(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 686 834**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/08 (2009.01)
H04W 36/14 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **30.03.2011 PCT/GB2011/000486**

(87) Fecha y número de publicación internacional: **06.10.2011 WO11121294**

(96) Fecha de presentación y número de la solicitud europea: **30.03.2011 E 11713333 (0)**

(97) Fecha y número de publicación de la concesión europea: **27.06.2018 EP 2553898**

(54) Título: **Método y sistema para autenticar un punto de acceso**

(30) Prioridad:

30.03.2010 EP 10250655

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.10.2018

(73) Titular/es:

British Telecommunications public limited company (100.0%)
81 Newgate Street
London EC1A 7AJ, GB

(72) Inventor/es:

JOVER SEGURA, XAVIER y
EL-MOUSSA, FADI

(74) Agente/Representante:

CURELL AGUILÁ, Mireia

DESCRIPCIÓN

Método y sistema para autenticar un punto de acceso.

Campo técnico

La presente invención se refiere a la seguridad en redes inalámbricas y, particularmente, a un método y un sistema para autenticar un punto de acceso para un dispositivo inalámbrico.

Antecedentes

Los puntos de acceso y las estaciones base (a los que se hace referencia en ocasiones, de manera general, como puntos de conexión) proporcionan una pasarela entre una red inalámbrica y una red por cable. Las redes inalámbricas tienen un riesgo de seguridad de herencia por el que las señales transmitidas en una red inalámbrica pueden ser recibidas por cualquier dispositivo inalámbrico dentro del alcance del transmisor. La popular normativa de redes inalámbricas IEEE 802.11 combate esto incluyendo mecanismos de seguridad conocidos como Privacidad Equivalente por Cable (WEP) y Acceso Protegido Wi-Fi, (WPA y WPA2). La WEP y el WPA proporcionan una autenticación y un cifrado de datos rudimentarios para clientes inalámbricos. Por encima de la WEP y el WPA, muchos proveedores implementan cortafuegos y filtrado de direcciones MAC en un intento de proteger la infraestructura de red interna y a los clientes inalámbricos.

Lo que se subestima normalmente en la seguridad de las redes inalámbricas es la amenaza planteada por los puntos de acceso (AP) no autorizados.

El ataque por suplantación de AP fue desarrollado originalmente para engañar a clientes incautos de manera que se conectasen a una red inalámbrica controlada por un atacante. Esto se puede lograr estableciendo un punto de acceso no autorizado (del inglés, *rogue access point*) con el mismo SSID (Identificador de Conjunto de Servicios) que la red de destino. Por ejemplo, un atacante podría suplantar una red inalámbrica difundiendo de forma general el SSID de esa red inalámbrica específica con una intensidad alta de la señal para proporcionar una conectividad óptima. Los dispositivos inalámbricos exploran en busca del SSID de su red inalámbrica favorita y se asocian al punto de acceso que ofrece la señal de mayor intensidad. Un atacante puede configurar un punto de acceso para responder a solicitudes de clientes y, en definitiva, engañar al cliente para que se conecte a su punto de acceso. A continuación, el atacante puede monitorizar, controlar o modificar todo tráfico enviado hacia y desde el cliente.

Por ejemplo, el atacante puede servirles entonces una página Web que le pida al usuario que vuelva a introducir sus credenciales, darles una dirección IP y, a continuación, dirigirlos a Internet. El ataque puede pasar inadvertido para el usuario del dispositivo inalámbrico.

En la solicitud de patente WO2008/095291 se describe un método para hacer frente a puntos de acceso no autorizados. En algunas formas de realización, se verifica la combinación del SSID de una red inalámbrica y de la dirección MAC (dirección de Control de Acceso a Medios) del AP cuando un dispositivo inalámbrico se conecta por primera vez a un punto de acceso. El administrador de la WLAN proporciona información de registro referente a sí mismo, incluyendo los SSIDs deseados, a un servidor central. El servidor central recibe la información de registro y se conecta con un registro de base de datos que contiene todos los SSIDs registrados. Se lleva a cabo una comprobación para garantizar que el SSID deseado no ha sido ya registrado. Si el SSID deseado no ha sido registrado, el servidor central crea una asociación entre el SSID y cada dirección MAC de AP de la WLAN. Esta asociación se almacena en el registro de base de datos. A continuación, el servidor central transmite la información de registro a una autoridad de certificación. La autoridad de certificación lleva a cabo una validación de la información de registro y, si la validación se supera, la autoridad de certificación emite, para cada punto de acceso dentro de la WLAN, certificados digitales que asocian la dirección MAC del AP con el SSID de la WLAN. Dicho certificado digital se transmite a cada punto de acceso de la WLAN.

Una vez que el dispositivo inalámbrico se ha conectado al punto de acceso de la WLAN, el punto de acceso de la WLAN transmite el certificado digital al dispositivo inalámbrico. El dispositivo inalámbrico se conecta el servidor central a través del punto de acceso, y presenta el certificado y el SSID al servidor central. El servidor central autentica el certificado digital y verifica que el identificador de red alegado está realmente asociado a la WLAN a la cual pertenece el AP con esta dirección MAC. Esto garantiza que la WLAN a la cual se está conectando el dispositivo inalámbrico es aquella a la cual tiene intención de conectarse dicho dispositivo inalámbrico.

El método conocido sigue siendo vulnerable a un ataque denominado del tipo hombre en el medio; el certificado puede ser rastreado (*sniffed*) y copiado y puede ser usado por puntos de acceso no autorizados. La solicitud sugiere el uso de información de trazado de ruta para evitar el rastreo; no obstante, el trazado de ruta no es adecuado en una red IP ya que los paquetes se pueden encaminar a través de muchas rutas diferentes entre los mismos puntos extremos y, además, nada evita que un punto de acceso no autorizado falsee también los paquetes del trazado de ruta.

El documento US20040198220 da a conocer otro sistema para acceder de forma segura a una red inalámbrica. El sistema incluye un servidor de seguridad que suscribe a mensajes de una trampa de SNMP en el punto de acceso. Cuando una unidad móvil se asocia a ese punto de acceso, la trampa envía un mensaje que indica la información de asociación. Un cliente de control de itinerancia en el dispositivo móvil interroga al servidor de seguridad, el cual verifica (o no) que ha recibido el mensaje correspondiente a esa asociación.

Una desventaja de este sistema es que, debido a que el dispositivo inalámbrico interroga al servidor de seguridad por medio del punto de acceso no autenticado, es probable que el dispositivo haya intercambiado varios mensajes, que incluyan probablemente datos sensibles, con un punto de acceso posiblemente no autorizado antes incluso de darse cuenta de que se trata de un punto de acceso falso.

El documento EP1542406 da a conocer un sistema de detección de suplantaciones para un nodo inalámbrico. El nodo comprende un módulo de detección de intrusiones para correlacionar tramas de datos originales, transmitidas directamente por el nodo inalámbrico a través de un enlace seguro al módulo de detección de intrusiones, con tramas de datos entrantes recibidas a través de la interfaz aérea. Si el nodo inalámbrico está inactivo pero el módulo de detección de intrusiones recibe tráfico que indica que el nodo monitorizado es el originador, entonces esto sería una señal de un comportamiento sospechoso puesto que la correlación de los conjuntos de datos no daría como resultado un conjunto de datos vacío.

Este es un sistema bastante complicado en el cual el módulo de detección de intrusiones debe monitorizar constantemente los canales asignados al nodo usando una antena, con el fin de comparar tramas. Otra de las desventajas es que el nodo inalámbrico debe conectarse al módulo de detección de intrusiones a través del enlace seguro, y si este enlace falla por algún motivo, el sistema no funciona. Es también una desventaja el hecho de que el nodo necesita disponer de dos conexiones que están en funcionamiento la mayor parte del tiempo.

Sumario de la invención

Según un primer aspecto de la presente invención, se proporciona un método de detección de la intervención de un punto de acceso no autorizado en un trayecto de comunicaciones entre un dispositivo inalámbrico y uno o más recursos en una red de datos accesible por medio de un punto de acceso genuino, según se expone en la reivindicación 1.

Según otro aspecto de la presente invención, se proporciona un sistema tal como se expone en la reivindicación 7.

Según otro aspecto de la presente invención, se proporciona un comparador tal como se expone en la reivindicación 11.

Esto tiene la ventaja de que a un usuario no se le engañará para asociarse a un dispositivo malicioso que pretende ser un punto de acceso genuino, ya que el comparador revelará que la comunicación entre el dispositivo inalámbrico y la red por cable ha sido interceptada y reenviada por un dispositivo malicioso a la red por cable puesto que los datos indicativos recibidos de la red por cable y los datos indicativos recibidos directamente del dispositivo inalámbrico diferirán.

Preferentemente, dicho comparador es accesible para dicho dispositivo inalámbrico por medio de una segunda interfaz inalámbrica de dicho dispositivo inalámbrico, y dicho dispositivo inalámbrico envía datos indicativos de su identificador de primera interfaz inalámbrica a dicho comparador por medio de la segunda interfaz inalámbrica.

El envío de los datos por medio de una segunda interfaz inalámbrica hace que se incremente la posibilidad de detectar que un punto de acceso no autorizado ha interceptado la comunicación ya que es improbable que el punto de acceso no autorizado pueda intervenir en dos canales de comunicaciones inalámbricas.

Preferentemente, el comparador está colocado conjuntamente con un servidor de información, el cual soporta el traspaso de dicho dispositivo inalámbrico entre redes inalámbricas heterogéneas.

Esto tiene la ventaja de que el comparador puede usar datos almacenados por el servidor de información para soportar un traspaso heterogéneo. Además, el servidor de información está colocado de forma centralizada y puede ser compartido entre muchos proveedores de red y dispositivos inalámbricos, con lo cual la carga computacional de la comparación puede ser compartida y resulta más sencillo implementar la invención.

Preferentemente, los datos indicativos se procesan en la red por cable, de tal manera de que aportan al comparador una garantía de que los datos indicativos fueron generados por la red por cable y no han sido alterados desde entonces.

Procesando los datos indicativos, por ejemplo, mediante firma o cifrado de los datos con una clave privada del proveedor de red, se evita el falseamiento de los datos indicativos.

Preferentemente, la credencial cifrada de inicio de sesión de usuario se reenvía al dispositivo inalámbrico desde el comparador cuando el servidor del comparador ha verificado que el punto de acceso es genuino. Esto tiene la ventaja de que no es necesario que el usuario recuerde sus credenciales de usuario para cada red, y la ventaja adicional de que, puesto que las credenciales están cifradas, y se envían directamente desde el dispositivo inalámbrico al servidor de inicio de sesión, se evita que los usuarios compartan credenciales.

A continuación se ofrece, únicamente a título de ejemplo, una descripción de formas de realización preferidas de la presente invención. Esta descripción se ofrece en referencia a los dibujos adjuntos, en los cuales

La figura 1 muestra un diagrama de flujo de mensajes para una primera forma de realización de la invención.

La figura 2 muestra un diagrama de flujo de mensajes para una segunda forma de realización de la invención.

La figura 3 muestra un diagrama de flujo de mensajes para una tercera forma de realización de la invención.

La figura 4 muestra un sistema para verificar una conexión inalámbrica.

