(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 670 998**

(51) Int. CI.:

H04L 12/24 (2006.01)
H04L 29/06 (2006.01)
H04L 29/08 (2006.01)
H04M 1/725 (2006.01)
H04W 4/00 (2008.01)
H04W 4/02 (2008.01)
H04W 12/08 (2009.01)
H04W 48/04 (2009.01)
H04W 84/12 (2009.01)
H04W 84/18 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **26.06.2014 PCT/US2014/044371**

(87) Fecha y número de publicación internacional: **31.12.2014 WO14210330**

(96) Fecha de presentación y número de la solicitud europea: **26.06.2014 E 14744225 (5)**

(97) Fecha y número de publicación de la concesión europea: **28.03.2018 EP 3014845**

(54) Título: **Control basado en la presencia del usuario de la comunicación remota con dispositivos de Internet de las Cosas (IoT)**

(30) Prioridad:

26.06.2013 US 201361839815 P
25.06.2014 US 201414314498

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.06.2018

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
5775 Morehouse Drive
San Diego, CA 92121, US

(72) Inventor/es:

GUPTA, BINITA

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Control basado en la presencia del usuario de la comunicación remota con dispositivos de Internet de las Cosas (IoT)

Campo de divulgación

[1] Las realizaciones de esta divulgación se refieren al acceso remoto a dispositivos de IoT y / o a recibir notificaciones remotas desde los dispositivos de IoT. Más en particular, las realizaciones ejemplares están dirigidas a sistemas y procedimientos para inhabilitar o habilitar la comunicación remota, incluyendo acceso remoto a, o servicio remoto de, notificaciones desde dispositivos de IoT, basándose en criterios de comunicación remota, que incluyen su presencia o ausencia, de uno o más usuarios dentro de una red próxima designada de los dispositivos de IoT, entre otros criterios de comunicación remota.

Antecedentes

[2] Internet es un sistema global de ordenadores interconectadas y redes informáticas que utilizan una serie de protocolos de Internet estándar (por ejemplo, el Protocolo de control de transmisión (TCP) y el Protocolo de Internet (IP)) para comunicarse entre sí. Internet de las cosas (IoT, Internet of Things) se basa en la idea de que los objetos cotidianos, no solo los ordenadores y las redes informáticas, pueden ser legibles, reconocibles, localizables, direccionables y controlables a través de una red de comunicaciones de IoT (por ejemplo, un sistema ad-hoc o Internet).

[3] Las tendencias del mercado, relacionadas con mejoras del hogar, por ejemplo, impulsan el desarrollo de nuevos servicios "inteligentes", incluida la consolidación por parte de proveedores de servicios que comercializan juegos "N" (por ejemplo, datos, voz, vídeo, seguridad, gestión energética, etc.) y expanden redes domésticas. Algunas aplicaciones para IoT incluyen hogares inteligentes y edificios capaces de tener control centralizado sobre prácticamente cualquier dispositivo o aparato en el hogar u oficina.

[4] Como tal, en el futuro próximo, el desarrollo creciente en las tecnologías de IoT dará lugar a numerosos dispositivos de IoT que rodean a un usuario en el hogar, en vehículos, en el trabajo y en muchos otros lugares. En una configuración doméstica, por ejemplo, puede haber numerosos dispositivos de IoT dentro de una vecindad designada que estén conectados a la red de Wi-Fi doméstica. Dicha red también puede denominarse "red próxima", en contraste con una red remota, a través de la cual un usuario puede acceder de forma remota a dispositivos de IoT en la red próxima. Más específicamente, cientos de dispositivos de IoT, tales como electrodomésticos, televisores, lámparas, acondicionadores de aire, sistemas de música, puertas de garaje, sistemas de seguridad para el hogar, ventiladores, sistema de rociadores, horno de microondas, horno, lavaplatos, lavadora y secadora de ropa, etc., pueden estar conectado a una red de IoT doméstica próxima. Un usuario puede desear acceder y controlar uno o más de estos dispositivos remotamente desde fuera de la red de IoT doméstica, por ejemplo, desde la oficina del usuario. Por lo tanto, es deseable proporcionar capacidad de acceso remoto a la red de IoT doméstica.

[5] Sin embargo, permitir dicho acceso remoto da lugar a preocupaciones de seguridad. Por ejemplo, habilitar el acceso / control remoto a la red de IoT doméstica de un usuario provoca vulnerabilidad ante las amenazas de seguridad de la red y deja la red de IoT doméstica expuesta a ataques de usuarios no autorizados o agentes maliciosos. Los dispositivos de IoT también se pueden configurar para proporcionar actualizaciones de estado y notificaciones de sucesos importantes al usuario. Sin embargo, si estas notificaciones se proporcionan al usuario cuando el usuario se encuentra en una ubicación remota, por una red a través de la cual es posible la comunicación remota, los usuarios no autorizados pueden obtener acceso a estas notificaciones remotas, lo que también podría generar amenazas de seguridad y privacidad al usuario autorizado.

[6] En consecuencia, existe la necesidad de reducir el riesgo de ataques que pueden surgir al permitir la comunicación remota con dispositivos de IoT.

[7] El documento US 2010/164720 A1 divulga un aparato y un procedimiento para el control de acceso basado en la localización en redes inalámbricas. El documento US 2011/039579 A1 divulga un procedimiento para la comunicación a / desde un terminal multimodal operable para comunicarse mediante múltiples tecnologías de comunicación alternativas.

SUMARIO

[8] La presente invención está definida por el asunto en cuestión de las reivindicaciones independientes 1, 8 y 13. Las realizaciones ejemplares incluyen sistemas y procedimientos relacionados con un SuperAgente / Pasarela de Internet de las cosas (IoT) para controlar la comunicación remota con una red próxima de Internet de las cosas (IoT) que comprende uno o más dispositivos de IoT. Se detecta la presencia de un dispositivo de usuario de IoT en la red próxima de IoT. La comunicación remota se inhabilita si el dispositivo de usuario de IoT está presente en la red próxima de IoT y si se cumplen los criterios de comunicación remota para inhabilitar la comunicación remota. La

comunicación remota está habilitada si el dispositivo de usuario de IoT no está presente en la red próxima de IoT y si se cumplen los criterios de comunicación remota para habilitar la comunicación remota. La comunicación remota incluye el acceso remoto de los uno o más de los dispositivos de IoT por parte del dispositivo de usuario de IoT, así como el servicio remoto de notificaciones de mensajes o sucesos desde los uno o más dispositivos de IoT al dispositivo de usuario de IoT.

[9] Por ejemplo, una realización ejemplar corresponde a un procedimiento para controlar la comunicación remota con una red próxima de Internet de las cosas (IoT) que comprende uno o más dispositivos de IoT, comprendiendo el procedimiento: detectar la presencia de un dispositivo de usuario de IoT en la red próxima de IoT y determinar si se cumplen uno o más criterios de comunicación remota para inhabilitar la comunicación remota con los uno o más dispositivos de IoT en la red próxima de IoT. La comunicación remota se inhabilita si el dispositivo de usuario de IoT está presente en la red próxima de IoT y si se cumplen los criterios de comunicación remota para inhabilitar la comunicación remota.

[10] Otra realización ejemplar se orienta a un procedimiento para controlar la comunicación remota con una red próxima de Internet de las cosas (IoT) que comprende uno o más dispositivos de IoT, comprendiendo el procedimiento: detectar la ausencia de un dispositivo de usuario de IoT en la red próxima de IoT y determinar si se cumplen uno o más criterios de comunicación remota para permitir la comunicación remota con los uno o más dispositivos de IoT en la red próxima de IoT. La comunicación remota se habilita si el dispositivo de usuario de IoT está ausente de la red próxima de IoT y si se cumplen los criterios de comunicación remota para habilitar la comunicación remota.

[11] Otra realización ejemplar más se orienta a un aparato que comprende: un SuperAgente / Pasarela de Internet de las cosas (IoT), configurado para controlar la comunicación remota con una red próxima de IoT que comprende uno o más dispositivos de IoT, un bloque de detección de presencia configurado para detectar si un dispositivo de usuario de IoT está presente en la red próxima de IoT, y un bloque de reglas de control de acceso remoto / servicio remoto, configurado para determinar si se cumplen uno o más criterios de comunicación remota para habilitar o inhabilitar la comunicación remota con los uno o más dispositivos de IoT en la red próxima de IoT. El aparato comprende además un bloque de habilitación / inhabilitación de acceso remoto / servicio remoto, configurado para inhabilitar la comunicación remota si el dispositivo de usuario de IoT está presente en la red próxima de IoT y si se cumplen los criterios de comunicación remota para inhabilitar la comunicación remota.

[12] Otra realización ejemplar más se orienta a un sistema de comunicación que comprende: medios para controlar la comunicación remota con una red próxima de Internet de las cosas (IoT), que comprende uno o más dispositivos de IoT, medios para detectar si un dispositivo de usuario de IoT está presente en la red próxima de IoT, medios para determinar si se cumplen uno o más criterios de comunicación remota para habilitar o inhabilitar la comunicación remota con los uno o más dispositivos de IoT en la red próxima de IoT, y medios para inhabilitar la comunicación remota si el dispositivo de usuario de IoT está presente en la red próxima de IoT y si se cumplen los criterios de comunicación remota para inhabilitar la comunicación remota.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[13] Una apreciación más completa de aspectos de la divulgación y muchas de las ventajas intrínsecas de la misma se obtendrán inmediatamente a medida que la misma se entienda mejor por referencia a la siguiente descripción detallada, cuando se considere en relación con los dibujos adjuntos, que se presentan únicamente para ilustración, y no limitación, de la divulgación, y en los que:

la figura 1 ilustra una arquitectura de sistema de alto nivel de un sistema de comunicaciones inalámbricas de acuerdo a un aspecto de la divulgación.

La figura 2 ilustra un sistema de comunicación inalámbrica ejemplar que comprende una red próxima de IoT capaz de comunicación remota con dispositivos de IoT en la red próxima, de acuerdo a aspectos de esta divulgación.

La figura 3 ilustra aspectos de esta divulgación relativos al control de la comunicación remota con dispositivos de IoT en una red próxima de IoT, basándose en criterios de comunicación remota ejemplares.

Las figuras 4 a 5 ilustran procedimientos ejemplares para controlar la comunicación remota con dispositivos de IoT de una red próxima de IoT basándose en criterios de comunicación remota ejemplares.

DESCRIPCIÓN DETALLADA

[14] Diversos aspectos se divulgan en la siguiente descripción y en los dibujos relacionados para mostrar ejemplos específicos relacionados con realizaciones ejemplares de detección de proximidad entre dispositivos de Internet de las cosas (IoT). Las realizaciones alternativas serán evidentes para los expertos en la técnica pertinente tras leer esta divulgación, y pueden construirse y llevarse a la práctica sin apartarse del alcance de la divulgación.

Además, los elementos bien conocidos no se describirán en detalle, o pueden omitirse, para no ocultar los detalles relevantes de los aspectos y las realizaciones divulgadas en este documento.

