámbrica.

11. Dispositivo (110) inalámbrico para comunicación inalámbrica para uso en el sistema de acuerdo con la reivindicación 1, comprendiendo el sistema un dispositivo (200) portátil y un primer dispositivo inalámbrico de un grupo de dispositivos inalámbricos, el primer dispositivo inalámbrico con capacidad para una primera función de servidor y un segundo dispositivo inalámbrico del grupo con capacidad para una segunda función de servidor, el primero y el segundo dispositivos inalámbricos son el mismo dispositivo inalámbrico o dispositivos inalámbricos diferentes,

el dispositivo inalámbrico comprende

un transceptor de radio para intercambiar datos de forma inalámbrica con el dispositivo portátil y los dispositivos inalámbricos primero y segundo, y

un procesador (112) de comunicaciones para

- recibir una primera instrucción a través de una primera conexión segura con el primer dispositivo inalámbrico y, de acuerdo con la primera instrucción,

- configurar una conexión segura inalámbrica directa con el dispositivo (200) portátil usando un procedimiento de emparejamiento con base en terceros datos (420) secretos, los datos secretos terceros difieren de los primeros datos (240) secretos en donde se basa la primera conexión segura, Los terceros datos secretos que se reciben con la primera instrucción.

12. Dispositivo inalámbrico de acuerdo con la reivindicación 11, en donde el procesador (112) de comunicaciones está dispuesto para

- iniciar la configuración de la conexión segura inalámbrica directa al dispositivo (200) portátil.

13. Dispositivo inalámbrico de acuerdo con la reivindicación 11, en donde el procesador (112) de comunicaciones está dispuesto para

- desconectar la primera conexión segura antes de configurar la conexión segura inalámbrica directa al dispositivo (200) portátil, y/o

- restaurar la primera conexión segura después de desconectar la conexión segura inalámbrica directa al dispositivo (200) portátil.

14. Método de comunicación inalámbrica en un sistema de dispositivos inalámbricos de acuerdo con la reivindicación 1,

el método comprende

- configurar una segunda conexión segura entre un dispositivo (200) portátil y un segundo dispositivo (210) inalámbrico que admite una segunda función de servidor mediante un procedimiento de emparejamiento con base en segundos datos (250) secretos diferente de los primeros datos (240) secretos en donde se basa la primera conexión con un primer dispositivo inalámbrico;

- transferir a al menos un dispositivo inalámbrico de un grupo de dispositivos inalámbricos a través de la primera conexión segura una primera instrucción para aplicar los terceros datos (420) secretos transferido en la primera instrucción para configurar una conexión segura inalámbrica directa con el dispositivo (200) portátil, los terceros datos secretos que difieren de los primeros datos (240) secretos, y

- transferir al dispositivo (200) portátil a través de la segunda conexión segura una segunda instrucción para aplicar los terceros datos (420) secretos transferidos en la segunda instrucción para configurar la conexión segura inalámbrica directa con al menos un dispositivo inalámbrico con base en los terceros datos (420) secretos;

- configurar una conexión segura inalámbrica directa respectiva entre el dispositivo portátil y al menos un dispositivo inalámbrico utilizando un procedimiento de emparejamiento respectivo con base en los terceros datos (420) secretos.

15. Producto de programa informático para la comunicación inalámbrica entre dispositivos inalámbricos, cuyo programa es operativo cuando se ejecuta, para hacer que los procesadores del sistema de la reivindicación 1 realicen el método de acuerdo con la reivindicación 14.