La figura 5 muestra un diagrama de flujo para un dispositivo móvil que solicita una autenticación de un punto de acceso

La figura 6 muestra un diagrama de flujo para un punto de acceso que va a ser autenticado

La figura 7 muestra un diagrama de flujo para un controlador de un proveedor de red

La figura 8 muestra un diagrama de flujo para un servidor de información o MIIS que participa en el proceso de autenticación del punto de acceso

Descripción detallada

Las formas de realización descritas en la presente se implementan en una red que funciona de acuerdo con la IEEE 802.21.

La normativa IEEE 802.21 soporta algoritmos que permiten un traspaso sin fisuras entre redes del mismo tipo, así como un traspaso entre tipos diferentes de red, denominado también Traspaso independiente de los medios (MIH) o traspaso vertical. La normativa proporciona información para permitir la realización de traspasos hacia y desde redes celulares, GSM, GPRS, WiFi, Bluetooth, 802.11 y 802.16 a través de diferentes mecanismos de traspaso.

La funcionalidad clave proporcionada por el MIH es la comunicación entre las diversas capas inalámbricas, y entre ellas y la capa IP. Los mensajes requeridos son retransmitidos por la Función de Traspaso Independiente de los Medios, MIHF, que está ubicada en la pila de protocolos entre las tecnologías inalámbricas de la capa 2 y el IP en la capa 3.

En la normativa 802.21 se definen tres servicios diferentes:

- El Servicio de Eventos Independiente de los Medios (MIES) se implementa en dispositivos móviles y les permite recibir notificaciones, tales como Degradación del enlace, enlace activo e intensidad de la señal.

- El Servicio de Órdenes Independiente de los Medios (MICS) se implementa también en dispositivos móviles y les permite controlar los módulos de radiocomunicaciones con el fin de encenderlos y apagarlos.

- El Servicio de Información Independiente de los Medios (MIIS) está situado en la red y permite que los usuarios soliciten información sobre redes circundantes.

El MIES y el MICS en el dispositivo móvil forman conjuntamente un administrador de conexiones.

El MIIS contiene información sobre redes y puntos de acceso. Un punto de acceso puede ser, por ejemplo, un punto de acceso WLAN o una estación base en una red celular o 3G. Algunos ejemplos de lo que podría ser esta información son: nombre de operador, coste por minuto, coste por hora, ancho de banda, dirección MAC del punto de acceso, canal y ubicación del punto de acceso. A cada uno de estos campos se le denomina Elemento de Información (IE), y la normativa define algunos de ellos aunque permite el uso de algunos ampliados.

La característica principal del MIH es que los dispositivos pueden obtener información sobre redes circundantes sin tener las interfaces de radiocomunicaciones específicas encendidas. Por ejemplo, un dispositivo con módulos de radiocomunicaciones, o interfaces, 3G, WiFi y WiMAX, podría tener activado solamente el módulo de radiocomunicaciones 3G, y podría seguir sabiendo si hay puntos de acceso WiFi o WiMAX en las proximidades preguntándole al MIIS a través de la interfaz 3G, lo cual supone ahorrarse una exploración infructífera y permitir que el dispositivo solamente tenga activada una interfaz en todo momento.

El traspaso independiente de los medios se logra con la ayuda del MIIS y el MICS. El dispositivo solicita información del MIIS sobre redes circundantes, y el MIIS responde con las redes disponibles para las interfaces de radiocomunicaciones de ese dispositivo específico. A continuación, el MICS usa la información proporcionada por el MIIS para decidir hacia qué red realizar el traspaso. Activa esa interfaz de radiocomunicaciones y se conecta directamente al punto de acceso elegido, el cual puede ser, por ejemplo, un punto de acceso WLAN o una estación base en una red 3G. Cuando se ha realizado esto, el administrador de conexiones puede transferir o activar la transferencia de aplicaciones que están en marcha al punto de acceso nuevo, usando la interfaz que se acaba de activar, y, cuando todos los datos han pasado a través de la interfaz nueva, la interfaz antigua se desactiva para ahorrar batería.

El usuario de un dispositivo inalámbrico que implementa las formas de realización preferidas descritas a continuación ha decidido usar un servicio proporcionado, por ejemplo, por un proveedor de red. Para implementar el método, el usuario descarga un programa de software ofrecido por el proveedor de red al dispositivo inalámbrico. El programa de software se puede descargar, por ejemplo, desde el sitio web de un proveedor de red o se puede instalar desde una memoria portátil o un DVD-ROM. Después de instalar el programa, el administrador de conexiones en el dispositivo se configura para llevar a cabo, además de las etapas normales para acceder a un proveedor de red a través de una red inalámbrica, las etapas adicionales que se describen en las diferentes formas de realización a continuación y en el diagrama de flujo de la figura 5.

En referencia a la figura 5, el dispositivo en primer lugar se conecta a o usa una red ya autenticada [500] con el fin de recuperar información desde un servidor de información en relación con redes y puntos de acceso disponibles en el área [502], y, a continuación, selecciona uno de los puntos de acceso [504]. El dispositivo inalámbrico envía una solicitud de un mensaje de autenticación al proveedor de red por medio del punto de acceso seleccionado [506]. Si no recibe ninguna respuesta de autenticación, el administrador de conexiones termina la conexión [508]; en caso contrario, reenvía la respuesta de autenticación a un servidor de información, o MIIS, por medio de un canal de comunicaciones en la red previamente autenticada [510]. A continuación, el dispositivo inalámbrico o bien recibe un mensaje de que el punto de acceso se ha autenticado, en cuyo caso inicia sesión en la red por medio de dicho punto de acceso [514], o bien recibe un mensaje de que el punto de acceso no se ha autenticado o no recibe ningún mensaje en absoluto, en cuyos casos el administrador de conexiones termina la sesión [512].

El proveedor de red ha instalado además software en los puntos de acceso de la red así como software en un controlador de NP, el cual es un servidor en la red que gestiona los puntos de acceso de esta última. El controlador es configurado por el programa de software para generar mensajes de autenticación y, por tanto, se le denominará también “servidor de mensajes de autenticación”. Por ello, los puntos de acceso y el controlador de NP se configuran para llevar a cabo las etapas descritas en las siguientes formas de realización y en los diagramas de flujo de las figuras 6 y 7, respectivamente.

En referencia a la figura 6, el punto de acceso seleccionado recibe una solicitud de asociación desde un dispositivo inalámbrico [600]. El punto de acceso genera una solicitud de autenticación que incluye un número de secuencia de solicitud de autenticación, y envía la solicitud al controlador de NP en la red por cable del proveedor de red y almacena la dirección MAC del dispositivo, es decir, la dirección MAC de la tarjeta de interfaz de red WiFi del dispositivo, y el número de secuencia correspondiente [602]. A continuación, recibe una respuesta o mensaje de autenticación que incluye un número de secuencia de solicitud de autenticación desde el controlador de NP [604], y que es enviado al dispositivo inalámbrico por el punto de acceso usando la dirección MAC presentada originalmente por el dispositivo inalámbrico cuando se envía la solicitud [606].

En referencia a la figura 7, el servidor o controlador de la red por cable recibe una solicitud de autenticación de punto de acceso, proveniente del punto de acceso [700]. El servidor comprueba, en una lista almacenada que almacena direcciones IP y direcciones MAC correspondientes a los puntos de acceso en la red por cable, que la dirección IP se encuentra en la lista, y comprueba que la dirección MAC almacenada se corresponde con la dirección MAC del punto de acceso que entregó el mensaje de autenticación [702]. Si las direcciones MAC no se corresponden, el servidor termina el proceso y no crea ningún mensaje de autenticación [704]. En caso contrario, crea el mensaje de autenticación procesando, por ejemplo, un algoritmo de firma digital, un identificador, tal como una dirección MAC, del dispositivo inalámbrico que envió la solicitud de un mensaje de autenticación, y, opcionalmente, también procesa la dirección MAC correspondiente al punto de acceso y el tiempo de la misma manera [706]. A continuación, el servidor envía el mensaje de autenticación al punto de acceso usando la dirección IP del punto de acceso, a través de la red por cable [708].

Como parte del servicio de autenticación del punto de acceso, el servidor de información, MIIS, será configurado por un programa de software instalado para actuar como comparador o servidor de verificación con el fin de determinar si un punto de acceso es genuino o un punto de acceso no autorizado o malicioso. Las etapas llevadas a cabo por el servidor de información se describen en el diagrama de flujo de la figura 8.

En referencia a la figura 8, el servidor de información, o MIIS, recibe un mensaje de autenticación de punto de acceso desde un dispositivo inalámbrico a través de una red ya autenticada, tal como una GSM, 3G o una conexión WiFi ya autenticada [800]. El MIIS realiza una comprobación de la firma digital con su clave privada, en caso de que se use un cifrado de clave [802], y, a continuación, descifra el mensaje con la clave pública del proveedor de red al que pertenece el punto de acceso que se va a autenticar [804]. A continuación, el MIIS compara la dirección MAC recuperada, o descifrada, del dispositivo inalámbrico con la dirección MAC del dispositivo inalámbrico que reenvió el mensaje de autenticación al MIIS [806]. Si no coinciden, el MIIS termina la sesión [808]. Si coinciden, el MIIS, opcionalmente, compara la dirección MAC recuperada del punto de acceso con direcciones MAC de puntos de acceso pertenecientes a dicho proveedor de red y almacenados en una lista en el MIIS [810]. Si la dirección MAC del punto de acceso no se encuentra en la lista, el MIIS termina la sesión [812] o, alternativamente, envía un mensaje de que el punto de acceso no se ha autenticado. Si las direcciones coinciden, el MIIS enviará un mensaje al dispositivo, en relación con que el punto de acceso se ha autenticado, y, opcionalmente, también envía credenciales de inicio de sesión al dispositivo [814].

A continuación se describirá una primera forma de realización con respecto a la figura 1. Los números que se encuentran en la figura se refieren a las etapas que se describen seguidamente.

Un usuario que tiene un dispositivo inalámbrico desea acceder a Internet y, por lo tanto, activa su dispositivo para que realice una exploración en búsqueda de redes disponibles en sus alrededores. Alternativamente, el usuario del dispositivo móvil se podría conectar al servidor de información y solicitar una lista de redes y puntos de acceso disponibles en esa área. El proceso de autenticación de un punto de acceso es el siguiente:

1. El dispositivo inalámbrico selecciona un punto de acceso.

2. El administrador de conexiones en el dispositivo inalámbrico se conecta al punto de acceso y solicita, según instrucciones del programa de seguridad instalado, un mensaje de autenticación del proveedor de red (NP). La solicitud incorpora un identificador correspondiente al dispositivo inalámbrico que envía la solicitud. Preferentemente, como solicitud de un mensaje de autenticación se utiliza también la solicitud actual de asociación IEEE 802.11. La 802.11 es la normativa WiFi por lo que se trata de un paquete que debe ser enviado de todos modos, y ya contiene la dirección MAC del AP y la dirección MAC correspondiente al dispositivo, que se puede usar como identificador para el dispositivo inalámbrico. A continuación, este paquete se encapsula en un paquete IP por parte del punto de acceso, y es enviado directamente a un controlador de NP.

3. Tras recibir la solicitud, el controlador de NP responderá con el mensaje de autenticación, para cuya creación ha sido configurado el controlador por el programa instalado.

$$((MAC_{dispositivo} + tiempo + ID\ NP)$$

El mensaje de autenticación está compuesto por lo siguiente:

- MAC del dispositivo inalámbrico y tiempo de la solicitud y, preferentemente, un identificador del proveedor de red. A continuación, el mensaje es cifrado por el controlador de NP; por ejemplo, se podría cifrar con la clave pública del MIIS compartida con el proveedor de red, aunque se puede usar cualquier método de cifrado adecuado.

