(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 800 430**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/06 (2009.01)
H04W 12/08 (2009.01)
H04W 84/12 (2009.01)
H04W 88/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.06.2018 PCT/US2018/040101**

(87) Fecha y número de publicación internacional: **03.01.2019 WO19006175**

(96) Fecha de presentación y número de la solicitud europea: **28.06.2018 E 18755577 (6)**

(97) Fecha y número de publicación de la concesión europea: **18.03.2020 EP 3533247**

(54) Título: **Método de detección de tipo de red inalámbrica y dispositivo electrónico**

(30) Prioridad:

28.06.2017 CN 201710506456

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.12.2020

(73) Titular/es:

ALIBABA GROUP HOLDING LIMITED (100.0%)
Fourth Floor, One Capital Place P.O. Box 847
George Town
Grand Cayman, KY

(72) Inventor/es:

WANG, BAOCHU

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método de detección de tipo de red inalámbrica y dispositivo electrónico

CAMPO TÉCNICO

La presente solicitud se refiere al campo de la tecnología de comunicaciones y, en particular, a un método y aparato de detección de tipo de red inalámbrica, y un dispositivo electrónico.

ANTECEDENTES

Con el desarrollo del Internet móvil, el acceso a una red inalámbrica a través de Wi-Fi se ha vuelto cada vez más frecuente para dispositivos electrónicos. Pero al mismo tiempo, los problemas de seguridad de Wi-Fi se han vuelto cada vez más prominentes. Los dispositivos electrónicos pueden conectarse a puntos de acceso Wi-Fi no seguros, lo que ocasiona filtraciones de información personal, filtraciones de contraseña o robo de cuentas.

Para facilitar las conexiones de usuario y permitir que más usuarios accedan a puntos de acceso Wi-Fi no seguros, la mayoría de los puntos de acceso Wi-Fi no seguros no establecen contraseñas de inicio de sesión. Por lo tanto, actualmente, muchas aplicaciones de herramientas de seguridad verificarán, después de que un dispositivo electrónico se conecte a Wi-Fi, si la Wi-Fi actual requiere una contraseña para la conexión. Si no se requiere contraseña para la conexión, las aplicaciones de herramientas de seguridad bloquearán el acceso del dispositivo electrónico al punto de acceso Wi-Fi o mostrarán un mensaje de seguridad. Sin embargo, en algún momento después de conectarse al punto de acceso Wi-Fi sin contraseña, los usuarios aún deberían tener una verificación de inicio de sesión secundaria. La verificación de inicio de sesión secundaria significa que aunque un dispositivo no necesita una contraseña para conectarse a un punto de acceso Wi-Fi, aparecerá una pantalla de inicio de sesión en el dispositivo al acceder al Internet, requiriendo al usuario que ingrese un nombre de usuario y contraseña para acceder al Internet.

El documento US 2013/155876 da a conocer que se detecta un portal cautivo al consultar un dominio conocido y esperar respuesta. La verificación de conectividad puede solicitar que se incluya un cierto identificador en la respuesta.

RESUMEN

En base a esto, la presente solicitud proporciona un método de detección de tipo de red inalámbrica y un dispositivo electrónico como se especifica en las reivindicaciones.

Opcionalmente, la determinación de si una red inalámbrica actualmente conectada requiere una contraseña para la conexión incluye: llamar a una interfaz de gestión de contraseña de red inalámbrica proporcionada por un sistema operativo, obtener un resultado de llamada y determinar, en base al resultado de la llamada, si la red inalámbrica actualmente conectada requiere una contraseña para la conexión.

Opcionalmente, la dirección de red especificada incluye una dirección de red de una API definida por usuario, y la API se utiliza para devolver información de identificación especificada cuando se accede a la API; y la determinación de si se puede acceder con éxito a la dirección de red especificada incluye: obtener un resultado de acceso al acceder a la dirección de red de la API y determinar, en base a si el resultado de acceso incluye la información de identificación especificada, si se puede acceder con éxito a la dirección de red de la API.

Opcionalmente, la dirección de red especificada incluye direcciones de red de al menos dos páginas web diferentes; y la determinación de si se puede acceder con éxito a la dirección de red especificada incluye: obtener los datos de la página web devueltos después de acceder a una dirección de red de cada una de las páginas web y determinar, comparando los datos de página de las páginas web, si cada una de las páginas web accedidas salta a una página de verificación de inicio de sesión secundaria, para determinar si se puede acceder con éxito a la dirección de red especificada de cada una de las páginas web.

Opcionalmente, los datos de página de la página web incluyen la dirección de red de la página web; y la determinación, al comparar los datos de página de las páginas web, si cada una de las páginas web accedida salta a una página de verificación de inicio de sesión secundaria incluye: actualizar los datos de página de cada una de las páginas web, donde la actualización incluye eliminar la dirección de red incluida en el datos de página de cada una de las páginas web o reemplazar la dirección de red incluida en los datos de página de cada una de las páginas web con datos de identificación unificados; y comparar datos de página actualizados de las páginas web para determinar si los datos de página son los mismos, y determinar, en base a un resultado de comparación, si cada una de las páginas web accedida salta a la página de verificación de inicio de sesión secundaria.

Las soluciones técnicas proporcionadas en las realizaciones de la presente solicitud pueden incluir los siguientes efectos beneficiosos:

En el método de detección de tipo de red inalámbrica en la presente solicitud, después de determinar que la red inalámbrica actualmente conectada no requiere una contraseña para la conexión, se accede a la dirección de red especificada. También se determina si se puede acceder con éxito a la dirección de red especificada. Si se puede acceder a la dirección de red, se puede determinar que la red inalámbrica actualmente conectada es una red inalámbrica sin contraseña. Si no se puede acceder a la dirección de red, se puede determinar que la red inalámbrica requiere una verificación de inicio de sesión secundaria. En las implementaciones de la presente solicitud, se puede determinar con precisión si una red inalámbrica sin contraseña necesita una verificación de inicio de sesión secundaria para la conexión. Por lo tanto, un usuario puede ser advertido con precisión acerca de un riesgo de seguridad de la red inalámbrica, reduciendo la tasa de falsos positivos y la interrupción del usuario.

Debería entenderse que, la descripción general anterior y la siguiente descripción detallada son solo ejemplares y explicativas, y no constituyen limitación en la presente solicitud.

BREVE DESCRIPCIÓN DE LAS FIGURAS

Los dibujos adjuntos incluidos en la presente solicitud constituyen una parte de la presente solicitud, ilustran realizaciones consistentes con la presente solicitud y, junto con la descripción, se utilizan para explicar los principios de la presente solicitud.

La FIG. 1 es un diagrama esquemático que ilustra la conexión a una red inalámbrica a través de Wi-Fi mediante un dispositivo electrónico en una realización ejemplar de la presente solicitud;

la FIG. 2A es un diagrama de flujo que ilustra un método de detección de tipo de red inalámbrica en una realización ejemplar de la presente solicitud;

la FIG. 2B es un diagrama esquemático que ilustra una solución de detección de tipo de red inalámbrica de un dispositivo electrónico en una realización ejemplar de la presente solicitud;

la FIG. 2C es un diagrama de flujo que ilustra un método de detección de tipo de red inalámbrica en una realización ejemplar de la presente solicitud;

la FIG. 2D es un diagrama de flujo que ilustra un método de detección de tipo de red inalámbrica en una realización ejemplar de la presente solicitud;

la FIG. 3 es un diagrama de hardware estructural que ilustra un dispositivo electrónico que incluye un aparato de detección de tipo de red inalámbrica de la presente solicitud; y

la FIG. 4 es un diagrama de bloques que ilustra un aparato de detección de tipo de red inalámbrica en una realización ejemplar de la presente solicitud.

la FIG. 5 es un diagrama de flujo que ilustra un ejemplo de un método implementado por computadora para determinar un tipo de red inalámbrica, de acuerdo con una implementación de la presente divulgación.

DESCRIPCIÓN DE LAS REALIZACIONES

Aquí, se describen en detalle las realizaciones ejemplares y en los dibujos adjuntos se ilustran los ejemplos de las realizaciones ejemplares. Cuando la siguiente descripción se refiere a los dibujos adjuntos, los mismos números en diferentes dibujos adjuntos indican elementos iguales o similares, a menos que se especifique lo contrario. Las implementaciones descritas en las siguientes realizaciones ejemplares no representan todas las realizaciones consistentes con la presente solicitud. En cambio, son meramente ejemplos de aparatos y métodos consistentes con algunos aspectos de la presente solicitud, como se establece en las reivindicaciones adjuntas.

Los términos utilizados en la presente solicitud tienen el mero fin de ilustrar realizaciones específicas y no pretenden limitar la presente solicitud. Los términos “un”, “dicho” y “el” de formas singulares utilizados en la presente solicitud y las reivindicaciones adjuntas de la presente solicitud también pretenden incluir formas plurales, a menos que el contexto indique lo contrario. También debería entenderse que, el término “y/o” utilizado en el presente documento indica e incluye cualquiera o todas las combinaciones posibles de uno o más elementos enumerados asociados.

Debería entenderse que, aunque términos tales como “primero”, “segundo” y “tercero” se utilizan en la presente solicitud para describir diversos tipos de información, la información no debería estar limitada por estos términos. Estos términos se utilizan simplemente para diferenciar información de un mismo tipo. Por ejemplo, sin apartarse del alcance de la presente solicitud, la primera información también puede denominarse segunda información y, de manera similar, la segunda información también puede denominarse primera información. Dependiendo del contexto, la palabra “si” como se utiliza aquí puede interpretarse como “cuando” o “en caso de que... ” o “en respuesta a determinar”.

En las realizaciones de la presente solicitud, Wi-Fi es una tecnología que permite que un dispositivo electrónico se conecte a una red de área local inalámbrica (WLAN), y permite que terminales tales como una computadora personal y un dispositivo portátil (por ejemplo, una PDA o un teléfono móvil) se interconecten de forma inalámbrica entre sí.

Un punto de acceso Wi-Fi es un dispositivo que puede proporcionar un recurso de red compartido y permitir que otros terminales (por ejemplo, un teléfono móvil y o una computadora portátil) se conecten a una red a través de una conexión Wi-Fi. Por ejemplo, si la interconexión de red inalámbrica se puede realizar a través de la conexión Wi-Fi en un área de cobertura efectiva de una onda de radio de un enrutador inalámbrico, el enrutador inalámbrico se denomina un “punto de acceso Wi-Fi”.

Verificación de inicio de sesión secundaria de Wi-Fi: aunque no se requiere una contraseña cuando un dispositivo se conecta a un punto de acceso Wi-Fi, al acceder al Internet, aparecerá una pantalla de inicio de sesión para solicitar al usuario que ingrese un nombre de usuario y contraseña. Este método de conexión de inicio de sesión se denomina “autenticación de inicio de sesión secundaria de Wi-Fi”.