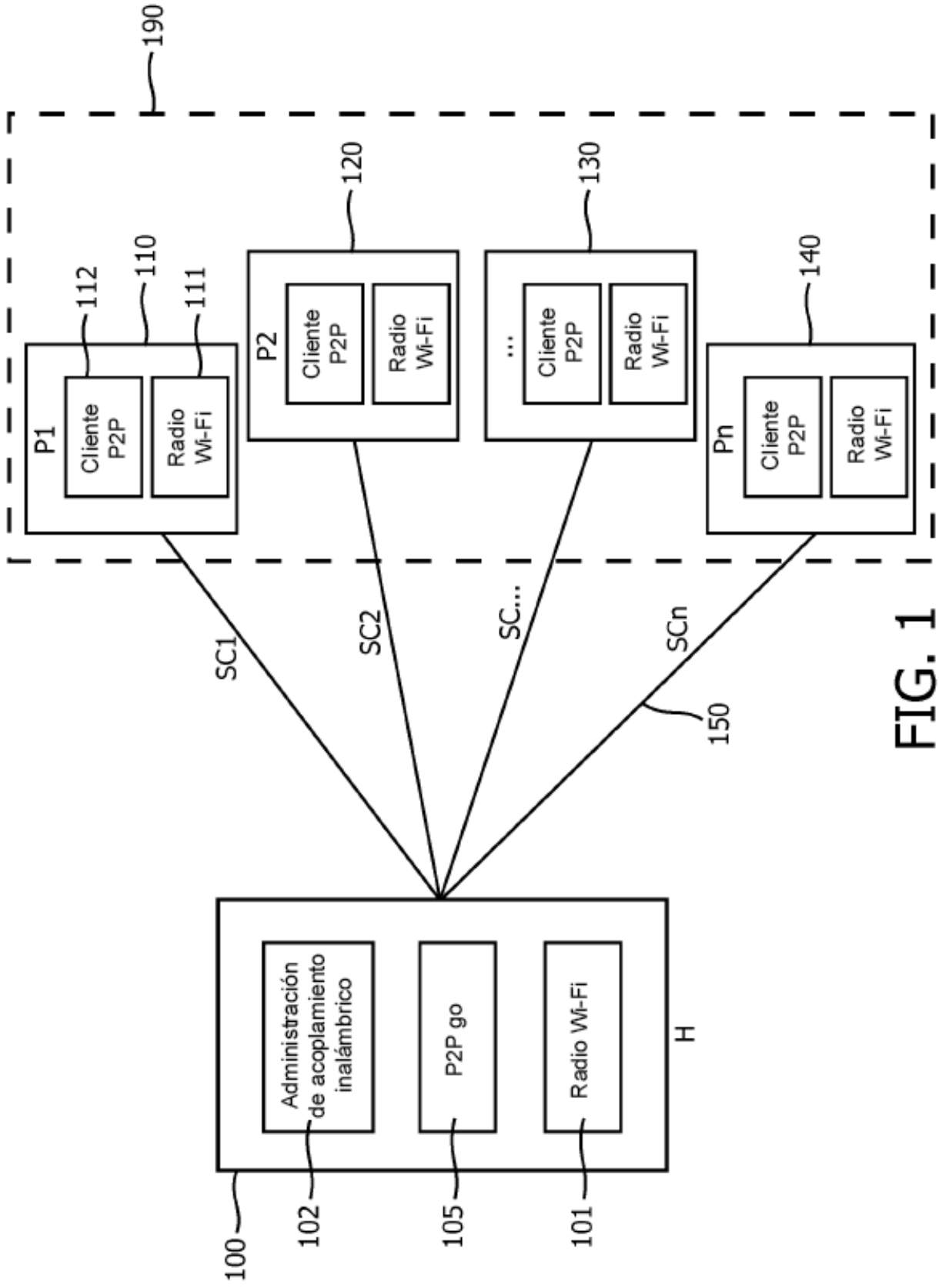
190
120
130
110
112
111
140
P1
Cliente P2P
Radio Wi-Fi
P2
Cliente P2P
Radio Wi-Fi
...
Cliente P2P
Radio Wi-Fi
Pn
Cliente P2P
Radio Wi-Fi
SC1
SC2
SC...
SCn
150
Administración de acoplamiento inalámbrico
P2P go
Radio Wi-Fi
H
100
102
105
101