[15] La expresión "a modo de ejemplo" se usa en el presente documento para significar "que sirve como ejemplo, caso o ilustración". Cualquier modo de realización descrito en el presente documento como "ejemplar" no ha de interpretarse necesariamente como preferido o ventajoso sobre otros modos de realización. Del mismo modo, el término "modos de realización" no requiere que todos los modos de realización incluyan la característica, ventaja o modalidad de funcionamiento expuesta.

[16] La terminología utilizada en este documento describe realizaciones particulares solamente y solamente debería interpretarse como limitadora de cualquier realización divulgada en este documento. Como se usa en el presente documento, las formas singulares "un", "uno" y "el/la" pretenden incluir asimismo las formas plurales, a menos que el contexto indique claramente lo contrario. Se comprenderá adicionalmente que, cuando se utilizan en el presente documento, los términos “comprende”, "comprendiendo", “incluye” y/o “incluyendo” especifican la presencia de las características, enteros, etapas, operaciones, elementos y/o componentes mencionados, pero no excluyen la presencia o el añadido de una o más de otras características, enteros, etapas, operaciones, elementos, componentes y/o grupos de los mismos.

[17] Además, muchos aspectos se describen en términos de secuencias de acciones a realizar, por ejemplo, por elementos de un dispositivo informático. Se reconocerá que diversas acciones descritas en este documento pueden realizarse mediante circuitos específicos (por ejemplo, un circuito integrado específico de la aplicación (ASIC)), mediante instrucciones de programa que son ejecutadas por uno o más procesadores, o mediante una combinación de ambos. Además, se puede considerar que esta secuencia de acciones, descrita en este documento, está incorporada completamente en cualquier forma de medio de almacenamiento legible por ordenador que tenga almacenado en el mismo un conjunto correspondiente de instrucciones informáticas que, tras la ejecución, provocarían que un procesador asociado realizara la funcionalidad descrita en este documento. Por lo tanto, los diversos aspectos de la divulgación pueden realizarse de varias formas diferentes, todas las cuales se han contemplado como incluidas dentro del alcance del asunto en cuestión reivindicado. Además, para cada uno de los aspectos descritos en este documento, la forma correspondiente de cualquiera de tales aspectos se puede describir en el presente documento como, por ejemplo, "lógica configurada para" llevar a cabo la acción descrita.

[18] Como se usa en este documento, el término "dispositivo de Internet de las cosas" (o "dispositivo de IoT") puede referirse a cualquier objeto (por ejemplo, un aparato, un sensor, etc.) que tiene una interfaz direccionable (por ejemplo, una dirección del protocolo de Internet (IP), un identificador (ID) de Bluetooth, un Identificador de comunicación de campo cercano (NFC), etc.) y que puede transmitir información a uno o más dispositivos por una conexión por cable o inalámbrica. Un dispositivo de IoT puede tener una interfaz de comunicación pasiva, tal como un código de respuesta rápida (QR), una etiqueta de identificación por radiofrecuencia (RFID), una etiqueta NFC o similar, o una interfaz de comunicación activa, tal como un módem, un transceptor, un transmisor-receptor o similar. Un dispositivo de IoT puede tener un conjunto particular de atributos (por ejemplo, un estado o categoría de dispositivo, tal como si el dispositivo de IoT está encendido o apagado, abierto o cerrado, inactivo o activo, disponible para la ejecución de tareas u ocupado, y así sucesivamente; una función de enfriamiento o calentamiento, una función de monitorización o grabación ambiental, una función de emisión de luz, una función de emisión de sonido, etc.) que puede ser integrado en y / o controlado / monitorizado por una unidad central de procesamiento (CPU), un microprocesador, un ASIC o similar, y configurado para la conexión a una red de IoT, tal como una red local ad-hoc o Internet.

[19] Las realizaciones ejemplares pueden pertenecer a dispositivos de IoT a los que se puede acceder de forma remota. El acceso remoto puede estar disponible para dispositivos de IoT que se encuentran dentro del hogar de un usuario o, más generalmente, dentro de cualquier "red próxima", que puede referirse a dispositivos dentro de un límite geográfico predefinido o directamente conectados a una red doméstica. Por ejemplo, un usuario puede ser capaz de monitorizar una cámara de seguridad, operar sistemas de calefacción, refrigeración, aire acondicionado (AC), operar puertas de entrada al hogar, abrir puertas de garaje, etc., desde una ubicación remota o cuando el usuario está lejos de una red doméstica próxima. Además, los dispositivos de IoT también pueden ser capaces de enviar notificaciones de mensajes o sucesos (por ejemplo, que se ha desbloqueado una puerta de patio trasero) al usuario. Tales notificaciones también se pueden proporcionar cuando el usuario se encuentra en una ubicación remota o lejos de casa o en una ubicación próxima predefinida. El envío de tales notificaciones a un usuario en una ubicación remota por un dispositivo de IoT se menciona en el presente documento como "servicio remoto" de las notificaciones o como que las notificaciones son "servidas remotamente", donde las notificaciones incluyen notificaciones de mensajes o sucesos. Más en general, la "comunicación remota", como se expone en este documento, incluye el acceso remoto de uno o más de los dispositivos de IoT en la red próxima de IoT a través de una red remota o medio de comunicación, así como el servicio remoto de notificaciones por uno o más dispositivos de IoT en la red próxima de IoT, transmitidas o difundidas a través de una red remota o medio de comunicación. Dicha comunicación remota puede ser vulnerable o estar expuesta a amenazas de seguridad a través de la red remota o medio de comunicación que permite la comunicación remota.

[20] Como tal, los aspectos ejemplares están orientados a mejorar la seguridad del acceso remoto y / o las

funcionalidades de servicio remoto para una red próxima designada de dispositivos de IoT y reducir la exposición de los dispositivos de IoT a las amenazas a la seguridad. En algunos aspectos, la exposición se reduce al reducir la duración y / o controlar las situaciones cuando se permiten las comunicaciones remotas hacia / desde dispositivos de IoT en la red próxima. Por ejemplo, el acceso remoto y el servicio remota solo pueden permitirse cuando un usuario se encuentra lejos de la red doméstica o próxima. Cuando el usuario se encuentra dentro de la red próxima, puede que no sea necesario que el usuario acceda a los dispositivos de IoT a través de una conexión remota, ya que el usuario puede ser capaz de acceder a los dispositivos de IoT a través de una red local o doméstica. Por lo tanto, la exposición a amenazas externas a través de conexiones remotas puede minimizarse cuando el usuario está en casa, al desconectar por completo el acceso remoto cuando no se requiere acceso remoto. De manera similar, el servicio remoto también puede apagarse cuando el usuario se encuentra dentro de la red doméstica. Por ejemplo, puede evitarse que una notificación de un dispositivo de IoT en cuanto a que una puerta del patio trasero en el hogar del usuario está desbloqueada, o que una ventana del hogar del usuario está rota, se envíe por una red remota, o se preste como servicio remoto, cuando el usuario está en casa.

[21] Por lo tanto, las realizaciones están configuradas para detectar o reconocer la presencia o ausencia de uno o más usuarios dentro de una red próxima y basan la inhabilitación o la habilitación del acceso remoto y del servicio remoto basándose en esta detección o reconocimiento. De esta manera, los dispositivos de IoT dentro de una red doméstica o cualquier otra red próxima designada se pueden proteger de ataques externos al menos durante los momentos en que el acceso remoto y / o el servicio remoto están inhabilitados. En consecuencia, en algunos casos, la presencia de uno o más usuarios primarios en la vecindad o proximidad de una red próxima se puede usar para habilitar o inhabilitar el acceso remoto y / o el servicio remoto. Se proporcionarán varios otros criterios y / o sucesos adicionales o alternativos en esta divulgación como factores ejemplares que pueden usarse para imponer restricciones al acceso remoto y / o al servicio remoto. Los sistemas y procedimientos ejemplares de acuerdo a las realizaciones se describirán ahora con referencia a las figuras.

[22] Con referencia a la FIG. 1, se ilustra una vista de alto nivel de la arquitectura de sistema del sistema de comunicaciones inalámbricas 100, de acuerdo a un aspecto de esta divulgación. El sistema de comunicaciones inalámbricas 100 comprende una pluralidad de dispositivos de IoT, que, como se ilustra, incluyen la televisión 110, la unidad de aire acondicionado (CA) 112, el termostato 114, el refrigerador 116 y la lavadora y secadora 118. Los dispositivos de IoT 110 a 118 están configurados para comunicarse con una red de acceso (por ejemplo, un punto de acceso 125) sobre la interfaz aérea 108 y / o la conexión por cable directo 109. La interfaz aérea 108 puede cumplir con un protocolo de Internet (IP) inalámbrico, tal como IEEE 802.11. Internet 175 incluye un cierto número agentes de encaminamiento y procesamiento (no mostrados en la FIG. 1 por conveniencia) y es un sistema global de ordenadores interconectadas y redes de ordenadores que usa una serie de protocolos de Internet estándar (por ejemplo, el Protocolo de control de transmisión (TCP) e IP) para comunicarse entre dispositivos / redes dispares. En realizaciones ejemplares, el acceso remoto y / o el servicio remoto pueden ser posibles a través de Internet 175, por ejemplo, como se analizará más adelante.

[23] El ordenador 120, tal como un ordenador de escritorio o personal (PC), se muestra como conectándose a Internet 175 directamente (por ejemplo, a través de una conexión de Ethernet o Wi-Fi o una red basada en la norma 802.11). El ordenador 120 puede, alternativamente o adicionalmente, tener una conexión por cable a Internet 175 o el ordenador 120 puede conectarse directamente al punto de acceso 125. Aunque se ilustra como un ordenador de escritorio, el ordenador 120 puede ser un ordenador portátil, una tableta, un PDA, un teléfono inteligente o similares. El ordenador 120 puede ser un dispositivo de IoT y / o contener funcionalidad para gestionar una red / grupo de IoT, tal como la red / grupo de dispositivos de IoT 110 a 118.

[24] El servidor de IoT 170 puede ser optativo, y puede implementarse como una pluralidad de servidores estructuralmente independientes o, alternativamente, puede corresponder a un único servidor. El grupo de dispositivos de IoT 110 a 120 puede ser una red de igual a igual (P2P), y pueden comunicarse entre sí directamente a través de la interfaz aérea 108 y / o la conexión por cable 109. Alternativamente, o adicionalmente, algunos de, o todos, los dispositivos de IoT 110 a 120 pueden configurarse con una interfaz de comunicación independiente de la interfaz de aire 108 y la conexión por cable 109. Por ejemplo, si la interfaz aérea 108 corresponde a una interfaz de Wi-Fi, algunos de los dispositivos de IoT 110 a 120 pueden tener interfaces de Bluetooth o de NFC para comunicarse directamente entre sí o con otros dispositivos habilitados para Bluetooth o NFC.

