(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 685 420**

(51) Int. CI.:

G06F 9/445 (2008.01)
G06F 11/14 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **13.06.2006 PCT/US2006/023047**

(87) Fecha y número de publicación internacional: **21.12.2006 WO06135905**

(96) Fecha de presentación y número de la solicitud europea: **13.06.2006 E 06784842 (4)**

(97) Fecha y número de publicación de la concesión europea: **13.06.2018 EP 1897386**

(54) Título: **Aparatos y procedimientos para administrar la verificación de firmware en un dispositivo inalámbrico**

(30) Prioridad:

13.06.2005 US 690209 P
15.12.2005 US 303156

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.10.2018

(73) Titular/es:

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

(72) Inventor/es:

JHA, SANJAY K.;
ABDI, BEHROOZ L.;
SCOTT, CLIFTON EUGENE;
FOK, KENNY;
CASSETT, TIA, MANNING y
HWANG, JIHYUN

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Aparatos y procedimientos para administrar la verificación de firmware en un dispositivo inalámbrico

REIVINDICACIÓN DE PRIORIDAD BAJO 35 U.S.C. §119

[0001] La presente solicitud de patente reivindica prioridad a la solicitud provisional n.º 60/690 209, titulada "METHOD AND APPARATUS FOR FIRMWARE VERIFICATION ON A WIRELESS DEVICE [PROCEDIMIENTO Y APARATO PARA VERIFICACIÓN DE FIRMWARE EN UN DISPOSITIVO INALÁMBRICO]", presentada el 13 de junio, 2005.

ANTECEDENTES

[0002] Los aspectos descritos se refieren en general a dispositivos de comunicación inalámbrica y redes de ordenadores. Más particularmente, los aspectos descritos se refieren a la verificación de la integridad del firmware de un dispositivo inalámbrico, junto con la recopilación, el informe y el análisis de la información relacionada con el firmware recopilada desde el dispositivo inalámbrico.

[0003] La red inalámbrica conecta uno o más dispositivos inalámbricos a otros dispositivos informáticos sin una conexión eléctrica directa, tal como un cable de cobre o un cable óptico. Los dispositivos inalámbricos comunican datos, típicamente en forma de paquetes, a través de una red informática inalámbrica o parcialmente inalámbrica y abren un canal de "datos" o "comunicación" en la red de modo que el dispositivo puede enviar y recibir paquetes de datos. Los dispositivos inalámbricos a menudo tienen recursos de dispositivos inalámbricos, como programas y componentes de hardware, que funcionan individual y cooperativamente para usar y generar datos de acuerdo con su diseño y protocolo o configuración específico, como usando conexiones de comunicación abiertas para transmitir y recibir datos en la red.

[0004] Además, estos dispositivos inalámbricos contienen firmware que comprende código de datos y un programa que permite al dispositivo inalámbrico funcionar. Este código de programa y datos es crítico para el funcionamiento del dispositivo inalámbrico. Por ejemplo, los datos y el código de programa pueden especificar el protocolo para que el dispositivo inalámbrico lo use para comunicarse con la red, o los datos y el código de programa pueden especificar la(s) red(es) inalámbrica(s) con la(s) que el dispositivo inalámbrico puede funcionar.

[0005] En un aspecto, la integridad del firmware de un dispositivo inalámbrico se refiere a si los valores en el firmware de un dispositivo inalámbrico son los valores correctos para esa versión del firmware. Por ejemplo, una medida de la integridad del firmware puede determinar si el firmware ha sido dañado, ya sea involuntariamente, por ejemplo, por un error en un programa, o intencionalmente, como por un virus informático o manipulación intencional. En otro aspecto, la integridad del firmware de un dispositivo inalámbrico se relaciona con si la versión del firmware es la versión actual del dispositivo inalámbrico. Tal vez sea necesario actualizar o reemplazar la versión de firmware para un dispositivo inalámbrico determinado de manera periódica. Además, incluso es posible que el dispositivo inalámbrico tenga el firmware incorrecto instalado o que el firmware instalado no sea aceptable para un proveedor de red inalámbrica en particular.

[0006] El documento EP 1533 695 A1 divulga un procedimiento de actualización diferencial de datos almacenados en un terminal móvil desde una primera versión de datos hasta una versión de datos actualizada. Incluye detectar si los datos almacenados en el terminal móvil incluyen partes dañadas de los datos almacenados incoherentes con la primera versión de datos, cargar instrucciones de actualización diferencial y generar la versión de datos actualizada, incluida la reparación de cualquier parte dañada detectada.

[0007] Otra técnica anterior es la solicitud de patente internacional WO2005/008940.

[0008] Pueden ocurrir muchos problemas si se ve comprometida la integridad del firmware del dispositivo inalámbrico. Por ejemplo, el dispositivo inalámbrico puede no funcionar o puede interferir con el funcionamiento de la red mediante el uso de protocolos de comunicación incorrectos en la red inalámbrica. En otro ejemplo, los cambios en el firmware pueden permitir que el dispositivo inalámbrico sea usado para un proveedor de servicios de red inalámbrica diferente del proveedor para el que se adquirió. En este caso, el proveedor original de servicios de red inalámbrica puede perder dinero si subsidió el precio del dispositivo inalámbrico basándose en el acuerdo de que el dispositivo inalámbrico solo se utilizará en la red del proveedor de servicios de red original. Por lo tanto, cambiar el firmware para que el dispositivo inalámbrico funcione con otro proveedor de servicios de red inalámbrica puede violar el acuerdo firmado por el propietario del dispositivo inalámbrico.

[0009] Por consiguiente, sería ventajoso proporcionar un aparato y un procedimiento mejorados que permitan la verificación de la integridad de firmware en un dispositivo inalámbrico.

BREVE RESUMEN

[0010] Los aspectos descritos comprenden aparatos, procedimientos, medios legibles por ordenador y procesadores operables para la verificación de firmware en un dispositivo inalámbrico.

[0011] En algunos aspectos, un dispositivo de comunicación inalámbrica comprende una plataforma informática que tiene firmware, y un módulo de verificación de firmware operable para ejecutar una configuración de verificación para recoger información de firmware, en el que la información de firmware es indicativa de una integridad del firmware.

[0012] En otros aspectos, un dispositivo inalámbrico comprende un medio para controlar las operaciones en el dispositivo inalámbrico, y un medio para aplicar una configuración de verificación a los medios para controlar operaciones del dispositivo inalámbrico para recoger información indicativa de una integridad de los medios de controlar las operaciones del dispositivo inalámbrico.

[0013] En aún otros aspectos, un aparato para la gestión de la integridad de firmware en un dispositivo inalámbrico comprende un módulo de gestión de firmware operable para generar y transmitir una configuración de verificación para el dispositivo inalámbrico. La configuración de verificación comprende un esquema de verificación para aplicar al firmware para probar una integridad del firmware. El aparato comprende además un repositorio de información operable para recibir y almacenar un resultado de prueba de verificación generado basándose en una ejecución de la configuración de verificación mediante el dispositivo inalámbrico. Adicionalmente, el aparato comprende un analizador operable para generar una determinación de integridad basándose en el resultado de prueba de verificación generado, en el que la determinación de integridad representa una integridad del firmware.

[0014] En otros aspectos, un aparato para la gestión de la integridad de firmware en un dispositivo inalámbrico comprende un medio de generación para generar y transmitir una configuración de verificación a través de una red inalámbrica hasta un dispositivo inalámbrico. La configuración de verificación comprende un esquema de verificación para aplicar al firmware para probar una integridad del firmware. El aparato comprende además un medio de almacenamiento para recibir y almacenar un resultado de prueba de verificación basándose en una ejecución de la configuración de verificación mediante el dispositivo inalámbrico. Adicionalmente, el aparato comprende además un medio de análisis para analizar el resultado de prueba de verificación y generar un informe basado en el análisis, en el que el informe comprende una determinación de integridad que indica una integridad del firmware.

[0015] En otros aspectos, un procedimiento de verificación de la integridad de firmware en un dispositivo inalámbrico comprende generar una configuración de verificación que comprende un esquema de verificación para probar una integridad de firmware en el dispositivo inalámbrico, reenviar la configuración de verificación a un dispositivo inalámbrico, recibir un resultado de prueba de verificación generado basado en una aplicación del esquema de verificación en el firmware mediante el dispositivo inalámbrico y generar una determinación de integridad basada en el resultado de prueba de verificación generado, en el que la determinación de la integridad indica la integridad del firmware.

[0016] En otros aspectos, un procedimiento de verificación de la integridad de firmware en un dispositivo inalámbrico comprende recibir un esquema de verificación para probar una integridad de firmware en el dispositivo inalámbrico, generar un resultado de prueba de verificación basado en la aplicación del régimen de verificación para el firmware, y reenviar el resultado de prueba de verificación para el análisis para determinar la integridad del firmware.

[0017] En algunos aspectos, un medio legible por máquina comprende instrucciones que, cuando son ejecutadas por una máquina, hacen que la máquina realice operaciones, incluyendo la generación de una configuración de verificación que comprende un esquema de verificación para probar una integridad de firmware en el dispositivo inalámbrico, reenviar el configuración de verificación a un dispositivo inalámbrico, la recepción de un resultado de prueba de verificación generado basado en una aplicación del esquema de verificación en el firmware mediante el dispositivo inalámbrico, y la generación de una determinación de integridad basada en el resultado de prueba de verificación generado, en el que la determinación de integridad indica la integridad del firmware. En algunos aspectos relacionados, al menos en el procesador puede configurarse para realizar las acciones mencionadas anteriormente.

[0018] En otros aspectos, un medio legible por máquina comprende instrucciones que, cuando son ejecutadas por una máquina, hacen que la máquina realice operaciones, incluyendo la recepción de un esquema de verificación para probar una integridad de firmware en el dispositivo inalámbrico, la generación de un resultado de prueba de verificación basado en la aplicación del esquema de verificación al firmware y reenviar el resultado de prueba de verificación para su análisis con el fin de determinar la integridad del firmware. En aspectos relacionados, al menos en el procesador se puede configurar para realizar las acciones mencionadas anteriormente.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0019] Los aspectos divulgados se describirán a continuación junto con los dibujos adjuntos, proporcionados para ilustrar y no para limitar los aspectos divulgados, en los que designaciones iguales denotan elementos iguales, y en los que:

La Fig. 1 es un diagrama esquemático de un aspecto de un sistema para verificar la integridad del firmware en el dispositivo inalámbrico;

La Fig. 2 es un diagrama de flujo de mensajes asociado con un aspecto de una operación del sistema de la Fig. 1;

La Fig. 3 es un diagrama esquemático de un aspecto del dispositivo inalámbrico de la Fig. 1;

La Fig. 4 es un diagrama esquemático de un aspecto de una segmentación del firmware del dispositivo inalámbrico de la Fig. 3;

La Fig. 5 es un diagrama esquemático de un aspecto de un módulo configurador asociado con el administrador de usuarios de la Fig. 1;

La Fig. 6 es un diagrama esquemático de un aspecto del módulo de control de dispositivo asociado con el administrador de usuarios y/o el dispositivo inalámbrico de la Fig. 1;

La Fig. 7 es un diagrama esquemático de un aspecto de una red telefónica celular asociada con la Fig. 1;

La Fig. 8 es un diagrama de flujo de un aspecto de un procedimiento operable en un dispositivo inalámbrico para determinar la integridad del firmware en el dispositivo inalámbrico; y

La Fig. 9 es un diagrama de flujo de un aspecto de un procedimiento operable en un aparato para determinar la integridad del firmware en un dispositivo inalámbrico.

DESCRIPCIÓN DETALLADA

[0020] Con referencia a las Figs. 1 y 2, un aspecto de un sistema de verificación de firmware de dispositivo inalámbrico 10 para realizar una determinación de integridad de firmware 11 incluye un dispositivo inalámbrico 12 que tiene un módulo de verificación de firmware residente 20 que comprueba la integridad del firmware residente 14 basándose en una configuración de verificación 65. En este aspecto, la configuración de verificación 65 se genera y se recibe desde un módulo de gestión de firmware remoto 21 asociado con un servidor administrador de usuarios 40 (eventos 200 y 201). Por ejemplo, el servidor administrador de usuarios 40 puede residir en un dispositivo informático 18, tal como un servidor, ubicado a través de una red inalámbrica 42 desde el dispositivo inalámbrico 12. Además, por ejemplo, la configuración de verificación 65 se puede generar ejecutando un módulo configurador 44 asociado con el módulo de gestión de firmware 21. La configuración de verificación 65 incluye, en un aspecto, un esquema de verificación 89 ejecutable por el dispositivo inalámbrico 12 para aplicar al firmware 14 para generar un resultado de prueba de verificación 47 (evento 202). Por ejemplo, en un aspecto, el esquema de verificación 89 incluye, pero no se limita a, una comprobación de redundancia predeterminada que se aplica a al menos una parte del firmware 14 para generar un valor de suma de comprobación como resultado de prueba de verificación 47. Sin embargo, debe observarse que se pueden utilizar otros esquemas de verificación 89 y se pueden obtener los resultados de la prueba de verificación 47, como se analiza a continuación con más detalle. En cualquier caso, el módulo de verificación de firmware residente 20 almacena el resultado de prueba de verificación 47, por ejemplo, en un registro de información 46. Además, en un aspecto, el módulo de verificación de firmware 20 reenvía el registro de información 46 a través de la red inalámbrica 42 al servidor administrador de usuarios 40 (evento 204). El servidor administrador de usuarios 40 puede funcionar para almacenar el registro de información 46 en el repositorio de información 73.

[0021] El módulo de gestión de firmware 21 asociado con el servidor administrador de usuarios 40 accede al registro de información 46 y ejecuta un analizador 45 para generar un informe de integridad 61 que refleja la integridad del firmware 14 en el dispositivo inalámbrico 12 (evento 206). Por ejemplo, en un aspecto, el analizador 45 incluye un resultado de verificación predeterminado 37 que se compara con el resultado de prueba de verificación generado 47 en el registro de información 46 para producir la determinación de la integridad 11. El resultado de verificación predeterminado 37 comprende información o datos conocidos, en cualquier formato, que corresponde al resultado de la aplicación del esquema de verificación predeterminado 89 a una versión inalterada del firmware 14. En el aspecto analizado anteriormente, por ejemplo, el resultado de verificación predeterminado 37 puede incluir un valor de suma de comprobación predeterminado, que se compara con el valor de suma de comprobación generado mencionado anteriormente. En este caso, si hay una coincidencia entre el resultado de verificación predeterminado 37 y el resultado de prueba de verificación generado 47, la determinación de integridad 11 puede ser una salida que indique que el firmware 14 no está alterado o tiene un estado apropiado. De forma alternativa, por ejemplo, si no hay una coincidencia, entonces la determinación de integridad 11 puede ser una salida que indique que el firmware 14 ha sido alterado. Además, el analizador 45 genera el informe de integridad 61 que incluye la determinación de integridad 11, y, basándose en la configuración de verificación 65, que puede incluir información de firmware adicional 15 asociada con el firmware 14, como se analiza a continuación con más detalle.