La FIG. 1 es un diagrama esquemático que ilustra la conexión a una red inalámbrica a través de Wi-Fi mediante un dispositivo electrónico en una realización ejemplar de la presente solicitud. Cuando se conecta a un punto de acceso de red inalámbrica, el dispositivo electrónico puede acceder a la red inalámbrica sin utilizar una contraseña. Sin embargo, un usuario necesita ingresar un nombre de usuario y contraseña cuando el dispositivo electrónico accede al Internet a través de la red inalámbrica. Por lo tanto, la red inalámbrica no es un Wi-Fi sin contraseña en un sentido práctico.

La solución de detección de tipo de red inalámbrica en las realizaciones de la presente solicitud, después de determinar que una red inalámbrica actualmente conectada no requiere contraseña para la conexión, se puede acceder además a una dirección de red especificada. También se determina si se puede acceder con éxito a la dirección de red especificada. En caso afirmativo, se puede determinar que la red inalámbrica actualmente conectada es una red inalámbrica sin contraseña. En caso negativo, se puede determinar que la red inalámbrica requiere una verificación de inicio de sesión secundaria. En las realizaciones de la presente solicitud, se puede determinar con precisión si una red inalámbrica sin contraseña necesita una verificación de inicio de sesión secundaria para la conexión. Por lo tanto, un usuario puede ser advertido con precisión acerca de un riesgo de seguridad de la red inalámbrica, reduciendo la tasa de falsos positivos y la interrupción del usuario. Lo siguiente describe en detalle las realizaciones de la presente solicitud.

la FIG. 2A es un diagrama de flujo que ilustra un método de detección de tipo de red inalámbrica en una realización ejemplar de la presente solicitud. El método de detección de tipo de red inalámbrica incluye los siguientes pasos 202 a 206.

Paso 202: Determinar si una red inalámbrica actualmente conectada requiere una contraseña para la conexión.

Paso 204: Después de determinar que no se requiere contraseña, en base a al menos una dirección de red especificada, acceder a la dirección de red especificada.

Paso 206: Determinar, determinando si se puede acceder con éxito a la dirección de red especificada, si la red inalámbrica actualmente conectada requiere verificación de inicio de sesión secundaria.

El método en esta realización se puede aplicar a un dispositivo electrónico configurado con un módulo de red inalámbrica. Por ejemplo, el método se puede aplicar a una aplicación instalada en el dispositivo electrónico. La aplicación puede detectar un tipo de red inalámbrica a la que accede el dispositivo electrónico y proporcionar una advertencia de riesgo de seguridad acerca de la red inalámbrica para un usuario en base a un tipo detectado. El dispositivo electrónico en esta realización puede incluir un teléfono inteligente, una computadora tableta, un asistente digital personal, un reproductor multimedia, etc. Este tipo de dispositivo electrónico está configurado con un módulo de red inalámbrica y puede acceder a una red inalámbrica. La FIG. 2B es un diagrama esquemático que ilustra una solución de detección de tipo de red inalámbrica de un dispositivo electrónico en una realización ejemplar de la presente solicitud.

Cuando un dispositivo electrónico se conecta a una red inalámbrica proporcionada por un enrutador, un dispositivo de puerta de enlace u otro terminal de red, la aplicación puede determinar que el dispositivo electrónico se conecta a la red inalámbrica de varias maneras y determinar si se requiere una contraseña para el acceso. Por ejemplo, si el programa de aplicación tiene el permiso, el dispositivo electrónico puede determinar que el dispositivo electrónico tiene acceso al punto de acceso Wi-Fi de la red inalámbrica comunicándose directamente con el módulo de red inalámbrica o leyendo una interfaz proporcionada por el módulo de red inalámbrica o utilizando otro método. El programa de aplicación también puede determinar si el punto de acceso Wi-Fi de la red inalámbrica accedida requiere una contraseña para la conexión. En otro ejemplo, el programa de aplicación puede tener un permiso y un sistema operativo del dispositivo electrónico proporciona una interfaz, el programa de aplicación puede hacer las determinaciones en base a un resultado de llamada de llamar a la interfaz. En la aplicación práctica, el programa de aplicación puede hacer determinaciones de manera flexible en base a una pluralidad de factores, tal como un sistema

operativo utilizado por el dispositivo electrónico, un permiso del sistema operativo que puede obtener un proveedor de aplicaciones y una interfaz proporcionada por el sistema operativo.

En un método de implementación opcional, la determinación de si una red inalámbrica actualmente conectada requiere una contraseña para la conexión incluye: llamar a una interfaz de gestión de contraseña de red inalámbrica proporcionada por un sistema operativo, obtener un resultado de llamada y determinar, en base al resultado de la llamada, si la red inalámbrica actualmente conectada requiere una contraseña para la conexión.

Tomando un sistema operativo Android como ejemplo, el sistema operativo proporciona una interfaz de gestión de contraseña de red inalámbrica para un módulo de red inalámbrica. La aplicación puede llamar a la interfaz y determinar, en base al resultado de llamar a la interfaz, si la red inalámbrica actualmente conectada requiere una contraseña para la conexión. Lo siguiente ilustra código para llamar a la interfaz de gestión de contraseña de red inalámbrica:

```
/**
 * Se determina, utilizando un mecanismo de gestión
WiFiConfiguration.KeyMgmt, si una Wi-Fi actualmente conectada requiere una
contraseña para el acceso.
 *
 * @return true: requerir una contraseña para el acceso, false: no
requerir contraseña para el acceso
 */
public static boolean needPassword(Context context) {
    WiFiManager WiFiManager = (WiFiManager)
context.getSystemService(Context.WiFi_SERVICE);
    if (WiFiManager != null) {
        List<WiFiConfiguration> WiFiConfiguration =
WiFiManager.getConfiguredNetworks();
        if (WiFiConfiguration != null && WiFiConfiguration.size() > 0) {
            for (WiFiConfiguration configuration : WiFiConfiguration) {
                if (configuration != null && configuration.status ==
WiFiConfiguration.Status.CURRENT) {
                    if
(configuration.allowedKeyManagement.get(WiFiConfiguration.KeyMgmt.NONE)) {
                        return false;
                    } else {
                        return true;
                    }
                }
            }
        }
    }
    // Por defecto se require una contraseña de conexión
    return true;
}
```

WiFiManager.getConfiguredNetworks () representa la interfaz de gestión de contraseña de red inalámbrica.

La lógica principal del código es detectar: si WiFiConfiguration.allowedKeyManagement del punto de acceso Wi-Fi incluye un campo WiFiConfiguration.KeyMgmt.NONE. En caso afirmativo, se considera que no se requiere contraseña; o en caso negativo, se considera que se requiere una contraseña. Cuando no se requiere contraseña para la conexión de red inalámbrica, el resultado de la llamada incluye el campo KeyMgmt.NONE.

Tomando un sistema operativo iOS como ejemplo, el sistema operativo iOS proporciona una API (llamada NEHotspotNetwork) para obtener una lista de Wi-Fi a través de principalmente los siguientes pasos: solicitar a Apple un permiso para desarrollar Network Extension, solicitar un archivo de descripción que incluya Network Extension, configurar Info.plist, configurar derechos, obtener la implementación de código de la lista de Wi-Fi por iOS, y obtener una devolución de llamada de la lista de Wi-Fi.

Después de llamar a NEHotspotNetwork, la información devuelta de NEHotspotNetwork incluye: SSID: nombre de Wi-Fi; BSSID: dirección MAC de un sitio; signalStrength: intensidad de señal de Wi-Fi, con un valor que oscila entre 0,0-1,0; secure: indica si una red es segura (un valor es falso para Wi-Fi que no requieren contraseña para acceder); autoJoined: indica si el dispositivo se conecta automáticamente a la red Wi-Fi; justJoined: indica si se acaba de acceder a la red; y chosenHelper: indica si HotspotHelper está seleccionado para la red.

Por lo tanto, en base a la seguridad en el resultado de la llamada, se puede determinar si el punto de acceso Wi-Fi de red inalámbrica actualmente conectada requiere una contraseña.

Sin embargo, después de acceder a redes inalámbricas sin utilizar una contraseña, algunas redes aún requieren una verificación de inicio de sesión secundaria del usuario. Por lo tanto, en esta realización, si se requiere verificación de inicio de sesión secundaria se determina especificando una o más direcciones de red por adelantado y accediendo a la dirección de red especificada. Suponiendo que se requiere verificación de inicio de sesión secundaria, el usuario puede acceder al Internet solo después de ingresar un nombre de cuenta y contraseña. Si el usuario no realiza la verificación de inicio de sesión secundaria, el dispositivo electrónico no puede obtener los datos de red deseados después de acceder al Internet. En base a esto, en esta realización, se especifican una o más direcciones de red y se accede a la dirección de red especificada. Si se accede con éxito a la dirección de red especificada, indica que la red inalámbrica accedida no requiere verificación de inicio de sesión secundaria. Si no se puede acceder a la dirección de red especificada, la red inalámbrica accedida requiere verificación de inicio de sesión secundaria.

En el uso práctico, si el acceso es exitoso puede determinarse de varias maneras. Por ejemplo, se pueden preconfigurar los datos de red correspondientes a la dirección de red especificada. Después de acceder a la dirección de red especificada, se obtiene un resultado de acceso y se determina si el acceso es exitoso en base a si el resultado de acceso es el mismo que los datos de red preconfigurados.

En esta realización, la dirección de red especificada incluye una dirección de red de una API definida por usuario, y la API se utiliza para devolver información de identificación especificada cuando se accede.

La determinación de si se puede acceder con éxito a la dirección de red especificada incluye: obtener un resultado de acceso al acceder a la dirección de red de la API y determinar, en base a si el resultado de acceso incluye la información de identificación especificada, si la dirección de red de la API se puede acceder con éxito.

En esta realización, se puede desarrollar de antemano una API en un servidor. Una aplicación puede acceder a una dirección de red de la API y la dirección de red puede ser una dirección IP. Si una red es alcanzable, la información de identificación especificada se puede obtener después de acceder a la API. Si la red es inalcanzable, la información de identificación especificada no se puede obtener. Como tal, se puede determinar si se puede acceder con éxito a la dirección de red de la API y si se requiere verificación de inicio de sesión secundaria.

En algunos otros ejemplos, el trabajo previo al desarrollo puede no realizarse. La dirección de red puede ser una dirección de red de una página web pública. El contenido de página de la página web puede analizarse previamente y almacenarse previamente. Se determina si un resultado de acceso al acceder a la página web incluye el contenido de página previamente almacenado, con el fin de determinar si el acceso es exitoso. Sin embargo, el contenido de página web puede cambiar dinámicamente. Por lo tanto, en esta realización, se pueden especificar direcciones de red de dos o más páginas web, para proporcionar un método de determinación más fiable. Específicamente, la presente solicitud proporciona la siguiente realización.

La dirección de red especificada incluye direcciones de red de al menos dos páginas web diferentes; y la determinación de si se puede acceder con éxito a la dirección de red especificada incluye: obtener los datos de página web devueltos después de acceder a una dirección de red de cada una de las páginas web y determinar, comparando los datos de página de las páginas web, si cada una de las páginas web accedidas salta a una página de verificación de inicio de sesión secundaria, con el fin de determinar si se puede acceder con éxito a la dirección de red especificada de la página web.

Se pueden seleccionar dos o más páginas web públicas existentes, o páginas web con contenido de página relativamente simple como las páginas web mencionadas anteriormente, para reducir el consumo de tráfico de datos.