[25] Además, el sistema 100 de comunicaciones inalámbricas puede incluir un dispositivo controlador 130 que, alternativamente, puede denominarse supervisor o administrador de IoT. Si bien el dispositivo controlador 130 ha sido ilustrado como un dispositivo o unidad independiente, en algunas implementaciones, el dispositivo controlador 130 se puede integrar en uno de los dispositivos de IoT 110 a 120, tal como el ordenador 120. Por ejemplo, el dispositivo controlador 130 puede estar integrado en el ordenador 120, implementado como un teléfono inteligente. En algunos aspectos, el dispositivo controlador 130 puede ser un dispositivo físico o una aplicación de software que se ejecuta en un dispositivo físico. En una realización, el dispositivo controlador 130 generalmente puede observar, monitorizar, controlar o gestionar de otro modo los otros diversos componentes en el sistema de comunicaciones inalámbricas 100. Por ejemplo, el dispositivo controlador 130 puede comunicarse con una red de acceso (por ejemplo, el punto de acceso 125) por la interfaz aérea 108 y / o la conexión directa por cable 109 para interactuar con dispositivos de IoT, donde dicha interacción puede incluir monitorizar o gestionar atributos, actividades u otros

estados asociados a los diversos dispositivos de IoT 110 a 120 en el sistema de comunicaciones inalámbricas 100. La interacción también puede incluir la recepción de notificaciones de sucesos o actualizaciones de estado desde los diversos dispositivos de IoT 110 a 120, que pueden ser servidos remotamente en algunos casos. En realizaciones ejemplares, la red de acceso que incluye la interfaz aérea 108 y / o la conexión por cable directa 109 puede ser parte de una red próxima que comprende los dispositivos de IoT 110 a 120. El dispositivo controlador 130, como se ha mencionado anteriormente, puede ser, o residir en, un teléfono inteligente o dispositivo portátil a través del cual un usuario puede interactuar con los dispositivos de IoT 110 a 120 por la red próxima. Los aspectos del dispositivo controlador 130 también pueden implementarse usando una aplicación de software, tal como, una “App” (aplicación) de teléfono inteligente, que puede incluir una interfaz de usuario.

[26] El dispositivo controlador 130 también puede tener una conexión por cable o inalámbrica a Internet 175 y, optativamente, al servidor de IoT 170 (mostrado como una línea de puntos). El dispositivo controlador 130 puede obtener información de Internet 175 y / o del servidor de IoT 170, que se puede usar para monitorizar o gestionar adicionalmente atributos, actividades u otros estados asociados a los diversos dispositivos de IoT 110 a 120. En realizaciones ejemplares, el dispositivo controlador 130 puede conectarse a Internet 175 desde una ubicación remota que esté espacialmente alejada de la red próxima, por ejemplo, para interactuar con los dispositivos de IoT 110 a 120. Esto puede comprender el acceso remoto de los dispositivos de IoT 110 a 120, así como el servicio remoto desde los dispositivos de IoT 110 a 120. que se describirá adicionalmente con referencia a la FIG. 2.

[27] El sistema de comunicaciones inalámbricas 100 también puede incluir una Pasarela o SuperAgente / Pasarela de IoT 145, que se analizará con más detalle en las siguientes secciones. En breve, el SuperAgente / la Pasarela de IoT 145 puede comunicarse con los dispositivos de IoT 110 a 120 en la red próxima para monitorizarlos y controlarlos, así como recibir notificaciones desde los dispositivos de IoT 110 a 120, donde tales notificaciones pueden ser iniciadas por los dispositivos mismos, basándose en una detección de suceso o un cambio de estado y, como tal, las notificaciones desde el dispositivo de IoT 110 a 120 no necesitan basarse solo en consultas del SuperAgente 145, por ejemplo. La Pasarela o el SuperAgente / la Pasarela de IoT 145 pueden proporcionar interfaces para que un usuario acceda de forma remota a los dispositivos de IoT 110 a 120 y / o para servir notificaciones remotas, por parte de los dispositivos de IoT 110 a 120, a un usuario.

[28] Con referencia a la FIG. 2, se ilustra una realización ejemplar que comprende el sistema de comunicación inalámbrica 200. En general, el sistema de comunicaciones inalámbricas 200 puede incluir diversos componentes que son iguales y / o esencialmente similares al sistema de comunicaciones inalámbricas 100 de la FIG. 1 y, por brevedad y facilidad de descripción, varios detalles relacionados con ciertos componentes en el sistema de comunicaciones inalámbricas 200 pueden omitirse en la presente memoria, en la medida en que ya se hayan proporcionado los mismos, o similares, detalles en relación con el sistema de comunicaciones inalámbricas 100. El sistema de comunicaciones inalámbricas 200 ilustra la red próxima de IoT 160 que incluye un grupo de dispositivos de IoT conectados localmente 110 a 118. Si bien se muestran enlaces de comunicación esquemáticos (que pueden ser cableados o inalámbricos) entre el dispositivo controlador 130 y el dispositivo de IoT 110 a 118, son posibles otras varias comunicaciones de igual a igual entre los dispositivos de IoT 110 a 118, así como con el dispositivo controlador 130, como se conoce en la técnica, pero se han omitido de la ilustración en la presente memoria, en aras de la concisión.

[29] La red próxima 160 puede ser la red doméstica de un usuario en algunos ejemplos. Los dispositivos de IoT 110 a 118 pueden conectarse y / o comunicarse entre sí mediante un SuperAgente / una Pasarela de IoT 145, conectados a Internet 175. El SuperAgente / la Pasarela de IoT 145 puede proporcionar funcionalidad para gestionar y controlar dispositivos de IoT 110 a 118 en la red próxima 160. El SuperAgente / la Pasarela de IoT 145 puede proporcionar funcionalidad para recibir notificaciones desde los dispositivos de IoT 110 a 118 en la red próxima 160, donde, en algunos casos, el SuperAgente / la Pasarela de IoT 145 puede ser capaz de servir remotamente estas notificaciones a un usuario por Internet 175. En algunos aspectos, el dispositivo controlador 130 puede estar ubicado fuera de la red próxima 160 (no ilustrado en la figura 2, pero ilustrado en la figura 3), y el SuperAgente / la Pasarela de IoT 145 también puede proporcionar interfaces para acceder remotamente y controlar los dispositivos de IoT 110 a 118, así como para servir remotamente notificaciones desde los dispositivos de IoT 110 a 118, por ejemplo, a través del dispositivo controlador 130. En aspectos no expuestos aquí en detalle, el SuperAgente / la Pasarela de IoT 145 también pueden ser capaces de comunicarse con, y administrar, uno o más dispositivos de IoT (o, en algunos casos, uno o más grupos de dispositivos de IoT) fuera de la red próxima. En un nivel alto, el dispositivo controlador 130 puede comunicarse desde fuera de la red próxima 160 con el dispositivo de IoT 110 a 118 mediante el SuperAgente / la Pasarela de IoT 145. El SuperAgente / la Pasarela de IoT 145 pueden corresponder a, o incluir, la funcionalidad del punto de acceso 125. Alternativamente, el SuperAgente / la Pasarela de IoT 145 puede corresponder o incluir la funcionalidad de un servidor de IoT, como el servidor de IoT 170. En general, el SuperAgente / la Pasarela de IoT 145 puede encapsular la funcionalidad de pasarela 145, que se expondrá con más detalle con respecto a las realizaciones.

[30] Con referencia a la FIG. 3, se ilustra una vista esquemática simplificada del sistema de comunicación inalámbrica 300, para resaltar ciertos aspectos clave de esta divulgación. En muchos aspectos, el sistema de comunicación inalámbrica 300 es similar a los sistemas de comunicación inalámbrica 100 y 200 de las FIGs. 1 y 2 y, en consecuencia, se omitirá en la presente memoria una descripción detallada de las características comunes, en

aras de la brevedad. En la FIG. 3, el dispositivo controlador 130 se ilustra como un teléfono de usuario, representado en dos ubicaciones separadas: una vez dentro de las proximidades de la red próxima de IoT 160, y una vez en una ubicación remota. Los dispositivos de IoT 301 a 303 son representaciones genéricas de dispositivos de IoT ejemplares, tales como el dispositivo de IoT 110 a 118 en las FIGs. 1 a 2. Los dispositivos de IoT 301 a 303 están ubicados dentro de la red próxima de IoT 160. Los dispositivos de IoT 301 a 303 son capaces de comunicarse entre sí (mostrado en líneas discontinuas) y también pueden comunicarse directamente con el SuperAgente / la Pasarela de IoT 145, así como con el dispositivo controlador / teléfono de usuario 130, mientras el teléfono de usuario 130 se encuentre dentro de la red próxima de IoT 160. En ciertos aspectos, los objetos tales como los dispositivos de IoT 301 a 303 se pueden definir como pertenecientes a la red próxima de IoT 160 si están ubicados físicamente dentro de un límite geográfico predefinido o confines físicos similares. En algunos aspectos, los dispositivos dentro de la red próxima de IoT 160 pueden necesitar ser accesibles y / o controlables desde dispositivos / objetos fuera de la red próxima de IoT 160. Por ejemplo, el usuario puede desear controlar y / o recibir notificaciones desde los dispositivos de IoT 110 a 118 en la red próxima 160, cuando el usuario se encuentra en una ubicación remota, tal como la oficina del usuario. En algunos aspectos, el acceso remoto también puede ser iniciado por el servicio en la nube (que se muestra como parte de Internet 175), en lugar de ser iniciado por el usuario o el teléfono del usuario 130. Para prestar soporte a tales accesos por el usuario o el servicio en la nube, el SuperAgente / la Pasarela de IoT 145 pueden actuar como una pasarela a la red próxima de IoT 160 y proporcionar interfaces para acceder de forma remota a los dispositivos de IoT 110 a 118 y / o para servir remotamente notificaciones del dispositivo de IoT 110 a 118. Sin embargo, para proteger la red próxima de IoT 160 de los ataques, tales como los ataques basados en Internet a través de Internet 175, el SuperAgente / la Pasarela de IoT 145 pueden implementar un conjunto de reglas o imponer que se satisfagan ciertos criterios, basándose en los cuales el acceso remoto y / o el servicio remoto puedan ser habilitados o inhabilitados.

[31] En un aspecto, los criterios pueden estar relacionados con la presencia o ausencia del teléfono de usuario 130 dentro de la red próxima de IoT 160. También son posibles otras diversas reglas o criterios de acceso remoto y servicio remoto, que pueden basarse, por ejemplo, en sucesos o tiempos. Como se expone en este documento, el "acceso" remoto de un dispositivo de IoT dentro de una red próxima por parte de un usuario puede referirse esencialmente a una primera dirección de comunicación iniciada por el usuario (incluso aunque esta comunicación pueda implicar algunas interacciones de ida y vuelta entre el dispositivo de IoT y el usuario). Además, se observará que la primera dirección también incluye comunicación que puede ser iniciada por el servicio en la nube. Sin embargo, en aras de la facilidad de descripción, esta divulgación se centrará en la comunicación iniciada por el usuario, si bien se entenderá que dicha comunicación también puede ser iniciada por el servicio en la nube. Por otro lado, el "servicio remoto" desde un dispositivo de IoT dentro de una red próxima a un usuario puede referirse a una segunda dirección de comunicación contraria, iniciada por el dispositivo de IoT. Colectivamente, estas dos direcciones de comunicación pueden denominarse "comunicación remota", lo que puede incluir el acceso remoto así como el servicio remoto, según sea el caso. De forma correspondiente, los criterios utilizados para habilitar o inhabilitar la comunicación remota (acceso remoto y / o servicio remoto) pueden denominarse criterios de comunicación remota. Varios criterios de comunicación remota en el contexto de la comunicación entre un usuario remoto y dispositivos de IoT en una red próxima se describirán en la presente memoria con referencia a ejemplos y escenarios específicos. Sin embargo, se entenderá que estos ejemplos y escenarios se proporcionan meramente a modo de explicación, y no han de interpretarse como una limitación. Como tal, estos criterios de comunicación remota pueden abarcar cualquier otra regla o criterio que pueda usarse para habilitar o inhabilitar la comunicación remota entre uno o más usuarios y dispositivos de IoT de una red próxima, en función de la presencia o ausencia de los usuarios dentro de la red próxima.