[0022] El módulo de gestión de firmware 21 puede entonces ejecutarse para transmitir el informe de integridad 61 a un ordenador de operador 22 para su análisis (evento 208). En un aspecto, por ejemplo, un operador 23 en el ordenador de operador 22 revisa a continuación el informe de integridad 61 y, basándose en el contenido del informe 61, puede tomar la decisión de enviar un comando de control 78 al dispositivo inalámbrico 12 a través del servidor administrador de usuarios 40 (eventos 210, 212 y 216). En un aspecto, el operador 23 ejecuta el módulo de gestión de firmware 21 para transmitir el comando de control 78 a través de la red inalámbrica 42 al dispositivo inalámbrico 12. Por ejemplo, el comando de control 78 incluye, pero no se limita a, comandos tales como: un comando "inhabilitar" para cerrar la capacidad del usuario del dispositivo inalámbrico 12 para comunicarse con la red inalámbrica 42; un comando de "reconfiguración" para volver a cargar o restablecer una configuración de firmware; y un comando "habilitar" para restablecer la capacidad del usuario del dispositivo inalámbrico 12 para comunicarse con la red inalámbrica 42. Como ejemplo, el operador 23 puede decidir inhabilitar el dispositivo inalámbrico 12 para proteger la red inalámbrica 42 para que el dispositivo inalámbrico 12 no envíe mensajes que no se ajustan al protocolo apropiado para la red inalámbrica 42. De forma similar, se puede enviar un comando de "reconfiguración" para corregir el firmware alterado 14 para restaurar el firmware y devolverlo a su estado inalterado predeterminado, y se puede enviar un comando "habilitar" después de un comando "inhabilitar" para permitir comunicaciones una vez que se haya corregido el firmware alterado 14.

[0023] Además, en un aspecto, el módulo de gestión de firmware 21 puede incluir un módulo de control de dispositivo 94 que revisa el comando de control 78 y toma una decisión de permiso 95 en cuanto a si enviar comandos de control 78 al dispositivo inalámbrico 12 (evento 214). Por ejemplo, como se analizará con más detalle a continuación, la decisión de permiso 95 puede basarse en una fuente o generador de comandos de control 78, el tipo de acción asociada con el comando de control 78 y otros factores asociados con el dispositivo inalámbrico 12 y su red inalámbrica asociada 42. Además, en algunos aspectos, el módulo de control de dispositivo 94 puede consultar la fuente del comando de control 78 para confirmar y/o verificar el comando de control antes de enviarlo al dispositivo inalámbrico 12, como se analizará a continuación con más detalle.

[0024] En conjunto, en un aspecto, el módulo de verificación de firmware 20 puede incluir un módulo de control de dispositivo 94, que recibe y ejecuta el comando de control 78 (evento 218). En otros aspectos, el módulo de control de dispositivo local 94 puede consultar a la fuente o el generador de comandos de control 78 para confirmar el comando de control antes de ejecutarlo. Además, de forma adicional o de forma alternativa, el módulo de control de dispositivo 94 puede consultar al administrador de usuarios 40 para verificar que el comando de control 78 sea válido y/o que el originador del comando de control 78 tenga la autorización para emitir el comando.

[0025] Por lo tanto, el presente aparato, procedimientos, medios de legibles por ordenador y procesadores permiten generar y aplicar un esquema de verificación 89 al firmware 14 de dispositivo inalámbrico 12 con el fin de obtener el resultado de prueba de verificación 47 para usar en la creación de determinación de integridad 11. Además, los aspectos descritos pueden permitir la recopilación, análisis y notificación de información de firmware adicional 15 basada en la configuración de verificación 65, y pueden permitir además que los comandos de control 78 se ejecuten en el dispositivo inalámbrico 12 en respuesta a la determinación de integridad 11.

[0026] Con referencia a la Fig. 3, el dispositivo inalámbrico 12 puede incluir cualquier tipo de dispositivo inalámbrico informatizado, tal como teléfono celular 12, asistente digital personal, buscapersonas de texto bidireccional, ordenador portátil e incluso una plataforma informática independiente que tenga un portal de comunicaciones inalámbricas, y que también puede tener una conexión alámbrica a una red o a Internet. El dispositivo inalámbrico puede ser un dispositivo remoto secundario o de otro tipo que no tenga un usuario final, sino que simplemente transmita datos a través de la red inalámbrica 42, tal como un sensor remoto, una herramienta de diagnóstico, un retransmisor de datos y similares. El aparato y el procedimiento de verificación, recopilación y notificación de firmware del dispositivo inalámbrico pueden por consiguiente funcionar en cualquier forma de dispositivo inalámbrico o módulo de ordenador, incluido un portal de comunicación alámbrico o inalámbrico, que incluye, entre otros, módems inalámbricos, tarjetas PCMCIA, terminales de acceso, ordenadores personales, teléfonos o cualquier combinación o sub-combinación de los mismos.

[0027] Además, el dispositivo inalámbrico 12 tiene el mecanismo de entrada 96 para la generación de entradas en el dispositivo inalámbrico, y el mecanismo de salida 97 para generar información para el consumo por parte del usuario del dispositivo inalámbrico. Por ejemplo, el mecanismo de entrada 96 puede incluir un mecanismo tal como una tecla o teclado, un ratón, una pantalla táctil, un módulo de reconocimiento de voz, etc. Además, por ejemplo, el mecanismo de salida 97 puede incluir una pantalla, un altavoz de audio, un mecanismo de respuesta háptica, etc.

[0028] Además, el dispositivo inalámbrico 12 tiene la plataforma informática 13 que puede transmitir datos a través de la red inalámbrica 42, y que puede recibir y ejecutar aplicaciones de software y mostrar los datos transmitidos desde el servidor del administrador de usuarios 40 o en otro dispositivo informático conectado a la red inalámbrica 42. La plataforma informática 13 incluye un repositorio de datos 31, que puede comprender memoria volátil y no volátil tal como memoria de solo lectura y/o acceso aleatorio (RAM y ROM), EPROM, EEPROM, tarjetas de memoria flash, o cualquier memoria común a plataformas informáticas. Además, el repositorio de datos 31 puede incluir una o más células de memoria flash o puede ser cualquier dispositivo de almacenamiento secundario o terciario, tal como unos medios magnéticos, unos medios ópticos, una cinta o un disco flexible o duro.

[0029] Además, la plataforma informática 13 incluye también un motor de procesamiento 87, que puede ser un circuito integrado específico de aplicación ("ASIC"), u otro conjunto de chips, procesador, circuito lógico, u otro dispositivo de procesamiento de datos. El motor de procesamiento 87 u otro procesador tal como ASIC puede ejecutar una capa de interfaz de programación de aplicaciones ("API") 34 que interactúa con cualquier programa residente, tal como el módulo de verificación de firmware 20, en un repositorio de datos 31 del dispositivo inalámbrico 12. API 34 es un entorno de tiempo de ejecución que se ejecuta en el dispositivo inalámbrico respectivo. Uno de estos entornos de tiempo de ejecución es el software *Binary Runtime Environment for Wireless*® (*BREW*®) producido por Qualcomm, Inc., San Diego, California. Se pueden utilizar otros entornos de tiempo de ejecución que, por ejemplo, funcionan para controlar la ejecución de aplicaciones en dispositivos informáticos inalámbricos.

[0030] El motor de procesamiento 87 incluye varios subsistemas de procesamiento 88 incorporados en hardware, firmware, software y combinaciones de los mismos, que permiten la funcionalidad del dispositivo inalámbrico 12 y la operatividad del dispositivo inalámbrico en la red inalámbrica 42. Por ejemplo, los subsistemas de procesamiento 88 permiten iniciar y mantener comunicaciones e intercambiar datos con otros dispositivos en red. En un aspecto, tal como en un teléfono celular, el motor de procesamiento de comunicaciones 87 puede incluir uno o una combinación de subsistemas de procesamiento 88, tales como: sonido, memoria no volátil, sistema de archivos, transmitir, recibir, buscador, capa 1, capa 2, capa 3, control principal, procedimiento remoto, auricular, gestión de energía, diagnóstico, procesador de señal digital, codificador de voz, mensajería, administrador de llamadas, sistema Bluetooth®, Bluetooth® LPOS, determinación de posición, motor de posición, interfaz de usuario, suspensión, servicios de datos, seguridad, autentificación, USIM/SIM, servicios de voz, gráficos, USB, multimedia como MPEG, GPRS, etc. Para los aspectos divulgados, los subsistemas de procesamiento 88 del motor de procesamiento 87 pueden incluir cualquier componente del subsistema que interactúe con aplicaciones que se ejecutan en la plataforma informática 13. Por ejemplo, los subsistemas de procesamiento 88 pueden incluir cualquier componente de subsistema que reciba lecturas de datos y escrituras de datos desde la API 34 en nombre del módulo de verificación de firmware residente 20. Además, toda o una parte de la información de firmware 15 adicional que se recopila y luego se registra en el registro de información 46 está disponible desde estos subsistemas 88.

[0031] La plataforma informática 13 puede incluir además un módulo de comunicaciones 85 incorporado en hardware, firmware, software y combinaciones de los mismos, que permite las comunicaciones entre los diversos componentes del dispositivo inalámbrico 12, así como entre el dispositivo inalámbrico 12 y la red inalámbrica 42.

[0032] Además, la plataforma informática 13 incluye firmware 14, que puede comprender cualquier memoria no volátil que contiene datos, tales como datos de firmware 83, y/o un conjunto de instrucciones ejecutables, tales como código de firmware 84, que afectan al funcionamiento del dispositivo inalámbrico 12. Por ejemplo, el firmware 14 puede comprender un software que está incorporado en un dispositivo de hardware. Entre algunos ejemplos de memoria no volátil se incluyen ROM, EPROM, EEPROM y tarjetas flash. Además, el firmware 14 incluye información de verificación 19 que se utiliza para determinar la integridad del firmware 14. Por ejemplo, la información de verificación 19 incluye, pero no se limita a, la totalidad o una parte de los datos y/o instrucciones ejecutables que comprenden el firmware 14, y puede incluir datos que son una función de todos o una parte de los datos y/o instrucciones ejecutables que comprenden el firmware 14. En un aspecto, por ejemplo, la información de verificación 19 incluye una firma de firmware 80, que es información que identifica y/o autentifica el firmware dado. Por ejemplo, la firma de firmware 80 incluye, pero no se limita a, datos representativos de al menos uno de un nombre de firmware, una versión de firmware, un tamaño de firmware, un fabricante de firmware, etc. En otro ejemplo, la información de verificación 19 puede incluir un valor predeterminado 81 almacenado en una ubicación predeterminada 82 dentro del firmware 14, donde cualquier intento de alteración del firmware 14 cambiaría el valor y/o la ubicación. En otro aspecto más, la información de verificación 19 incluye la totalidad o una parte de los datos de firmware 83, y/o la totalidad o una parte del código de firmware 84. En este caso, los datos de firmware 83 y/o el código de firmware 84 pueden ser operados por el esquema de verificación 89 para generar el resultado de prueba de verificación 47.

[0033] La plataforma informática 13 incluye además módulo de verificación de firmware 20 para administrar las actividades de verificación del firmware en el dispositivo inalámbrico 12. El módulo de verificación de firmware 20 puede incluir hardware, software, firmware y/u otro conjunto de instrucciones ejecutables operables para administrar la recopilación en el dispositivo inalámbrico 12 y la transmisión a través de la red inalámbrica 42 de cualquier información relacionada con la integridad del firmware 14 del dispositivo inalámbrico 12. En un aspecto, el módulo de verificación de firmware 20 incluye una lógica de verificación 24 que proporciona la capacidad de recopilar, almacenar y proporcionar acceso a, o reenviar, información basada en la configuración de verificación 65. Además, en algunos aspectos, la lógica de verificación 24 puede proporcionar la capacidad de generar el resultado de prueba de verificación 47 y compararlo con el resultado de verificación predeterminado 37 para generar la determinación de la integridad 11. El módulo de verificación de firmware 20 puede iniciarse en cualquier momento, y el resultado de prueba de verificación 47 y/o información de firmware 15 registrado en el registro de información 46 puede almacenarse en el dispositivo inalámbrico 12 y obtenerse en cualquier momento a través de una conexión alámbrica o inalámbrica al dispositivo inalámbrico 12.

[0034] El módulo de verificación de firmware 20 puede recopilar cualquier información de verificación de firmware relevante para el uso y/o verificación del firmware. Basándose en la configuración de verificación 65, el módulo de verificación de firmware 20 puede aplicar el esquema de verificación de firmware 89 al firmware 14 y generar el resultado de prueba de verificación 47. Además, el módulo de verificación de firmware 20 puede almacenar esta información en un registro de información 46, ya sea en el repositorio de datos residente 31 o en otro dispositivo de memoria conectable al dispositivo inalámbrico o accesible al dispositivo inalámbrico 12 a través de la red inalámbrica 42. Además, el registro de información 46 puede incluir los detalles de la configuración de verificación 65 en asociación con la información de verificación de firmware recopilada.

[0035] En un aspecto donde el resultado de verificación predeterminado 37 es conocido para el dispositivo inalámbrico 12, por ejemplo, cuando se incluye en la configuración de verificación 89, el módulo de verificación de firmware 20 puede entonces ejecutar la lógica de verificación 24 para comparar localmente el resultado de prueba 47 con el resultado predeterminado 37 para obtener la integridad 11 del firmware 14. Por lo tanto, en un aspecto, el módulo de verificación de firmware 20 proporciona al dispositivo inalámbrico 12 una capacidad residente o autónoma para recuperar y registrar información de firmware en un dispositivo inalámbrico 12, así como para permitir la transmisión y el análisis remoto de dicha información de firmware.

[0036] De forma alternativa, el módulo de verificación de firmware 20 puede transmitir el resultado de prueba 47 y/o el registro de información 46 a otro dispositivo informático para obtener la integridad del firmware 14 del dispositivo inalámbrico 12. Por ejemplo, el módulo de verificación de firmware 20 puede hacer que el dispositivo inalámbrico 12 transmita selectivamente el registro de información 46 al servidor administrador de usuarios 40 a través de la red inalámbrica 42. En un aspecto, el registro de información 46 se transmite a través de una conexión de comunicación abierta desde el dispositivo inalámbrico 12 a la red inalámbrica 42, y de este modo "a cuestas" a través de una conexión abierta, tal como una llamada de voz o datos en el dispositivo inalámbrico 12. En una configuración de red celular, el registro de información 46 puede transmitirse al servidor de administrador de usuarios 40 a través del servicio de mensajes cortos.

[0037] En otro aspecto, es servidor del administrador de usuarios remoto 40 lee el registro de información 46 desde el dispositivo inalámbrico 12 a través del módulo de verificación de firmware residente 20, y en algunos casos, escribe comandos de control 78 a la plataforma informática 13 y altera el funcionamiento del dispositivo inalámbrico 12, como volver a configurar el firmware 14. En consecuencia, el acceso al módulo de verificación de firmware 20 permite que el servidor administrador de usuarios 40 controle de forma remota los parámetros para la recopilación, análisis e informes de verificación de firmware.