La dirección de red puede incluir una dirección de nombre de dominio o una dirección IP de la página web. Si la red es inalcanzable, cada una de las páginas web accedida salta a la página de verificación de inicio de sesión secundaria. En esta situación, se devuelven los datos de página de la página de verificación de inicio de sesión secundaria, y los datos de página devueltos son básicamente los mismos. Si la red es alcanzable, después de acceder a las dos o más páginas web, se devuelven los datos de página de cada una de las páginas web y los datos de página de cada una de las páginas web son diferentes. Por lo tanto, en esta realización, se puede determinar, comparando los datos de página de las páginas web, si cada una de las páginas web accedida salta a la página de verificación de inicio de sesión secundaria, con el fin de determinar si se puede acceder con éxito a la dirección de red especificada de cada una de las páginas web.

Después de iniciar el acceso a una dirección de red, se pueden obtener los datos de página devueltos desde la dirección de red. Los datos de página incluyen la dirección de red de la página web. Si la red es inalcanzable, los datos de página devueltos incluyen los datos de página de verificación de inicio de sesión secundaria. En esta situación, todos los datos de página son los mismos, excepto para la dirección de red. En base a esto, en esta realización, para mejorar la eficiencia y la precisión de la determinación, la determinación, comparando los datos de página de las páginas web, si cada una de las páginas web accedida salta a una página de verificación de inicio de sesión secundaria incluye: actualizar los datos de página de cada una de las páginas web, donde la actualización incluye eliminar la dirección de red incluida en los datos de página de cada una de las páginas web o reemplazar la dirección de red incluida en los datos de página de cada una de las páginas web con datos de identificación unificados; y comparar datos de página actualizados de las páginas web para determinar si los datos de página son los mismos, y determinar, en base a un resultado de comparación, si cada una de las páginas web accedida salta a la página de verificación de inicio de sesión secundaria.

En esta realización, después de que las direcciones de red en los datos de página se eliminan o reemplazan con los datos de identificación unificados, los datos de página actualizados de las páginas web se comparan para determinar si los datos de página actualizados son los mismos. Por lo tanto, se pueden mejorar significativamente la eficiencia y la precisión de la comparación.

Lo siguiente describe en detalle la presente solicitud utilizando dos realizaciones.

La FIG. 2C es un diagrama de flujo que ilustra un método de detección de tipo de red inalámbrica en una realización ejemplar de la presente solicitud. En la FIG. 2C, se utiliza un sistema operativo Android como ejemplo. Se llama a una interfaz de gestión de contraseña de red inalámbrica del sistema operativo, es decir, WiFiManager.getConfiguredNetworks (), y se determina en base a si un resultado de llamada incluye un campo WiFiConfiguration.KeyMgmt.NONE. En caso negativo, se considera que se requiere una contraseña y se devuelve inmediatamente un resultado determinante. En caso afirmativo, se puede determinar además si un punto de acceso Wi-Fi de red inalámbrica actualmente conectada requiere una verificación de inicio de sesión secundaria.

Específicamente, se puede desarrollar una API en un servidor propietario y la API se utiliza para devolver una bandera de éxito simple. Una aplicación accede directamente a la API. Si se puede recibir la bandera de éxito, se considera que la aplicación puede acceder directamente al Internet a través del punto de acceso Wi-Fi de red inalámbrica actualmente conectada y no se requiere verificación de inicio de sesión secundaria. De lo contrario, se considera que se requiere la verificación de inicio de sesión secundaria.

La FIG. 2D es un diagrama de flujo que ilustra otro método de detección de tipo de red inalámbrica en una realización ejemplar de la presente solicitud. En la FIG. 2D, se utiliza un sistema operativo Android como ejemplo. Se llama a una interfaz de gestión de contraseña de red inalámbrica del sistema operativo, es decir, WiFiManager.getConfiguredNetworks(), y se determina en base a si un resultado de llamada incluye un campo WiFiConfiguration.KeyMgmt.NONE. En caso negativo, se considera que se requiere una contraseña y se devuelve inmediatamente un resultado determinante. En caso afirmativo, se puede determinar además si un punto de acceso Wi-Fi de red inalámbrica actualmente conectada requiere verificación de inicio de sesión secundaria.

Específicamente, en comparación con el desarrollo de la API en el servidor propietario en la FIG. 2C, en esta realización, se pueden seleccionar las direcciones de dos sitios web simples y conocidos (las páginas del sitio web pueden ser lo más simples posible para reducir el consumo de tráfico de datos). Suponiendo que los sitios web son un sitio web A (la dirección del sitio web es url_A) y un sitio web B (la dirección del sitio web es url_B), las direcciones url_A y url_B de los sitios web se acceden secuencialmente, y los datos de respuesta devueltos por las direcciones se almacenan en los correspondientes registros: response_A y response_B. Finalmente, se compara el contenido de response_A y response_B.

Si el punto de acceso Wi-Fi de red inalámbrica actualmente conectada requiere verificación de inicio de sesión secundaria, las direcciones url_A y url_B de los sitios web accedidos saltan a una página de verificación de inicio de sesión secundaria, es decir, el contenido de response_A y response_B incluyen ambos los datos de página de la misma página verificación de inicio de sesión secundaria. De lo contrario, response_A y response_B representan el contenido de diferentes sitios web y son definitivamente diferentes. Por lo tanto, se puede determinar si la Wi-Fi actual requiere verificación de inicio de sesión secundaria.

Sin embargo, dado que response_A y response_B incluyen una correspondiente dirección de red, la dirección de red se puede reemplazar con datos de identificación unificados antes de la comparación entre response_A y response_B. En esta realización, la dirección de red se reemplaza con url_B. Por lo tanto, se puede ejecutar response_A.replace("url_A", "url_B"), es decir, la dirección de red en response_A se reemplaza con url_B, para eliminar una diferencia de dirección de red en los datos de página, evitando así un error de juicio y aumentando la eficiencia y la precisión de la determinación.

Correspondiente a la realización anterior del método de detección de tipo de red inalámbrica, la presente solicitud proporciona además realizaciones de un aparato de detección de tipo de red inalámbrica y un dispositivo electrónico al que se aplica el aparato de detección de tipo de red inalámbrica.

La realización del aparato de detección de tipo de red inalámbrica de la presente solicitud se puede aplicar a un dispositivo electrónico. La realización del aparato se puede implementar utilizando hardware, software o una combinación de hardware y software. Por ejemplo, en una implementación software, el aparato de detección de tipo de red inalámbrica es un aparato lógico, y se forma cuando un procesador de detección de tipo de red inalámbrica del aparato de detección de tipo de red inalámbrica lee una correspondiente instrucción de programa informático en una memoria no volátil y ejecuta la instrucción de programa informático en una memoria. En un aspecto de hardware, la FIG. 3 es un diagrama de hardware estructural que ilustra un dispositivo electrónico que incluye un aparato de detección de tipo de red inalámbrica de la presente solicitud. Además de un procesador 310, una memoria 330, una interfaz 320 de red y una memoria 340 no volátil mostrados en la FIG. 3, en esta realización, el dispositivo electrónico donde está ubicado normalmente el aparato 331 puede incluir además otro hardware en base a una función real del dispositivo informático. Los detalles no se repiten aquí.

la FIG. 4 es un diagrama de bloques que ilustra un aparato de detección de tipo de red inalámbrica en una realización ejemplar de la presente solicitud. El aparato incluye: un módulo 41 de determinación de contraseña de conexión, configurado para determinar si una red inalámbrica actualmente conectada requiere una contraseña para la conexión; un módulo 42 de acceso, configurado para: después de determinar que no se requiere contraseña, acceder a al menos a una dirección de red especificada en base a la dirección de red especificada; y un módulo 43 de verificación de inicio de sesión, configurado para determinar, determinando si se puede acceder con éxito a la dirección de red especificada, si la red inalámbrica actualmente conectada requiere verificación de inicio de sesión secundaria.

Opcionalmente, el módulo de determinación de contraseña de conexión está configurado además para: llamar a una interfaz de gestión de contraseña de red inalámbrica proporcionada por un sistema operativo, obtener un resultado de la llamada y determinar, en base al resultado de la llamada, si la red inalámbrica actualmente conectada requiere una contraseña para la conexión.

Opcionalmente, la dirección de red especificada incluye una dirección de red de una API definida por usuario, y la API se utiliza para devolver información de identificación especificada cuando se accede a la API; y el módulo de verificación de inicio de sesión se configura además para: obtener un resultado de acceso al acceder a la dirección de red de la API y determinar, en base a si el resultado de acceso incluye la información de identificación especificada, si la dirección de red de la API se puede acceder con éxito.

Opcionalmente, la dirección de red especificada incluye direcciones de red de al menos dos páginas web diferentes; y el módulo de verificación de inicio de sesión está configurado para: obtener los datos de página web devueltos después de acceder a una dirección de red de cada una de las páginas web y determinar, comparando los datos de página de las páginas web, si cada una de las páginas web accedida salta a una página de verificación de inicio de sesión secundaria, con el fin de determinar si se puede acceder con éxito a la dirección de red especificada de cada una de las páginas web.

Opcionalmente, los datos de página de la página web incluyen la dirección de red de la página web; y el módulo de verificación de inicio de sesión está configurado para: actualizar los datos de página de cada una de las páginas web, donde la actualización incluye eliminar la dirección de red incluida en los datos de página de cada una de las páginas web o reemplazar la dirección de red incluida en los datos de página de cada una de las páginas web con datos de identificación unificados; y compare los datos de página actualizados de las páginas web para determinar si los datos de página son los mismos, y determinar, en base a un resultado de comparación, si cada una de las páginas web accedida salta a la página de verificación de inicio de sesión secundaria.

Un dispositivo electrónico incluye: un procesador; y una memoria, configurada para almacenar una instrucción que puede ser ejecutarse por el procesador, donde el procesador está configurado para: determinar si una red inalámbrica actualmente conectada requiere una contraseña para la conexión; después de determinar que no se requiere contraseña, acceder a al menos a una dirección de red especificada en base en la dirección de red especificada; y determinar, determinando si se puede acceder con éxito a la dirección de red especificada, si la red inalámbrica actualmente conectada requiere verificación de inicio de sesión secundaria.

Para obtener detalles sobre los procesos de implementación de funciones y propósitos de los módulos en el aparato, consultar los procesos de implementación de los pasos correspondientes en el método, y los detalles no se repiten aquí.

Una realización del aparato corresponde básicamente a una realización del método; por lo tanto, para partes relacionadas, consultar las descripciones parciales en la realización del método. La realización del aparato descrita es simplemente un ejemplo. Los módulos descritos como partes separadas pueden o no estar físicamente separados, y las partes mostradas como módulos pueden o no pueden ser módulos físicos, es decir, pueden ubicarse en una posición o pueden distribuirse en una pluralidad de módulos de red. Algunos o todos los módulos se pueden seleccionar en base a los requisitos reales para lograr los objetivos de las soluciones de la presente solicitud. Un experto en la técnica puede comprender e implementar las realizaciones de la presente solicitud sin esfuerzos creativos.