  Después de que el mensaje se haya creado, se envía como un suplemento en la respuesta de asociación 802.11 al punto de acceso, el cual está programado para reenviar el mensaje al dispositivo inalámbrico.

4. El administrador de conexiones en el dispositivo inalámbrico acusará recibo de la respuesta y, según está programado, enviará el mensaje de autenticación al servidor de información, o al MIIS de acuerdo con la IEEE 802.21, para su autenticación, preferentemente utilizando una red autenticada de forma previa, tal como la 3G. El MIIS está configurado por el programa de software instalado para descifrar el mensaje recibido; si se usa un cifrado de clave pública/cifrada, utilizará su clave privada para descifrar el mensaje. Una vez que el MIIS ha descifrado el mensaje, validará el tiempo del mensaje y comparará la dirección MAC del dispositivo inalámbrico con un identificador correspondiente del dispositivo inalámbrico que reenvió el mensaje de autenticación al servidor de autenticación. Si, por ejemplo, el mensaje de autenticación se reenvía sobre una red Wi-Fi ya autenticada, la dirección MAC del dispositivo que envía el mensaje se puede obtener a partir del encabezamiento 802.11. Si se usa una red 3G, se puede extraer otro identificador, por ejemplo, el número de teléfono, el SIM o el IMEI del dispositivo, y se puede buscar

la dirección MAC correspondiente al dispositivo en una base de datos en el servidor, almacenando dicha base de datos, por ejemplo, números de teléfono y direcciones MAC correspondientes de dispositivos registrados en el servicio de autenticación.

5. El MIIS envía un mensaje al administrador de conexiones en el dispositivo inalámbrico informando al dispositivo, es decir, a su usuario, de que el punto de acceso es genuino o no autorizado. Si el punto de acceso es genuino, el mensaje incluye, preferentemente, las credenciales de inicio de sesión del usuario para el proveedor de red seleccionado.

Después de esto, el dispositivo inalámbrico se puede conectar a Internet por medio del punto de acceso autenticado del proveedor de red.

Se observará, en esta primera forma de realización, cómo el MIIS proporciona una localización adecuada para comparar el $MAC_{DISPOSITIVO}$ aportado en el mensaje del controlador de red, con el MAC que es indicado por el dispositivo por medio de la red previamente autenticada. Normalmente, el dispositivo inalámbrico ya dispondrá de una conexión autenticada con el MIIS, y el MIIS también podría disponer de datos pre-existentes sobre redes por cable a las cuales podría estar intentando conectarse el dispositivo inalámbrico (por ejemplo, una clave secreta compartida de cifrado).

A continuación se describirá una segunda forma de realización en referencia a la figura 2. La segunda forma de realización difiere de la primera forma de realización en que el dispositivo de usuario usa el servidor de información con el fin de obtener información sobre redes disponibles en el área, y el servidor de información verifica también la identidad del punto de acceso.

Los números que aparecen en la figura se refieren a etapas que se describen a continuación.

Un usuario con un dispositivo móvil desea a acceder a Internet. El dispositivo móvil usa, en primer lugar, el 3G o el GPRS para registrarse en el MIIS y solicitar información de sus proximidades con el fin de saber si hay disponible un punto de acceso adecuado cercano. Por lo tanto, todo proveedor de red que desee implementar este servicio se registra en el MIIS local y proporciona todas las direcciones MAC de AP y SSIDs, claves públicas, y credenciales para iniciar sesión en la red; este proceso de registro se enumera como etapa 0 en la figura 2. El MIIS almacena la información en una base de datos.

El proceso de autenticación del dispositivo inalámbrico es:

1. El cliente usa 3G o GPRS para registrarse en el MIIS y solicitar redes vecinas.

2. El MIIS responderá al administrador de conexiones en el dispositivo inalámbrico con una lista de los APs conocidos que circundan al usuario. Esta respuesta contiene información sobre el AP, tal como SSID, dirección MAC, Proveedor de red, Coste, Ancho de banda, etcétera.

3. Con esta información, el administrador de conexiones puede seleccionar el AP al que conectarse sobre la base de los requisitos del usuario.

4. Después de esto, el administrador de conexiones en el dispositivo inalámbrico se conectará al punto de acceso seleccionado y, según ha sido configurado por el programa de software instalado, solicitará un mensaje de autenticación del proveedor de red (NP). Preferentemente, como solicitud de un mensaje de autenticación se usa también la solicitud de asociación 802.11 actual. La 802.11 es la normativa WiFi por lo que se trata de un paquete que debe enviarse de todos modos, y ya contiene las direcciones MAC del AP y del dispositivo. A continuación, este paquete se encapsula en un paquete IP por parte del punto de acceso, y se envía directamente al controlador de NP.

5. Tras recibir la solicitud, el controlador de NP está configurado para crear el siguiente mensaje de autenticación, el cual se envía como un suplemento en la respuesta de asociación 802.11 al punto de acceso que, a continuación, reenvía el mensaje al dispositivo inalámbrico:

$$MIISpu\ (NPpr\ (MAC_{AP} + MAC_{dispositivo} + tiempo) + ID\ NP)$$

El mensaje de autenticación está compuesto por lo siguiente:

- MAC del AP, MAC del dispositivo inalámbrico que solicita acceso a Internet y el tiempo de solicitud, cifrados, todos ellos, con la clave privada del proveedor de red (NP) (el MIIS tiene ya almacenada la clave pública del NP). El cifrado con la clave privada actúa como firma. Podrían usarse varios algoritmos de firma (por ejemplo, DSA (Algoritmo de Firma Digital)), o cuando se use un cifrado simétrico entre el controlador de NP y el MIIS, podría usarse la Autenticación de Mensajes. En cualquiera de los casos, el cifrado de la firma no es un requisito para garantizar la autenticidad y la

integridad del mensaje en su llegada al MIIS.

En esta forma de realización, el mensaje previo completo se cifra además con la clave pública del MIIS compartida con el proveedor de red.

6. El administrador de conexiones acusará recibo de la respuesta y está configurado, por medio del programa de software, para enviar el mensaje de autenticación al MIIS con vistas a su autenticación usando una red previamente autenticada, tal como la 3G. El MIIS descifrará el mensaje recibido usando su clave privada, y, a continuación, leerá el ID de NP para localizar la clave pública adecuada con el fin de descifrar el resto del mensaje (MAC_{AP} + $MAC_{dispositivo}$ + tiempo). Una vez que el MIIS ha descifrado el mensaje usando la clave pública del NP, entonces validará el tiempo del mensaje y comparará la dirección MAC descifrada del punto de acceso con direcciones MAC almacenadas de puntos de acceso en la base de datos, así como comparando la dirección MAC descifrada del dispositivo inalámbrico con la dirección MAC del dispositivo que reenvió el mensaje de autenticación al servidor de información con el fin de asegurarse de que el punto de acceso así como el dispositivo inalámbrico que reenvió el mensaje son genuinos y son autorizados. Si, por ejemplo, el mensaje de autenticación se reenvía sobre una red Wi-Fi ya autenticada, en lugar de una red 3G, la dirección MAC del dispositivo que envía el mensaje se puede obtener a partir del encabezamiento 802.11. Si se usa una red 3G, puede extraerse otro identificador, por ejemplo, el número de teléfono correspondiente al dispositivo, y la dirección MAC del dispositivo se puede buscar en la base de datos del servidor, base de datos que almacena números de teléfono y direcciones MAC correspondientes de dispositivos registrados en el servicio de autenticación.

7. Si el MIIS verifica el mensaje de autenticación, el mismo está configurado para enviar las credenciales de inicio de sesión al administrador de conexiones en el dispositivo inalámbrico.

8. El administrador de conexiones usará las credenciales de inicio de sesión para acceder a la red del proveedor de red por medio del punto de acceso seleccionado y autenticado. Por tanto, no es necesario que un usuario recuerde sus credenciales para cada proveedor de red, sino que puede iniciar sesión automáticamente en la red seleccionada sabiendo que el punto de acceso está autenticado y, por lo tanto, puede estar seguro de que no se está conectando a un punto de acceso no autorizado. Todas las credenciales de inicio de sesión están cifradas y ninguna de ellas está disponible para el usuario; únicamente el administrador de conexiones en el dispositivo puede descifrar las credenciales de inicio de sesión, evitando así que usuarios compartan credenciales.

A continuación se describirá una tercera forma de realización en referencia a la figura 3.

La diferencia entre esta forma de realización y la segunda forma de realización es que el punto de acceso requiere una autenticación por clave WEP/WPA para que el dispositivo inalámbrico se autentique, primero, en el punto de acceso, antes de autenticarse en el proveedor de red. La tercera forma de realización funciona de forma idéntica a la segunda forma de realización, excepto por la respuesta del MIIS en la etapa 2 que proporciona también la Clave de Autenticación WEP/WPA cifrada del AP y, en la etapa 4, el administrador de conexiones envía la clave WEP/WPA adecuada al AP con vistas a su autenticación.

Una vez autenticado, el administrador de conexiones en el dispositivo inalámbrico solicitará, etapa 5, un mensaje de autenticación del proveedor de red (NP) de la misma manera que la descrita en la segunda forma de realización.

Las etapas 6 a 9 en la figura 3 se corresponden con las etapas 5 a 8 de la segunda forma de realización, y el dispositivo seguirá estas etapas para autenticarse en el proveedor de red y acceder a Internet.

Las formas de realización descritas proporcionan varias medidas de seguridad que harán que mejore la seguridad en redes inalámbricas.

Como primera medida de seguridad, incorporando la dirección MAC del dispositivo inalámbrico que solicita el mensaje de autenticación en el mensaje de autenticación cifrado, el MIIS, u otros medios de comparación de identificadores de interfaz, podrán comparar esa dirección MAC con la dirección MAC recibida directamente del dispositivo, para detectar que un dispositivo inalámbrico no autorizado o un AP no autorizado ha falseado y capturado o bien la solicitud de un mensaje de autenticación proveniente de un dispositivo inalámbrico o bien el mensaje de autenticación cifrado y ha respondido con él al MIIS con el fin de autenticarse en el proveedor de red. Puesto que la dirección MAC de este dispositivo no autorizado no será igual a la dirección MAC del dispositivo inalámbrico que inicialmente envió la solicitud de un mensaje de autenticación, el servidor de información, cuando compare las direcciones MAC, percibirá que algo va mal, y no verificará el punto de acceso o el dispositivo inalámbrico y, por tanto, no proporcionará ningún mensaje en relación con que el punto de acceso es genuino y/o no proporcionará credenciales de inicio de sesión al dispositivo.

A continuación, se describirán dos escenarios diferentes para mostrar cómo funciona esto.

En el primer ejemplo un usuario A (que ha instalado el programa en su dispositivo móvil al mismo tiempo que ha proporcionado detalles, tales como el número de teléfono móvil y la dirección MAC correspondiente de este dispositivo móvil para su almacenamiento en el servidor de información) se sienta en una cafetería y activa su dispositivo inalámbrico A para enviar una solicitud de un mensaje de autenticación a un punto de acceso genuino en la cafetería. La solicitud incluye la dirección MAC correspondiente al dispositivo A y, por tanto, el controlador de NP incluirá esta dirección MAC en el mensaje cifrado y la enviará de vuelta al administrador de conexiones en el dispositivo A. El administrador de conexiones reenvía el mensaje cifrado al servidor de información usando una conexión 3G.

