(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 341 314**

(51) Int. Cl.:
H04W 24/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **01309352 .1**
(96) Fecha de presentación : **05.11.2001**
(97) Número de publicación de la solicitud: **1309214**
(97) Fecha de publicación de la solicitud: **07.05.2003**

(54) Título: **Envío de resultados de análisis de auto-rendimiento y operacional de una estación móvil a una red en respuesta a un mensaje de solicitud cifrado.**

(45) Fecha de publicación de la mención BOPI:
18.06.2010

(45) Fecha de la publicación del folleto de la patente:
18.06.2010

(73) Titular/es: **Nokia Corporation**
Keilalahdentie 4
02150 Espoo, FI

(72) Inventor/es: **Koivukangas, Tapio;**
Tervo, Timo P;
Luiro, Vesa;
Salow, Seppo y
Hayrynen, Antti

(74) Agente: **López Bravo, Joaquín Ramón**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

Venta de fascículos: Oficina Española de Patentes y Marcas. Pº de la Castellana, 75 – 28071 Madrid

DESCRIPCIÓN

Envío de resultados de análisis de auto-rendimiento y operacional de una estación móvil a una red en respuesta a una mensaje de solicitud cifrado.

La presente invención se refiere, en general, a radioteléfonos y, en particular, a radioteléfonos o estaciones móviles tales como los que pueden operar en una red celular y que pueden ejecutar además un autoanálisis y otros procedimientos de diagnóstico y grabar los resultados.

Un problema persistente en el mercado de las estaciones móviles son los casos en los que se produce la denominada indicación de "no se han encontrado fallos" (NFF) después de que un usuario o abonado devuelva a un comerciante o a un proveedor de servicios de red una estación móvil que supuestamente no opera o está averiada. Por ejemplo, el abonado puede informar que la estación móvil presenta un problema o un tipo de fallo particular; sin embargo, un técnico en un almacén o centro de reparaciones no encuentra ningún tipo de fallo o problema en la estación móvil devuelta y debe expedir un informe NFF. En un caso típico, el problema experimentado por el abonado puede ser realmente el resultado de algún problema temporal experimentado por la propia red inalámbrica y no por la estación móvil. Por ejemplo, un problema de red puede provocar que la estación móvil interrumpa llamadas repetidamente o que no pueda obtener servicio.

Debe apreciarse que este tipo de problema puede ser costoso para el comerciante y/o para el proveedor de servicios, y también para el fabricante. Además, el usuario puede llevarse una impresión desfavorable del fabricante de la estación móvil, incluso aunque el problema experimentado por el usuario esté completamente fuera del control del fabricante.

El documento US 6.088.588 describe un procedimiento para supervisar el rendimiento de una red y diagnosticar problemas en la cobertura de la red. Un terminal inalámbrico transmite a la red información relacionada con sus comunicaciones con la red, información que se utiliza para el análisis de rendimiento del sistema para dar soporte y localizar fallos de funcionamiento en la red.

Por lo tanto, un primer objeto y ventaja de la presente invención es proporcionar una mejor interacción entre los radioteléfonos y los proveedores de servicios que solucione los problemas anteriores y otros problemas.

Otro objeto y ventaja de la presente invención es proporcionar una estación móvil que almacene y mantenga una pluralidad de contadores de rendimiento de producto (PPC) los cuales indican el estado eléctrico y operativo de la estación móvil.

Un objeto y ventaja adicionales de la presente invención es proporcionar una estación móvil que almacene y mantenga un conjunto de PPC y que además pueda transmitir el conjunto completo o un subconjunto de los PPC a una ubicación externa para su análisis.

Un objeto y ventaja adicionales de la presente invención es proporcionar un ordenador en una ubicación externa a la estación móvil, pudiendo analizar el ordenador los PPC, así como otras entradas de datos, para determinar un estado de fallo de la estación móvil y/o de la red inalámbrica.

Otro objeto y ventaja de la presente invención es proporcionar una estación móvil que almacene y mantenga un conjunto de PPC y que opere, en respuesta a la recepción de un mensaje de solicitud PPC cifrado, para transmitir el conjunto completo o un subconjunto de los PPC a una ubicación externa.

Los problemas anteriores y otros problemas se solucionan, y los objetos y ventajas se llevan a cabo, mediante procedimientos y un aparato según realizaciones de la presente invención. En el presente documento se describe un procedimiento para operar una estación móvil, que comprende: durante la operación de la estación móvil en una red, determinar y almacenar un conjunto de datos relacionados con el rendimiento en la estación móvil, comprendiendo dichos datos relacionados con el rendimiento información que representa estados normales y anormales en la red y en la estación móvil; en respuesta a la aparición de un evento de activación, transmitir el conjunto o un subconjunto de los datos relacionados con el rendimiento a un ordenador para su análisis; y recibir en la estación móvil un mensaje para informar a un usuario con relación al análisis; caracterizado porque el evento de activación comprende recibir en la estación móvil un mensaje cifrado para transmitir el conjunto o subconjunto de los datos relacionados con el rendimiento, y comprende además descifrar el mensaje recibido utilizando una clave pública asociada almacenada en la estación móvil y transmitir el conjunto o el subconjunto de los datos relacionados con el rendimiento solamente en respuesta a un descifrado correcto del mensaje cifrado, en el que además la clave pública almacenada en la estación móvil es una clave de un conjunto de claves públicas almacenadas en la estación móvil, donde los elementos individuales del conjunto de claves públicas están asociados con aplicaciones que pueden ejecutarse por la estación móvil en cooperación con al menos uno de entre un comando cifrado y un conjunto de datos cifrados recibidos desde la red inalámbrica que se descifran por la estación móvil utilizando una clave del conjunto de claves públicas.