Las realizaciones específicas de la presente solicitud están descritas arriba. Otras realizaciones caen dentro del alcance de las reivindicaciones adjuntas. En algunas situaciones, las acciones o pasos enumerados en las reivindicaciones se pueden realizar en un orden diferente que en las realizaciones y aún así lograr resultados deseables. Además, los procesos representados en los dibujos adjuntos no requieren necesariamente el orden particular o el orden secuencial ilustrado para lograr resultados deseables. En ciertas realizaciones, el procesamiento multitarea y paralelo también es posible o puede ser posiblemente ventajoso.

Los expertos en la técnica reconocerán fácilmente otras realizaciones de la presente solicitud al considerar la presente solicitud y practicar la invención tal como se aplica aquí. La presente solicitud está destinada a cubrir cualquier variación, uso o adaptación de la presente solicitud que se ajuste a los principios generales de la presente solicitud y que incluya conocimiento general común o un medio técnico en la técnica que no se reivindica en la presente solicitud. La presente solicitud y las realizaciones se consideran meros ejemplos, con el alcance real de la presente solicitud indicado por las siguientes reivindicaciones.

Debería entenderse que la presente solicitud no se limita a las estructuras precisas que se han descrito anteriormente y que se muestran en los dibujos adjuntos, y que se pueden realizar diversas modificaciones y cambios sin apartarse del alcance de la presente solicitud. El alcance de la presente solicitud está limitado solo por las reivindicaciones adjuntas.

Las descripciones anteriores son simplemente ejemplos preferidos de las realizaciones de la presente solicitud, pero no pretenden limitar esta solicitud. Cualquier modificación, reemplazo equivalente y mejora realizada caerá dentro del alcance de protección de la presente invención como se define en las reivindicaciones.

La FIG. 5 es un diagrama de flujo que ilustra un ejemplo de un método 500 implementado por computadora para determinar un tipo de red inalámbrica, de acuerdo con una implementación de la presente divulgación. Para mayor claridad de presentación, la descripción que sigue describe en general el método 500 en el contexto de las otras figuras en esta descripción. Sin embargo, se entenderá que el método 500 puede realizarse, por ejemplo, por cualquier sistema, entorno, software y hardware, o una combinación de sistemas, entornos, software y hardware, según corresponda. En algunas implementaciones, se pueden ejecutar varios pasos del método 500 en paralelo, en combinación, en bucles o en cualquier orden.

En 505, se realiza una determinación de si se requiere una contraseña para conectarse a una red inalámbrica. En algunas implementaciones, la determinación se realiza automáticamente mediante un dispositivo móvil (tal como un teléfono móvil, una computadora portátil) cuando se conecta a la red inalámbrica. La red inalámbrica puede ser una red de área local inalámbrica (WLAN). Un punto de acceso Wi-Fi (tal como un enrutador inalámbrico) puede proporcionar una conexión Wi-Fi a la WLAN cuando el dispositivo móvil está en un área de cobertura del punto de acceso Wi-Fi. Por ejemplo, un usuario puede seleccionar el punto de acceso Wi-Fi en el dispositivo móvil para iniciar una conexión Wi-Fi a la WLAN. En algunas implementaciones, el dispositivo móvil puede iniciar automáticamente una conexión Wi-Fi a la WLAN cuando detecta el punto de acceso Wi-Fi. Cuando se solicita, el punto de acceso Wi-Fi puede preguntar al dispositivo móvil que proporcione una contraseña para conectar el dispositivo móvil a la WLAN. En algunas implementaciones, el punto de acceso Wi-Fi puede conectar el dispositivo móvil a la WLAN sin una contraseña del dispositivo móvil.

En algunas implementaciones, en respuesta a determinar que se requiere una contraseña para conectarse a la red inalámbrica, se realiza una determinación de que la conexión a la red inalámbrica es una conexión segura. En tal situación, un usuario puede ingresar una contraseña en el dispositivo móvil para conectarse a la red inalámbrica. Si el dispositivo móvil tiene una contraseña almacenada para la red inalámbrica, el dispositivo móvil puede proporcionar la contraseña automáticamente para conectarse a la red inalámbrica. Dado que se determina que la conexión a la red inalámbrica es una conexión segura, no hay advertencia de riesgo de seguridad acerca de la conexión mostrada en el dispositivo móvil, y la conexión a la red inalámbrica no se bloquea, por ejemplo, por una aplicación de seguridad en el dispositivo móvil.

En algunas implementaciones, para determinar si se requiere una contraseña para conectarse a una red inalámbrica, un dispositivo móvil puede llamar, por ejemplo, a una interfaz de gestión de contraseña de red inalámbrica proporcionada por un sistema operativo del dispositivo móvil. El dispositivo móvil puede obtener un resultado de llamada en respuesta a llamar a la interfaz de gestión de contraseña de red inalámbrica. Luego, el dispositivo móvil puede determinar si se requiere una contraseña para conectarse a la red inalámbrica en base a al menos el resultado de llamada. Por ejemplo, si el sistema operativo es un sistema operativo ANDROID, WiFiManager.getConfiguredNetworks() puede ser la interfaz de gestión de contraseña de red inalámbrica en el sistema operativo ANDROID. El dispositivo móvil puede llamar a la interfaz. En base a al menos el resultado de llamada, el dispositivo móvil puede determinar si WiFiConfiguration.allowedKeyManagement de un punto de acceso Wi-Fi de la red inalámbrica incluye un campo WiFiConfiguration.KeyMgmt.NONE. Si se incluye el campo, el dispositivo móvil puede determinar que no se requiere contraseña para conectarse a la red inalámbrica. Sin embargo, si no se incluye el campo, el dispositivo móvil puede determinar que se requiere una contraseña para conectarse a la red inalámbrica. Si el sistema operativo es un sistema operativo APPLE iOS, NEHotspotNetwork puede ser una interfaz de programación de aplicaciones (API) en el sistema operativo APPLE iOS. El dispositivo móvil puede llamar a la API. En base a al menos un indicador de seguridad en el resultado de llamada, el dispositivo móvil puede determinar si se requiere una contraseña para conectarse a la red inalámbrica. Desde 505, el método 500 procede a 510.

En 510, en respuesta a determinar que no se requiere contraseña para conectarse a la red inalámbrica, los datos se recuperan desde al menos una dirección de red predefinida a través de la red inalámbrica. En algunas implementaciones, los datos se recuperan automáticamente desde al menos una dirección de red predefinida a través de la red inalámbrica en respuesta a la determinación. Por ejemplo, para aplicaciones de clientes de empresas, se puede desarrollar una API definida por usuario en un servidor propietario de la empresa. La al menos una dirección de red predefinida puede incluir una dirección de red asociada con la API definida por usuario. La API se puede configurar para devolver información de identificación especificada (tal como un identificador “Éxito”) cuando se accede a la API. Para aplicaciones de clientes personales, se pueden predefinir al menos dos direcciones de red, cada una asociada a una página web diferente. Cada una de las páginas web puede ser una página web pública conocida existente. En algunas implementaciones, para reducir el tráfico de datos, se pueden utilizar páginas web con contenido de página simple para seleccionar las direcciones de red predefinidas. Desde 510, el método 500 procede a 515.

En 515, se realiza una determinación de si se requiere una verificación de inicio de sesión secundaria para conectarse a la red inalámbrica. La determinación se toma en base a al menos los datos recuperados desde la al menos una dirección de red predefinida. En algunas implementaciones, la determinación se realiza automáticamente por un dispositivo móvil. En algunas implementaciones, aunque un dispositivo móvil no necesite una contraseña para conectarse a un punto de acceso Wi-Fi de la red inalámbrica en el paso 505, puede existir una verificación de inicio de sesión secundaria cuando el dispositivo móvil accede al Internet a través de la red inalámbrica. Por ejemplo, una pantalla de inicio de sesión, que requiere un nombre de usuario, una contraseña o una combinación de ambos, puede aparecer en el dispositivo móvil cuando el dispositivo móvil accede al Internet a través de la red inalámbrica. En algunos casos, el punto de acceso Wi-Fi de la red inalámbrica puede redirigir la solicitud de acceso a una página de verificación de inicio de sesión secundaria, en lugar de la al menos una dirección de red predefinida, si se requiere una verificación de inicio de sesión secundaria para conectarse a la red inalámbrica. En algunas implementaciones, el punto de acceso Wi-Fi puede pasar la solicitud de acceso a la al menos una dirección de red predefinida a través de la red inalámbrica sin una verificación de inicio de sesión secundaria desde el dispositivo móvil.

En algunas implementaciones, cuando la al menos una dirección de red predefinida incluye la dirección de red asociada con la API definida por usuario, el dispositivo móvil puede acceder a la dirección de red asociada con la API definida por usuario a través de la red inalámbrica. El dispositivo móvil puede obtener una respuesta de red al acceder a la dirección de red asociada con la API definida por usuario a través de la red inalámbrica. Luego, el dispositivo móvil puede determinar si se requiere una verificación de inicio de sesión secundaria para conectarse a la red inalámbrica. La determinación se realiza en base a al menos si la respuesta de red obtenida incluye información de identificación especificada.

Por ejemplo, si la respuesta de la red incluye un identificador “Éxito”, el dispositivo móvil puede determinar que la solicitud de acceso ha alcanzado la dirección de red asociada con la API definida por usuario sin una verificación de inicio de sesión secundaria. Por lo tanto, el dispositivo móvil puede determinar que no se requiere verificación de inicio de sesión secundaria para conectarse a la red inalámbrica. Sin embargo, si la respuesta de red no incluye un identificador “Éxito”, el dispositivo móvil puede determinar que la solicitud de acceso no ha alcanzado la dirección de red asociada con la API definida por usuario sin una verificación de inicio de sesión secundaria. Por lo tanto, el dispositivo móvil puede realizar una determinación de que se requiere una verificación de inicio de sesión secundaria para conectarse a la red inalámbrica.

En algunas implementaciones, cuando la al menos una dirección de red predefinida incluye al menos dos direcciones de red asociadas con diferentes páginas web, el dispositivo móvil puede acceder a cada una de las direcciones de red de las al menos dos direcciones de red asociadas con diferentes páginas web. Para cada una de las direcciones de red accedida, se obtienen datos de página web, que incluyen los datos de la primera página web asociados con una de las al menos dos direcciones de red y los datos de la segunda página web asociados con una diferente de las al menos dos direcciones de red. Luego, los datos de la primera página web se comparan con los datos de la segunda

página web para determinar si los datos de la primera página web coinciden con los datos de la segunda página web. En respuesta a determinar que los datos de la primera página web coinciden con los datos de la segunda página web, el dispositivo móvil puede determinar que se requiere una verificación de inicio de sesión secundaria para conectarse a la red inalámbrica.