FIG. 1

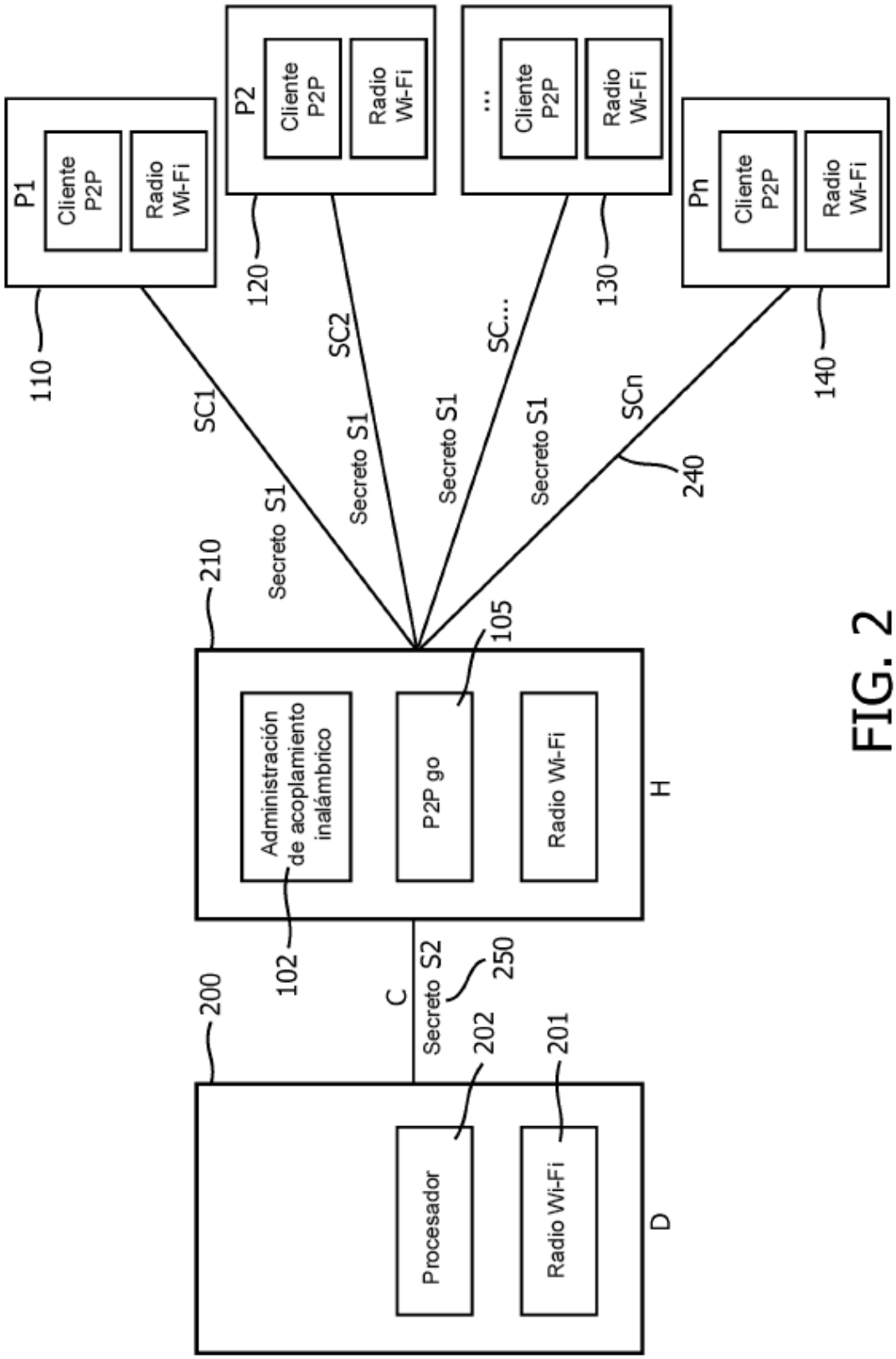
P1
Cliente P2P
Radio Wi-Fi
P2
Cliente P2P
Radio Wi-Fi
...
Cliente P2P
Radio Wi-Fi
Pn
Cliente P2P
Radio Wi-Fi
110
120
130
140
SC1
SC2
SC...
SCn
Secreto S1
Secreto S1
Secreto S1
Secreto S1
240
210
105
Administración de acoplamiento inalámbrico
P2P go
Radio Wi-Fi
H
102
C
Secreto S2
250
200
202
201
Procesador
Radio Wi-Fi
D