[32] Por consiguiente, en aspectos donde las reglas de acceso remoto pueden basarse en la presencia del usuario, las reglas de acceso remoto pueden implementarse de manera que cuando el teléfono de usuario 130 esté en una ubicación remota, el teléfono de usuario 130 pueda comunicarse o interactuar con el dispositivo de IoT 301 a 303 a través de Internet 175 (por los trayectos 306, 308), mediante el SuperAgente / la Pasarela de IoT 145. Como se ha indicado anteriormente, Internet 175 también puede incluir servicios en la nube, que pueden ser capaces de iniciar la comunicación remota de acuerdo a los aspectos divulgados. El teléfono de usuario 130 puede incluir aplicaciones móviles tales como una aplicación de control que se puede utilizar para controlar los dispositivos de IoT 301 a 303 de forma remota, así como recibir notificaciones remotas desde el dispositivo de IoT 301 a 303. Como se ha expuesto anteriormente, permitir tal acceso remoto y / o servicio remoto puede exponer la red próxima de IoT 160 a amenazas de seguridad de agentes maliciosos o usuarios no autorizados fuera de la red próxima de IoT 160. Es posible que estos ataques se lleven a cabo accediendo a la red próxima de IoT 160 por Internet 175 (por ejemplo, mediante el trayecto 308) y / o atacando la privacidad / seguridad del usuario con el acceso no autorizado de notificaciones desde los dispositivos de IoT 301 a 303 que se sirven remotamente por Internet 175. En consecuencia, el SuperAgente / la Pasarela de IoT 145 puede configurarse para denegar la comunicación remota, por ejemplo, el acceso remoto y / o el servicio remoto, por tales trayectos susceptibles cuando el usuario puede no requerir acceso remoto, por ejemplo, cuando el usuario está presente dentro de la red próxima de IoT 160 y, por lo tanto, puede ser capaz de acceder al dispositivo de IoT 301 a 303 sin depender de Internet 175 para dicho acceso. En aras de la exhaustividad, también se observará que denegar la comunicación remota en este caso significaría que al servicio en la nube, si lo hay, también se le denegará la comunicación remota.

[33] En aspectos relacionados, el SuperAgente / la Pasarela de IoT 145 puede registrar primero el teléfono de

usuario 130, como un usuario autorizado o registrado en el bloque de registro de usuario 310. En algunos casos, esto puede realizarse mediante un registro local (por ejemplo, usando el número de teléfono u otra identidad del teléfono de usuario 130) cuando el teléfono de usuario 130 está presente dentro de la red próxima de IoT 160. La aplicación de control precitada también se puede usar en lugar de, o en combinación con, la identidad del usuario para realizar el registro. El registro puede implicar procesos de autenticación adicionales que serán reconocidos por personas calificadas (por ejemplo, que requieren que el usuario esté conectado a una red doméstica de Wi-Fi y / o que borran las autenticaciones de contraseñas, etc.). Una vez registrado, el teléfono de usuario 130 se almacenará como un usuario autorizado reconocido en el SuperAgente / la Pasarela de IoT 145, por ejemplo, como usuario principal. En este caso, se supone que el teléfono de usuario 130 es el usuario principal.

[34] Aunque no está ilustrado en particular para múltiples usuarios, se apreciará que uno o más dispositivos de usuario pueden registrarse en campos similares. Por ejemplo, los teléfonos móviles de los residentes o un subconjunto de residentes en un hogar pueden registrarse como usuarios autorizados. En algunos casos, los usuarios pueden estar organizados en niveles, con diferentes reglas aplicables a diferentes usuarios según su nivel; por ejemplo, en un hogar convencional, los teléfonos móviles de uno o más padres o adultos pueden registrarse como usuarios principales, mientras que los teléfonos móviles de los niños o los menores pueden registrarse como usuarios secundarios del nivel inferior, de modo que la habilitación / inhabilitación de las comunicaciones remotas puede estar basada en reglas predefinidas asociadas a la designación de un usuario. En otras palabras, basándose en el registro del dispositivo de usuario de IoT en la red próxima de IoT, uno o más criterios de comunicación remota para habilitar o inhabilitar la comunicación remota a la red próxima de IoT 160 pueden incluir designaciones o niveles de prioridad de cada dispositivo de usuario de IoT entre un conjunto de uno o más dispositivos de IoT que son capaces de comunicarse con los dispositivos de IoT en la red próxima de IoT 160. El conjunto de dispositivos de usuario de IoT puede organizarse en niveles según sus registros. Los criterios de comunicación remota pueden definirse de manera que el acceso remoto / servicio remoto para un primer conjunto de uno o más dispositivos de IoT (por ejemplo, calentador de agua, entrada a la puerta principal, horno, etc., no explícitamente ilustrados) esté inhabilitado cuando la presencia de uno o más usuarios principales o de dispositivos de usuario de IoT de alta prioridad se detectan en la red próxima de IoT 160. Sin embargo, la comunicación remota, incluido el acceso remoto / servicio remoto, puede permanecer habilitada para un segundo conjunto de dispositivos de IoT (por ejemplo, Iluminación de dormitorio, no ilustrada explícitamente), para usuarios de otros niveles, tales como usuarios secundarios.

[35] Además, en algunos casos, la inhabilitación de la comunicación remota puede estar relacionada con la inhabilitación selectiva de la capacidad de comunicación remota con respecto a las funcionalidades seleccionadas de los uno o más dispositivos de usuario de IoT. Por ejemplo, con respecto al dispositivo de IoT que comprende un horno, puede ser posible inhabilitar la funcionalidad de encendido / apagado para el horno cuando se detecta que los uno o más usuarios primarios están presentes en la red próxima de IoT 160. Sin embargo, aunque la funcionalidad de encendido / apagado puede inhabilitarse para usuarios secundarios cuando están presentes uno o más usuarios primarios, un subconjunto de funcionalidades del horno puede, no obstante, estar disponible. Este subconjunto de funcionalidades seleccionadas puede ponerse a disposición de los usuarios secundarios, por ejemplo. Por lo tanto, los usuarios secundarios pueden ser capaces de monitorizar si el horno está encendido y qué se está cocinando dentro del horno, incluso cuando los uno o más usuarios primarios están presentes dentro de la red próxima de IoT 160.

[36] Las reglas de control de acceso remoto, así como las reglas correspondientes a cuándo puede permitirse el servicio remoto, pueden personalizarse, definirse de antemano y almacenarse en el bloque representado como las reglas de control de acceso remoto / servicio remoto 314 en el SuperAgente / la Pasarela de IoT 145. También se muestra en la ilustración del SuperAgente / la Pasarela de IoT 145 el bloque de habilitación / inhabilitación de acceso remoto / servicio remoto 312, que se puede configurar para habilitar o inhabilitar el acceso remoto o el servicio remoto de acuerdo a las reglas de control de acceso remoto / servicio remoto, determinadas en el bloque 314.

[37] El bloque de detección de presencia 316 se representa fuera del SuperAgente / la Pasarela de IoT 145, y en comunicación con al menos el bloque de habilitación / inhabilitación de acceso remoto / servicio remoto 312. Se entenderá que no hay ningún requisito para que el bloque de detección de presencia 316 esté físicamente ubicado fuera del SuperAgente / la Pasarela de IoT 145 pero, en algunos aspectos, la funcionalidad del bloque de detección de presencia 316 puede implementarse dentro del SuperAgente / la Pasarela de IoT 145 y, aún más específicamente, fusionarse con uno cualquiera, o más, de los bloques 310 a 314. Esencialmente, el bloque de detección de presencia 316 puede configurarse para detectar la presencia o ausencia de los uno o más usuarios registrados o el teléfono de usuario 130 dentro de la red próxima de IoT 160. El bloque de detección de presencia 316 puede detectar la presencia / ausencia del teléfono de usuario 130 utilizando mecanismos cualesquiera de descubrimiento conocidos, incluyendo, sin limitarse a, detectar la conexión del teléfono de usuario 130 a una red local solo disponible dentro de la red próxima de IoT 160, basándose en una ubicación geográfica del teléfono de usuario 130 (por ejemplo, basándose en sistemas de localización global (GPS)) y / o mediante el descubrimiento de la aplicación de control en el teléfono del usuario 130. En algunos casos, el bloque de detección de presencia 316 puede detectar la presencia / ausencia basándose en el registro del teléfono de usuario 130, por ejemplo, verificando periódicamente si el registro del teléfono de usuario 130 es actual. El teléfono de usuario 130 puede generar un registro periódico en el bloque de registro de usuario 310, que puede usarse para actualizar el bloque de detección

de presencia 316 en cuanto a la presencia del teléfono de usuario 130 dentro de la red próxima de IoT 160. Alternativamente, el bloque de detección de presencia 316 puede generar solicitudes o comandos ping periódicos para el teléfono de usuario 130, de respuesta o confirmación a los comandos ping, o para el refresco periódico del registro, por ejemplo, por la red doméstica. Si un número de umbral de tales comandos ping quedan sin respuesta o se pierden un número de umbral de registros, entonces el bloque de detección de presencia 316 puede deducir que el teléfono de usuario 130 ha abandonado el territorio o las proximidades de la red próxima de IoT 160. El bloque de detección de presencia 316 también puede usar medios indirectos para detectar la presencia del usuario. Por ejemplo, uno de los dispositivos de IoT 301 a 303 puede ser el automóvil del usuario, y la presencia o ausencia del automóvil del usuario puede estar correlacionada con la presencia o ausencia del usuario. De esta manera, las actualizaciones de sucesos / estado desde otros dispositivos de IoT también se pueden usar para detectar la presencia del usuario. En aspectos adicionales, la aplicación de control en el teléfono de usuario 130 puede comunicarse con el bloque de detección de presencia 316 para enterar al bloque de detección de presencia con respecto a la presencia o ausencia (o, en algunos casos, la entrada o salida correspondiente) del teléfono de usuario 130 en la red próxima de IoT 160. El bloque de detección de presencia 316 también puede hacer uso de otras plataformas o mecanismos de descubrimiento para detectar la presencia / ausencia de uno o más usuarios registrados o del teléfono de usuario 130.