[0038] El módulo de verificación de firmware 20 funciona basándose en la configuración de verificación 65. La configuración de verificación 65 puede generarse mediante cualquier dispositivo informático conectado a la red inalámbrica 42, o puede transmitirse localmente al dispositivo inalámbrico 12 tal como mediante una entrada manual de un usuario, y/o mediante la transmisión desde un lector de medios conectado localmente, o incluso puede haber sido cargado en el dispositivo inalámbrico 12 en el momento de la fabricación. En un aspecto, por ejemplo, la configuración de verificación 65 es generada por el servidor administrador de usuarios 40 como se explica a continuación.

[0039] La configuración de verificación 65 incluye instrucciones y datos que dictan las operaciones a realizar por el módulo de verificación de firmware 20. Por ejemplo, como se analizó anteriormente, la configuración de verificación 65 puede incluir el esquema de verificación 89, que comprende instrucciones para probar la integridad del firmware 14. El esquema de verificación 89 puede incluir, entre otros, instrucciones relacionadas con pruebas tales como: una comprobación de redundancia, que incluye una suma de comprobación, bits de paridad, dígitos de verificación, comprobación de redundancia longitudinal, comprobación de redundancia cíclica ("CRC"), comprobación de redundancia horizontal, comprobación de redundancia vertical, resumen de mensaje criptográfico, suma de comprobación de Fletcher y Adler-32; probar un valor predeterminado en una ubicación predeterminada dentro del firmware 14; y probar un resultado predeterminado de aplicar una función predeterminada a la totalidad o a una parte de los datos y/o el código contenido en el firmware 14. De forma alternativa, el esquema de verificación 89 puede incluir instrucciones para recuperar un esquema de verificación predeterminado desde una fuente predeterminada, tal como desde otro dispositivo informático a través de la red inalámbrica 42. Además, por ejemplo, para realizar un seguimiento de los cambios en ciertas partes del firmware 14 o para aumentar la seguridad, el firmware 14 puede estar segmentado, y uno o más esquemas de verificación 89 pueden aplicarse a uno o más de los segmentos del firmware 14. Como tal, el esquema de verificación 89 puede identificar un esquema para aplicar a cada segmento del firmware 14.

[0040] Por ejemplo, en referencia a la Fig. 4, un aspecto de esquema de verificación de firmware 89 comprende un algoritmo de CRC en el que el módulo de verificación de firmware 20 aplica el algoritmo de CRC a diferentes segmentos del firmware 14. En un aspecto, el firmware 14 está dividido en un número predeterminado de segmentos de código, tales como segmentos de código 306, 308, 310, y un número predeterminado de segmentos de datos, tales como segmentos de datos 312, 314, 316. La lógica de verificación 24 ejecuta la configuración de verificación 65 para aplicar el algoritmo CRC a cada segmento 306, 308, 310, 312, 314, 316, y generar los valores de resultado de prueba de verificación 322, 324, 326, 328, 330, 332. Además, en este aspecto, cuando la configuración de

verificación 65 incluye el resultado de verificación predeterminado 37, la lógica de verificación 24 se ejecuta para comparar los valores de resultado de prueba 322, 324, 326, 328, 330, 332 con valores de verificación predeterminados 334, 336, 338, 340, 342, 344 para generar una determinación de integridad 11 para cada segmento del firmware 14. Sin embargo, en casos alternativos, los valores de verificación predeterminados 334, 336, 338, 340, 342, 344 pueden almacenarse en otro dispositivo informático, como en el administrador de usuarios 40, y los valores de resultado de prueba de verificación generado 322, 324, 326, 328, 330, 332 se transmiten desde el dispositivo inalámbrico 12 al otro dispositivo para la comparación. En cualquier caso, este procedimiento de dividir el firmware en segmentos es ventajoso por varias razones. Primero, si solo uno o más de los segmentos tienen un problema con su integridad, solo esos segmentos necesitarán ser reparados. Además, si los segmentos que no son críticos para el funcionamiento del dispositivo inalámbrico son los únicos segmentos que se ha encontrado que tienen un problema con su integridad, entonces el dispositivo inalámbrico 12 tal vez no tenga que ser inhabilitado. Además, muchos esquemas de verificación de firmware 89 pueden funcionar de manera más fiable cuando se aplican a menos elementos de datos del firmware 14. Por ejemplo, un esquema de verificación de firmware 89 basado en la paridad puede ser más fiable con menos elementos de datos del firmware 14.

[0041] Continuando con referencia a la Fig. 4, otro esquema de verificación de firmware 89 puede simplemente registrar la firma de firmware 80. Por ejemplo, en este caso, la firma de firmware 80 puede incluir valores o datos relacionados con una versión de firmware 81, un tamaño de firmware 82 y una fecha actual 83. Esta información se compara a continuación con valores de resultado de prueba de verificación predeterminados 37, que en este caso son una versión de firmware predeterminada, un tamaño de firmware predeterminado y una fecha predeterminada para determinar la integridad del firmware 14.

[0042] Además, con referencia de nuevo a la Fig. 3, la configuración de verificación 65 puede incluir además un parámetro de seguimiento 90 que dicta qué información recoger en el registro de información 46 y la frecuencia con la que recoger esta información. Por ejemplo, el parámetro de seguimiento 90 puede incluir instrucciones sobre la frecuencia con la que se inicia el esquema de verificación 89, y las instrucciones para registrar el resultado de prueba de verificación generado 47. Además, por ejemplo, el parámetro de seguimiento 90 puede incluir instrucciones que definen qué información de firmware adicional 15 se debe recopilar y cuándo recopilarse. Por ejemplo, el parámetro de seguimiento 90 puede identificar el estado o la información de estado predeterminado para recopilar como información de firmware adicional 15 en momentos predeterminados de aplicaciones predeterminadas y/o subsistemas predeterminados 88. La información de firmware 15 adicional puede comprender, pero no se limita a, cualquier información relacionada con intentos de acceso al firmware exitosos y/o fallidos, cambios realizados en el firmware, operaciones realizadas por el dispositivo inalámbrico 12 y/o los subsistemas 88, información de diagnóstico del dispositivo inalámbrico, información relacionada con el estado y/o el funcionamiento de cualquier aplicación residente en el dispositivo inalámbrico 12, etc. Además, por ejemplo, el parámetro de seguimiento 90 dicta el seguimiento de ciertas actividades o acciones que tienen lugar en el dispositivo, tales como la ejecución del comando de control 78, y requieren el almacenamiento de información relacionada con estas actividades/acciones en el registro de información 46, como en el registro de acciones 49.

[0043] Además, la configuración de verificación 65 puede incluir un parámetro de información 91 que especifica cuándo el módulo de verificación de firmware 20 debería informar o transmitir el registro de información 46, o a quién para permitir el acceso al registro de información 46. Por ejemplo, el parámetro de notificación 91 puede incluir instrucciones para transmitir el registro de información 46 inmediatamente después de aplicar el esquema de verificación de firmware 89 al firmware 14. Otros parámetros de notificación 91 pueden incluir instrucciones para transmitir el registro de información 46 en un tiempo predeterminado o un intervalo predeterminado, o a la aparición de eventos predeterminados, como al establecer un canal de comunicación con la red de comunicaciones 42.

[0044] Además, en un aspecto, la configuración de verificación 65 puede incluir parámetros de comando de control 92, que pueden incluir un comando de control 78 asociado con una condición predeterminada 93 con el fin de controlar las operaciones en el dispositivo inalámbrico 12. Por ejemplo, en el caso donde el dispositivo inalámbrico 12 genera localmente la determinación de integridad 11 comparando el resultado de prueba de verificación generado 47 con el resultado de prueba de verificación predeterminado 37, los parámetros de comando de control 92 pueden permitir que el módulo de verificación de firmware 20 controle localmente el dispositivo inalámbrico 12 en el caso donde sea incorrecto o se descubre el firmware alterado 14. Por ejemplo, la condición 93 puede ser una cierta determinación de integridad 11, tal como: (1) una determinación que indica que el firmware correcto está presente; y (2) una determinación que indica que el firmware 14 ha sido alterado. En el caso de la condición (1), el comando de control 78 puede ser un comando "continuar la operación" para llevar a cabo las operaciones del dispositivo inalámbrico 12. En el caso de la condición (2), el comando de control 78 puede ser un comando de "inhabilitación" para impedir la capacidad del dispositivo inalámbrico 12 para comunicarse con la red inalámbrica 42. Puede haber una amplia variedad de condiciones 93 y comandos de control 78 correspondientes, dependiendo de la aplicación dada, que se pueden incluir en el parámetro de comando de control 92. Por ejemplo, en algunos modos de realización, los diversos parámetros, comparaciones y resultados pueden registrarse en el registro de información 46. Adicionalmente, las acciones realizadas basándose en la configuración de verificación 65, tales como aquellas acciones asociadas con el comando de control 78, se pueden registrar en el registro de acciones 49 (Fig. 3).

[0045] Por lo tanto, la configuración de verificación 65 proporciona un medio flexible para controlar el funcionamiento del módulo de verificación de firmware 20.

[0046] Además, en algunos aspectos, el módulo de verificación de firmware 20 incluye un módulo de control de dispositivo 94 operable para recibir un comando de control generado localmente o generado remotamente 78. Además, el módulo de control de dispositivo 33 puede incluir una lógica de control operable para ejecutar el comando de control 78 en el dispositivo inalámbrico 12. Como se explicará con más detalle a continuación, el módulo de control de dispositivo 94 puede verificar un comando de control 78 antes de ejecutar el comando de control 78 en el dispositivo inalámbrico 12.

[0047] Por ejemplo, el comando de control 78 puede ser cualquier operación que se puede ejecutar en el dispositivo inalámbrico respectivo 12 e incluye, pero no se limita a, los comandos tales como un comando de inhabilitación, un comando de habilitación, y un comando reconfiguración, donde el comando de inhabilitación hace que el dispositivo inalámbrico 12 no sea operativo para comunicaciones que no sean de emergencia o completamente no operativo, donde el comando de habilitación hace que el dispositivo inalámbrico 12 sea operativo para comunicaciones, y donde el comando de reconfiguración establece al menos uno de los valores de firmware relacionados con una característica operativa del dispositivo inalámbrico. En algunos modos de realización, por ejemplo, el comando de reconfiguración puede incluir el cambio de datos y/o valores de firmware por aire, tal como mediante la inclusión de un parche de software operable para sobrescribir software en el firmware 14. En general, el comando de control 78 se emite local o remotamente en respuesta a los resultados del módulo de verificación de firmware 20 y normalmente será una respuesta a la obtención de la integridad del firmware 14.

[0048] Además, módulo de verificación de firmware 20 puede incluir una configuración de servicio limitado 38 que puede hacerse funcionar para establecer un canal de comunicaciones de acceso limitado a través de la red inalámbrica 42, que, en un aspecto, en general, no está disponible para el usuario final del dispositivo inalámbrico 12. Por ejemplo, el canal de comunicaciones de acceso limitado se puede usar para transmitir el registro de información 46 o para recibir el comando de control 78. Además, en el caso en que las comunicaciones del dispositivo inalámbrico 12 hayan sido inhabilitadas de otra forma, el canal de comunicaciones de acceso limitado puede permitir llamadas de emergencia, tales como llamadas "911", o puede permitir llamadas a un operador u otra parte designada asociada con el proveedor de red inalámbrica. La identificación y la configuración del canal de comunicaciones de acceso limitado se basan en una configuración de servicio limitada 39. La configuración de servicio limitada 39 puede identificar el tipo de comunicaciones que están permitidas, y puede identificar los canales de comunicación asociados que pueden utilizarse. La configuración de servicio limitada 38 puede recibirse a través de la red inalámbrica 42, puede transferirse localmente al dispositivo inalámbrico 12, como por ejemplo a través de una conexión en serie, o puede precargarse en el dispositivo inalámbrico 12.

[0049] Con referencia de nuevo a la Fig. 1, la red inalámbrica 42 incluye cualquier red de comunicaciones operable, al menos en parte, para permitir las comunicaciones inalámbricas entre el dispositivo inalámbrico 12 y cualquier otro dispositivo conectado a la red inalámbrica 42. Además, la red inalámbrica 42 puede incluir todos los componentes de red y todos los dispositivos conectados que forman la red. Por ejemplo, la red inalámbrica 42 puede incluir al menos uno, o cualquier combinación, de: una red telefónica celular; una red telefónica terrestre; una red telefónica satelital; una red de infrarrojos tal como una red basada en la Infrared Data Association ("IrDA"); una red inalámbrica de corto alcance; una red de tecnología Bluetooth®; una red de protocolo ZigBee®; una red de protocolo de banda ultra ancha ("UWB"); una red de radiofrecuencia doméstica ("HomeRF"); una red de protocolo de acceso inalámbrico compartido ("SWAP"); una red de banda ancha, como una red de alianza de compatibilidad con Ethernet inalámbrica ("WECA"), una red de alianza de fidelidad inalámbrica ("Wi-Fi Alliance") y una red 802.11; una red telefónica pública conmutada; una red de comunicaciones pública heterogénea, como Internet; una red de comunicaciones privada; y la red de radio móvil terrestre. Entre los ejemplos adecuados de redes telefónicas se incluyen al menos una, o cualquier combinación, de redes/tecnologías analógicas y digitales, tales como: acceso múltiple por división de código ("CDMA"), acceso múltiple por división de código de banda ancha ("WCDMA"), sistema universal de telecomunicaciones móviles ("UMTS"), servicio avanzado de telefonía móvil ("AMPS"), acceso múltiple por división de tiempo ("TDMA"), acceso múltiple por división de frecuencia ("FDMA"), acceso múltiple por división de frecuencia ortogonal ("OFDMA"), sistema global para comunicaciones móviles ("GSM"), portadora única ("1X") tecnología de transmisión de radio ("RTT"), tecnología de evolución de solo datos ("EV-DO"), servicio general de radio por paquetes ("GPRS"), entorno GSM De datos mejorados ("EDGE"), acceso de paquete de datos de enlace descendente de alta velocidad ("HSPDA"), sistemas de satélite analógicos y digitales, y cualquier otra tecnología/protocolo que pueda usarse en al menos una de una red de comunicaciones inalámbricas y una red de comunicaciones de datos.