El servidor de información descifrará el mensaje y hallará la dirección MAC correspondiente al dispositivo A. Buscando el número de teléfono del dispositivo A (que envió el mensaje al servidor de información) en la base de datos almacenada, el servidor de información hallará la dirección MAC correspondiente al dispositivo A. Puesto que las direcciones MAC coinciden, el servidor de información enviará un mensaje que incluye credenciales de inicio de sesión de usuario al dispositivo A.

En el segundo ejemplo, el usuario del dispositivo A envía una solicitud de un mensaje de autenticación a lo que él cree que es un punto de acceso genuino en la cafetería, pero el mismo es, en cambio, un dispositivo B (por ejemplo, un portátil) que transmite un SSID falseado con una alta intensidad de señal. La solicitud de un mensaje de autenticación proveniente del dispositivo A es capturada por el dispositivo B, y dicho dispositivo B reenvía la solicitud al punto de acceso genuino. No obstante, la MAC del dispositivo enviada al punto de acceso genuino será la dirección MAC del dispositivo B y, por lo tanto, el controlador de NP firmará digitalmente la dirección MAC B del dispositivo en el mensaje de autenticación y enviará el mensaje de vuelta al dispositivo B. El administrador de conexiones en el dispositivo malicioso B enviará este mensaje al administrador de conexiones del dispositivo A, el cual, a continuación, reenviará el mensaje de autenticación al servidor de información a través de una conexión 3G. El servidor de información descifrará el mensaje y hallará la dirección MAC B. El servidor de información también buscará el número de teléfono correspondiente al dispositivo A, que reenvió la solicitud al servidor de información, en la base de datos almacenada, y hallará la dirección MAC A. Comparando las dos direcciones MAC, el servidor de información observará que no coinciden y, por lo tanto, enviará un mensaje al dispositivo A en relación con que el punto de acceso no se puede autenticar y, por ello, no enviará las credenciales de inicio de sesión de usuario al usuario A.

Si el dispositivo B, en lugar de reenviar el mensaje de autenticación cifrado al dispositivo A, reenvía él mismo el mensaje de autenticación al servidor de información, el servidor de información buscará el número de teléfono recibido del dispositivo B. Puesto que, probablemente, B no se ha registrado en el servicio de autenticación de este punto de acceso, el servidor de información no hallará ninguna dirección MAC correspondiente y, por tanto, no podrá comparar las dos direcciones MAC.

Si el dispositivo B se ha registrado en el servicio de autenticación del punto de acceso, todo parecerá ir bien pero el servidor de información enviará un mensaje al dispositivo B con las credenciales de inicio de sesión para el usuario B y, por tanto, el usuario B no podrá obtener la credencial correspondiente al usuario A, y dicho usuario A no se podrá conectar al proveedor de red ni siquiera si el usuario recibe un mensaje reenviado por el dispositivo B en relación con que el punto de acceso es genuino, ya que las credenciales de inicio de sesión de usuario son erróneas.

Como segunda medida de seguridad, si un punto de acceso suplantador, que ha falseado la dirección MAC o dirección IP de un AP genuino, consiguiese conectarse físicamente a la red del proveedor de red, y consiguiese reenviar una solicitud de un mensaje de autenticación, el mismo no recibiría tampoco el mensaje de autenticación del proveedor de red ya que el mensaje se encaminaría por medio de un mecanismo de encaminamiento (por ejemplo, un rúter) a través de una conexión por cable, al punto de acceso legítimo al que le han falseado la dirección IP. Por tanto, el punto de acceso no autorizado no puede reenviar un mensaje de autenticación al dispositivo inalámbrico, y el dispositivo inalámbrico tendrá que encontrar otro punto de acceso, legítimo, con el fin de conectarse a una red deseada. El punto de acceso genuino que recibe el mensaje de autenticación descartará el paquete ya que el dispositivo inalámbrico no está conectado a este AP.

Como tercera medida de seguridad, el servidor de información comprueba que el identificador descifrado de un punto de acceso se corresponde con un identificador de punto de acceso almacenado en el servidor de información, y, por tanto, pertenece a un proveedor de red registrado y, en caso negativo, se informará al dispositivo inalámbrico de que el punto de acceso no está autenticado.

Como cuarta medida de seguridad, incorporando también el tiempo en el mensaje de autenticación, se evita que un usuario malicioso envíe el mensaje de autenticación incluso cuando sus credenciales hayan caducado. No obstante, no es necesario incorporar el tiempo en el mensaje de autenticación con el fin de verificar que un punto de acceso es genuino, pero es una medida ventajosa puesto que incrementa adicionalmente la posibilidad de detectar dispositivos inalámbricos no autorizados o menos fiables.

Como quinta medida de seguridad, el mensaje de autenticación se reenvía desde el dispositivo inalámbrico al servidor de información a través de una red ya autenticada, tal como GSM o GPRS, de manera que no hay riesgo de que un punto de acceso no autorizado reenvíe la solicitud a un servidor de información falso o falseado.

Las etapas 1 a 3 de la segunda y la tercera formas de realización son opcionales; el dispositivo inalámbrico podría solicitar un mensaje de autenticación de un proveedor de servicio por medio de un punto de acceso que el mismo haya encontrado mediante una exploración normal de redes de radiocomunicaciones disponibles.

Además no es necesario que la credencial de inicio de sesión para un proveedor de red se envíe al dispositivo inalámbrico por parte del servidor de información. Las credenciales de inicio de sesión se podrían almacenar, en cambio, en el dispositivo inalámbrico, y se podrían presentar al proveedor de red una vez que el servidor de información ha autenticado el punto de acceso, por lo que las etapas 7 a 8 se podrían sustituir por una etapa en la que el servidor de información únicamente envía un mensaje al dispositivo inalámbrico en relación con que el punto de acceso se ha verificado.

En los ejemplos anteriores, como identificador para cada uno del punto de acceso y del dispositivo inalámbrico se usa una dirección MAC. Debe entenderse que las direcciones MAC del dispositivo y/o del AP podrían ser las direcciones MAC de sus tarjetas de interfaz de red inalámbricas. No obstante, el identificador podría ser un ID de hardware tanto para el AP como para el dispositivo inalámbrico, o cualquier otro identificador que sea exclusivo del dispositivo o de un usuario, tal como un número de teléfono o un ID SIM. En este caso, la solicitud de asociación podría seguirse usando para enviar la solicitud del mensaje de autenticación al proveedor de red; no obstante, el ID tendría que añadirse a la solicitud.

Cuando se usa la solicitud de asociación del dispositivo al AP como solicitud de un mensaje de autenticación, el AP no sabrá si el dispositivo desea simplemente conectarse o está solicitando el mensaje de autenticación. No obstante, existen dos maneras de plantear esto:

El AP siempre trata toda solicitud de asociación como solicitud de un mensaje de autenticación, y, a continuación, envía el mensaje en la respuesta de asociación, el cual será ignorado en un dispositivo que no se haya configurado para usar el mensaje de autenticación, pero será entendido por cualquier dispositivo que se haya programado para entenderlo, es decir, cualquier dispositivo que se haya registrado para usar el servicio de autenticación.

En lugar de usar la solicitud de asociación tal como está, se podría introducir un suplemento especial para marcar que se solicita el mensaje de autenticación.

Esta es simplemente una de las formas de pedir el mensaje de autenticación. Como alternativa, podría usarse un paquete privativo para solicitar el mensaje de autenticación.

Todas las formas de realización anteriores se implementan en una red IEEE 802.21, aunque las mismas también se podrían implementar en redes que funcionen de acuerdo con otras normativas siempre que se ofrezca un servicio de información similar. Por ejemplo, en el 3GPP (Proyecto de Asociación de 3a Generación), se implementa un servicio de información similar denominado Función de Descubrimiento y Selección de Redes de Acceso (ANDSF) con el fin de ayudar a dispositivos inalámbricos a descubrir redes disponibles y sus capacidades.

Además de verificar que un punto de acceso es genuino y no un punto de acceso no autorizado o malicioso, el servidor de información también puede informar al dispositivo inalámbrico sobre un nivel de seguridad para el punto de acceso seleccionado. El nivel de seguridad se almacenará en el MIIS, o en el servidor de información, en calidad de elemento de información de ese AP, y el nivel de seguridad dependerá de la seguridad del proveedor de servicio del punto de acceso; si la información por vía aérea está cifrada; y el tipo de cifrado usado. Todos los elementos de información almacenados en el MIIS estarán disponibles para usuarios y/o proveedores servicios.

El nivel de seguridad determina a qué tipos de servicios debería acceder o no un usuario por medio del punto de acceso, por ejemplo:

Nivel 0: Un nivel de seguridad por defecto que permite que un usuario utilice el AP para una navegación normal en Internet. El usuario debería acceder solamente a páginas Web que no requieran inicio de sesión y autenticación de usuario.

Nivel 1: El usuario puede acceder a servicios sin transacciones, que requieren autenticación del usuario, tales como foros o correos electrónicos.

Nivel 2: El usuario puede acceder a servicios que requieren transacciones, tales como eBay o Amazon.

Nivel 3: Para ejecutar banca electrónica.

Si el usuario se conecta a un punto de acceso de nivel 0 e intenta conectarse a su correo electrónico, el administrador de conexiones presentará un mensaje que informa de que el AP actual no es suficientemente seguro. Proporcionará también al usuario 3 opciones:

- Ignorar el consejo y usar el AP actual para comprobar el correo electrónico;
- Usar 3G para comprobar el correo electrónico, en caso de que esté disponible (esta opción también se podría configurar como opción por defecto cuando el nivel de seguridad del AP no se considere suficiente para la aplicación actual).
- En la medida en la que el administrador de conexiones conoce la ubicación del AP vecino, podría aconsejar al usuario a dónde ir para ejecutar el servicio/aplicación requerido. La indicación podría ser “desplazarse 100 metros por la calle actual”. Por lo tanto, el administrador de conexiones puede comunicarle al usuario que “Hay un AP adecuado a menos de 40 metros, ¿quiere que le indiquemos como llegar allí?”

A continuación se describirá, en relación con la figura 4, un sistema en el cual se pueden implementar las formas de realización descritas.

El sistema comprende una serie de diferentes puntos de acceso 31 que pertenecen a diferentes proveedores de red 32 con tipos diferentes de redes que proporcionan servicios a usuarios. Los puntos de acceso pueden ser, por ejemplo, puntos de acceso WLAN o puntos de acceso Bluetooth. Cada punto de acceso 31 está conectado a un controlador, o servidor de gestión de red, 33 en la red por cable. El controlador 33 está diseñado para controlar todos los puntos de acceso de la red según una manera conocida, así como creando mensajes de autenticación solicitados por administradores de conexiones en dispositivos móviles 34. Alternativamente, los mensajes de autenticación pueden ser creados por otros servidores 35 de la red en particular. Tanto el controlador 33 como el servidor 35 pueden ser ordenadores de propósito general que comprenden bases de datos y programas de software diseñados para llevar a cabo diferentes tareas, tales como la gestión de los puntos de acceso en la red y la creación de mensajes de autenticación solicitados, así como el cifrado u otro tipo de procesado de estos mensajes de autenticación. El software requerido para llevar a cabo el método de autenticación descrito se puede almacenar en DVD-ROMs u otros soportes de almacenamiento portátiles, y se puede instalar en servidores de gestión/controladores comunes en una red que pertenezca a un proveedor de red que desee implementar el servicio del método de autenticación descrito. Cuando el software instalado se está ejecutando en el controlador o servidor, el mismo, tras recibir una solicitud de asociación, creará automáticamente el mensaje de autenticación y lo enviará de vuelta al dispositivo solicitante en la respuesta de asociación. Los medios para crear el mensaje de autenticación y los medios criptográficos también se podrían implementar en forma de hardware.