[38] En función de si el teléfono de usuario 130 está presente o ausente en la red próxima de IoT 160, según lo detectado por el bloque de detección de presencia 316, por ejemplo, las reglas de control para el acceso remoto / servicio remoto pueden actualizarse en el bloque 314, y el acceso remoto / servicio remoto pueden estar habilitados o inhabilitados en consecuencia en el bloque 312. Una vez más, la actualización de las reglas de control de acceso remoto /servicio remoto en el bloque 314 puede basarse adicionalmente en el registro del usuario, tal como lo proporciona el bloque 310 (por ejemplo, si el usuario específico del teléfono de usuario 130 es un usuario primario cuya presencia / ausencia debería determinar decisiones de habilitación / inhabilitación para la comunicación remota). En algunos aspectos, el mismo conjunto, o un conjunto común, de reglas de control se puede definir para el acceso remoto a los dispositivos de IoT, así como para el servicio remoto de notificación desde los dispositivos de IoT. En otra realización, se pueden definir conjuntos independientes de reglas de control para las características del acceso remoto y del servicio remoto.

[39] Más detalladamente, el bloque de reglas de control de acceso remoto / servicio remoto 314 determinará, basándose en el registro de un usuario, si se permite el acceso remoto / servicio remoto. En un caso, el acceso remoto / servicio remoto solamente puede habilitarse cuando el teléfono de usuario 130 está designado como usuario primario y el teléfono de usuario 130 está ubicado fuera de la red próxima de IoT 160, según lo determinado desde el bloque de detección de presencia 316. De manera similar, el acceso remoto / servicio remoto puede inhabilitarse cuando el teléfono de usuario 130 está designado como usuario principal y el teléfono de usuario 130 está presente dentro de la red próxima de IoT 160, según lo determinado por el bloque de detección de presencia 316. Una vez más, estas actualizaciones de reglas pueden basarse en la hipótesis de que cuando el usuario primario está presente en su hogar, por ejemplo, el acceso remoto a, y / o el servicio remoto desde, los dispositivos de IoT 301 a 303 es innecesario y, por lo tanto, el SuperAgente / la Pasarela de IoT 145 pueden cerrar los trayectos para el acceso remoto y el servicio remoto.

[40] En algunos casos, cuando está presente más de un usuario principal, las reglas de control de acceso remoto / servicio remoto en el bloque 314 se pueden personalizar de varias maneras. Por ejemplo, si hay uno o más dispositivos adicionales de usuario de IoT (tales como el teléfono de usuario 130, pero no mostrados explícitamente) en la red próxima de IoT 160, la habilitación / inhabilitación de la comunicación remota puede basarse en la detección de presencia / ausencia de un subconjunto de, o uno cualquiera entre, la pluralidad de dispositivos de usuario de IoT en la red próxima de IoT 160. Los criterios de comunicación remota que corresponden a cada uno de los uno o más dispositivos de usuario de IoT se pueden configurar individualmente. La inhabilitación / habilitación de la comunicación remota puede basarse en varias combinaciones que implican dispositivos específicos de usuario de IoT y los correspondientes criterios de comunicación remota.

[41] Por ejemplo, el acceso remoto / servicio remoto puede inhabilitarse solo cuando todos los dispositivos de usuario de IoT designados como usuarios principales están dentro de la red próxima de IoT 160 (por ejemplo, cuando ambos progenitores de un hogar están en casa, puede no ser necesario el acceso remoto / servicio remoto y, por lo tanto, se puede inhabilitar). Alternativamente, el acceso remoto / servicio remoto puede inhabilitarse cuando uno cualquiera, o cualquier subconjunto predefinido, de los usuarios principales se encuentran dentro de la red próxima de IoT 160 (por ejemplo, cuando un progenitor está en casa, el acceso remoto / servicio remoto puede ser inhabilitado para el otro progenitor). En otra alternativa más, el acceso remoto / servicio remoto puede habilitarse cuando se detecta que cualquiera de los usuarios primarios está fuera de la red próxima de IoT 160 (por ejemplo, cuando se detecta que uno cualquiera de los dos progenitores ha abandonado el hogar, el acceso remoto / servicio remoto puede ser habilitado). Varias otras alternativas y personalizaciones según las líneas anteriores están dentro del alcance de las realizaciones. En general, la presencia o ausencia de uno o más dispositivos controladores en una red próxima se puede usar como criterio para determinar si se inhabilita o se habilita el acceso remoto / servicio remoto desde dispositivos de IoT en la red próxima.

[42] Si bien las reglas de control de acceso remoto / servicio remoto en el bloque 314 pueden referirse a la

presencia o ausencia del teléfono de usuario 130, de la manera anterior, adicionalmente o alternativamente, las reglas de control de acceso remoto / servicio remoto también pueden referirse a sucesos o funciones cronológicas. Como ejemplo de un suceso que puede usarse para influir en decisiones para habilitar / inhabilitar el acceso remoto / servicio remoto, uno o más dispositivos de IoT 301 a 303 dentro de la red próxima de IoT 160 pueden desencadenar una actualización, tal como una emergencia o falla, que puede ser utilizada junto con otras reglas de control de acceso remoto / servicio remoto. En una ilustración específica, la avería o mal funcionamiento de un dispositivo de IoT, tal como un calentador de agua, puede desencadenar una notificación de emergencia al SuperAgente de IoT 160. En este caso, si el SuperAgente de IoT 160 reconoce que un usuario primario (por ejemplo, un primer usuario primario designado previamente como que requiere acceso remoto en tales situaciones de emergencia) no está dentro de la red próxima de IoT 160, incluso aunque un segundo usuario primario esté presente dentro de la red próxima de IoT 160 (por ejemplo, basándose en la entrada desde el bloque de detección de presencia 316), las reglas de control de acceso remoto / servicio remoto pueden actualizarse en el bloque 314 para instruir al bloque de habilitación / inhabilitación de acceso remoto / servicio remoto 312 para otorgar acceso remoto / habilitar el servicio remoto para el primer usuario primario. Esta actualización de la regla de control de acceso remoto / servicio remoto puede prevalecer sobre reglas de control configuradas previamente (por ejemplo, para habilitar el acceso remoto / servicio remoto solamente cuando están ausentes todos los usuarios primarios). Varias otras personalizaciones de este tipo son posibles en función de los sucesos, sin apartarse del alcance de esta divulgación.

[43] Las reglas de control de acceso remoto / servicio remoto en el bloque 314 también pueden basarse en las horas del día o la semana. Por ejemplo, independientemente de si están o no presentes los usuarios primarios designados en la red próxima de IoT 160, las reglas de control de acceso remoto / servicio remoto en el bloque 314 pueden establecerse de manera que el acceso remoto / servicio remoto se inhabilite durante ciertos períodos de tiempo. Por ejemplo, el acceso remoto / servicio remoto puede apagarse desde las 22:00 hasta las 6:00. En el caso de un entorno de oficina, el acceso remoto / servicio remoto puede apagarse durante el horario comercial durante la semana, y solo habilitarse después del horario comercial o durante el fin de semana, o viceversa, según las preferencias particulares y los requisitos de seguridad. Las reglas de control acceso remoto / servicio remoto en el bloque 314 también se pueden definir basándose en una combinación de presencia / ausencia del usuario y horas del día. Por ejemplo, si un usuario primario determinado de un hogar (por ejemplo, una esposa) está presente dentro de la red próxima de IoT 160, las reglas de control de acceso remoto / servicio remoto pueden corresponder a la inhabilitación del acceso remoto a un dispositivo de IoT, tal como un horno (no se muestra explícitamente), excepto los viernes por la noche entre las 17:00 y las 20:00, cuando es probable que otro usuario principal del hogar (por ejemplo, un esposo) haga funcionar el horno para preparar la cena del viernes por la noche.

[44] Por consiguiente, las realizaciones pueden referirse a controlar la habilitación o inhabilitación del acceso remoto / servicio remoto basándose en la presencia del usuario, las horas del día / semana y / o basándose generalmente en cualquier otra combinación de uno o más de los criterios descritos anteriormente. Los aspectos relacionados de la habilitación del acceso remoto / servicio remoto también pueden estar basados, de manera similar, en la presencia / ausencia del usuario y, optativamente, en criterios adicionales de acceso remoto. Por ejemplo, si se determina que un usuario autorizado (por ejemplo, un usuario primario) no está presente (o se determina que está ausente) en la red próxima de IoT 160, entonces, antes de habilitar el acceso remoto / servicio remoto, ciertos criterios adicionales pueden ser optativamente comprobados en el bloque de reglas de control del acceso remoto / servicio remoto 314. Si estos criterios adicionales también se cumplen, entonces el acceso remoto / servicio remoto puede habilitarse en el bloque 312. En algunos casos, puede no haber criterios adicionales y, si se detecta que el usuario está ausente, se puede habilitar el acceso remoto / servicio remoto.

[45] En algunos aspectos, las reglas de control de acceso remoto / servicio remoto en el bloque 314 también pueden configurarse para definir criterios de comunicación remota de manera diferente para diferentes dispositivos de IoT, basándose en uno o más usuarios primarios que operan los dispositivos de IoT. Por ejemplo, las reglas de control de acceso remoto / servicio remoto pueden configurarse para habilitar el acceso remoto / servicio remoto para dispositivos de IoT tales como un calentador de agua, un sistema HVAC y un sistema de cine en casa (estos dispositivos no se han ilustrado explícitamente) si se ha determinado que un primer usuario primario (por ejemplo, un marido) está ausente de la red próxima de IoT 160. Además, las reglas de control de acceso remoto / servicio remoto pueden configurarse para inhabilitar el acceso remoto / servicio remoto para estos dispositivos de IoT cuando se determina que el primer usuario primario está presente en la red próxima de IoT 160. En otro ejemplo relacionado, las reglas de control de acceso remoto / servicio remoto pueden configurarse para habilitar el acceso remoto / servicio remoto para dispositivos de IoT tales como una lavadora / secadora y un horno (no ilustrado explícitamente), cuando se ha determinado que un segundo usuario principal (por ejemplo, una esposa) está ausente de la red próxima de IoT 160. Además, las reglas de control de acceso remoto / servicio remoto pueden configurarse para inhabilitar el acceso remoto / servicio remoto a estos dispositivos de IoT cuando se determina que el segundo usuario primario está presente en la red próxima de IoT 160. Por consiguiente, las reglas de control de acceso remoto / servicio remoto pueden configurarse de manera tal que uno o más dispositivos de IoT seleccionados estén asociados con un usuario entre uno o más usuarios primarios, y que el acceso remoto / servicio remoto para estos uno o más dispositivos de IoT seleccionados esté habilitado cuando se determina que el usuario primario asociado está ausente de la red próxima de IoT y que su correspondiente acceso remoto / servicio remoto esté inhabilitado cuando se determina que el usuario primario asociado está presente en la red próxima de IoT.