FIG. 2

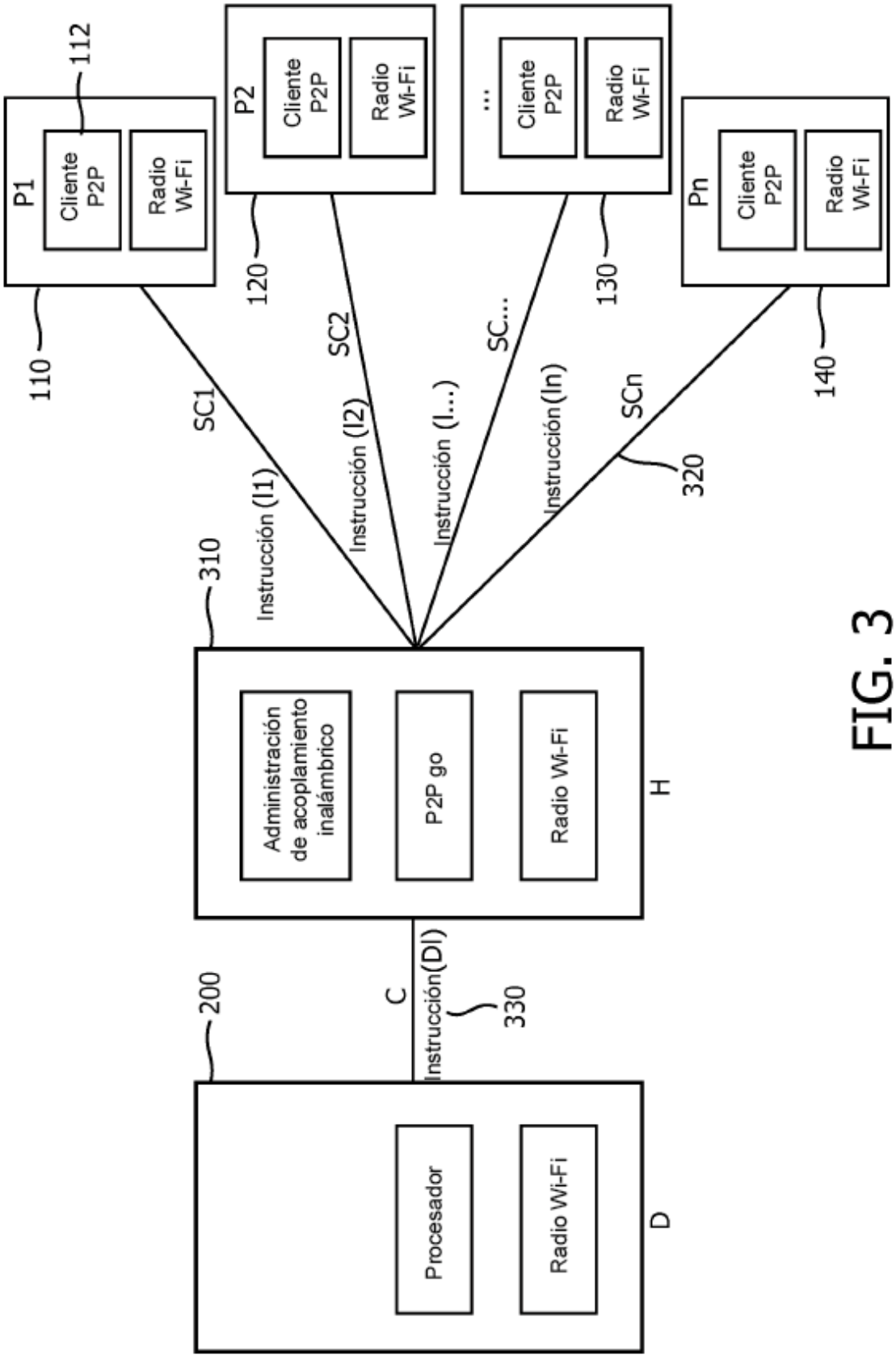
P1
Cliente P2P
Radio Wi-Fi
112
110
P2
Cliente P2P
Radio Wi-Fi
120
...
Cliente P2P
Radio Wi-Fi
130
Pn
Cliente P2P
Radio Wi-Fi
140
SC1
SC2
SC...
SCn
Instrucción (I1)
Instrucción (I2)
Instrucción (I...)
Instrucción (In)
320
310
Administración de acoplamiento inalámbrico
P2P go
Radio Wi-Fi
H
C
Instrucción(DI)
330
200
Procesador
Radio Wi-Fi
D