[0050] El servidor del administrador de usuarios 40 puede comprender al menos uno de cualquier tipo de hardware, software, firmware, servidor, ordenador personal, mini ordenador, ordenador central, o cualquier dispositivo informático, ya sea de propósito especial o dispositivo informático general. Además, el servidor administrador de usuarios 40 puede residir completamente en el dispositivo inalámbrico 12. Además, puede haber servidores o dispositivos informáticos independientes asociados con el servidor administrador de usuarios 40 que trabajan de forma coordinada para proporcionar datos en formatos utilizables a las partes y/o para proporcionar una capa de control independiente en el flujo de datos entre los dispositivos inalámbricos 12 y el servidor administrado de usuario

40. El servidor administrador de usuarios 40 (o pluralidad de módulos) puede enviar agentes o aplicaciones de software, tales como el módulo de verificación de firmware residente 20, al dispositivo inalámbrico 12 a través de la red inalámbrica 42, de manera que el dispositivo inalámbrico 12 devuelva información desde sus aplicaciones y subsistemas residentes. Por ejemplo, los dispositivos inalámbricos 12 pueden transmitir el resultado de aplicar un esquema de verificación de firmware 89 al firmware 14 en forma de un registro de información 46, donde el servidor administrador de usuarios 40 puede comparar este resultado con el resultado de verificación predeterminado 37 para generar una determinación de integridad 11 que representa la integridad del firmware del dispositivo inalámbrico 12.

[0051] El administrador de usuarios 40 incluye módulo de gestión de firmware remoto 21 para administrar las operaciones de verificación de firmware. El módulo de gestión de firmware remoto 21 puede incluir software, hardware, firmware y, en general, cualquier instrucción ejecutable operable por el servidor administrador de usuarios 40. El módulo de gestión de firmware remoto 21 puede descargar la totalidad o una parte de la versión residente del módulo de verificación de firmware 20 en un dispositivo inalámbrico 12. De forma alternativa, la versión residente del módulo de gestión de firmware remoto 21 puede cargarse en el dispositivo inalámbrico 12 durante el proceso de ensamblaje inicial o mediante conexiones directas durante un proceso de configuración. Además, el módulo de gestión de firmware remoto 21 incluye lógica de verificación 59 que es ejecutable por el servidor administrador de usuarios 40 para generar la configuración de verificación 65 y para administrar la recopilación y el análisis del registro de información 46 desde dispositivos inalámbricos 12. El módulo de gestión de firmware remoto 21 puede "tirar" el registro 46 basándose en los comandos de un usuario, o el registro puede "empujarse" desde los dispositivos inalámbricos 12 en momentos predeterminados, al alcanzar niveles predeterminados de almacenamiento de memoria/datos o al alcanzar condiciones predeterminadas tales como el dispositivo inalámbrico 12 que proporciona protocolos inapropiados entre el dispositivo inalámbrico 12 y la red inalámbrica 42.

[0052] Con referencia a las Figs. 1 y 5, en un aspecto, el módulo de gestión de firmware remoto 21 incluye un módulo configurador 44 que incluye hardware, firmware, software y/o cualquier otra lógica asociada que permite que el módulo configurador 44 genere la configuración de verificación 65. En un aspecto, el módulo configurador 65 ejecuta la lógica de configuración 56 que ensambla los diversos componentes de una configuración de verificación dada 65 basándose en realizar selecciones a partir de una serie de parámetros variables. Por ejemplo, los parámetros que componen la configuración de verificación 65 pueden variar dependiendo del tipo/marca/modelo del dispositivo inalámbrico y/o el proveedor de servicios de red. Como tal, la lógica de configuración 56 puede proporcionar a un usuario la capacidad de seleccionar de un menú de una pluralidad de tipos de dispositivos inalámbricos 16 y una pluralidad de proveedores de servicios de red 17 para generar un menú apropiado desde el cual seleccionar los parámetros de configuración de verificación 65. De manera similar, puede haber uno o más de cada tipo de parámetros para elegir para compensar la configuración de verificación 65. Por ejemplo, la lógica de verificación 56 puede proporcionar a un usuario la capacidad de seleccionar de un menú de al menos uno de una pluralidad de esquemas de verificación de firmware 50, una pluralidad de parámetros de seguimiento 51, una pluralidad de parámetros de notificación 52, una pluralidad de parámetros de comandos de control 53 y una pluralidad de valores de resultado de verificación predeterminados 54. De forma alternativa, en lugar de seleccionar los diversos parámetros individualmente, la lógica de configuración 56 puede proporcionar al usuario la capacidad de seleccionar de un menú de una pluralidad de configuraciones de verificación predeterminadas 55, que incluyen agrupaciones predeterminadas de los parámetros mencionados anteriormente que comprenden la configuración de verificación 65. Además, en un aspecto, el seleccionado de la pluralidad de tipos de dispositivos inalámbricos 16 y el seleccionado de la pluralidad de proveedores de servicios de red 17 puede estar correlacionado con uno dado de una pluralidad de tipos de firmware 65 y/o un conjunto predeterminado de los parámetros de verificación que son apropiados para un dispositivo inalámbrico particular 12. Por ejemplo, para una marca XYZ de dispositivo inalámbrico que opera en un proveedor de servicios inalámbricos ABC, la lógica de configuración 56 puede determinar qué firmware 14 debería tener instalado el dispositivo inalámbrico 12, y así puede generar la configuración de verificación 65 que incluye el conjunto apropiado de parámetros correspondientes.

[0053] Una vez que se determina la configuración de verificación 65, el módulo configurador 44 y/o el módulo de gestión de firmware remoto 21 son operables para transmitir la configuración de verificación 65 a uno o más dispositivos inalámbricos 12 para iniciar el seguimiento y la gestión de la verificación de firmware en ese dispositivo.

[0054] El módulo de gestión de firmware remoto 21 puede incluir un repositorio de información 73 para almacenar el registro de información 46, incluyendo el resultado de prueba de verificación 47 y/o información de firmware adicional 15, recibida desde el dispositivo inalámbrico 12 basándose en la ejecución de la configuración de verificación 65. El repositorio de información 73 puede incluir cualquier tipo de memoria o dispositivo de almacenamiento. Aunque se ilustra como asociado con el módulo de gestión de firmware remoto 21, el repositorio de información 73 puede ubicarse en cualquier lugar en comunicación con el administrador de usuarios 40, tal como en otro servidor o dispositivo informático conectado a la red inalámbrica 42, en el dispositivo inalámbrico 12 o en un ordenador de ayuda de red inalámbrica 22.

[0055] Además, como se señaló anteriormente, el módulo de gestión de firmware remoto 21 puede incluir analizador 45, que puede incluir hardware, software, firmware, y combinaciones de los mismos para el análisis y procesamiento conectado información de verificación de firmware registrada en el repositorio de información 73 con el fin de

generar un informe 61 y determinación de la integridad 11. Adicionalmente, el analizador 45 puede incluir además lógica de análisis 41 que comprende algoritmos, rutinas de toma de decisiones, programas estadísticos, etc. para analizar e interpretar los registros de información 46 contenidos en el módulo de repositorio de información 73. Aunque ilustrado como asociado con el módulo de firmware remoto 21, el analizador 45 puede ubicarse en cualquier lugar en comunicación con el servidor administrador de usuarios 40, en otro servidor conectado a la red inalámbrica 42, en el dispositivo inalámbrico 12 o en un ordenador de ayuda de red inalámbrica 22.

[0056] Además, hay que señalar que, dado que muchos esquemas de verificación de firmware 89 son heurísticos, la determinación de integridad obtenida 11 del firmware 14 puede ser una probabilidad o valor subjetivo. Además, como se describió anteriormente, la determinación de integridad obtenida 11 del firmware 14 puede depender adicionalmente de qué versión 81 del firmware 14 está instalada en una marca y/o modelo particular del dispositivo inalámbrico 12 en un momento particular. Entonces, por ejemplo, el firmware existente 14 puede no estar dañado y era el firmware 14 correcto para el dispositivo inalámbrico 12 en el momento de la fabricación, pero puede que ya no sea una versión válida actual del firmware 14; por lo tanto, en este caso, el analizador 45 puede determinar que la integridad del firmware 14 está comprometida.

[0057] Además, en un aspecto, la determinación de integridad de firmware 11 es una medida de los dos: si el dispositivo inalámbrico 12 tiene el firmware correcto 14; y, si el firmware en el dispositivo inalámbrico 12 está, o puede estar, dañado o una medida de certeza de que el firmware 14 no está dañado. Entonces, la determinación de integridad 11 del firmware 14 en el dispositivo inalámbrico 12 puede representar una baja integridad si, por ejemplo, un dispositivo inalámbrico 12 tiene una versión de firmware 14 que ya no es compatible con el proveedor de servicios de red, o si la versión del firmware 14 en el dispositivo inalámbrico 12 puede estar dañado medido mediante una comparación del resultado de prueba de verificación 47 con el resultado de verificación predeterminado 37. En algunos aspectos, esta comparación del resultado de prueba de verificación 47 con el resultado de verificación predeterminado 37 solo puede indicar si el firmware 14 está dañado o no y, por lo tanto, la determinación de integridad 11 puede ser una categoría de probabilidad o subjetiva, por ejemplo, "lo más probable". "10 % de probabilidad", etc.

[0058] En un aspecto, el informe de 61 y/o el registro de información 46 puede revisarse de forma manual, tal como por un técnico, ingeniero de campo, portadora, operador 23 o el usuario del dispositivo inalámbrico 12, para la evaluación de información relacionada con la verificación de firmware asociada con un dispositivo inalámbrico particular 12. El operador 23 o el usuario del dispositivo inalámbrico 12 pueden generar una nueva configuración de verificación 65 o comando de control 78, tal como un comando de "inhabilitar dispositivo inalámbrico", para el dispositivo inalámbrico respectivo 12 basándose en el registro de información 46 y/o en el informe 61. En general, el informe 61 puede ser útil para detectar y corregir problemas relacionados con la verificación de firmware a través del análisis del registro de información 46. Como tal, el informe 61 incluye cualquier forma de salida que representa el análisis del registro de información 46 y otra información contenida en el repositorio de información 73, así como cualquier otra información asociada que pueda incorporarse en estándares predeterminados 37 tales como informes de virus, versiones de firmware apropiadas para el dispositivo inalámbrico 12, tiempos de desconexión para versiones de firmware incorrectas, etc.

[0059] Aunque se ilustra como produciendo un informe 61, el módulo de gestión de firmware 21 y sus componentes correspondientes pueden dar una visualización a punto de la información relacionada con verificación de firmware recogida de los dispositivos inalámbricos 12 en cualquier forma, tal como tablas, mapas, visualizaciones de gráficos, texto sin formato, páginas web o programas interactivos, o cualquier otra visualización o presentación de los datos. Por ejemplo, el módulo de gestión de firmware 21 puede presentar información relacionada con la verificación de firmware en un monitor o dispositivo de visualización, y/o puede transmitir esta información, por ejemplo por correo electrónico, a otro dispositivo informático para su posterior análisis o revisión. Además, el módulo de gestión de firmware 21 puede ejecutarse para cambiar la configuración de verificación 65 y/o enviar un comando de control 78 para ejecutarse en el dispositivo inalámbrico respectivo 12 basándose en el registro de información 46 y/o basándose en el informe 61 generado por el analizador 45.

[0060] Con referencia a la Fig. 6, tanto el módulo de verificación de firmware remoto 21 como el módulo de verificación de firmware 20 pueden tener un módulo de control de dispositivo 94 operable para recibir/generar el comando de control 78, ya sea local o remotamente, y ejecutar comando de control 78 en el dispositivo inalámbrico 12 o transmitir el comando de control 78 al dispositivo inalámbrico 12. En un aspecto, por ejemplo, el comando de control 78 puede contener tanto una identificación ("ID") de usuario 28 como una actividad de control 29. La ID de usuario 28 puede ser alguna manera de identificación del originador del comando de control 78. Por ejemplo, el ID de usuario 28 puede ser un nombre, un número, una firma digital, un hash, un certificado digital o cualquier otro tipo de datos o valores que puedan asociarse con una parte. Además, la ID de usuario 28 puede no estar contenida explícitamente en el comando de control 78, pero en lugar de eso puede obtenerse a partir del origen del comando de control 78. Adicionalmente, la actividad de control 29 es la operación que debe realizarse mediante el módulo de verificación de firmware 20 mediante la ejecución del comando de control 78. Como se mencionó anteriormente, estas operaciones incluyen inhabilitar las comunicaciones, habilitar las comunicaciones, reconfigurar el firmware y/o los parámetros de comunicación, etc.

[0061] Antes de ejecutar o reenviar el comando de control 78, el administrador de control de dispositivos 94 puede ejecutar la lógica de permiso 25 para comprobar la autenticidad o la autoridad del usuario que emite un comando de control 78, y/o para verificar y confirmar que el usuario realmente quiere iniciar el comando. La verificación de un comando de control 78 puede incluir, por ejemplo, un aviso al operador 23 (u otro usuario) para confirmar si el operador 23 realmente desea ejecutar la actividad de control 29 en el dispositivo inalámbrico 12. La confirmación o cancelación del comando de control se puede recibir como verificación de comando 43. Además, por ejemplo, para autentificar el comando de control, la lógica de permiso 25 puede analizar el ID de usuario 28 y controlar la actividad 29 desde el comando de control 78 y puede utilizar una base de datos de una pluralidad de ID de usuario 26 correlacionadas con una pluralidad de permisos de control 27, y correlacionadas con una pluralidad de identificaciones de dispositivos inalámbricos (ID) 33, para comprobar la autorización para emitir el comando de control 78. Los permisos de control 27 pueden identificar una o más actividades de control autorizadas 29 para una ID de usuario 28 y/o ID de dispositivo inalámbrico, que es una identificación de un dispositivo inalámbrico específico. Por ejemplo, ciertos usuarios pueden estar restringidos a ciertas actividades de control o a poder controlar ciertos dispositivos inalámbricos. Sin embargo, debe observarse que la pluralidad de ID de usuario 26, la pluralidad de permisos de control 27 y la pluralidad de identificaciones (ID) de dispositivos inalámbricos 33 pueden correlacionarse de cualquier manera. Por ejemplo, el comando de control 78 puede contener una ID de usuario 28 de un operador 23, y una actividad de control 29 de "inhabilitar comunicaciones" para una particular de la pluralidad de identificaciones de dispositivo inalámbrico 33. La lógica de permiso 25 busca en la base de datos de permisos de control 27 y las ID de usuario 26 para determinar si se permitió que el operador 23 inhabilitara el dispositivo inalámbrico 12 dado. La lógica de permiso 25 genera una decisión de permiso 30 basada en esta comprobación de autorización, y/o basada en el valor de la verificación de comando 43.

[0062] Como se ha descrito anteriormente en referencia a la Fig. 1, aunque el operador 23 en este aspecto se ilustra como una persona, en otros aspectos el operador 23 puede ser un dispositivo informático que puede incluir hardware, software, firmware, y combinaciones de los mismos para analizar y responder al informe 61 o a una comunicación externa tal como desde el usuario del dispositivo inalámbrico 12. Además, el operador 23 puede residir en el mismo dispositivo informático que el servidor administrador de usuarios 40, que podría ser el dispositivo inalámbrico 12. En un aspecto, el operador 23 es una persona que puede responder a un informe 61. Adicionalmente, el operador 23 puede incluir algoritmos, rutinas de toma de decisiones, programas estadísticos, etc. para analizar e interpretar el informe 61. Aunque se ilustra como asociado con el ordenador de ayuda de red inalámbrica 22, el operador 23 puede estar ubicado en cualquier lugar en comunicación con la red inalámbrica 42, tal como en el servidor administrador de usuarios 40, otro servidor conectado a la red o incluso en el dispositivo inalámbrico 12.