[46] Se apreciará que las realizaciones incluyen diversos procedimientos para realizar los procesos, funciones y / o algoritmos divulgados en este documento. Por ejemplo, como se ilustra en la FIG. 4, una realización puede incluir un procedimiento para controlar el acceso remoto a una red próxima de Internet de las cosas (IoT) (por ejemplo, la red próxima de IoT 160 de la FIG. 3) que comprende uno o más dispositivos de IoT (por ejemplo, los dispositivos de IoT 301 a 303), comprendiendo el procedimiento: detectar la presencia de dispositivos de un usuario de IoT (por ejemplo, usando el bloque de detección de presencia 316 para detectar la presencia / ausencia del teléfono de usuario 130) en la red próxima de IoT - Bloque 402; determinar si se satisfacen uno o más criterios de comunicación remota (por ejemplo, las reglas de control de acceso remoto / servicio remoto del bloque 314) para inhabilitar la comunicación remota con los uno o más dispositivos de IoT en la red próxima de IoT - Bloque 404; e inhabilitar la comunicación remota (por ejemplo, mediante el bloque de habilitación / inhabilitación de acceso remoto / servicio remoto 312 del SuperAgente / la Pasarela de IoT 145) si el dispositivo de usuario de IoT está presente en la red próxima de IoT y si se cumplen los criterios de comunicación remota para inhabilitar la comunicación remota - Bloque 406.

[47] De forma similar, otra realización puede incluir un procedimiento para controlar la comunicación remota con una red próxima de Internet de las cosas (IoT) (por ejemplo, la red próxima de IoT 160 de la FIG. 3) que comprende uno o más dispositivos de IoT (por ejemplo, los dispositivos de IoT 301 a 303), comprendiendo el procedimiento: detectar la ausencia de un dispositivo de usuario de IoT (por ejemplo, usando el bloque de detección de presencia 316 para detectar la presencia / ausencia del teléfono de usuario 130), en la red próxima de IoT - Bloque 502; determinar si se cumplen uno o más criterios de comunicación remota para habilitar la comunicación remota (por ejemplo, mediante las reglas de control de acceso remoto / servicio remoto del bloque 314) con los uno o más dispositivos de IoT en la red próxima de IoT - Bloque 504; y habilitar la comunicación remota si el dispositivo de usuario de IoT está ausente de la red próxima de IoT y si se cumplen los criterios de comunicación remota para habilitar la comunicación remota - Bloque 506.

[48] Generalmente, a menos que se indique explícitamente lo contrario, la frase "lógica configurada para", tal como se usa a lo largo de esta divulgación, pretende invocar un aspecto que está, al menos parcialmente, implementado con hardware, y no pretende correlacionarse con implementaciones solamente de software que son independientes del hardware. Además, se apreciará que la lógica configurada o "lógica configurada para" en los diversos bloques no están limitadas a compuertas o elementos lógicos específicos, sino que generalmente se refieren a la capacidad de realizar la funcionalidad descrita en este documento (ya sea mediante hardware o una combinación de hardware y software). Por lo tanto, las lógicas configuradas o "lógica configurada para", como se ilustra en los diversos bloques, no se implementan necesariamente como compuertas lógicas o elementos lógicos a pesar de compartir la palabra "lógica". Otras interacciones u otra cooperación entre la lógica en los diversos bloques devendrán claras para uno medianamente experto en la materia, a partir de una revisión de los aspectos que se describen a continuación con más detalle.

[49] Los expertos en la técnica apreciarán que la información y las señales pueden representarse usando cualquiera de una variedad de tecnologías y técnicas diferentes. Por ejemplo, los datos, las instrucciones, los comandos, la información, las señales, los bits, los símbolos y los chips que puedan mencionarse a lo largo de la descripción anterior pueden representarse por tensiones, corrientes, ondas electromagnéticas, campos o partículas magnéticos, campos o partículas ópticos o cualquier combinación de los mismos.

[50] Los expertos en la técnica apreciarán además que los diversos bloques lógicos, módulos, circuitos y etapas algorítmicas ilustrativos, descritos en relación con los aspectos divulgados en el presente documento, pueden implementarse como hardware electrónico, software informático o como combinaciones de ambos. Para ilustrar claramente esta intercambiabilidad de hardware y software, se han descrito anteriormente en general varios componentes ilustrativos, bloques, módulos, circuitos y etapas, en términos de su funcionalidad. Que dicha funcionalidad se implemente como hardware o software depende de la aplicación particular y de las limitaciones de diseño impuestas sobre todo el sistema. Los expertos en la técnica pueden implementar la funcionalidad descrita de diversas formas para cada solicitud particular, pero no deberían interpretarse que dichas decisiones de implementación se aparten del alcance de la presente divulgación.

[51] Los diversos bloques lógicos, módulos y circuitos ilustrativos, descritos en relación con los aspectos divulgados en el presente documento, pueden implementarse o realizarse con un procesador de propósito general, un procesador de señales digitales (DSP), un circuito integrado específico de la aplicación (ASIC), una formación de compuertas programables en el terreno (FPGA) u otro dispositivo lógico programable, compuerta discreta o lógica de transistor, componentes de hardware discretos o cualquier combinación de los mismos diseñada para realizar las funciones descritas en el presente documento. Un procesador de propósito general puede ser un microprocesador pero, como alternativa, el procesador puede ser cualquier procesador, controlador, micro-controlador o máquina de estados convencional. Un procesador puede implementarse también como una combinación de dispositivos informáticos, por ejemplo, una combinación de un DSP y de un microprocesador, una pluralidad de microprocesadores, uno o más microprocesadores conjuntamente con un núcleo de DSP o cualquier otra configuración de ese tipo.

[52] Los procedimientos, secuencias y / o algoritmos descritos en relación con los aspectos divulgados en el

presente documento pueden realizarse directamente en hardware, en un módulo de software ejecutado por un procesador o en una combinación de los dos. Un módulo de software puede residir en una memoria RAM, en una memoria flash, en una memoria ROM, en una memoria EPROM, en una memoria EEPROM, en registros, en un disco duro, en un disco extraíble, en un CD-ROM o en cualquier otra forma de medio de almacenamiento conocido en la técnica. Un medio de almacenamiento ejemplar está acoplado al procesador de tal manera que el procesador pueda leer información de, y escribir información en, el medio de almacenamiento. Como alternativa, el medio de almacenamiento puede ser parte integrante del procesador. El procesador y el medio de almacenamiento pueden residir en un ASIC. El ASIC puede residir en un dispositivo de IoT. Como alternativa, el procesador y el medio de almacenamiento pueden residir como componentes discretos en un terminal de usuario.

[53] En uno o más aspectos ejemplares, las funciones descritas pueden implementarse en hardware, software, firmware o cualquier combinación de los mismos. Si se implementan en software, las funciones, como una o más instrucciones o código, pueden almacenarse en, o ser transmitidas por, en un medio legible por ordenador. Los medios legibles por ordenador incluyen tanto medios de almacenamiento informáticos como medios de comunicación, incluyendo cualquier medio que facilite la transferencia de un programa informático de un lugar a otro. Un medio de almacenamiento puede ser cualquier medio disponible al que se pueda acceder por un ordenador. A modo de ejemplo, y no de limitación, tales medios legibles por ordenador pueden comprender RAM, ROM, EEPROM, CD-ROM u otro almacenamiento en disco óptico, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que pueda ser utilizado para llevar o almacenar el código de programa deseado en forma de instrucciones o estructuras de datos, y al que se pueda acceder mediante un ordenador. Además, cualquier conexión se denomina correctamente un medio legible por ordenador. Por ejemplo, si el software es transmitido desde una página de la Red, un servidor o cualquier otro origen remoto, usando un cable coaxial, cable de fibra óptica, par trenzado, DSL o tecnologías inalámbricas, tales como infrarrojos, radio y microondas, entonces el cable coaxial, el cable de fibra óptica, par trenzado, el DSL o las tecnologías sin hilos como los infrarrojos, la radio o las microondas están incluidos en la definición de medio. Los discos, como se usan en el presente documento, incluyen discos compactos (CD), discos de láser, discos ópticos, discos versátiles digitales (DVD), discos flexibles y discos Blu-ray, donde algunos discos normalmente reproducen datos de manera magnética, mientras que otros discos reproducen datos de manera óptica con láser. Las combinaciones de lo que antecede también deberían incluirse dentro del alcance de los medios legibles por ordenador.

[54] Aunque la descripción anterior muestra aspectos ilustrativos de la divulgación, debería observarse que podrían realizarse diversos cambios y modificaciones en la presente memoria sin apartarse del alcance de la divulgación, tal como se define en las reivindicaciones adjuntas. Las funciones, etapas y / o acciones de las reivindicaciones de procedimiento de acuerdo a los aspectos de la divulgación descrita en la presente memoria no necesitan realizarse en ningún orden particular. Además, aunque los elementos de la divulgación pueden describirse o reivindicarse en singular, el plural se contempla a menos que se especifique explícitamente la limitación al singular.

REIVINDICACIONES

1. Un procedimiento para controlar la comunicación remota con una red próxima de Internet de las cosas, IoT (160), que comprende uno o más dispositivos de IoT (110 a 118, 301 a 303), comprendiendo el procedimiento:

detectar (402) la presencia de un dispositivo de usuario de IoT (130) en la red próxima de IoT;

determinar (404) si se cumplen uno o más criterios de comunicación remota para inhabilitar la comunicación remota con los uno o más dispositivos de IoT en la red próxima de IoT; e

inhabilitar (406) la comunicación remota si el dispositivo de usuario de IoT está presente en la red próxima de IoT y si se cumplen los criterios de comunicación remota para inhabilitar la comunicación remota.

2. El procedimiento de la reivindicación 1, en el que la detección de la presencia del dispositivo de usuario de IoT en la red próxima de IoT se basa en una aplicación de control para comunicar la presencia o ausencia del dispositivo de usuario de IoT a un SuperAgente / una Pasarela de IoT (145), sirviendo el SuperAgent / la Pasarela para controlar las comunicaciones remotas en la red próxima de IoT, en donde la aplicación de control se ejecuta en el dispositivo de usuario de IoT.

3. El procedimiento de la reivindicación 1, en el que la detección de la presencia del dispositivo de usuario de IoT en la red próxima de IoT se basa en un refresco periódico del registro del dispositivo de usuario de IoT en un SuperAgente / una Pasarela de IoT, sirviendo el SuperAgente / la Pasarela de IoT para controlar comunicaciones remotas en la red próxima de IoT.

4. El procedimiento de la reivindicación 1, en el que los uno o más criterios de comunicación remota para inhabilitar la comunicación remota a la red próxima de IoT incluyen al menos uno entre: uno o más sucesos o una o más instancias cronológicas.

5. El procedimiento de la reivindicación 1, en el que la inhabilitación de la comunicación remota comprende inhabilitar selectivamente la capacidad de comunicación remota con respecto a funcionalidades seleccionadas de los uno o más dispositivos de usuario de IoT.

6. El procedimiento de la reivindicación 1, que comprende además detectar la presencia de uno o más dispositivos adicionales de usuario de IoT en la red próxima de IoT; e inhabilitar la comunicación remota basándose en la presencia de un subconjunto de uno o más de los dispositivos de usuario de IoT en la red próxima de IoT y criterios de comunicación remota correspondientes a cada uno de los subconjuntos de los uno o más dispositivos de IoT que están presentes en la red próxima de IoT.