Por ejemplo, si se accede a los sitios A y B web, con las direcciones URL_A y URL_B web, respectivamente, se obtienen y comparan los datos devueltos de la página web, la response_A y la response_B, respectivamente. Si la response_A y la response_B son diferentes, el dispositivo móvil puede determinar que la solicitud de acceso ha alcanzado los sitios A y B web sin una verificación de inicio de sesión secundaria. Por lo tanto, el dispositivo móvil puede realizar una determinación de que no se requiere verificación de inicio de sesión secundaria para conectarse a la red inalámbrica. Sin embargo, si la response_A y la response_B son iguales, el dispositivo móvil puede determinar que la solicitud de acceso no ha alcanzado el sitio A o B web sin una verificación de inicio de sesión secundaria. Por ejemplo, la solicitud de acceso a los dos sitios A y B web se redirige a una misma página de verificación de inicio de sesión secundaria y, como resultado, la response_A y la response_B representan el mismo contenido de la página de verificación de inicio de sesión secundaria. Por lo tanto, el dispositivo móvil puede realizar una determinación de que se requiere una verificación de inicio de sesión secundaria para conectarse a la red inalámbrica.

En algunas implementaciones, comparar los datos de la primera página web con los datos de la segunda página web puede incluir actualizar los datos de la primera página web y los datos de la segunda página web para eliminar los correspondientes datos de dirección de red o reemplazar los correspondientes datos de dirección de red con datos de identificación unificados, y comparar los datos actualizados de la primera página web con los datos actualizados de la segunda página web. Por ejemplo, si response_A incluye URL_A y response_B incluye URL_B, una comparación de response_A y response_B será diferente si URL_A y URL_A son diferentes, incluso si se requiere una verificación de inicio de sesión secundaria para conectarse a la red inalámbrica. En una situación de este tipo, URL_A en response_A y URL_B en response_B pueden eliminarse antes de la comparación. En algunas implementaciones, URL_A en response_A y URL_B en response_B pueden reemplazarse con una misma dirección web antes de la comparación. Por ejemplo, URL_A en response_A puede reemplazarse por URL_B, URL_B en response_B puede reemplazarse por URL_A o URL_A en response_A y URL_B en response_B pueden reemplazarse por URL_C antes de la comparación.

En algunas implementaciones, en respuesta a determinar que no se requiere verificación de inicio de sesión secundaria para conectarse a la red inalámbrica, se realiza una determinación de que la conexión a la red inalámbrica no es una conexión segura. Se puede mostrar un mensaje de advertencia en el dispositivo móvil para recordarle a un usuario el riesgo potencial de seguridad de conectarse a la red inalámbrica. En algunas implementaciones, una conexión a la red inalámbrica se bloquea automáticamente, por ejemplo, mediante una aplicación de seguridad en el dispositivo móvil en respuesta a la determinación de que la conexión a la red inalámbrica no es una conexión segura.

En algunas implementaciones, en respuesta a determinar que se requiere una verificación de inicio de sesión secundaria para conectarse a la red inalámbrica, se realiza una determinación de que la conexión a la red inalámbrica es una conexión segura. En una situación de este tipo, un usuario puede ingresar un nombre de usuario, una contraseña o una combinación de ambos en el dispositivo móvil para conectarse a la red inalámbrica. Si el dispositivo móvil tiene un nombre de usuario almacenado, una contraseña almacenada o una combinación de ambos para la red inalámbrica, el dispositivo móvil puede proporcionar el nombre de usuario, la contraseña o una combinación de ambos automáticamente para conectarse a la red inalámbrica. Dado que se determina que la conexión a la red inalámbrica es una conexión segura, no hay advertencia de riesgo de seguridad acerca de la conexión mostrada en el dispositivo móvil, y la conexión a la red inalámbrica no se bloquea, por ejemplo, por una aplicación de seguridad en el dispositivo móvil. Después de 515, el método 500 se detiene.

Un usuario puede utilizar el software de aplicación instalado en un dispositivo móvil para conectarse a una red inalámbrica a través de, por ejemplo, un punto de acceso Wi-Fi. Normalmente, los puntos de acceso Wi-Fi no seguros no tienen contraseñas de inicio de sesión. Sin embargo, algunos puntos de acceso Wi-Fi seguros tampoco tienen contraseñas de inicio de sesión mientras implementan un proceso de verificación de inicio de sesión secundario. Como resultado, el dispositivo móvil no puede diferenciar un punto de acceso Wi-Fi no seguro sin una contraseña de inicio de sesión de un punto de acceso Wi-Fi seguro con una verificación de inicio de sesión secundaria. Una aplicación de seguridad en el dispositivo móvil tratará un punto de acceso Wi-Fi seguro con una verificación de inicio de sesión secundaria de la misma manera que un punto de acceso Wi-Fi no seguro sin una contraseña de inicio de sesión, por lo tanto, resulta una experiencia de usuario deficiente cuando se utiliza la aplicación de seguridad. El materia objeto descrita en esta memoria descriptiva se puede utilizar para diferenciar un punto de acceso Wi-Fi no seguro sin una contraseña de inicio de sesión de un punto de acceso Wi-Fi seguro con una verificación de inicio de sesión secundaria. Por ejemplo, después de determinar que un punto de acceso Wi-Fi no tiene una contraseña de inicio de sesión, se realiza otra determinación de si el punto de acceso Wi-Fi sin una contraseña de inicio de sesión implementa un proceso de verificación de inicio de sesión secundario. Como resultado, un punto de acceso Wi-Fi, sin una contraseña de inicio de sesión y con una verificación de inicio de sesión secundaria, puede identificarse con precisión como un punto de acceso Wi-Fi seguro. De esta forma, se puede proporcionar un riesgo de seguridad de red preciso de una conexión Wi-Fi a un usuario, reduciendo así la tasa de error de la conexión Wi-Fi y las molestias para el usuario.

Las realizaciones y las operaciones descritas en esta memoria descriptiva pueden implementarse en circuitería electrónica digital, o en software informático, firmware o hardware, incluyendo las estructuras dadas a conocer en esta memoria descriptiva o en combinaciones de uno o más de ellos. Las operaciones pueden implementarse como operaciones realizadas por un aparato de procesamiento de datos en datos almacenados en uno o más dispositivos de almacenamiento legibles por computadora o recibidos desde otras fuentes. Un aparato de procesamiento de datos, computadora o dispositivo de computación puede abarcar aparatos, dispositivos y máquinas para procesar datos, incluyendo a modo de ejemplo un procesador programable, una computadora, un sistema en chip, o múltiples, o combinaciones, de los anteriores. El aparato puede incluir circuitería lógica de propósito especial, por ejemplo, una unidad central de procesamiento (CPU), una matriz de compuertas programables en campo (FPGA) o un circuito integrado de aplicación específica (ASIC). El aparato también puede incluir código que crea un entorno de ejecución para el programa informático en cuestión, por ejemplo, código que constituye el firmware del procesador, una pila de protocolo, un sistema de gestión de bases de datos, un sistema operativo (por ejemplo, un sistema operativo o una combinación de sistemas), un entorno de tiempo de ejecución multiplataforma, una máquina virtual o una combinación de uno o más de ellos. El aparato y el entorno de ejecución pueden realizar diversas infraestructuras de modelos informáticos diferentes, tales como servicios web, infraestructuras distribuidas de computación y computación en malla.

Un programa informático (también conocido, por ejemplo, como un programa, software, aplicación de software, módulo de software, unidad de software, script o código) puede escribirse en cualquier forma de lenguaje de programación, incluidos los lenguajes compilados o interpretados, los lenguajes declarativos o procedimentales, y se puede desplegar de cualquier forma, incluido como un programa independiente o como un módulo, componente, subrutina, objeto u otra unidad adecuada para su uso en un entorno informático. Un programa puede almacenarse en una porción de un archivo que contiene otros programas o datos (por ejemplo, uno o más scripts almacenados en un documento de lenguaje de marcado), en un único archivo dedicado del programa en cuestión o en múltiples archivos coordinados (por ejemplo, archivos que almacenan uno o más módulos, subprogramas o porciones de código). Un programa de computadora se puede ejecutar en una computadora o en múltiples computadoras que están ubicadas en un sitio o distribuidas en múltiples sitios e interconectadas mediante una red de comunicaciones.

Los procesadores para la ejecución de un programa informático incluyen, a modo de ejemplo, microprocesadores de propósito general y especial, y uno o más procesadores de cualquier tipo de computadora digital. En general, un procesador recibirá instrucciones y datos desde una memoria de solo lectura o una memoria de acceso aleatorio o ambas. Los elementos esenciales de una computadora son un procesador para realizar acciones de acuerdo con las instrucciones y uno o más dispositivos de memoria para almacenar instrucciones y datos. En general, una computadora también incluirá, o estará acoplada operativamente para recibir datos desde o transferir datos a, o ambos, uno o más dispositivos de almacenamiento masivo para almacenar datos. Una computadora puede integrarse en otro dispositivo, por ejemplo, un dispositivo móvil, un asistente digital personal (PDA), una consola de juegos, un receptor del Sistema de Posicionamiento Global (GPS) o un dispositivo de almacenamiento portátil. Los dispositivos adecuados para almacenar instrucciones y datos de programa informático incluyen memoria, medios y dispositivos de memoria no volátiles, que incluyen, a modo de ejemplo, dispositivos de memoria de semiconductores, discos magnéticos y discos magnetoópticos. El procesador y la memoria pueden complementarse o incorporarse en circuitería lógica de propósito especial.

Los dispositivos móviles pueden incluir teléfonos, equipos de usuario (UE), teléfonos móviles (por ejemplo, teléfonos inteligentes), tabletas, dispositivos llevables (por ejemplo, relojes inteligentes y gafas inteligentes), dispositivos implantados dentro del cuerpo humano (por ejemplo, biosensores, implantes cocleares) u otros tipos de dispositivos móviles. Los dispositivos móviles pueden comunicarse de forma inalámbrica (por ejemplo, utilizando señales de radiofrecuencia (RF)) con diversas redes de comunicaciones (descritas a continuación). Los dispositivos móviles pueden incluir sensores para determinar las características del entorno actual del dispositivo móvil. Los sensores pueden incluir cámaras, micrófonos, sensores de proximidad, sensores GPS, sensores de movimiento, acelerómetros, sensores de luz ambiente, sensores de humedad, giroscopios, brújulas, barómetros, sensores de huellas digitales, sistemas de reconocimiento facial, sensores de RF (por ejemplo, radios Wi-Fi y móviles), sensores térmicos u otros tipos de sensores. Por ejemplo, las cámaras pueden incluir una cámara frontal o trasera con lentes móviles o fijas, un flash, un sensor de imagen y un procesador de imagen. La cámara puede ser una cámara de megapíxeles capaz de capturar detalles para reconocimiento facial y/o de iris. La cámara junto con un procesador de datos y la información de autenticación almacenada en memoria o accedida de forma remota puede formar un sistema de reconocimiento facial. El sistema de reconocimiento facial o uno o más sensores, por ejemplo, micrófonos, sensores de movimiento, acelerómetros, sensores GPS o sensores RF, se pueden utilizar para la autenticación de usuario.