[0063] Con referencia a la Fig. 7, en un aspecto, el dispositivo inalámbrico 12 comprende un teléfono celular. Un sistema telefónico celular 71 puede incluir una red inalámbrica 42 conectada a una red alámbrica 58 a través de una red de soporte 64. Los dispositivos inalámbricos 12 se fabrican con mayores capacidades informáticas y, a menudo, pueden comunicar paquetes que incluyen voz y datos a través de la red inalámbrica 42. Como se describió anteriormente, estos dispositivos inalámbricos "inteligentes" 12 tienen API 34 en su plataforma informática local 13 que permite a los desarrolladores de software crear aplicaciones de software que funcionen en el teléfono celular 12 y controlar ciertas funcionalidades en el dispositivo. La Fig. 7 es un diagrama representativo que ilustra de forma más completa los componentes de una red inalámbrica celular y la interrelación de los elementos de un aspecto del presente sistema. La red inalámbrica celular 71 sirve meramente de ejemplo y puede incluir cualquier sistema mediante el cual los módulos remotos, tales como los dispositivos inalámbricos 12, se comuniquen por aire entre sí, y/o entre los componentes de una red inalámbrica 14, incluyendo, sin limitación, los servidores y las portadoras de la red inalámbrica.

[0064] En el sistema 71, el servidor de administrador de usuarios 40 puede estar en comunicación a través de una red alámbrica 58 (por ejemplo, una red de área local, LAN) con un repositorio de datos independiente 60 para almacenar información de verificación de firmware, tal como los registros de datos 46, recopilados a partir de los dispositivos inalámbricos 12. Además, un servidor de gestión de datos 62 puede estar en comunicación con el servidor administrador de usuarios 40 para proporcionar capacidades de postprocesado, control de flujo de datos, etc. El servidor administrador de usuarios 40, el repositorio de datos 60 y el servidor de gestión de datos 62 pueden estar presentes en el sistema telefónico celular 91 con cualquier otro componente de red que se necesite para proporcionar servicios de telecomunicación celular. El servidor administrador de usuarios 40, y/o el servidor de gestión de datos 62 se comunican con la red portadora 64 a través de los enlaces de datos 70 y 66, que pueden ser enlaces de datos tales como Internet, una LAN o WAN segura, u otra red. La red portadora 64 controla los mensajes (que en general son paquetes de datos) enviados a un centro de conmutación móvil ("MSC") 68. Además, la red portadora 64 se comunica con el MSC 68 mediante una red 70, tal como Internet y/o el POTS ("servicio telefónico ordinario"). Típicamente, en la red 70, una red o parte de Internet transfiere datos, y la parte de POTS transfiere información de voz. El MSC 68 puede estar conectado a varias estaciones base ("BTS") 72 mediante otra red 74, tal como una red de datos y/o una parte de Internet para la transferencia de datos y una parte de POTS para la información de voz. BTS 72 finalmente transmite mensajes de forma inalámbrica a los dispositivos inalámbricos, como los dispositivos inalámbricos 12, mediante el servicio de mensajes cortos ("SMS") u otros procedimientos de transmisión inalámbrica.

[0065] Con referencia a la Fig. 8, un aspecto de un procedimiento para verificación de integridad de firmware en un dispositivo inalámbrico incluye cargar al menos una parte de un módulo de verificación de firmware 20 en una plataforma informática 13 de un dispositivo inalámbrico 12 (bloque 120). Por ejemplo, el módulo de verificación de firmware 20 puede incorporarse dentro del hardware y/o firmware del dispositivo inalámbrico durante la fabricación del dispositivo. De forma alternativa, la verificación de firmware puede ser "empujada" por un servidor administrador de usuarios 40 al dispositivo inalámbrico 12 o "retirada" desde un servidor administrador de usuarios por el dispositivo 12 inalámbrico a través de una red 42 inalámbrica. De forma alternativa, el módulo de verificación de firmware 20 puede ser "retirado" o "empujado" dependiendo de si el dispositivo inalámbrico 12 tiene o no la última versión del módulo de verificación de firmware 20 para el dispositivo inalámbrico respectivo 12. En otra alternativa, la carga del módulo de verificación de firmware 20 puede ser configurable de cualquier manera, por ejemplo, iniciada por un evento predeterminado, tal como el dispositivo inalámbrico 12 que tiene dificultad para comunicarse con la red inalámbrica 42, o el dispositivo inalámbrico 12 que se comunica con un proveedor de servicios de red diferente. En otra alternativa, el empuje o retirada del módulo de verificación de firmware 20 al dispositivo inalámbrico 12 puede ser configurable de cualquier manera, por ejemplo: siendo iniciado por un evento predeterminado.

[0066] Además, este aspecto del procedimiento incluye la carga de al menos una parte de una configuración de verificación 65 para probar la integridad de firmware en la plataforma informática 13 del dispositivo inalámbrico 12 (bloque 122). Por ejemplo, la configuración de verificación 65 puede incorporarse dentro del hardware y/o firmware del dispositivo inalámbrico durante la fabricación del dispositivo. De forma alternativa, la configuración de verificación 65 puede ser "empujada" por un servidor administrador de usuarios 40 al dispositivo inalámbrico 12, o "retirada" desde un servidor administrador de usuarios 40 por el dispositivo inalámbrico 12, a través de una red inalámbrica 42. En otra alternativa, la carga de la configuración de verificación 65 puede iniciarse de cualquier manera, por ejemplo, iniciada por un evento predeterminado, tal como el dispositivo inalámbrico 12 que tiene dificultad para comunicarse con la red inalámbrica 42, o el dispositivo inalámbrico 12 que se comunica con un proveedor de servicios de red diferente. En otra alternativa, el empuje o retirada de la configuración 65 al dispositivo inalámbrico 12 puede ser configurable de cualquier manera, por ejemplo: iniciada por un evento predeterminado.

[0067] Además, este aspecto del procedimiento incluye la recopilación de información de verificación de firmware, incluyendo un resultado de prueba de verificación, de conformidad con la configuración de verificación 65 (bloque 124). Por ejemplo, el resultado de prueba de verificación 47 puede generarse aplicando el esquema de verificación predeterminado 89 al firmware 14. Además, la información de firmware adicional 15 puede recuperarse del motor de procesamiento 87 del dispositivo inalámbrico durante su funcionamiento. Tanto el resultado de prueba de verificación 47 como la información de firmware adicional 15 pueden almacenarse en el registro de información 46.

[0068] Opcionalmente, este aspecto del procedimiento incluye determinar una integridad del firmware mediante la comparación de un resultado de verificación predeterminado con el resultado de prueba de verificación generado (bloque 126). En un aspecto, por ejemplo, esta determinación de integridad 11 puede registrarse en el registro de información 46.

[0069] Además, este aspecto del procedimiento incluye reenviar la información de verificación de firmware recopilada a otro dispositivo informático para el análisis (bloque 128). En un aspecto, por ejemplo, el registro de información 46 se carga desde el dispositivo inalámbrico 12 al servidor administrador de usuarios 40 de acuerdo con el parámetro de notificación 91 de la configuración de verificación 65, como a través de un HTTP estándar, un FTP o algún otro protocolo de transferencia de datos. En otros aspectos, la información de verificación de firmware recopilada se carga desde el dispositivo inalámbrico usando cualquier medio de comunicación al que pueda acceder el dispositivo inalámbrico 12.

[0070] Además, este aspecto del procedimiento puede incluir recibir, opcionalmente verificar y ejecutar un comando de control basado en el análisis de la información relacionada con la integridad de firmware (bloque 130). Como se analizó anteriormente, el módulo de gestión de firmware remoto 21 puede ejecutar el analizador 45 para generar el informe 61 que incluye la determinación de integridad 11. Basándose en la determinación de integridad 11 y/o una revisión del registro de información 47, el operador 23 u otro usuario puede utilizar el módulo de gestión de firmware remoto 21 para generar el comando de control 78 para controlar la actividad del dispositivo inalámbrico 12. El módulo de control de dispositivo 94 puede verificar la autenticidad y la autoridad del comando de control 78, y luego puede ejecutar la lógica de control 35 para iniciar la actividad de control 29.

[0071] Con referencia a la Fig. 9, un aspecto de un procedimiento operable en un aparato para verificar la integridad del firmware 14 en el dispositivo inalámbrico 12 incluye generar una configuración de verificación para probar la integridad del firmware en un dispositivo inalámbrico (bloque 140). En un aspecto, un usuario como un técnico u operador 23 accede al módulo de gestión de firmware 21 y ejecuta el módulo configurador 44 para generar la configuración de verificación 65 para un dispositivo inalámbrico 12 dado. El módulo configurador 44 puede utilizar la lógica de configuración 56 para determinar y/o personalizar los diversos parámetros que comprenden la configuración de verificación 65, y estos parámetros pueden variar dependiendo del tipo/marca/modelo del dispositivo inalámbrico, el proveedor de servicios de red real y el tipo de firmware.

[0072] Además, este aspecto del procedimiento incluye reenviar la configuración de verificación para el dispositivo inalámbrico (bloque 142). Por ejemplo, el servidor administrador de usuarios 40 puede transmitir la configuración de verificación 65 a través de la red inalámbrica 42 al dispositivo inalámbrico 12. De forma alternativa, en otro aspecto, la configuración de verificación 65 puede reenviarse a través de una conexión estática o en serie al dispositivo inalámbrico 12. En otra alternativa, la configuración de verificación 65 puede precargarse en el dispositivo inalámbrico 12 durante la fabricación.

[0073] Además, este aspecto del procedimiento incluye la recepción de información relacionada con la verificación de firmware del dispositivo inalámbrico basándose en la configuración de verificación (bloque 144). Por ejemplo, el servidor administrador de usuarios 40 puede recibir el registro de información 46, que incluye el resultado de prueba de verificación 47 y/o la información de firmware adicional 15, desde el dispositivo inalámbrico 12. Los datos en el registro de información 46 corresponden a un procesamiento de la configuración de verificación 65 mediante el dispositivo inalámbrico respectivo 12. Además, en un aspecto, el servidor administrador de usuarios 40 recibe el registro de información 46 a través de la red inalámbrica 42. Además, el registro de información 46 puede recibirse como un todo o en partes y ensamblarse mediante el servidor administrador de usuarios 40 y/o el módulo de gestión de firmware 21. En otro aspecto, el servidor administrador de usuarios 40 recibe el registro de información 46 mediante una conexión estática o en serie al dispositivo inalámbrico 12, o desde algún otro dispositivo informático o medio de almacenamiento en comunicación con el administrador de usuarios 40.

[0074] Además, este aspecto del procedimiento incluye la generación de un informe basado en los datos de registro de información que indica una integridad del firmware en el dispositivo inalámbrico (bloque 146). Por ejemplo, el analizador 45 genera el informe 61 basándose en la comparación del resultado de prueba de verificación generado 47 con el resultado de verificación predeterminado 37. El informe 61 puede incluir una determinación de integridad 11 que, basándose en esta comparación, indique la integridad prevista del firmware 14.

[0075] Opcionalmente, en un aspecto, el informe de la integridad de firmware se reenvía para el análisis (bloque 148). Por ejemplo, el módulo de gestión de firmware 21 puede ejecutar la lógica de verificación 59 para transmitir el informe 61 a otro dispositivo informático, al usuario del dispositivo inalámbrico o a un tercero para su revisión. En un aspecto, el módulo de gestión de firmware 21 transmite el informe 61 al dispositivo informático 22 para su revisión por el operador 23. El operador 23 puede tomar medidas basándose en el informe 61, tal como enviar al usuario del dispositivo inalámbrico respectivo 12 una solicitud para que se sustituya el firmware 14 del dispositivo inalámbrico 12. En otro aspecto, el análisis del informe 61 da como resultado un comando de control 78 que se emite para controlar las operaciones del dispositivo inalámbrico. Por ejemplo, si se detecta un firmware defectuoso, el operador 23 u otra parte puede emitir un comando, por ejemplo, para inhabilitar el dispositivo con el fin de evitar daños a la red inalámbrica o para evitar operaciones no autorizadas.

[0076] Opcionalmente, en un aspecto, el procedimiento incluye recibir (y, opcionalmente, verificar) un comando de control basándose en la información relacionada con la verificación de firmware en el informe (bloque 150). Por ejemplo, el módulo de gestión de firmware 21 puede recibir el comando de control 78 desde el operador 23 en respuesta al informe 61. Opcionalmente, el módulo de control de dispositivo 94 puede ejecutar la lógica de permiso 25 para tomar la decisión de permiso 30 de si se debe emitir el comando de control 78 al dispositivo inalámbrico respectivo 12.

[0077] Opcionalmente, en un aspecto, el procedimiento incluye el envío del comando de control al dispositivo inalámbrico (bloque 152). Por ejemplo, el módulo de control de dispositivo 94 puede ejecutar la lógica de control 35 para reenviar el comando de control 78 al dispositivo inalámbrico 12. En un aspecto, el módulo de control de dispositivo 94 transmite el comando de control 78 a través de la red inalámbrica 42 al dispositivo inalámbrico 12.

[0078] Por lo tanto, los aspectos descritos permiten que una parte, tal como un proveedor de servicios de red inalámbrica, un fabricante de dispositivos inalámbricos, un fabricante de firmware, etc., mantenga la integridad del firmware en un dispositivo inalámbrico. Por ejemplo, el proveedor de servicios de red puede necesitar detectar el firmware comprometido para que pueda proporcionar un buen servicio a sus clientes y generar ingresos. Además, los proveedores de servicios de red pueden necesitar desconectar los dispositivos inalámbricos que tienen firmware comprometido para proteger sus redes inalámbricas, por ejemplo, ya que un dispositivo inalámbrico con firmware comprometido puede usar un protocolo de comunicaciones que interfiera con otros dispositivos inalámbricos en la red inalámbrica. red. Además, es posible que el proveedor de servicios de red necesite poder inhabilitar un dispositivo inalámbrico cuando el firmware del dispositivo inalámbrico se haya quedado obsoleto o cuando el dispositivo inalámbrico se esté utilizando en una red de proveedor de servicios diferente en violación de un acuerdo.

[0079] Además, los aspectos descritos permiten a los fabricantes de los dispositivos inalámbricos configurar una aplicación de verificación de firmware para diferentes dispositivos inalámbricos y diferentes versiones de firmware de modo que no tiene que escribirse una aplicación para cada versión de firmware o cada tipo de inalámbrico dispositivo.