7. El procedimiento de la reivindicación 1, en el que los uno o más criterios de comunicación remota para inhabilitar la comunicación remota a la red próxima de IoT incluyen designaciones o niveles de prioridad del dispositivo de usuario de IoT, entre un conjunto de uno o más dispositivos de IoT que son capaces de comunicarse con los dispositivos de IoT en la red próxima de IoT, basándose en un registro del dispositivo de usuario de IoT en la red próxima de IoT.

8. Un procedimiento para controlar la comunicación remota con una red próxima de Internet de las cosas, IoT (160), que comprende uno o más dispositivos de IoT (110 a 118, 301 a 303), comprendiendo el procedimiento:

detectar (502) la ausencia de un dispositivo de usuario de IoT (130) de la red próxima de IoT;

determinar (504) si se cumplen uno o más criterios de comunicación remota para habilitar la comunicación remota con los uno o más dispositivos de IoT en la red próxima de IoT; y

habilitar (506) la comunicación remota si el dispositivo de usuario de IoT está ausente de la red próxima de IoT y si se cumplen los criterios de comunicación remota para habilitar la comunicación remota.

9. El procedimiento de la reivindicación 1 o la reivindicación 8, en el que la comunicación remota comprende el acceso remoto de uno o más de los dispositivos IoT en la red próxima de IoT mediante el dispositivo de usuario de IoT o un servicio en la nube.

10. El procedimiento de la reivindicación 1 o la reivindicación 8, en el que la comunicación remota comprende notificaciones remotas de mensajes o sucesos desde los uno o más de los dispositivos de IoT en la red próxima de IoT al dispositivo de usuario de IoT.

11. El procedimiento de la reivindicación 1 o la reivindicación 8, en el que los criterios de comunicación remota se

basan en una dirección de la comunicación remota.

12. El procedimiento de la reivindicación 8, en el que los uno o más criterios de comunicación remota para habilitar la comunicación remota a la red próxima de IoT incluyen designaciones o niveles de prioridad del dispositivo de usuario de IoT entre un conjunto de uno o más dispositivos de usuario de IoT que son capaces de comunicarse con los dispositivos de IoT en la red próxima de IoT, basándose en un registro del dispositivo de usuario de IoT en la red próxima de IoT.

13. Un sistema de comunicación que comprende:

medios para controlar la comunicación remota con una red próxima de Internet de las cosas, IoT (160), que comprende uno o más dispositivos de IoT (110 a 118, 301 a 303);

medios para detectar (402) si un dispositivo de usuario de IoT está presente en la red próxima de IoT;

medios para determinar (404) si se cumplen uno o más criterios de comunicación remota para inhabilitar la comunicación remota con los uno o más dispositivos de IoT en la red próxima de IoT; y

medios para inhabilitar (406) la comunicación remota si el dispositivo de usuario de IoT está presente dentro de la red próxima de IoT y si se cumplen los criterios de comunicación remota para inhabilitar la comunicación remota.

14. El sistema de comunicación de la reivindicación 13, que comprende además medios para habilitar (506) la comunicación remota si el dispositivo de usuario de IoT no está presente en la red próxima de IoT y si se cumplen los criterios de comunicación remota para habilitar la comunicación remota.

15. El sistema de comunicación de la reivindicación 13, en el que la comunicación remota comprende:

acceso remoto de uno o más de los dispositivos de IoT en la red próxima de IoT por el dispositivo de usuario de IoT o el servicio en la nube; y

servicio remoto de notificaciones de mensajes o sucesos desde los uno o más dispositivos de IoT en la red próxima de IoT al dispositivo de usuario de IoT.

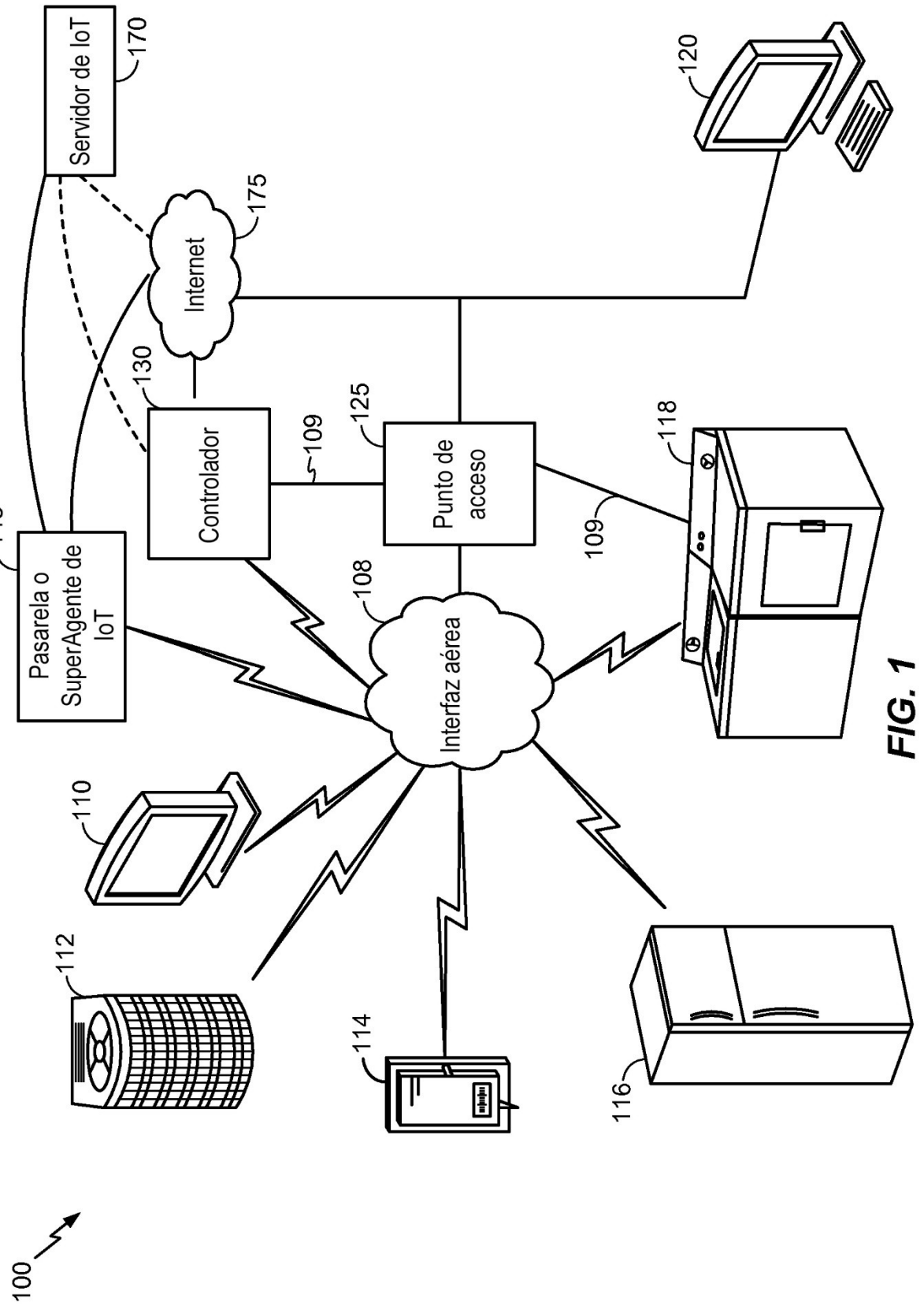
Servidor de IoT
170
120
Internet
175
130
Controlador
109
125
Punto de acceso
118
145
Pasarela o SuperAgente de IoT
108
Interfaz aérea
109
110
112
114
116
100

FIG. 1

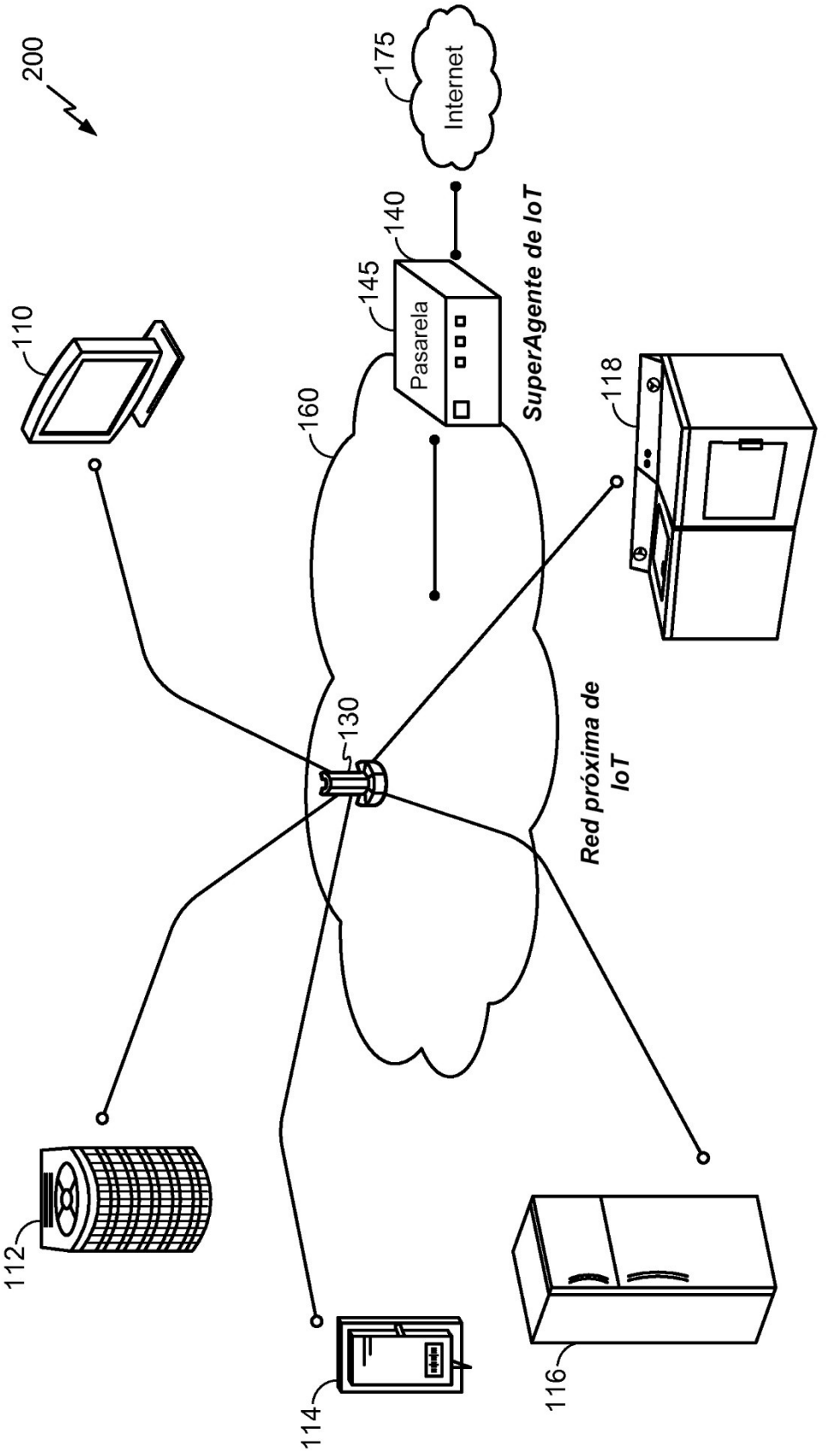
200
175
Internet
140
145
Pasarela
SuperAgente de IoT
110
160
118
130
Red próxima de IoT
112
114
116