FIG. 3

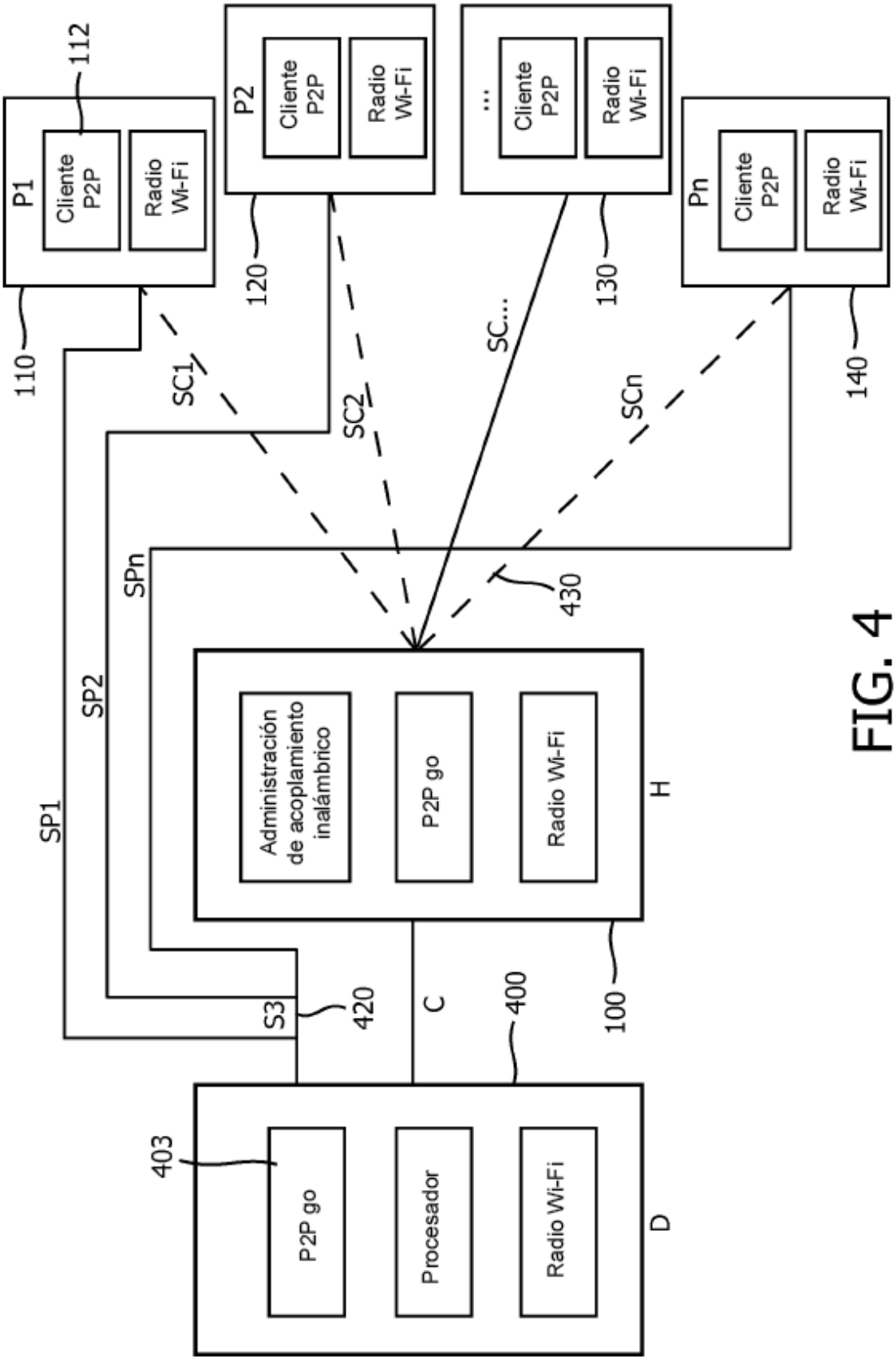
P1
Cliente P2P
Radio Wi-Fi
112
110
P2
Cliente P2P
Radio Wi-Fi
120
...
Cliente P2P
Radio Wi-Fi
130
Pn
Cliente P2P
Radio Wi-Fi
140
SC1
SC2
SC...
SCn
SPn
SP2
SP1
430
Administración de acoplamiento inalámbrico
P2P go
Radio Wi-Fi
H
S3
420
C
400
100
403
P2P go
Procesador
Radio Wi-Fi
D

FIG. 4