Para mejorar adicionalmente el método de autenticación, el controlador podría tener otra base de datos que comprenda direcciones IP y direcciones MAC para todos sus puntos de acceso. Cuando el controlador recibe la solicitud de un mensaje de autenticación, podría comprobar que la dirección IP del punto de acceso que envió la solicitud se encuentra en la base de datos y podría recuperar también la dirección MAC correspondiente para el punto de acceso y comprobar que es igual que la dirección MAC de AP recibida con la solicitud.

El sistema comprende además un servidor de información, o MIIS, 36. El servidor de información comprende una base de datos 37 que contiene información sobre redes y puntos de acceso. Algunos ejemplos de lo que podría ser esta información son: nombre de operador, coste por minuto, coste por hora, ancho de banda, dirección MAC del punto de acceso, canal y ubicación del punto de acceso. A cada uno de estos campos se le denomina Elemento de Información (IE) y la normativa define alguno de ellos pero permite el uso de algunos ampliados.

El servidor de información tiene una dirección IP Global, y el dispositivo inalámbrico puede usar cualquiera de sus interfaces de red para conectarse al servidor de información a través de Internet con el fin de obtener la información requerida. Preferentemente, habrá varios servidores de información pertenecientes a grupos diferentes de redes inalámbricas con capacidad de interfuncionamiento, cubriendo cada servidor un área geográfica diferente.

El servidor de información comprende además software o hardware criptográfico 38 para descifrar un mensaje de autenticación recibido de un dispositivo inalámbrico y una unidad de verificación o comparador 39, implementado o bien como módulo de software o bien como módulo de hardware, el cual está programado o diseñado para comparar el ID del punto de acceso y la dirección MAC del dispositivo, obtenidos, o cualquier otro ID asociado al dispositivo o al usuario, del mensaje de autenticación, con IDs de puntos de acceso almacenados en la base de datos 37 y con la dirección MAC del dispositivo inalámbrico almacenada en una base de datos 40 en el servidor de información. La base de datos 40 relaciona un identificador del dispositivo inalámbrico que es recuperable a

partir de una conexión 3G o GSM, con la dirección MAC del dispositivo.

El software requerido para llevar a cabo el método de verificación descrito se puede almacenar en DVD-ROMs u otros soportes de almacenamiento portátiles, y se puede instalar en el servidor de información, y, cuando se ejecuta en este servidor, lleva a cabo dicho método de autenticación.

Para posibilitar que un dispositivo móvil use el método de verificación, es necesario que el dispositivo tenga un programa de software instalado, preferentemente en el administrador de conexiones, el cual reconozca que la respuesta de asociación del proveedor de red comprende un mensaje de autenticación y extraiga el mensaje de autenticación de la respuesta de asociación y lo reenvíe a un servidor de información. Este programa de software se puede descargar, por ejemplo, directamente en el dispositivo desde un sitio de Internet aportado por el proveedor de red, o el programa de software se podría almacenar en un DVD-ROM u otros soportes de almacenamiento portátiles y se podría instalar en el dispositivo por medio de un ordenador en el cual se introduce y ejecuta el DVD-ROM u otros soportes de almacenamiento.

En resumen, los puntos de acceso no autorizados o maliciosos representan una amenaza para redes inalámbricas y los usuarios de estas redes. Con el fin de evitar o reducir esta amenaza, se propone un método y un sistema que verifique que un punto de acceso es genuino y autorizado, antes de establecer una conexión entre el punto de acceso y un dispositivo inalámbrico.

La autenticación se basa en la comparación de un identificador del dispositivo inalámbrico, obtenido a partir de un servidor de autenticación en la red por cable, con un identificador de un dispositivo inalámbrico, obtenido directamente a partir del dispositivo inalámbrico. Un comparador en un servidor de información recibe los dos conjuntos de datos y compara los dos identificadores, y, si los mismos coinciden, el punto de acceso se verifica como genuino.

REIVINDICACIONES

1. Método de detección de la intervención de un punto de acceso no autorizado en un trayecto de comunicaciones entre un dispositivo inalámbrico y uno o más recursos en una red de datos accesible por medio de un punto de acceso genuino, comprendiendo dicho método:

un servidor de mensajes de autenticación en la red de datos:

recibe por medio de dicho trayecto de comunicaciones, una solicitud emitida por dicho dispositivo inalámbrico de un mensaje de autenticación cifrado, incluyendo la solicitud datos indicativos de un identificador de dicho dispositivo inalámbrico;

genera un mensaje de autenticación cifrado usando los datos recibidos indicativos de dicho dispositivo inalámbrico presentados en dicho trayecto de comunicaciones, y

envía el mensaje de autenticación cifrado al dispositivo inalámbrico;

el dispositivo inalámbrico:

proporciona a un comparador en la red de datos por medio de un punto de acceso previamente autenticado con respecto a la red de datos,-

unos datos indicativos del identificador del dispositivo inalámbrico;

unos datos indicativos de un identificador del punto de acceso usado en el trayecto de comunicaciones entre el dispositivo inalámbrico y la red de datos; y

el mensaje de autenticación cifrado;

el comparador:

descifra el mensaje de autenticación cifrado, y

compara los dos conjuntos de datos indicativos del identificador del dispositivo inalámbrico;

compara los datos indicativos de un identificador del punto de acceso con unos identificadores de puntos de acceso conocidos, almacenados previamente en el comparador;

detecta la intervención de un punto de acceso no autorizado en una comunicación entre dicho dispositivo inalámbrico y la red por cable si dichos dos conjuntos de datos indicativos del identificador del dispositivo inalámbrico no coinciden, y el identificador del punto de acceso no coincide con los identificadores de puntos de acceso conocidos; y

señaliza el resultado de dicha comparación a dicho dispositivo inalámbrico por medio de dicho punto de acceso previamente autenticado con respecto a la red de datos.

2. Método según la reivindicación 1, en el que el identificador del dispositivo inalámbrico es un identificador de la interfaz de red inalámbrica del dispositivo.

3. Método según la reivindicación 2, en el que dicho comparador es accesible para dicho dispositivo inalámbrico por medio de una segunda interfaz inalámbrica de dicho dispositivo inalámbrico, y dicho dispositivo inalámbrico envía datos indicativos de su identificador de primera interfaz inalámbrica a dicho comparador por medio de la segunda interfaz inalámbrica.

4. Método según la reivindicación 3, en el que el comparador comprende una base de datos que relaciona el identificador de interfaz inalámbrica para cada dispositivo inalámbrico con otro identificador del dispositivo inalámbrico, estando además el comparador dispuesto para determinar dicho otro identificador a partir de información presentada por el dispositivo por medio de dicha segunda interfaz inalámbrica y dicha base de datos.

5. Método según la reivindicación 3 o 4, en el que el comparador está colocado conjuntamente con un servidor de información, que soporta el traspaso de dicho dispositivo inalámbrico entre redes inalámbricas heterogéneas.

6. Método según cualquiera de las reivindicaciones anteriores, en el que el comparador se hace funcionar para enviar una credencial de inicio de sesión al dispositivo inalámbrico tras determinar que los identificadores comparados coinciden.

7. Sistema para detectar la intervención de un punto de acceso no autorizado en un trayecto de comunicaciones entre un dispositivo inalámbrico y uno o más recursos en una red de datos accesible por medio de un punto de acceso genuino, comprendiendo dicho sistema:

un comparador;

un servidor de mensajes de autenticación en dicha red de datos dispuesto para:

recibir por medio de dicho trayecto de comunicaciones, una solicitud, emitida por dicho dispositivo inalámbrico de un mensaje de autenticación cifrado, incluyendo la solicitud unos datos indicativos de un identificador del dispositivo inalámbrico;

generar un mensaje de autenticación cifrado usando los datos recibidos indicativos de dicho dispositivo inalámbrico presentados en dicho trayecto de comunicaciones, y

enviar dicho mensaje de autenticación cifrado al dispositivo inalámbrico;

en el que el dispositivo inalámbrico está

dispuesto para proporcionar a dicho comparador, por medio de un punto de acceso previamente autenticado con respecto a la red de datos,

unos datos indicativos del identificador del dispositivo inalámbrico;

unos datos indicativos de un identificador del punto de acceso usado en el trayecto de comunicaciones entre el dispositivo inalámbrico y la red de datos; y

el mensaje de autenticación cifrado;

en el que dicho comparador está dispuesto en funcionamiento para:

descifrar el mensaje de autenticación cifrado;

comparar los dos conjuntos de datos indicativos del identificador del dispositivo inalámbrico, y

comparar los datos indicativos de un identificador del punto de acceso con unos identificadores de puntos de acceso conocidos previamente almacenados en el comparador;

y si la comparación de los dos conjuntos de datos indicativos del dispositivo inalámbrico no coincide y el identificador del punto de acceso no coincide con los puntos de acceso conocidos, detectar la intervención de un punto de acceso no autorizado en la comunicación entre dicho dispositivo inalámbrico y la red por cable; y

señalizar el resultado de dicha comparación a dicho dispositivo inalámbrico por medio de dicho punto de acceso previamente autenticado con respecto a la red de datos.

8. Sistema según la reivindicación 7, en el que el identificador del dispositivo inalámbrico es un identificador de la interfaz de red inalámbrica del dispositivo.

9. Sistema según la reivindicación 7 u 8, en el que el comparador está colocado conjuntamente con un servidor de información, que soporta el traspaso de dicho dispositivo inalámbrico entre unas redes inalámbricas heterogéneas.

10. Sistema según la reivindicación 9, en el que el comparador comprende una base de datos que relaciona el identificador de interfaz inalámbrica de cada dispositivo inalámbrico con otro identificador del dispositivo inalámbrico, comprendiendo además el comparador unos medios dispuestos para determinar dicho otro identificador a partir de la información presentada por el dispositivo inalámbrico a través de una segunda interfaz inalámbrica, y dicha base de datos.