[0080] Además, los aspectos descritos proporcionan un mecanismo de verificación de firmware que es capaz de determinar si se debe inhabilitar el dispositivo inalámbrico basándose en qué parte del firmware ha sido

comprometida. Por ejemplo, un programa con errores puede comprometer la integridad del firmware para un segmento de código del firmware que simplemente atrae imágenes que entretienen en el dispositivo de salida del dispositivo inalámbrico. En esta situación, los aspectos descritos permiten esta determinación, y por lo tanto permiten simplemente notificar al usuario del dispositivo inalámbrico que el firmware necesita ser reparado, en lugar de inhabilitar el dispositivo inalámbrico. En este caso, inhabilitar el dispositivo inalámbrico puede, al menos, ocasionar molestias al usuario del dispositivo inalámbrico y puede hacer que el proveedor de servicios de red pierda ingresos. Además, en lugar de inhabilitar el dispositivo o solicitar que el usuario del dispositivo inalámbrico haga revisar el dispositivo inalámbrico, los aspectos descritos proporcionan la reconfiguración del firmware para restaurar la integridad del dispositivo inalámbrico.

[0081] Las diversas lógicas, bloques lógicos, módulos y circuitos ilustrativos descritos en relación con los aspectos divulgados en el presente documento pueden implementarse o realizarse con un procesador de propósito general, un procesador de señales digitales (DSP), un circuito integrado de aplicación específica (ASIC), una matriz de puertas programables in situ (FPGA) u otro dispositivo de lógica programable, lógica discreta de puerta o transistor, componentes de hardware discretos o cualquier combinación de los mismos diseñada para realizar las funciones descritas en el presente documento. Un procesador de uso general puede ser un microprocesador pero, de forma alternativa, el procesador puede ser cualquier procesador, controlador, microcontrolador o máquina de estados convencional. Un procesador también puede implementarse como una combinación de dispositivos informáticos, por ejemplo, una combinación de un DSP y un microprocesador, una pluralidad de microprocesadores, uno o más microprocesadores junto con un núcleo de DSP o cualquier otra configuración de este tipo.

[0082] Además, los pasos y/o acciones de un procedimiento o algoritmo descrito en relación con los aspectos divulgados en el presente documento pueden realizarse directamente en hardware, en un módulo de software ejecutado mediante un procesador, o en una combinación de los dos. Un módulo de software puede residir en memoria RAM, memoria flash, memoria ROM, memoria EPROM, memoria EEPROM, unos registros, un disco duro, un disco extraíble, un CD-ROM o en cualquier otra forma de medio de almacenamiento conocida en la técnica. Un medio de almacenamiento a modo de ejemplo está conectado al procesador de tal manera que el procesador puede leer información de, y escribir información en, el medio de almacenamiento. De forma alternativa, el medio de almacenamiento puede estar integrado en el procesador. El procesador y el medio de almacenamiento pueden residir en un ASIC. El ASIC puede residir en un terminal de usuario. De forma alternativa, el procesador y el medio de almacenamiento pueden residir como componentes discretos en un terminal de usuario.

[0083] Aunque la divulgación precedente divulga aspectos ilustrativos, debería observarse que podrían realizarse varios cambios y modificaciones en el presente documento sin apartarse del alcance de los aspectos descritos, según lo definido en las reivindicaciones adjuntas. Además, aunque los elementos de los aspectos descritos pueden describirse o reivindicarse en singular, se contempla el plural, a no ser que se indique explícitamente la limitación al singular.

REIVINDICACIONES

1. Un dispositivo de comunicación inalámbrica (12) que comprende:

una plataforma informática (13) que tiene firmware (14); y

un módulo de verificación de firmware (20) operable para ejecutar una configuración de verificación (65) para recopilar información de firmware (47), en el que la información de firmware es indicativa de una integridad del firmware (14), en el que se recibe la configuración de verificación (65) de otro dispositivo informático (40) a través de una red inalámbrica, y en el que la configuración de verificación (65) comprende además un resultado de verificación predeterminado (37) seleccionado para el dispositivo inalámbrico (12), en el que la configuración de verificación (65) comprende además un esquema de verificación (89), y en el que el módulo de verificación de firmware (20) puede funcionar además para ejecutar el esquema de verificación (89) en el firmware para generar un resultado de prueba de verificación (47), en el que el resultado de prueba de verificación (47) es indicativo de la integridad del firmware, y en el que el módulo de verificación de firmware es operable para comparar el resultado de verificación predeterminado (37) con el resultado de prueba de verificación generado (47) para determinar la integridad del firmware (14), en el que el módulo de verificación de firmware (20) puede funcionar para controlar el dispositivo inalámbrico (12) en caso de que se descubra un firmware incorrecto o alterado impidiendo la capacidad del dispositivo inalámbrico (12) para comunicarse con la red inalámbrica (42).

2. El dispositivo según la reivindicación 1, en el que el módulo de verificación de firmware es operable para transmitir el resultado de prueba de verificación generado a través de una red inalámbrica.

3. El dispositivo de la reivindicación 1, en el que el esquema de verificación de firmware comprende al menos uno de una comprobación de redundancia, una prueba para un valor predeterminado en una ubicación predeterminada dentro del firmware, una comprobación de información de firma de firmware y una prueba para un resultado predeterminado de aplicación una función predeterminada a al menos una parte del firmware.

4. El dispositivo según la reivindicación 1, en el que el módulo de verificación de firmware es operable para aplicar la configuración de verificación a al menos un segmento predeterminado del firmware.

5. El dispositivo según la reivindicación 1, en el que la configuración de verificación comprende un esquema de verificación y un parámetro de notificación.

6. El dispositivo según la reivindicación 5, en el que el esquema de verificación se selecciona entre una pluralidad de esquemas de verificación basándose en al menos uno de un tipo de dispositivo inalámbrico, una identidad de un proveedor de servicios de red asociado con el dispositivo inalámbrico y un tipo de firmware.

7. El dispositivo según la reivindicación 5, en el que la configuración de verificación comprende además al menos uno de un parámetro de seguimiento seleccionado de una pluralidad de parámetros de seguimiento, el parámetro de notificación seleccionado de una pluralidad de parámetros de notificación y un parámetro de comando de control seleccionado de una pluralidad de parámetros de comando de control.

8. El dispositivo según la reivindicación 5, en el que la configuración de verificación comprende además un parámetro de seguimiento que identifica información de firmware adicional para recopilar.

9. El dispositivo según la reivindicación 1, en el que el módulo de verificación de firmware puede funcionar además para establecer un canal de comunicaciones de acceso limitado a través de una red inalámbrica, en el que el canal de comunicaciones de acceso limitado se basa en una configuración de servicio limitada predefinida.

10. El dispositivo según la reivindicación 9, en el que el canal de comunicaciones de acceso limitado no está disponible para un usuario final del dispositivo.

11. El dispositivo de la reivindicación 1, que comprende además un módulo de control de dispositivo operable para recibir y ejecutar un comando de control para cambiar una característica operativa del dispositivo, en el que el comando de control se basa en la integridad del firmware.

12. El dispositivo según la reivindicación 11, en el que el comando de control comprende al menos uno de un comando de inhabilitación, un comando de habilitación y un comando de reconfiguración, en el que el comando de inhabilitación hace que el dispositivo inalámbrico no funcione para comunicaciones que no sean de emergencia, en el que el comando de habilitación hace que el dispositivo inalámbrico sea operativo para comunicaciones, y en el que el comando de reconfiguración establece al menos un valor de datos relacionado con el firmware del dispositivo inalámbrico.

13. El dispositivo de la reivindicación 11, en el que el módulo de control de dispositivo es además operable para comprobar al menos una de una autorización asociada con un emisor del comando de control y una verificación del comando de control.

14. Un procedimiento para verificar la integridad del firmware en un dispositivo inalámbrico (12), que comprende:

recibir una configuración de verificación (65) que comprende un esquema de verificación (89) para probar una integridad del firmware (14) en el dispositivo inalámbrico (12), en el que la configuración de verificación comprende además un resultado de verificación predeterminado seleccionado para el dispositivo inalámbrico (12);

generar un resultado de prueba de verificación (47) basado en la aplicación del esquema de verificación (89) al firmware (14);

comparar el resultado de prueba de verificación predeterminada (37) con el resultado de prueba de verificación generado (47) para determinar la integridad del firmware (14); y

controlar el dispositivo inalámbrico (12) en caso de que se descubra un firmware incorrecto o alterado impidiendo la capacidad del dispositivo inalámbrico (12) para comunicarse con la red inalámbrica (42).

15. El procedimiento según la reivindicación 14, en el que el esquema de verificación de firmware comprende al menos uno de una comprobación de redundancia, una prueba para un valor predeterminado en una ubicación predeterminada dentro del firmware, una comprobación de la información de firma del firmware y una prueba para un resultado predeterminado de aplicación de una función predeterminada a al menos una parte del firmware.

16. El procedimiento según la reivindicación 14, que comprende además aplicar el esquema de verificación a al menos un segmento predeterminado del firmware.

17. El procedimiento según la reivindicación 14, en el que el esquema de verificación se selecciona a partir de una pluralidad de esquemas de verificación basándose en al menos uno de un tipo de dispositivo inalámbrico, una identidad de un proveedor de servicios de red asociado con el dispositivo inalámbrico y un tipo de firmware.

18. El procedimiento según la reivindicación 14, que comprende además recibir una configuración de verificación, en el que la configuración de verificación comprende al menos uno de un parámetro de seguimiento seleccionado de una pluralidad de parámetros de seguimiento, un parámetro de notificación seleccionado a partir de una pluralidad de parámetros de notificación y un parámetro de comando de control seleccionado a partir de una pluralidad de parámetros de comando de control.

19. El procedimiento según la reivindicación 14, que comprende además establecer un canal de comunicaciones de acceso limitado a través de una red inalámbrica basándose en una configuración de servicio limitada predefinida.

20. El procedimiento según la reivindicación 14, que comprende además recibir un comando de control para cambiar una característica operativa del dispositivo inalámbrico, donde el comando de control se basa en el resultado de prueba de verificación.

21. Un programa informático que comprende instrucciones ejecutables para hacer que al menos un ordenador realice un procedimiento de acuerdo con una de las reivindicaciones 14 a 20 cuando se ejecuten.

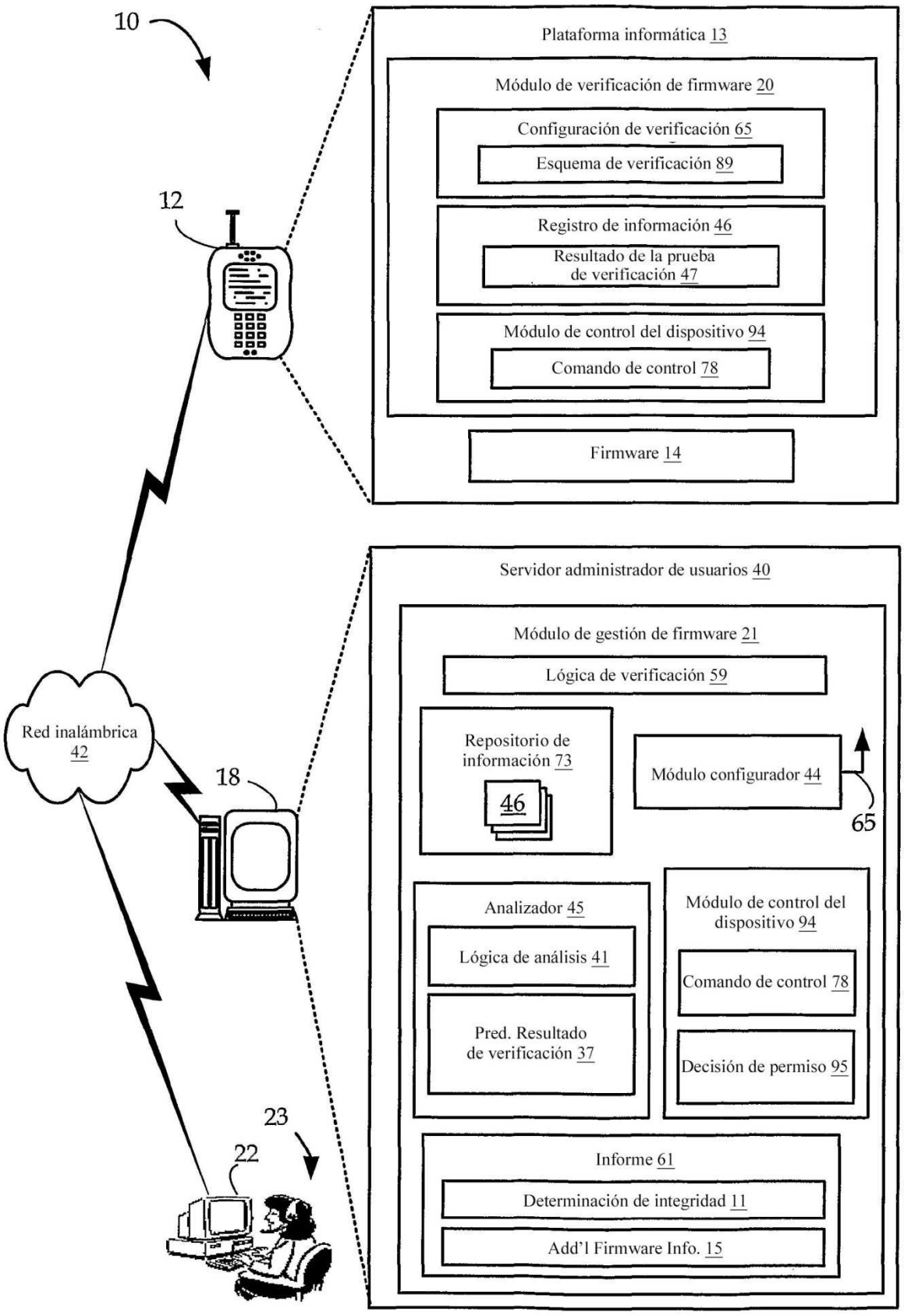
10
12
Plataforma informática 13
Módulo de verificación de firmware 20
Configuración de verificación 65
Esquema de verificación 89
Registro de información 46
Resultado de la prueba de verificación 47
Módulo de control del dispositivo 94
Comando de control 78
Firmware 14
Red inalámbrica 42
18
Servidor administrador de usuarios 40
Módulo de gestión de firmware 21
Lógica de verificación 59
Repositorio de información 73
46
Módulo configurador 44
65
Analizador 45
Lógica de análisis 41
Pred. Resultado de verificación 37
Módulo de control del dispositivo 94
Comando de control 78
Decisión de permiso 95
Informe 61
Determinación de integridad 11
Add'l Firmware Info. 15
23
22