Para proporcionar interacción con un usuario, las realizaciones se pueden implementar en una computadora que tiene un dispositivo de visualización y un dispositivo de entrada, por ejemplo, una pantalla de cristal líquido (LCD) o pantalla de diodo orgánico emisor de luz (OLED)/realidad virtual (VR)/pantalla de realidad aumentada (AR) para visualizar información al usuario y una pantalla táctil, teclado y un dispositivo señalador mediante el cual el usuario puede proporcionar entrada a la computadora. También se pueden utilizar otros tipos de dispositivos para proporcionar interacción con un usuario; por ejemplo, la retroalimentación proporcionada al usuario puede ser cualquier forma de retroalimentación sensorial, por ejemplo, retroalimentación visual, retroalimentación auditiva o retroalimentación táctil; y la entrada del usuario se puede recibir de cualquier forma, incluida la entrada acústica, de voz o táctil. Además, una computadora puede interactuar con un usuario enviando y recibiendo documentos de un dispositivo que el usuario

utiliza; por ejemplo, enviando páginas web a un navegador web en el dispositivo cliente del usuario en respuesta a solicitudes recibidas desde el navegador web.

Las realizaciones pueden implementarse utilizando dispositivos informáticos interconectados por cualquier forma o medio de comunicaciones de datos digitales por cable o inalámbrica (o combinación de los mismos), por ejemplo, una red de comunicaciones. Ejemplos de dispositivos interconectados son un cliente y un servidor generalmente remotos entre sí que típicamente interactúan a través de una red de comunicaciones. Un cliente, por ejemplo, un dispositivo móvil, puede realizar transacciones por sí mismo, con un servidor, o a través de un servidor, por ejemplo, realizando transacciones de compra, venta, pago, entrega, envío o préstamo, o autorizando las mismas. Las transacciones de este tipo pueden ser en tiempo real, de manera que una acción y una respuesta son temporalmente próximas; por ejemplo, un individuo percibe que la acción y la respuesta se producen de manera sustancialmente simultánea, la diferencia de tiempo para una respuesta después de la acción del individuo es inferior a 1 milisegundo (ms) o inferior a 1 segundo (s), o la respuesta es sin retardo intencional teniendo en cuenta limitaciones de procesamiento del sistema.

Los ejemplos de redes de comunicaciones incluyen una red de área local (LAN), una red de acceso de radio (RAN), una red de área metropolitana (MAN) y una red de área amplia (WAN). La red de comunicaciones puede incluir todo o una porción de la Internet, otra red de comunicaciones o una combinación de redes de comunicaciones. La información se puede transmitir en la red de comunicaciones de acuerdo con diversos protocolos y estándares, incluyendo la Evolución a Largo Plazo (LTE), 5G, IEEE 802, Protocolo de Internet (IP) u otros protocolos o combinaciones de protocolos. La red de comunicaciones puede transmitir datos de voz, video, biométricos o de autenticación u otra información entre los dispositivos informáticos conectados.

Las características descritas como implementaciones separadas pueden implementarse, en combinación, en una sola implementación, mientras que las características descritas como una sola implementación pueden implementarse en implementaciones múltiples, por separado o en cualquier subcombinación adecuada. Las operaciones descritas y reivindicadas en un orden particular no deberían entenderse como que requieren que el orden particular, ni que todas las operaciones ilustradas deban realizarse (algunas operaciones pueden ser opcionales). Según corresponda, se pueden realizar tareas múltiples o procesamiento paralelo (o una combinación de tareas múltiples y procesamiento paralelo).

REIVINDICACIONES

1. Un método para la detección de un tipo de red inalámbrica realizado por un dispositivo electrónico, el método que comprende:

determinar si una red inalámbrica actualmente conectada requiere una contraseña para acceder al Internet a través de la red inalámbrica en base a al menos una dirección (202) de red especificada;

en respuesta a determinar que no se requiere contraseña, acceder a la dirección (204) de red especificada;

determinar si la red inalámbrica actualmente conectada requiere una verificación de inicio de sesión secundaria determinando si se puede acceder (206) con éxito a la dirección de red especificada;

determinar que la red inalámbrica actualmente conectada es una red no segura si la red inalámbrica actualmente conectada no requiere una contraseña y no requiere una verificación de inicio de sesión secundaria; y

proporcionar una advertencia de riesgo de seguridad a un usuario del dispositivo electrónico o bloquear automáticamente el acceso del dispositivo electrónico a la red inalámbrica actualmente conectada, si se determina que la red inalámbrica actualmente conectada es una red no segura.

2**.** El método de acuerdo con la reivindicación 1, que comprende bloquear automáticamente el acceso mediante el dispositivo electrónico a la red inalámbrica actualmente conectada, si la red inalámbrica actualmente conectada es una red no segura.

3. El método de acuerdo con la reivindicación 1, que comprende proporcionar una advertencia de riesgo de seguridad a un usuario del dispositivo electrónico.

4. El método de acuerdo con una cualquiera de las reivindicaciones 1 a 3, en donde determinar si la red inalámbrica actualmente conectada requiere una contraseña para la conexión comprende:

llamar a una interfaz de gestión de contraseña de red inalámbrica proporcionada por un sistema operativo;

obtener un resultado de llamada; y

determinar, en base al resultado de llamada, si la red inalámbrica actualmente conectada requiere la contraseña para la conexión.

5**.** El método de acuerdo con una cualquiera de las reivindicaciones 1 a 4, en donde la dirección de red especificada comprende una dirección de red de una API definida por usuario para una empresa, y la API definida por usuario se utiliza para devolver información de identificación especificada cuando se accede a la API.

6. El método de acuerdo con la reivindicación 5, en donde determinar si se puede acceder con éxito a la dirección de red especificada comprende: obtener un resultado de acceso al acceder a la dirección de red de la API definida por usuario; el método que comprende además

determinar, en base a si el resultado de acceso comprende la información de identificación especificada, si se puede acceder con éxito a la dirección de red de la API definida por usuario.

7. El método de acuerdo con una cualquiera de las reivindicaciones 1 a 5, en donde la dirección de red especificada comprende direcciones de red de al menos dos páginas web diferentes.

8. El método de acuerdo con la reivindicación 7, en donde determinar si se puede acceder con éxito a la dirección de red especificada comprende:

obtener los datos de una página web devueltos después de acceder a una dirección de red de cada una de las páginas web y determinar, comparando los datos de página web de las páginas web, si cada una de las páginas web accedida salta a una página de verificación de inicio de sesión secundaria, con el fin de determinar si se puede acceder con éxito a la dirección de red especificada de la página web.

9. El método de acuerdo con la reivindicación 8, en donde los datos de página web de la página web comprenden la dirección de red de la página web.

10. El método de acuerdo con la reivindicación 8, en donde determinar, comparando los datos de página web de las páginas web, si cada una de las páginas web accedida salta a una página de verificación de inicio de sesión secundaria comprende:

actualizar los datos de página web de cada una de las páginas web, en donde la actualización comprende eliminar la dirección de red comprendida en los datos de página web de cada una de las páginas web o reemplazar la dirección de red comprendida en los datos de página web de cada una de las páginas web con datos de identificación unificados; y

comparar datos de página web actualizados de las páginas web para determinar si los datos de página web son los mismos y determinar, en base a un resultado de comparación, si cada una de las páginas web accedida salta a la página de verificación de inicio de sesión secundaria.

11. Un dispositivo electrónico que comprende:

un procesador; y

una memoria, configurada para almacenar una instrucción que puede ejecutarse por el procesador, en donde el procesador está configurado para:

determinar si una red inalámbrica actualmente conectada requiere una contraseña para acceder a un servicio a través de la red inalámbrica en base a la dirección (202) de red especificada;

después de determinar que no se requiere contraseña, acceder al menos a una dirección (204) de red especificada;

determinar si la red inalámbrica actualmente conectada requiere una verificación de inicio de sesión secundaria, determinando si se puede acceder (206) con éxito a la dirección de red especificada

determinar que la red inalámbrica actualmente conectada es una red no segura si la red inalámbrica actualmente conectada no requiere una contraseña y no requiere una verificación de inicio de sesión secundaria; y

proporcionar una advertencia de riesgo de seguridad a un usuario del dispositivo electrónico o bloquear automáticamente el acceso del dispositivo electrónico a la red inalámbrica actualmente conectada, si se determina que la red inalámbrica actualmente conectada es una red no segura.

12. El dispositivo de acuerdo con la reivindicación 11, en donde la memoria comprende un aparato de detección de tipo de red inalámbrica que está configurado para realizar el método de acuerdo con una cualquiera de las reivindicaciones 1 a 10.

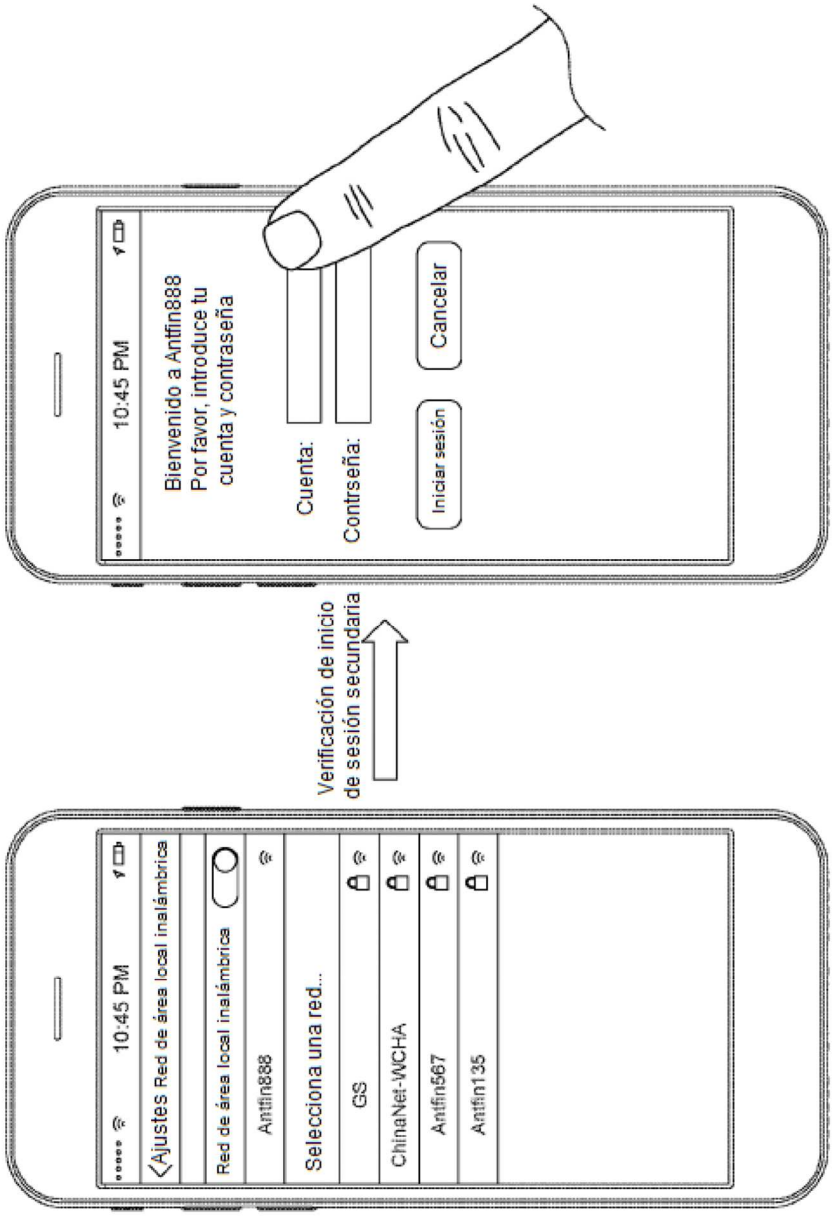
10:45 PM
Ajustes Red de área local inalámbrica
Red de área local inalámbrica
Antfin888
Selecciona una red...
GS
ChinaNet-WCHA
Antfin567
Antfin135
Verificación de inicio de sesión secundaria
10:45 PM
Bienvenido a Antfin888
Por favor, introduce tu cuenta y contraseña
Cuenta:
Contrseña:
Iniciar sesión
Cancelar