11. Comparador dispuesto en funcionamiento para:

recibir de un dispositivo inalámbrico, por medio de un punto de acceso previamente autenticado con respecto a una red de datos,

unos datos indicativos de un identificador del dispositivo inalámbrico que buscan autenticar un punto de acceso que proporciona acceso a la red de datos;

unos datos indicativos de un identificador del punto de acceso usado en el trayecto de comunicaciones entre el dispositivo inalámbrico y la red de datos; y

un mensaje de autenticación cifrado generado por un servidor de mensajes de autenticación en la red de datos, comprendiendo dicho mensaje datos indicativos del identificador usado por un dispositivo inalámbrico en la comunicación con la red de datos por medio de un punto de acceso que proporciona acceso inalámbrico a la red de datos, en el que dicho identificador fue presentado a dicha red de datos por dicho dispositivo inalámbrico a través de una comunicación entre dicho dispositivo inalámbrico y dicha red de datos accesible por medio de un punto de acceso genuino;

descifrar el mensaje de autenticación cifrado y

comparar los dos conjuntos de datos indicativos del identificador del dispositivo inalámbrico;

comparar los datos indicativos de un identificador del punto de acceso con unos identificadores de puntos de acceso conocidos previamente almacenados en el comparador; y

para detectar la intervención de un punto de acceso no autorizado en una comunicación entre dicho dispositivo inalámbrico y la red por cable si dichos dos conjuntos de datos indicativos del identificador del dispositivo inalámbrico no coinciden, y el identificador del punto de acceso no coincide con los identificadores de puntos de acceso conocidos, de manera que el resultado de la comparación se pueda proporcionar a dicho dispositivo inalámbrico a través de dicha red inalámbrica previamente autenticada.

Figura 1

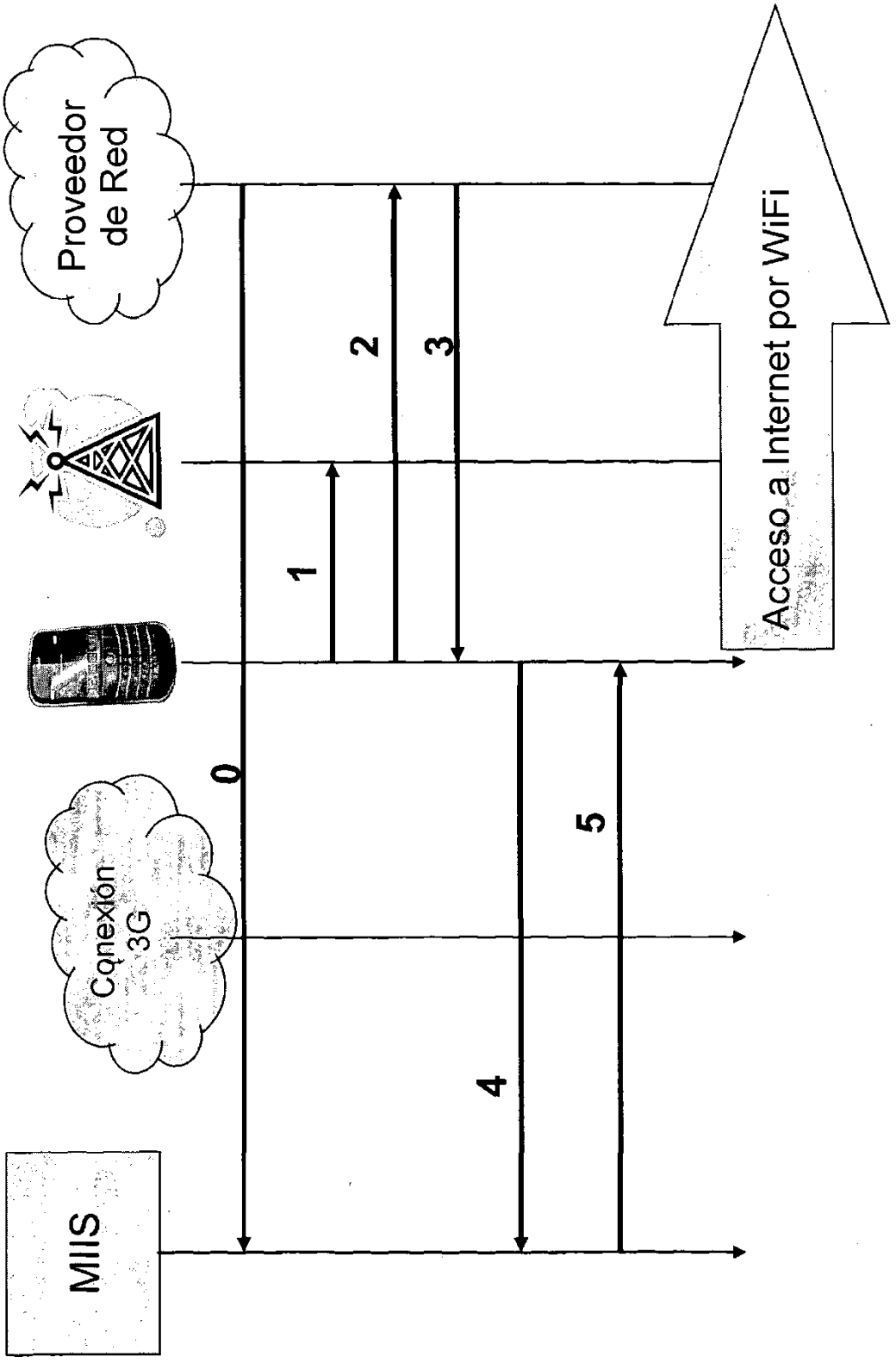

Proveedor de Red
Acceso a Internet por WiFi
Conexión 3G
MIIS
0
1
2
3
4
5

Figura 2

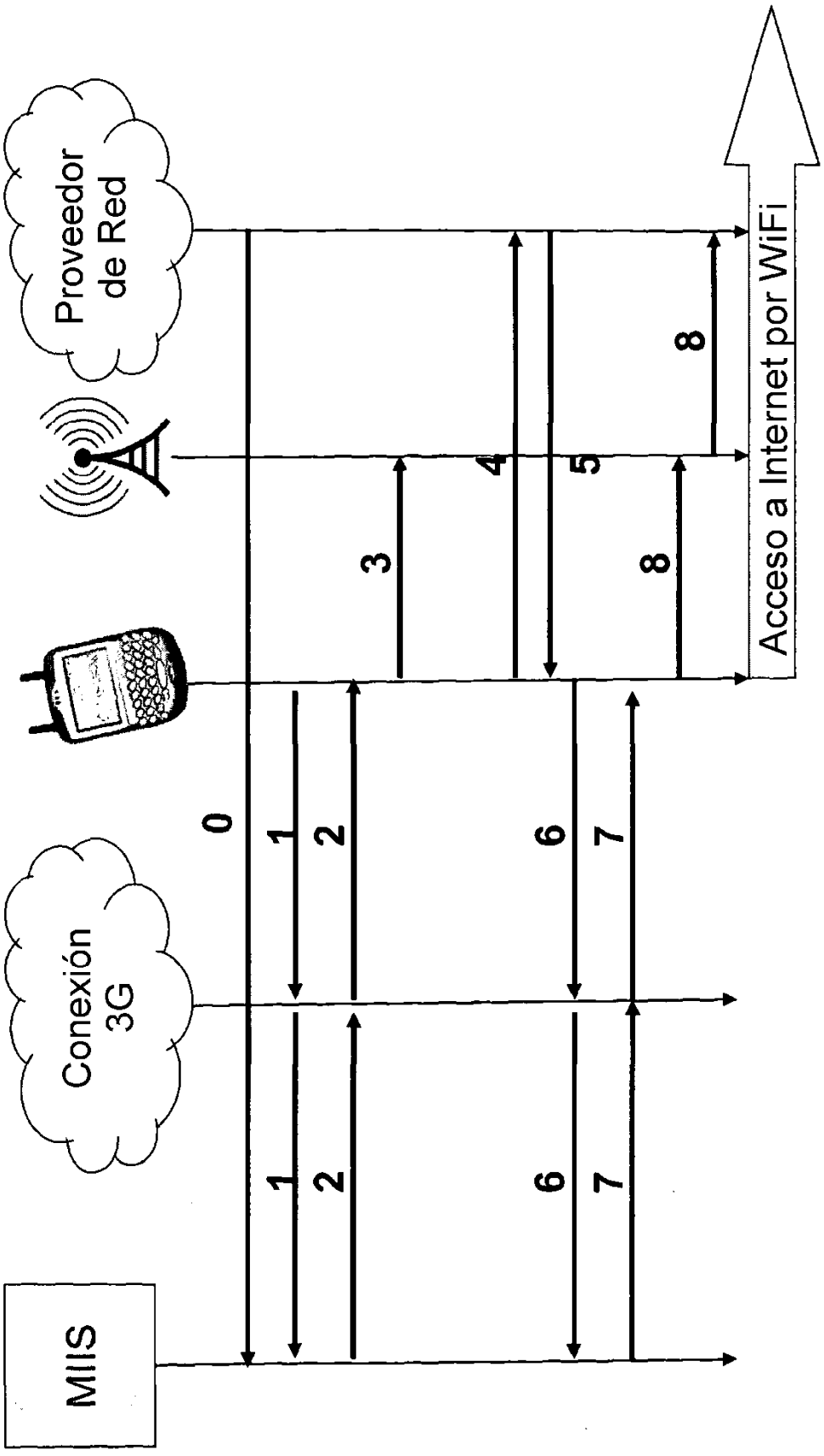

MIIS
Conexión 3G
Proveedor de Red
Acceso a Internet por WiFi
0
1
2
3
4
5
6
7
8
1
2
6
7
8