Fig. 1

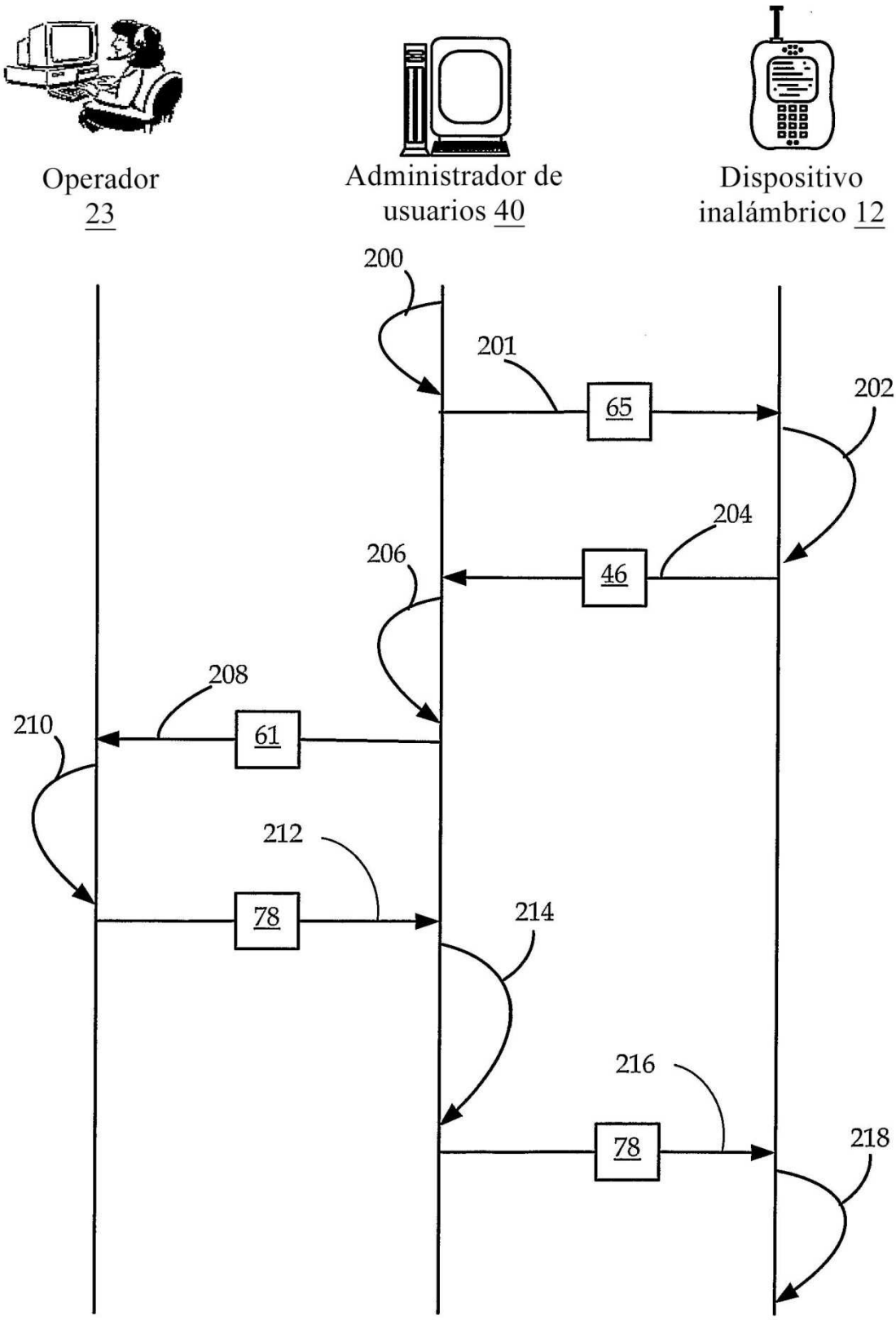
Operador
23
Administrador de
usuarios 40
Dispositivo
inalámbrico 12
200
201
65
202
204
206
46
208
210
61
212
78
214
216
78
218

Fig. 2

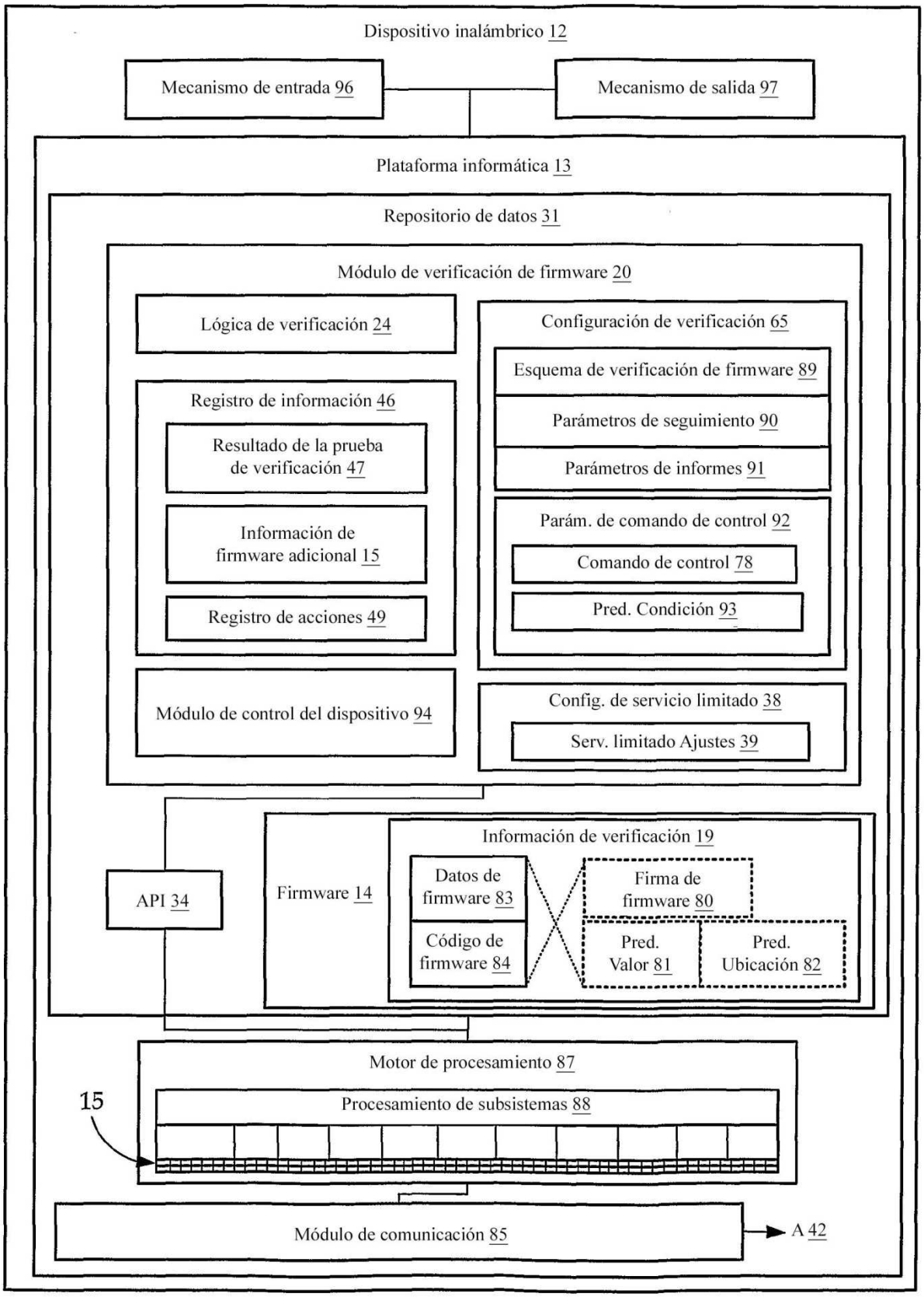
Dispositivo inalámbrico 12
Mecanismo de entrada 96
Mecanismo de salida 97
Plataforma informática 13
Repositorio de datos 31
Módulo de verificación de firmware 20
Lógica de verificación 24
Configuración de verificación 65
Esquema de verificación de firmware 89
Parámetros de seguimiento 90
Parámetros de informes 91
Registro de información 46
Resultado de la prueba de verificación 47
Información de firmware adicional 15
Registro de acciones 49
Parám. de comando de control 92
Comando de control 78
Pred. Condición 93
Módulo de control del dispositivo 94
Config. de servicio limitado 38
Serv. limitado Ajustes 39
API 34
Firmware 14
Información de verificación 19
Datos de firmware 83
Código de firmware 84
Firma de firmware 80
Pred. Valor 81
Pred. Ubicación 82
Motor de procesamiento 87
15
Procesamiento de subsistemas 88
Módulo de comunicación 85
A 42

Fig. 3

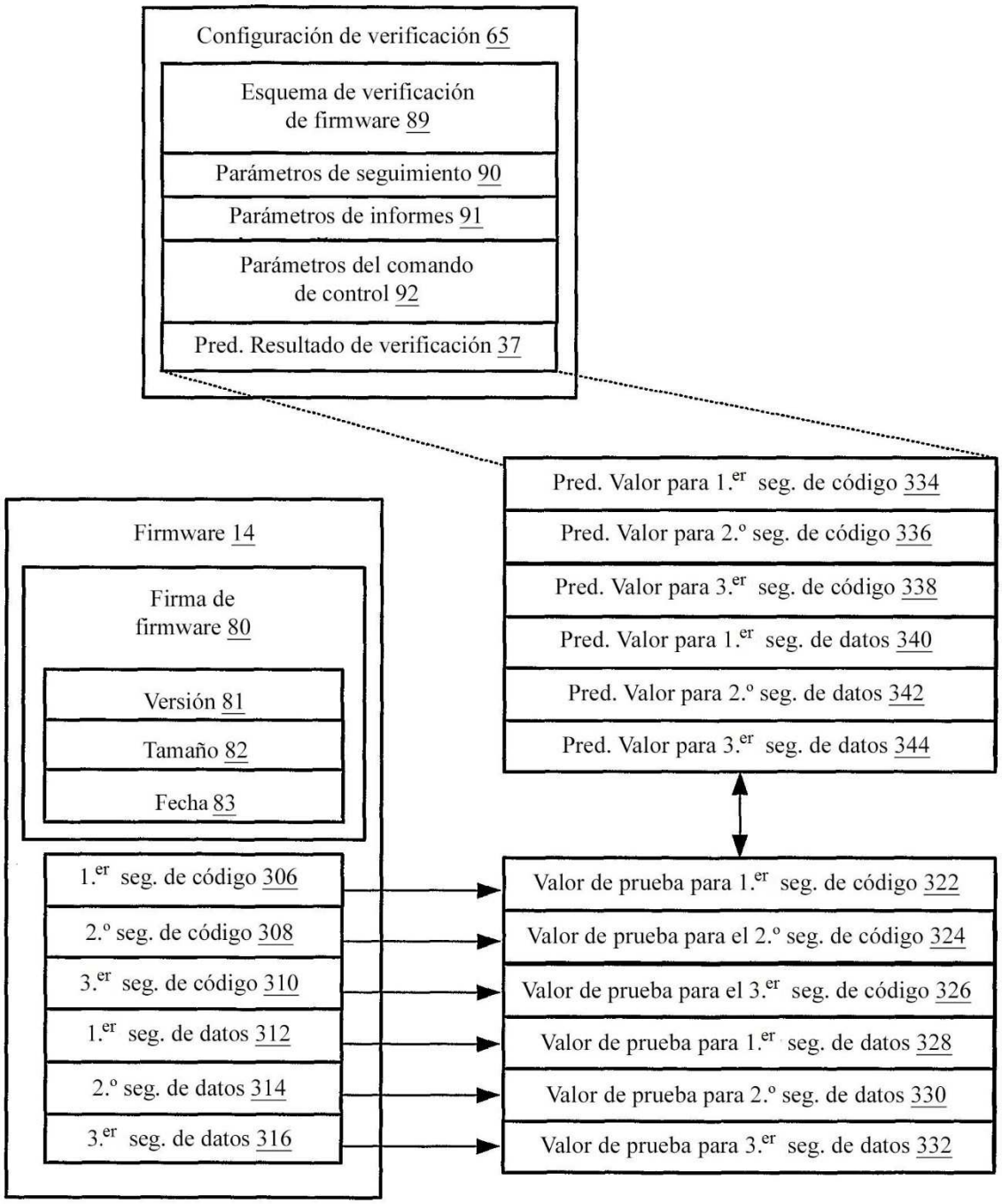
Configuración de verificación 65
Esquema de verificación de firmware 89
Parámetros de seguimiento 90
Parámetros de informes 91
Parámetros del comando de control 92
Pred. Resultado de verificación 37
Pred. Valor para 1.er seg. de código 334
Pred. Valor para 2.º seg. de código 336
Pred. Valor para 3.er seg. de código 338
Pred. Valor para 1.er seg. de datos 340
Pred. Valor para 2.º seg. de datos 342
Pred. Valor para 3.er seg. de datos 344
Firmware 14
Firma de firmware 80
Versión 81
Tamaño 82
Fecha 83
1.er seg. de código 306
2.º seg. de código 308
3.er seg. de código 310
1.er seg. de datos 312
2.º seg. de datos 314
3.er seg. de datos 316
Valor de prueba para 1.er seg. de código 322
Valor de prueba para el 2.º seg. de código 324
Valor de prueba para el 3.er seg. de código 326
Valor de prueba para 1.er seg. de datos 328
Valor de prueba para 2.º seg. de datos 330
Valor de prueba para 3.er seg. de datos 332

Fig. 4

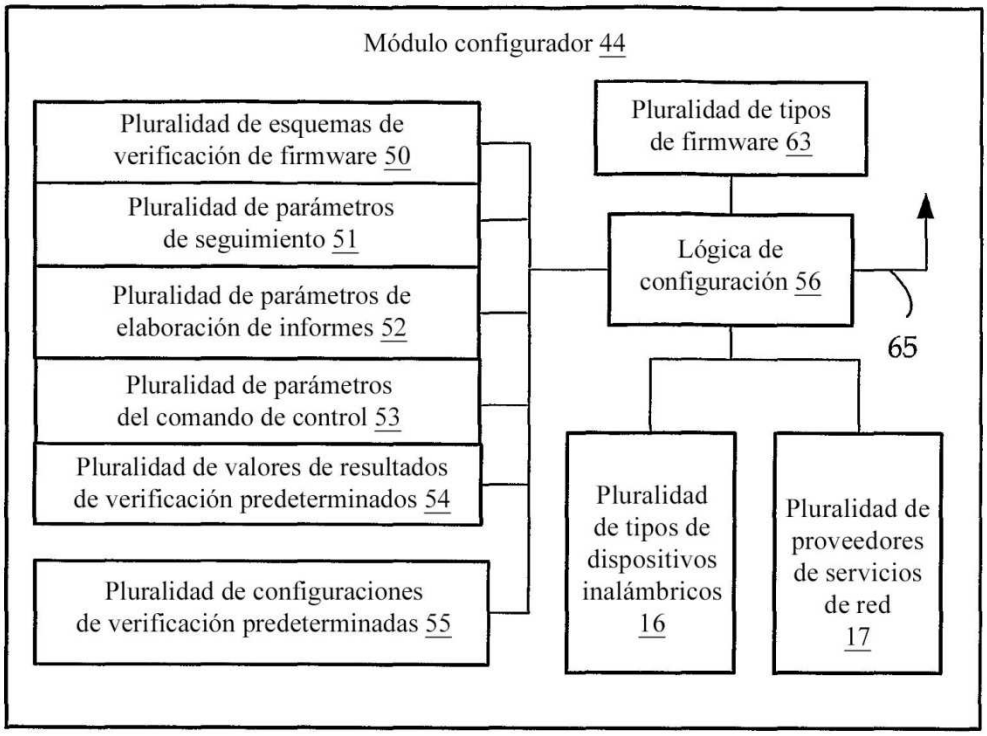
Módulo configurador 44
Pluralidad de esquemas de verificación de firmware 50
Pluralidad de parámetros de seguimiento 51
Pluralidad de parámetros de elaboración de informes 52
Pluralidad de parámetros del comando de control 53
Pluralidad de valores de resultados de verificación predeterminados 54
Pluralidad de configuraciones de verificación predeterminadas 55
Pluralidad de tipos de firmware 63
Lógica de configuración 56
65
Pluralidad de tipos de dispositivos inalámbricos 16
Pluralidad de proveedores de servicios de red 17