FIG. 1

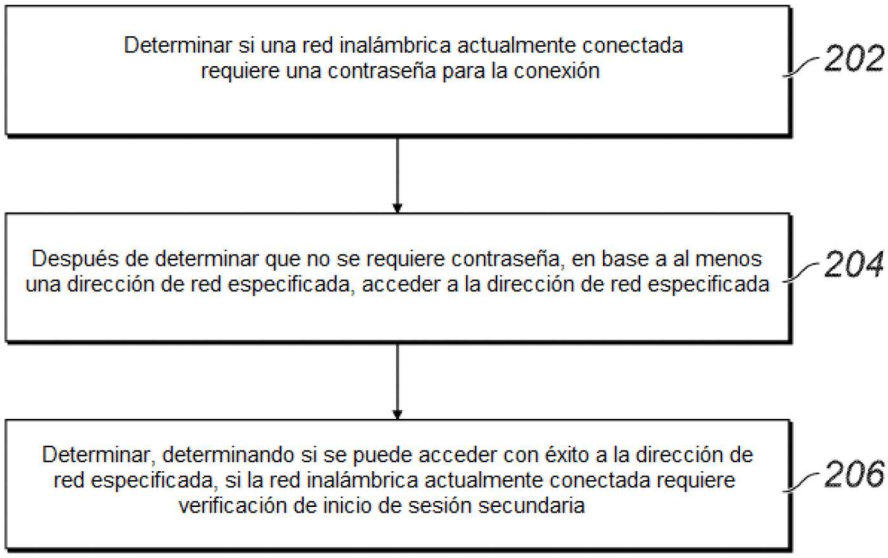
Determinar si una red inalámbrica actualmente conectada requiere una contraseña para la conexión
202
Después de determinar que no se requiere contraseña, en base a al menos una dirección de red especificada, acceder a la dirección de red especificada
204
Determinar, determinando si se puede acceder con éxito a la dirección de red especificada, si la red inalámbrica actualmente conectada requiere verificación de inicio de sesión secundaria
206

FIG. 2A

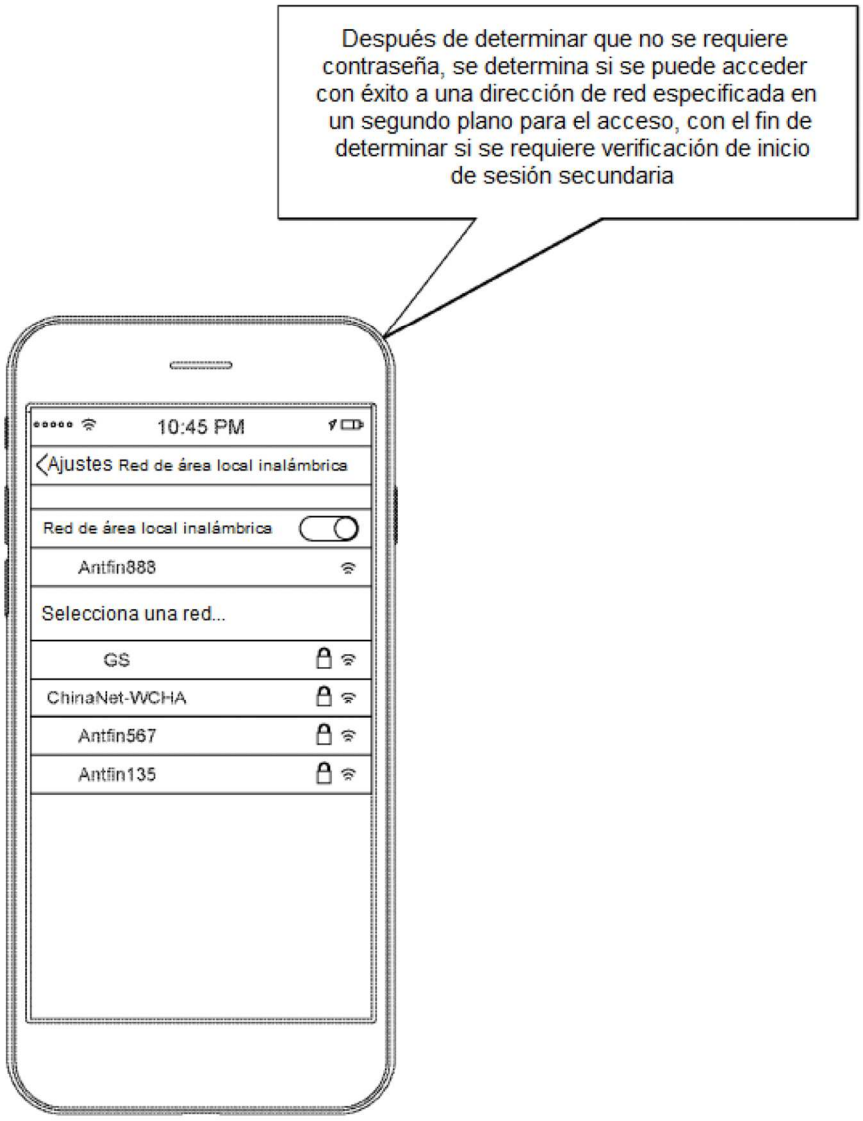
Después de determinar que no se requiere contraseña, se determina si se puede acceder con éxito a una dirección de red especificada en un segundo plano para el acceso, con el fin de determinar si se requiere verificación de inicio de sesión secundaria
10:45 PM
Ajustes Red de área local inalámbrica
Red de área local inalámbrica
Antfin888
Selecciona una red...
GS
ChinaNet-WCHA
Antfin567
Antfin135

FIG. 2B

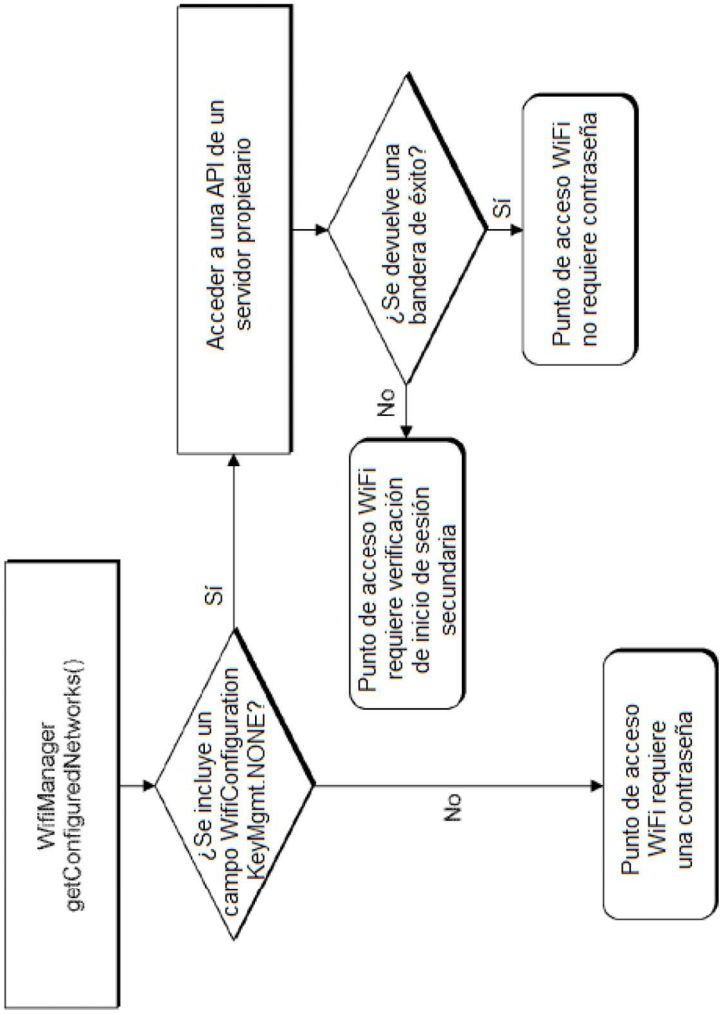
WifiManager
getConfiguredNetworks()
¿Se incluye un campo WifiConfiguration KeyMgmt.NONE?
Sí
No
Acceder a una API de un servidor propietario
¿Se devuelve una bandera de éxito?
Sí
No
Punto de acceso WiFi no requiere contraseña
Punto de acceso WiFi requiere verificación de inicio de sesión secundaria
Punto de acceso WiFi requiere una contraseña

FIG. 2C

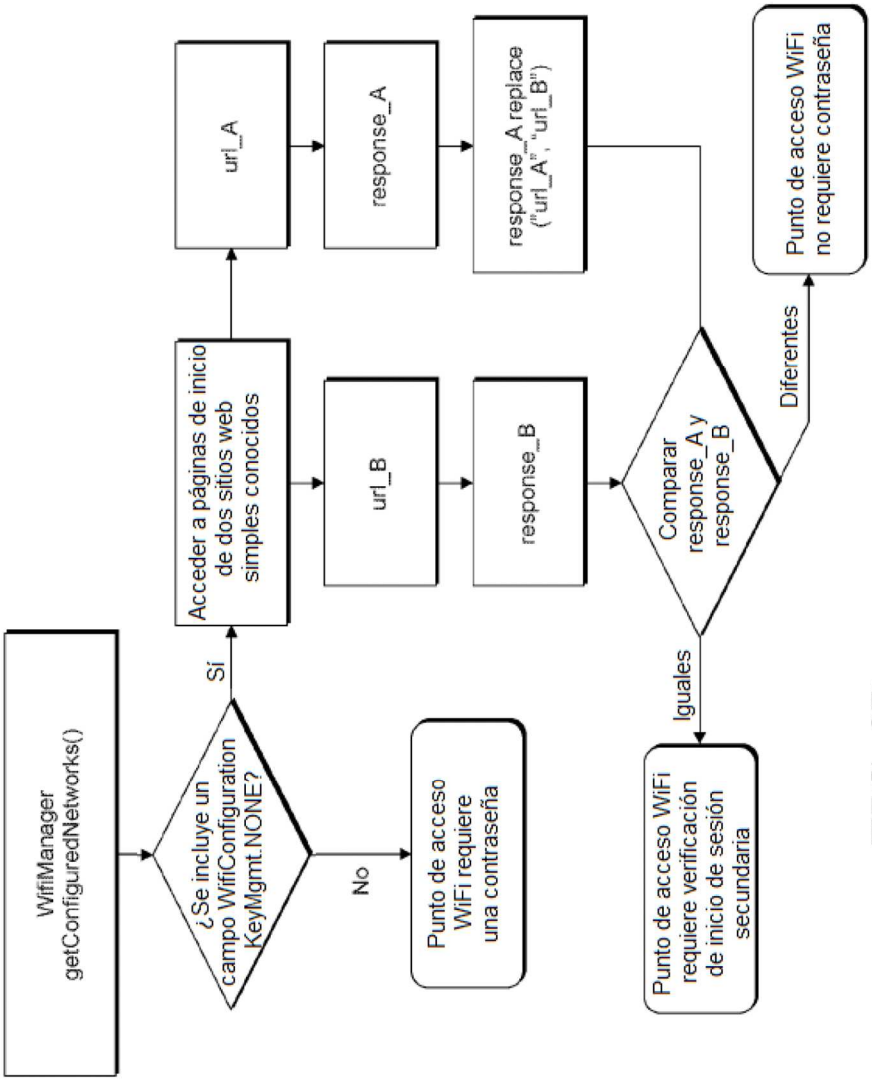
WifiManager
getConfiguredNetworks()
¿Se incluye un campo WifiConfiguration KeyMgmt.NONE?
Sí
No
Punto de acceso WiFi requiere una contraseña
Acceder a páginas de inicio de dos sitios web simples conocidos
url_A
response_A
response_A.replace ("url_A", "url_B")
url_B
response_B
Comparar response_A y response_B
Iguales
Diferentes
Punto de acceso WiFi requiere verificación de inicio de sesión secundaria
Punto de acceso WiFi no requiere contraseña