Figura 3

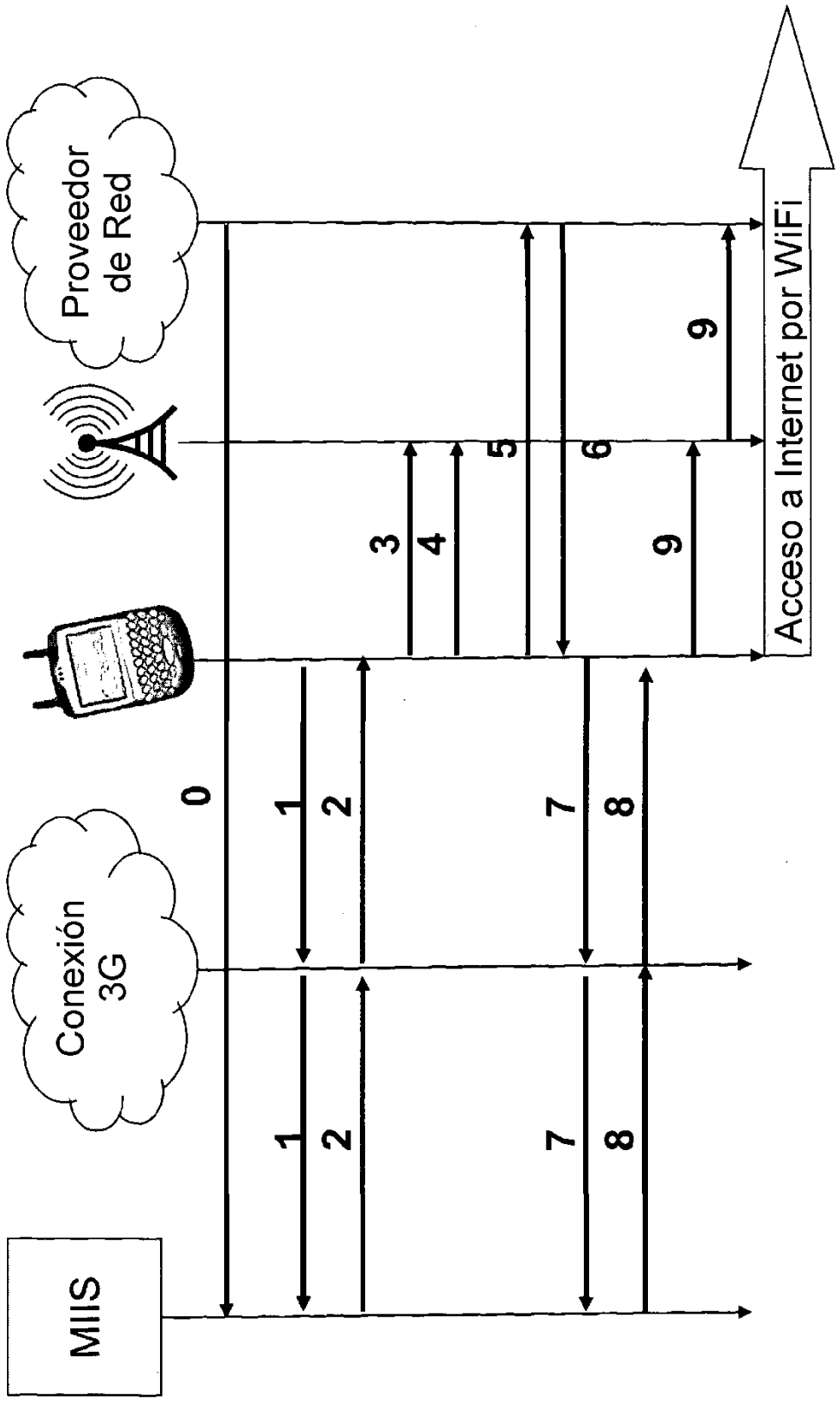

MIIS
Conexión 3G
Proveedor de Red
Acceso a Internet por WiFi
0
1
2
3
4
5
6
7
8
9

Figura 4

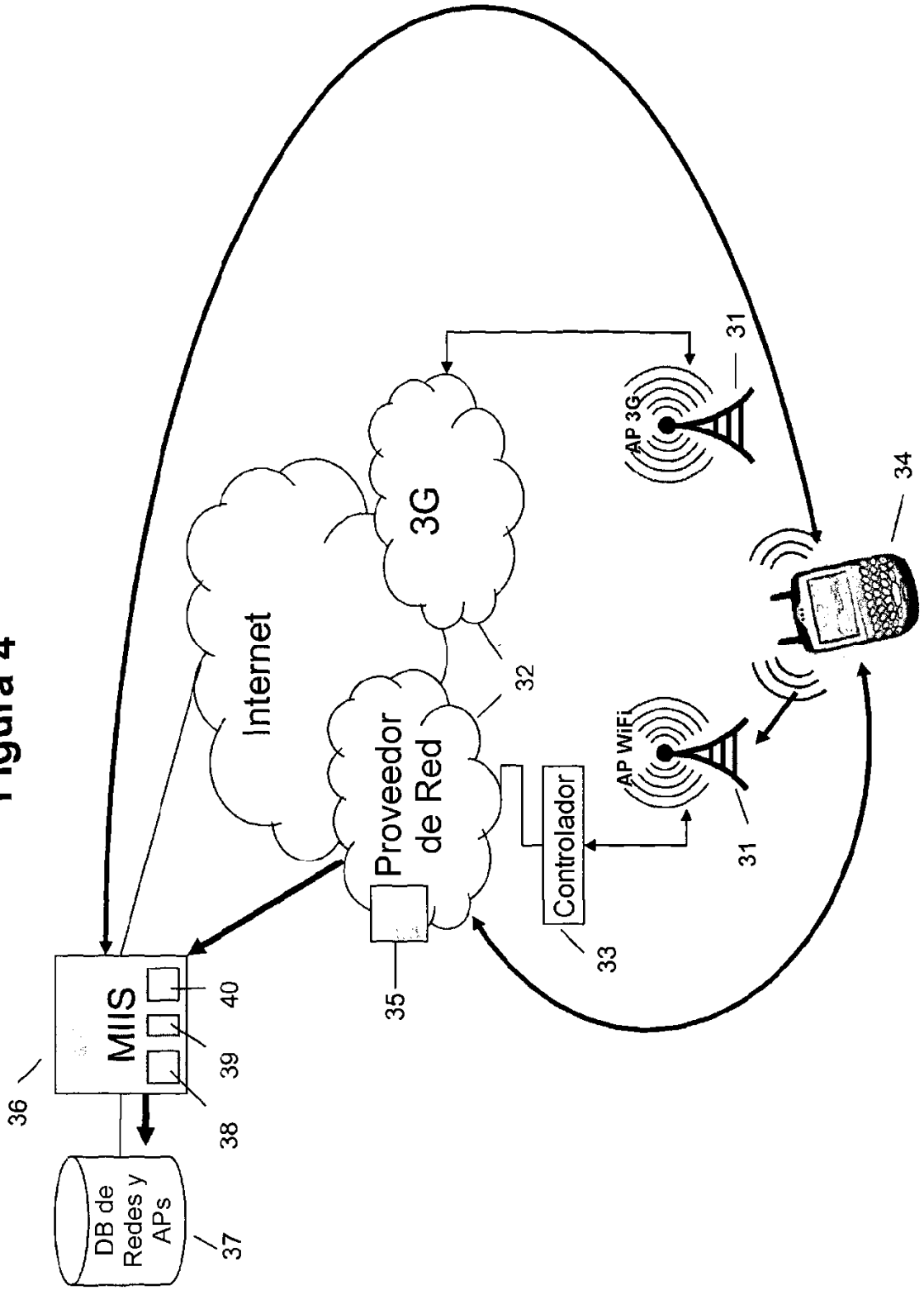

MIIS
DB de Redes y APs
Internet
3G
Proveedor de Red
Controlador
AP 3G
AP WiFi
31
32
33
34
35
36
37
38
39
40

Figura 5

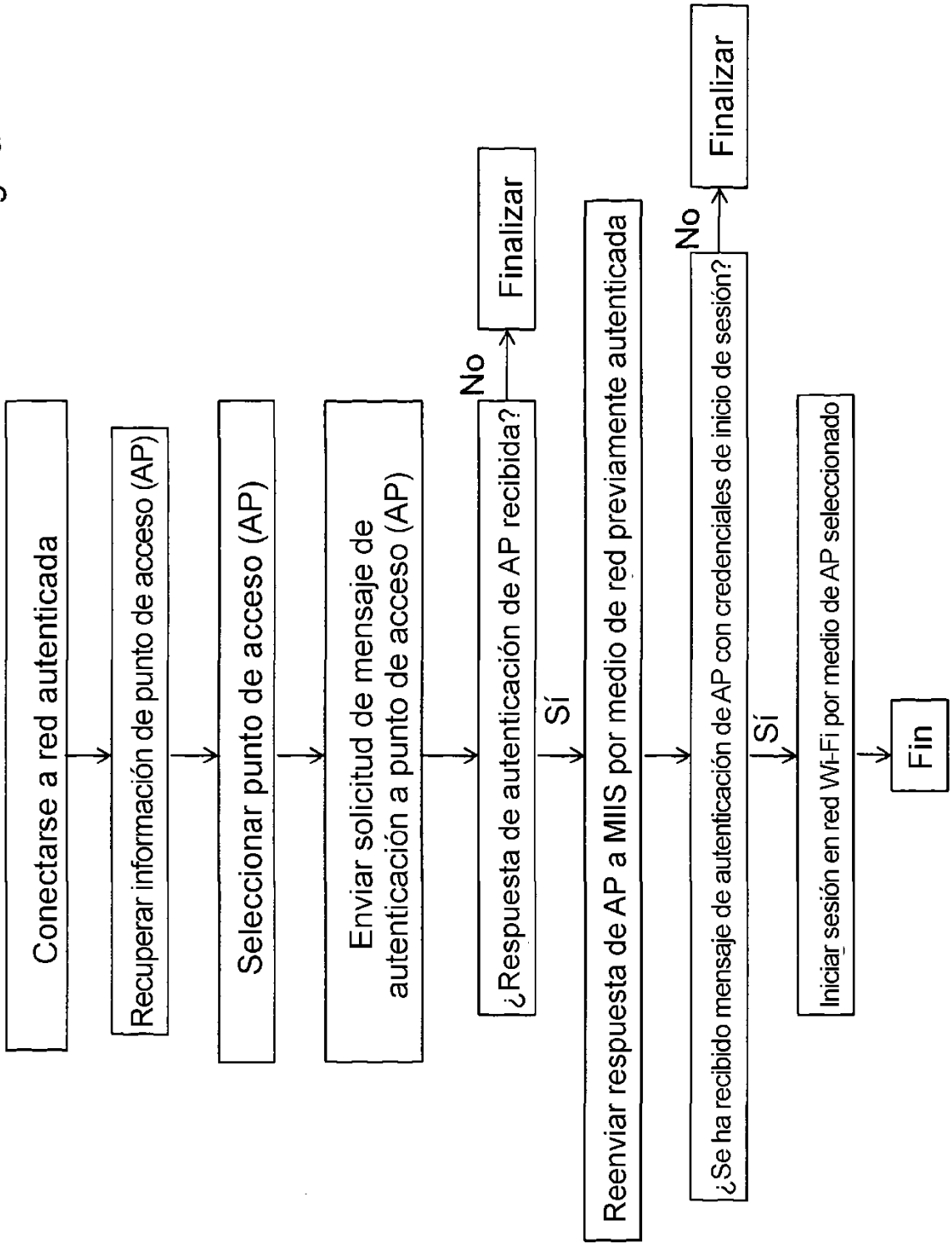

Conectarse a red autenticada
Recuperar información de punto de acceso (AP)
Seleccionar punto de acceso (AP)
Enviar solicitud de mensaje de autenticación a punto de acceso (AP)
¿Respuesta de autenticación de AP recibida?
No
Finalizar
Sí
Reenviar respuesta de AP a MIIS por medio de red previamente autenticada
¿Se ha recibido mensaje de autenticación de AP con credenciales de inicio de sesión?
No
Finalizar
Sí
Iniciar sesión en red Wi-Fi por medio de AP seleccionado
Fin