FIG. 2

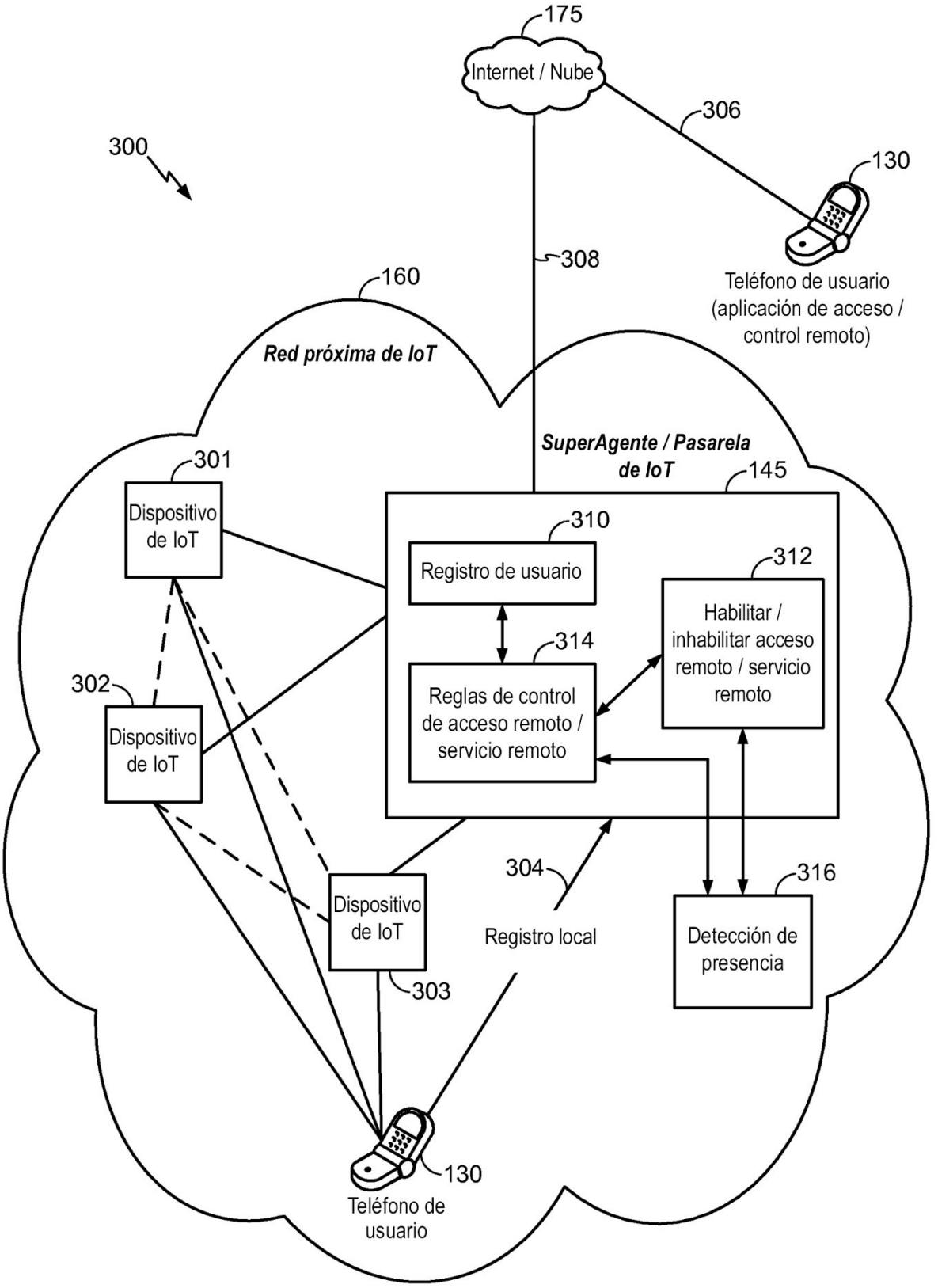
175
Internet / Nube
306
300
130
308
Teléfono de usuario (aplicación de acceso / control remoto)
160
Red próxima de IoT
SuperAgente / Pasarela de IoT
145
301
Dispositivo de IoT
310
Registro de usuario
312
Habilitar / inhabilitar acceso remoto / servicio remoto
314
302
Dispositivo de IoT
Reglas de control de acceso remoto / servicio remoto
304
316
Dispositivo de IoT
Registro local
Detección de presencia
303
130
Teléfono de usuario

FIG. 3

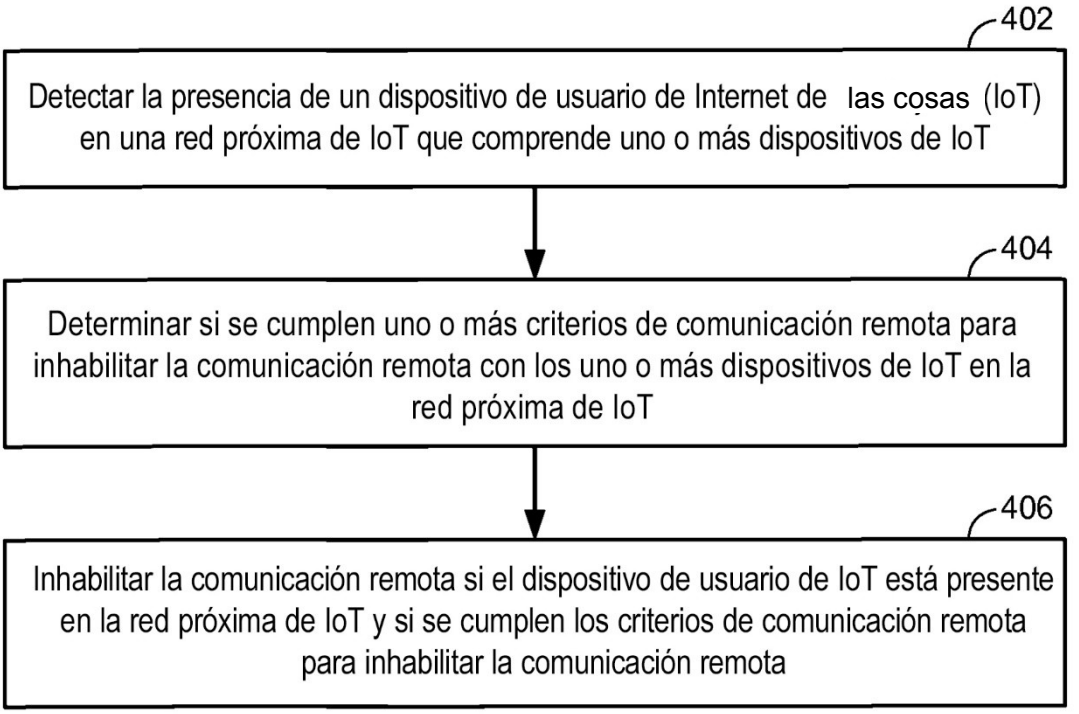
402
Detectar la presencia de un dispositivo de usuario de Internet de las cosas (IoT) en una red próxima de IoT que comprende uno o más dispositivos de IoT
404
Determinar si se cumplen uno o más criterios de comunicación remota para inhabilitar la comunicación remota con los uno o más dispositivos de IoT en la red próxima de IoT
406
Inhabilitar la comunicación remota si el dispositivo de usuario de IoT está presente en la red próxima de IoT y si se cumplen los criterios de comunicación remota para inhabilitar la comunicación remota

FIG. 4

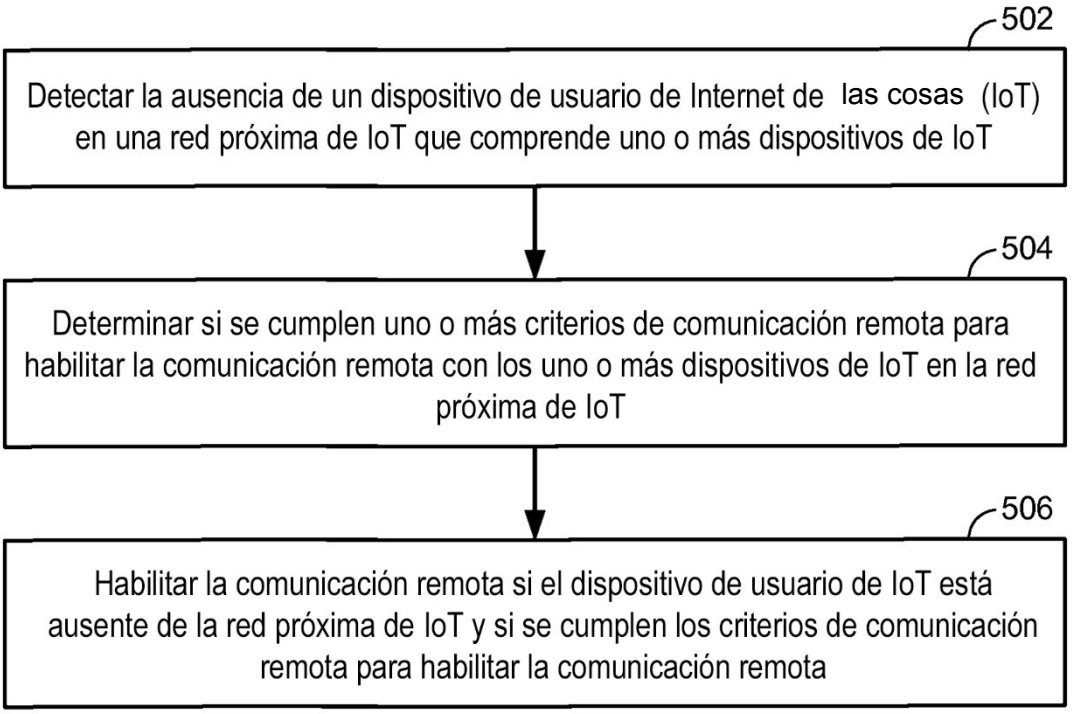
502
Detectar la ausencia de un dispositivo de usuario de Internet de las cosas (IoT) en una red próxima de IoT que comprende uno o más dispositivos de IoT
504
Determinar si se cumplen uno o más criterios de comunicación remota para habilitar la comunicación remota con los uno o más dispositivos de IoT en la red próxima de IoT
506
Habilitar la comunicación remota si el dispositivo de usuario de IoT está ausente de la red próxima de IoT y si se cumplen los criterios de comunicación remota para habilitar la comunicación remota

FIG. 5