FIG. 2D

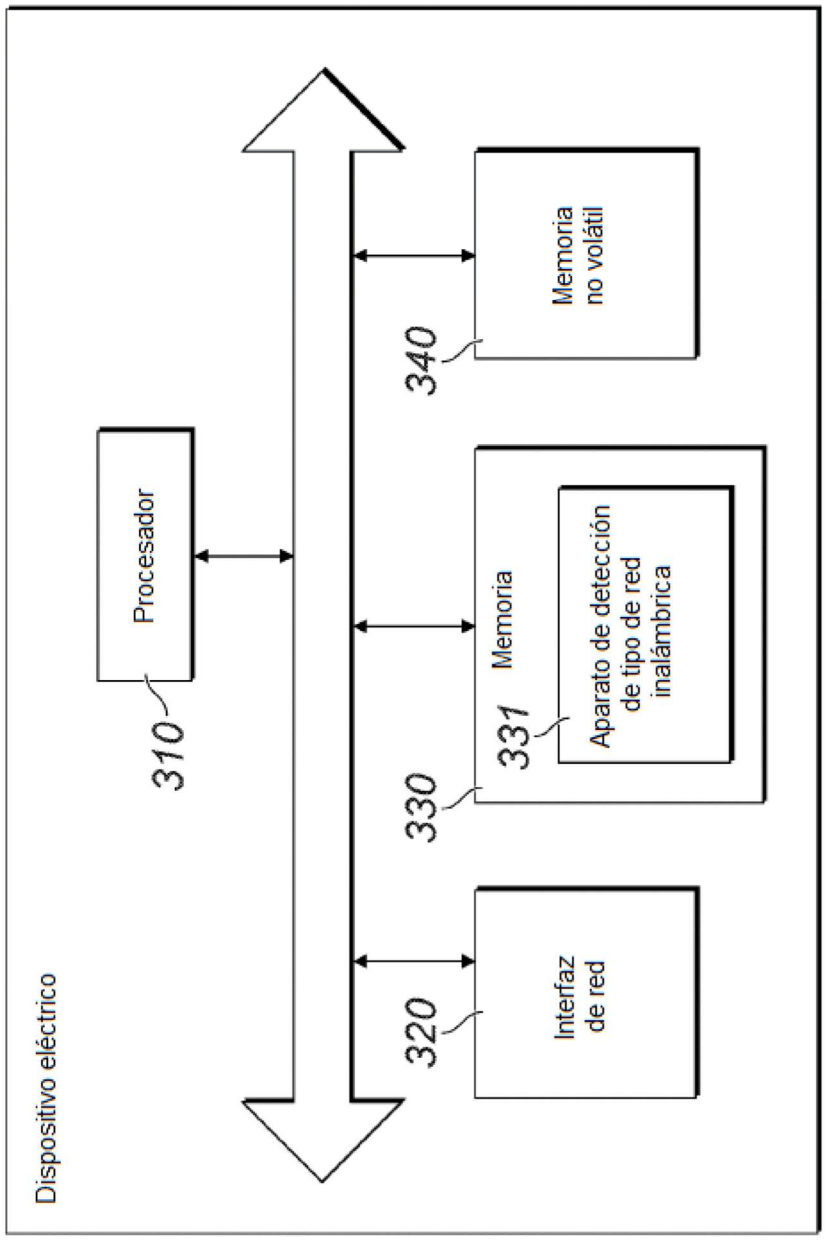
Dispositivo eléctrico
Procesador
310
Interfaz de red
320
Memoria
331
Aparato de detección de tipo de red inalámbrica
330
Memoria no volátil
340

FIG. 3

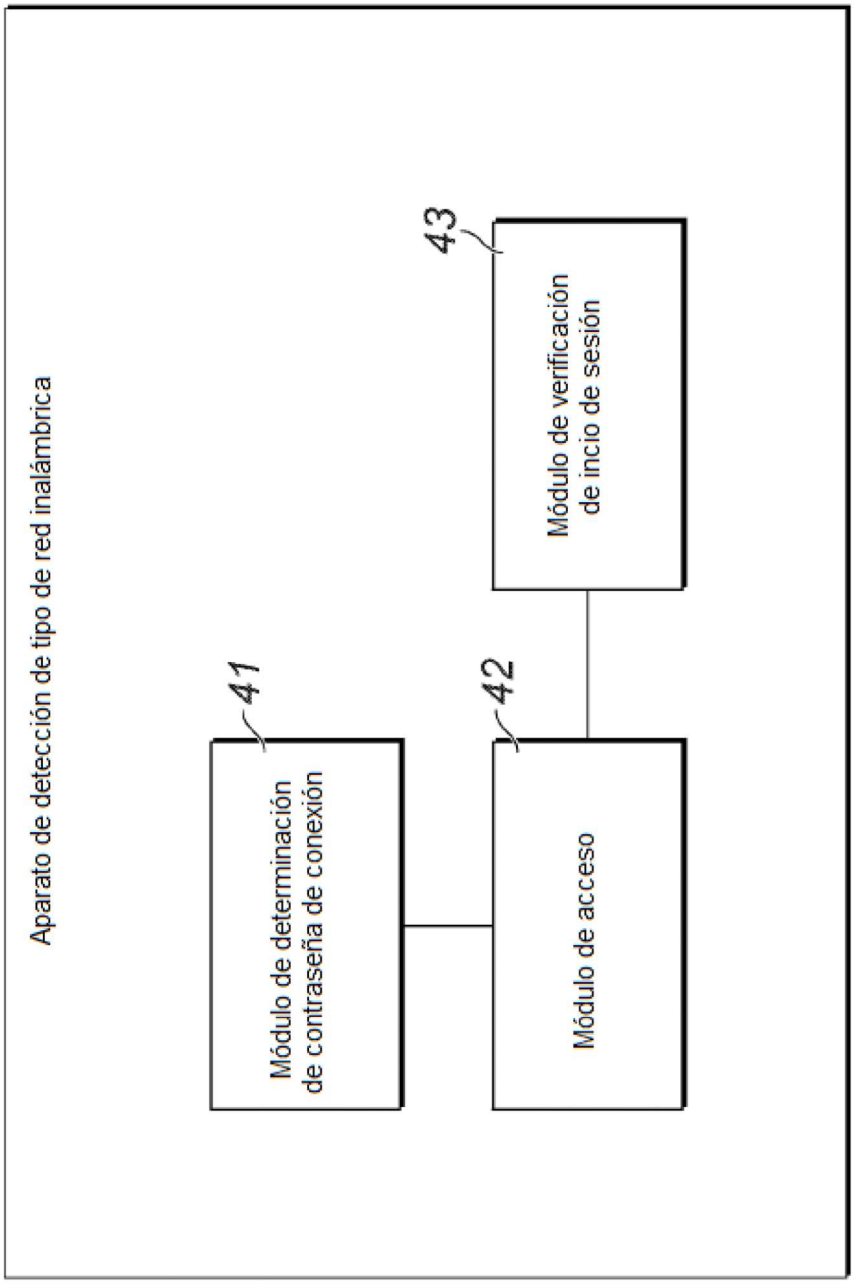
Aparato de detección de tipo de red inalámbrica
41
Módulo de determinación de contraseña de conexión
42
Módulo de acceso
43
Módulo de verificación de incio de sesión

FIG. 4

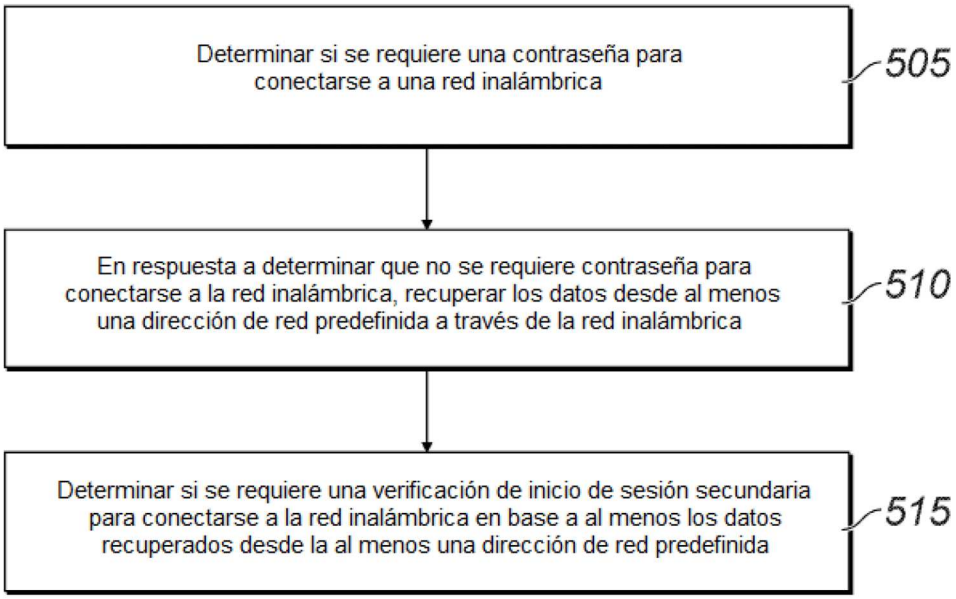
Determinar si se requiere una contraseña para conectarse a una red inalámbrica
505
En respuesta a determinar que no se requiere contraseña para conectarse a la red inalámbrica, recuperar los datos desde al menos una dirección de red predefinida a través de la red inalámbrica
510
Determinar si se requiere una verificación de inicio de sesión secundaria para conectarse a la red inalámbrica en base a al menos los datos recuperados desde la al menos una dirección de red predefinida
515

FIG. 5