Fig. 5

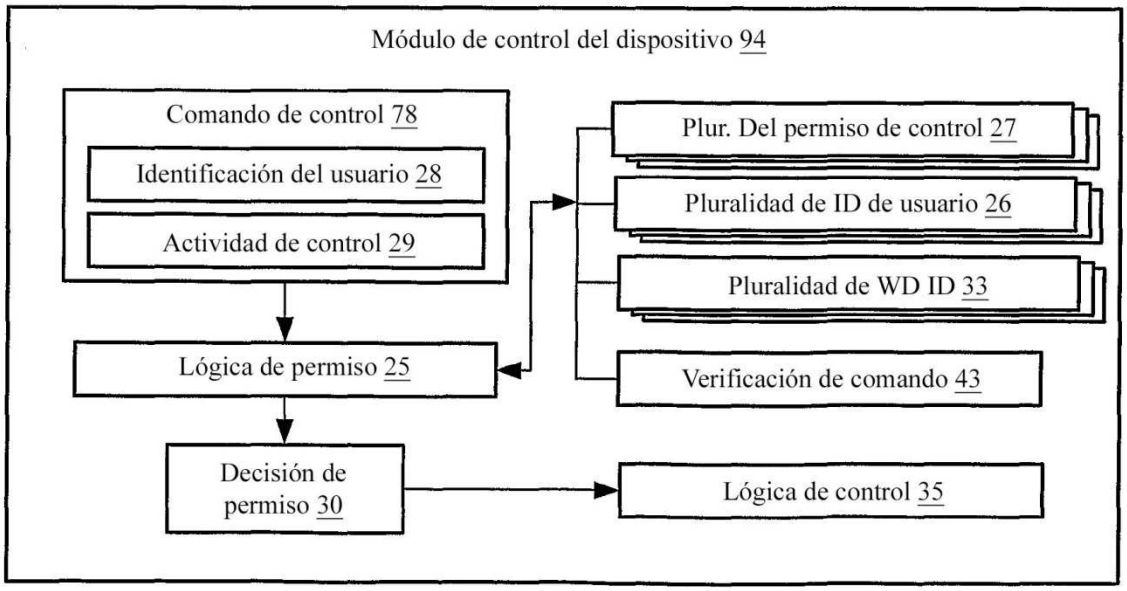
Módulo de control del dispositivo 94
Comando de control 78
Identificación del usuario 28
Actividad de control 29
Lógica de permiso 25
Decisión de permiso 30
Plur. Del permiso de control 27
Pluralidad de ID de usuario 26
Pluralidad de WD ID 33
Verificación de comando 43
Lógica de control 35

Fig. 6

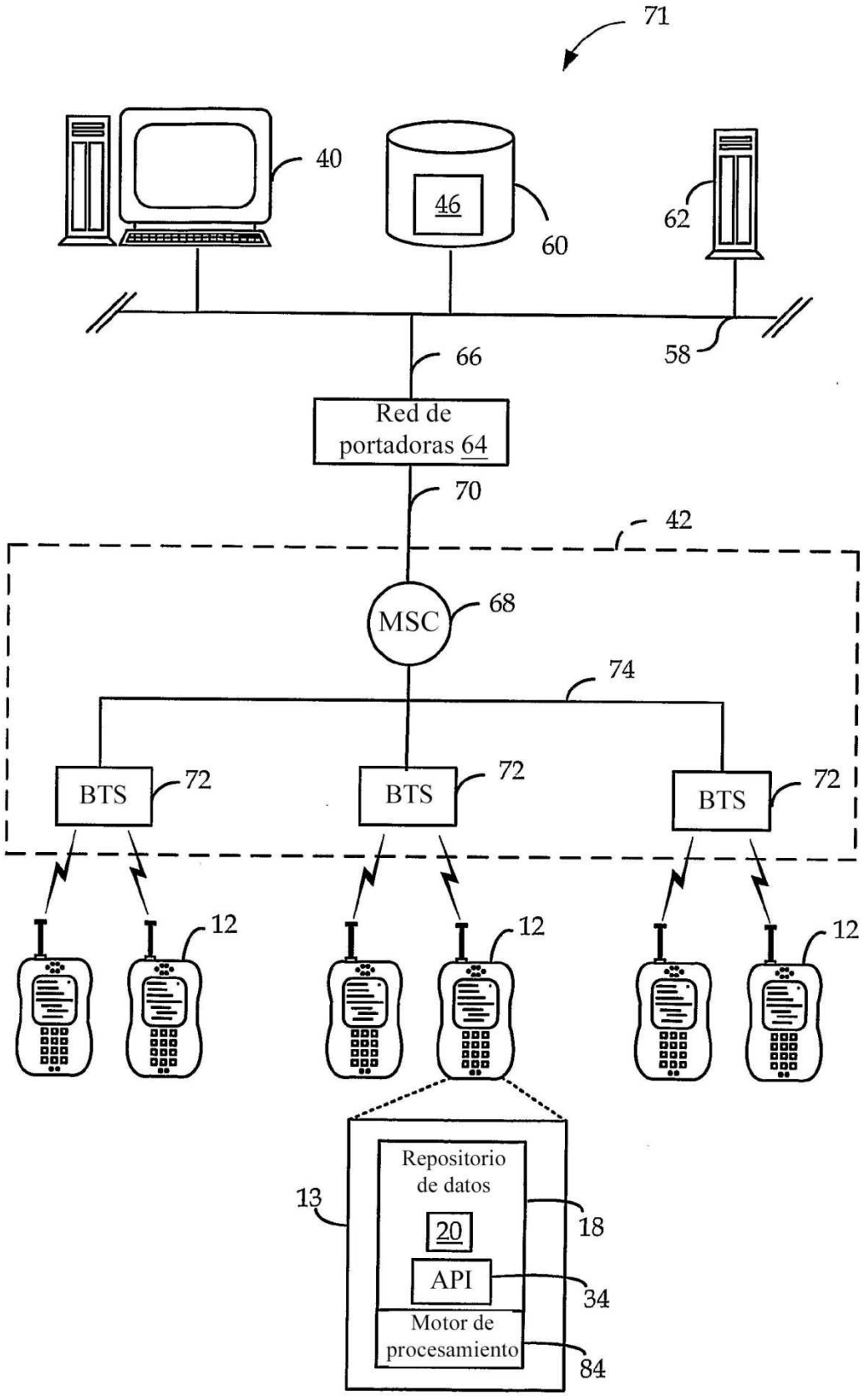
71
40
46
60
62
58
66
Red de portadoras 64
70
42
MSC
68
74
BTS
72
BTS
72
BTS
72
12
12
12
Repositorio de datos
13
18
20
API
34
Motor de procesamiento
84

Fig. 7

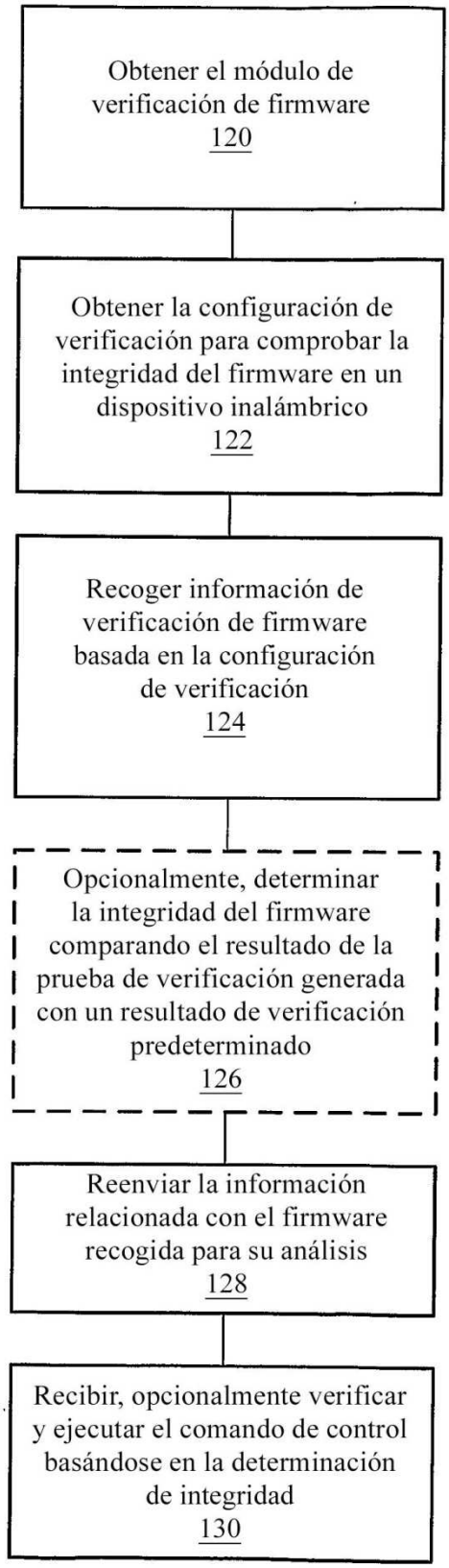
Obtener el módulo de verificación de firmware
120
Obtener la configuración de verificación para comprobar la integridad del firmware en un dispositivo inalámbrico
122
Recoger información de verificación de firmware basada en la configuración de verificación
124
Opcionalmente, determinar la integridad del firmware comparando el resultado de la prueba de verificación generada con un resultado de verificación predeterminado
126
Reenviar la información relacionada con el firmware recogida para su análisis
128
Recibir, opcionalmente verificar y ejecutar el comando de control basándose en la determinación de integridad
130

Fig. 8

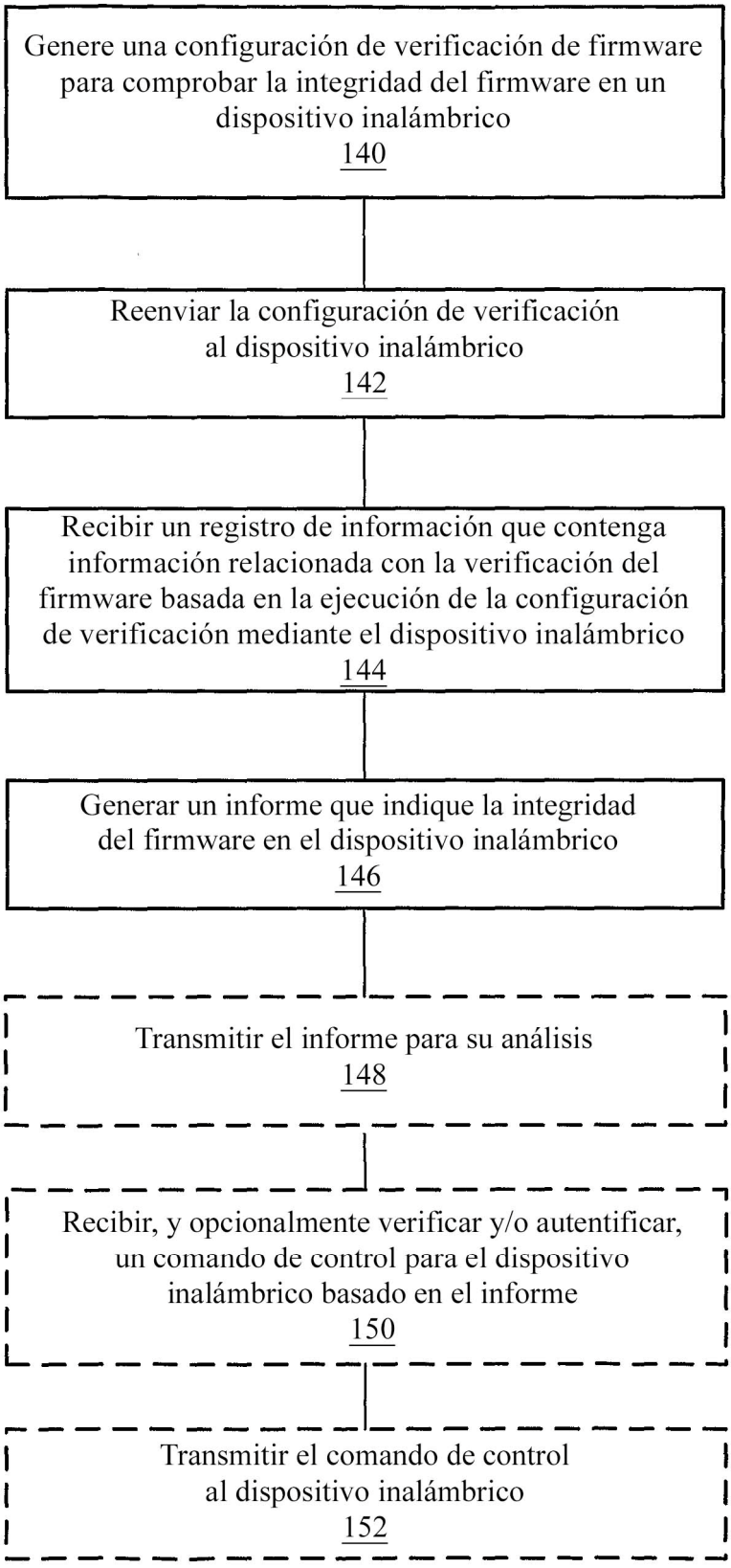
Genere una configuración de verificación de firmware para comprobar la integridad del firmware en un dispositivo inalámbrico
140
Reenviar la configuración de verificación al dispositivo inalámbrico
142
Recibir un registro de información que contenga información relacionada con la verificación del firmware basada en la ejecución de la configuración de verificación mediante el dispositivo inalámbrico
144
Generar un informe que indique la integridad del firmware en el dispositivo inalámbrico
146
Transmitir el informe para su análisis
148
Recibir, y opcionalmente verificar y/o autentificar, un comando de control para el dispositivo inalámbrico basado en el informe
150
Transmitir el comando de control al dispositivo inalámbrico
152

Fig. 9