Figura 6

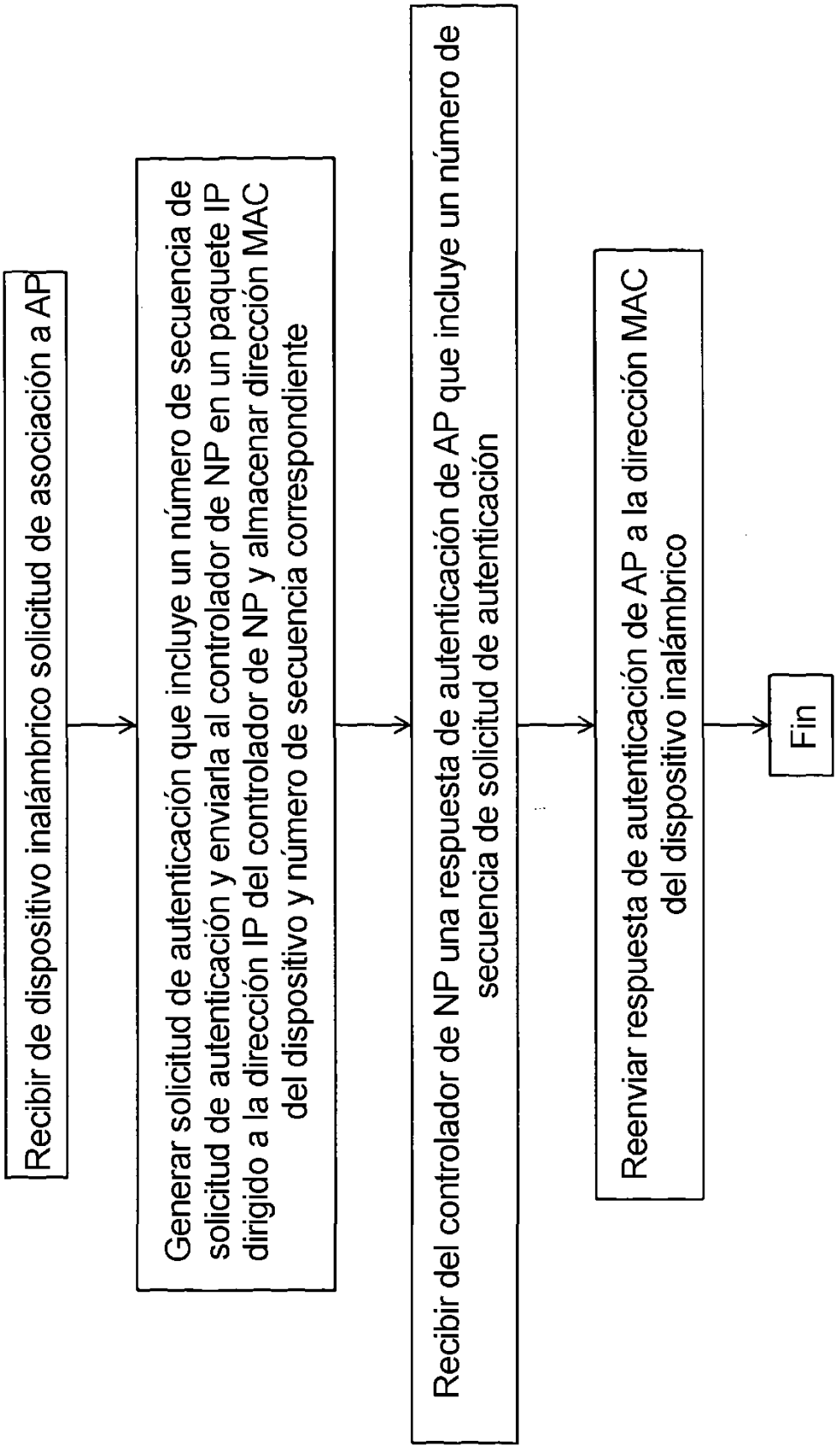

Recibir de dispositivo inalámbrico solicitud de asociación a AP
Generar solicitud de autenticación que incluye un número de secuencia de solicitud de autenticación y enviarla al controlador de NP en un paquete IP dirigido a la dirección IP del controlador de NP y almacenar dirección MAC del dispositivo y número de secuencia correspondiente
Recibir del controlador de NP una respuesta de autenticación de AP que incluye un número de secuencia de solicitud de autenticación
Reenviar respuesta de autenticación de AP a la dirección MAC del dispositivo inalámbrico
Fin

Figura 7

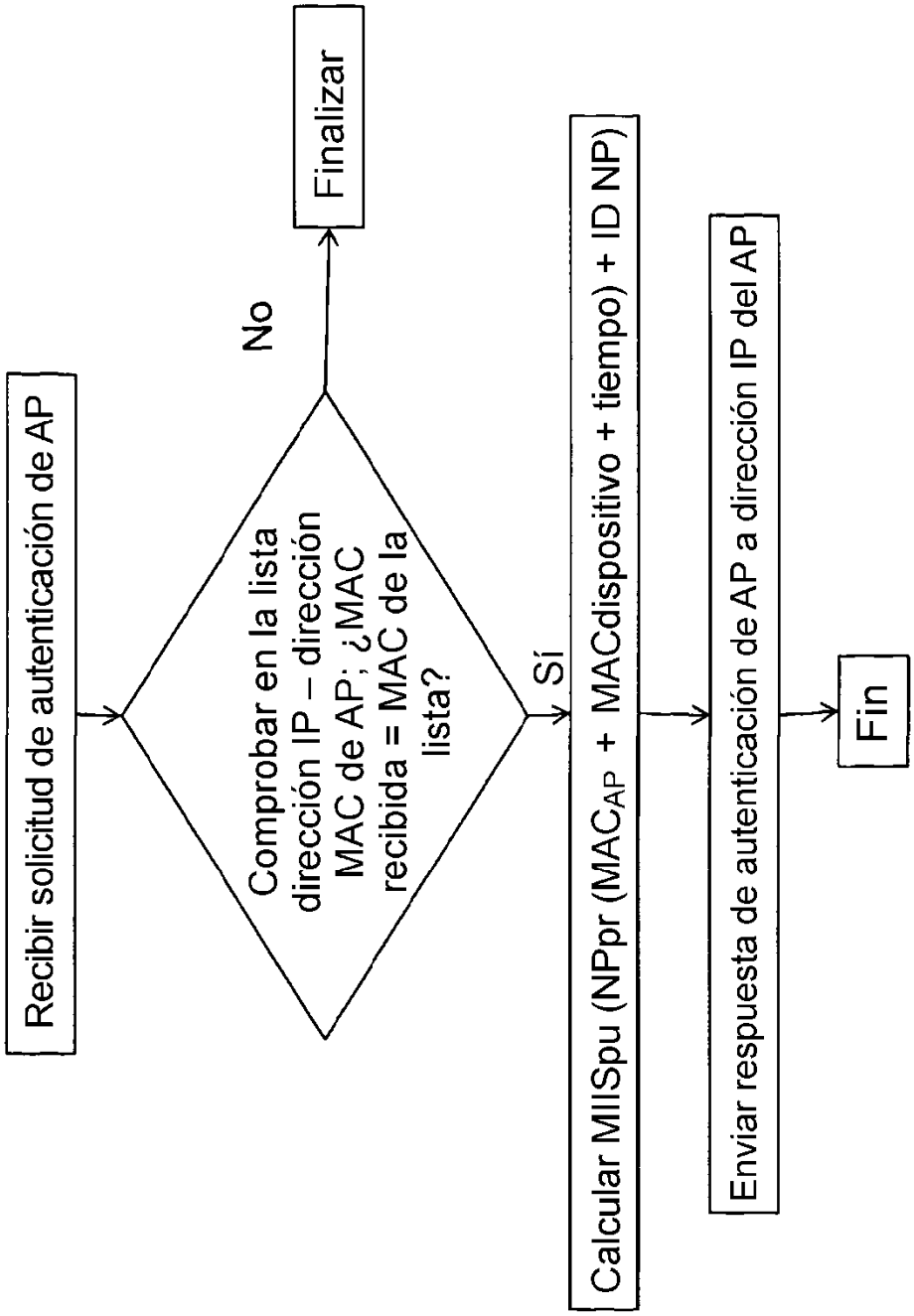
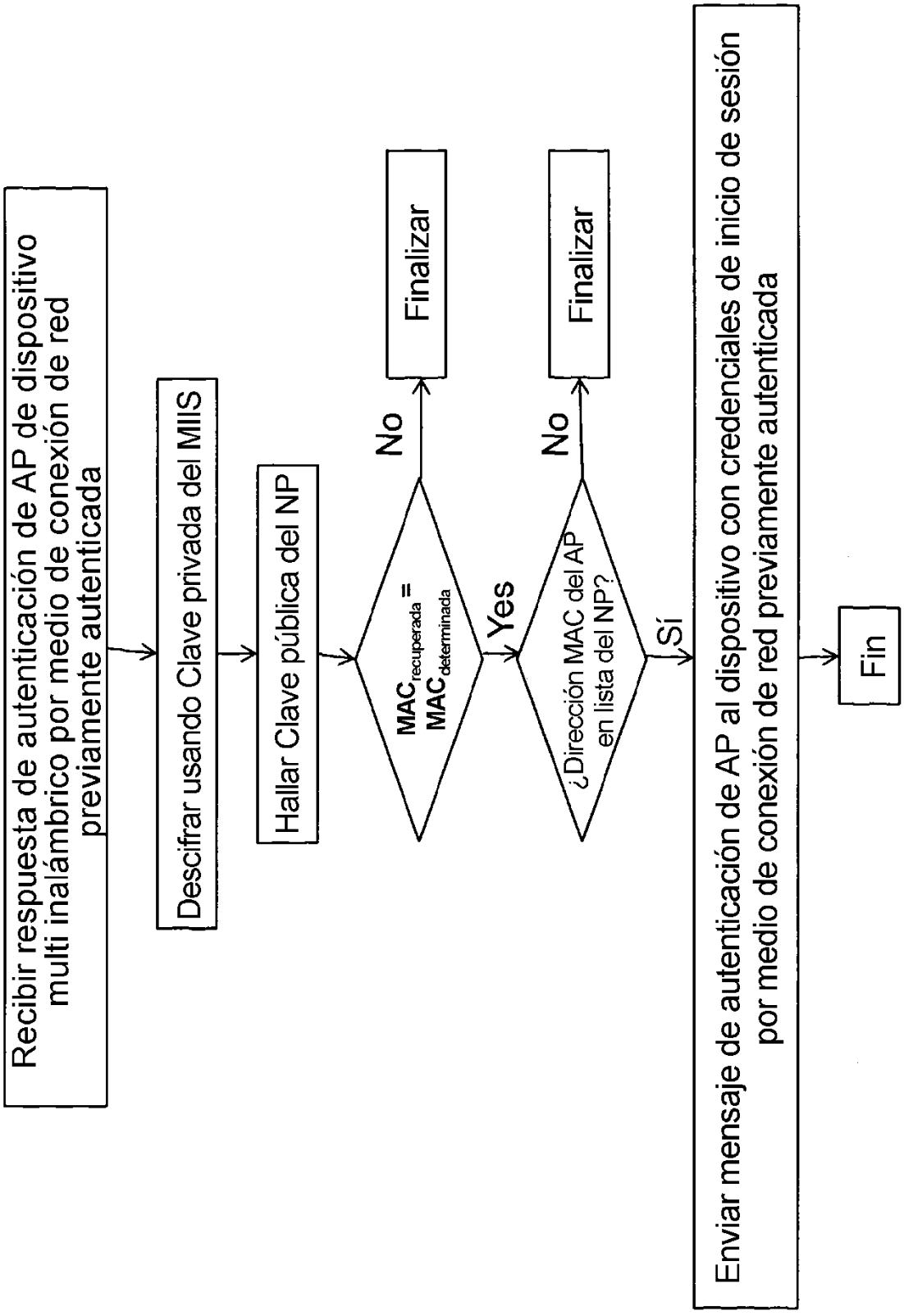

Recibir solicitud de autenticación de AP
Comprobar en la lista dirección IP – dirección MAC de AP; ¿MAC recibida = MAC de la lista?
No
Finalizar
Sí
Calcular MIISpu (NPpr (MACAP + MACdispositivo + tiempo) + ID NP)
Enviar respuesta de autenticación de AP a dirección IP del AP
Fin

Figura 8


Recibir respuesta de autenticación de AP de dispositivo multi inalámbrico por medio de conexión de red previamente autenticada
Descifrar usando Clave privada del MIIS
Hallar Clave pública del NP
MAC recuperada = MAC determinada
No
Finalizar
Yes
¿Dirección MAC del AP en lista del NP?
No
Finalizar
Sí
Enviar mensaje de autenticación de AP al dispositivo con credenciales de inicio de sesión por medio de conexión de red previamente autenticada
Fin