Los datos relacionados con el rendimiento pueden almacenarse en contadores y en registros, o en posiciones de memoria que se gestionan para operar como contadores y registros. Por ejemplo, los datos relacionados con el rendimiento pueden incluir un cómputo de llamadas interrumpidas y/o una indicación de un resultado de un modo de funcionamiento de autoanálisis de la estación móvil.

La estación móvil puede responder al mensaje de evento de activación transmitiendo a la red el conjunto o el subconjunto de datos PPC en un formado cifrado o no cifrado.

La etapa de transmisión del conjunto o de un subconjunto de los datos relacionados con el rendimiento puede incluir las etapas de recibir el conjunto o el subconjunto transmitido de datos relacionados con el rendimiento en un centro de control asociado con un proveedor de servicios de red y/o en un centro de diagnóstico (remoto) o en un ordenador local; y después analizar los datos con el ordenador para determinar una indicación de la aparición de al menos uno de entre un fallo en la estación móvil, un fallo en un sistema del proveedor de servicios de red o ningún estado de error. Una etapa opcional transmite la indicación determinada a la estación móvil. El análisis puede incluir además determinar información estadística relacionada con un grupo de estaciones móviles.

La etapa de analizar los datos relacionados con el rendimiento puede llevarse a cabo en combinación con al menos uno de entre datos de rendimiento de red inalámbrica o información obtenida de un usuario de la estación móvil.

Lo expuesto anteriormente y otras características de la invención resultarán más evidentes en la siguiente descripción detallada de la invención cuando se lee junto con los dibujos adjuntos, en los que:

la fig. 1 es un diagrama de bloques de una estación móvil que es adecuada para llevar a la práctica la presente invención;

la fig. 2 es una vista en alzado de la estación móvil mostrada en la fig. 1 y que ilustra además un sistema de comunicaciones inalámbricas y un proveedor de servicios a los que la estación móvil está conectada de manera bidireccional a través de enlaces de RF inalámbricos;

la fig. 3 es un diagrama que describe las entradas y salidas de un módulo de software que analiza los PPC y otra información, y que proporciona salidas que indican el estado operativo de la estación móvil;

la fig. 4 es un diagrama de flujo lógico según un procedimiento de la presente invención;

la fig. 5 es un diagrama de niveles de sistema que muestra un sistema de activación inalámbrico (OTA) según un aspecto de estas enseñanzas; y

la fig. 6 es un diagrama de flujo lógico de un procedimiento de recuperación de PPC según estas enseñanzas.

En primer lugar se hace referencia a las fig. 1 y 2 para ilustrar un radioteléfono, también denominado en el presente documento como una estación 10 móvil inalámbrica, que es adecuado para llevar a la práctica la presente invención. La estación 10 móvil puede ser, pero no está limitada a, un teléfono celular o un dispositivo de comunicación personal. La estación 10 móvil incluye una antena 12 para transmitir señales a y para recibir señales desde un emplazamiento base o estación 30 base. La estación 30 base puede ser una parte de una red celular que comprende un sistema 32 de proveedor de red inalámbrica, también denominado en el presente documento por motivos de simplicidad como una red 32 inalámbrica, que incluye además un centro 34 de conmutación móvil (MSC). El MSC 34 proporciona una conexión a enlaces troncales terrestres cuando la estación 10 móvil está implicada en una llamada. También puede proporcionarse un centro 33 de control de red, estando acoplado el centro 33 de control de red al MSC 34 para controlar la operación del sistema 32 de proveedor de red así como para recibir información desde la estación 10 móvil a través de la estación 30 base. El centro 33 de control de red puede estar conectado a uno o más puntos del sistema 32 de proveedor de red.

La estación móvil incluye un modulador 14A (MOD), un transmisor 14, un receptor 16, un desmodulador 16A (DEMOD) y un controlador 18 que proporciona señales al transmisor 14 y que recibe señales desde el receptor 16. Estas señales incluyen información de señalización según la norma de interfaz aérea del sistema celular aplicable y también datos generados por el usuario y/o de voz del usuario. El tipo particular de norma de interfaz aérea no es importante para la operación de la presente invención ya que las enseñanzas de la presente invención se aplican a sistemas inalámbricos analógicos (por ejemplo, sistemas AMPS), así como a sistemas digitales, incluyendo sistemas de acceso múltiple por división de tiempo (TDMA) y de acceso múltiple por división de código (CDMA). Como un ejemplo, los sistemas de tipo GSM tanto convencionales como avanzados pueden beneficiarse de las enseñanzas de la presente invención.

Debe entenderse que el controlador 18 también incluye el sistema de circuitos requerido para implementar las funciones lógicas y de audio (trayecto de voz) de la estación móvil. Por ejemplo, el controlador 18 puede comprender un dispositivo de procesador de señales digitales, un dispositivo de microprocesador y varios convertidores de analógico a digital, convertidores de digital a analógico y otros circuitos de soporte. Las funciones de control y de procesamiento de señales de la estación móvil están asignadas entre estos dispositivos según sus respectivas capacidades.

Una interfaz de usuario incluye un auricular o altavoz 17 convencional, un micrófono 19 convencional, un dispositivo 20 de visualización y un dispositivo de entrada de datos de usuario, normalmente un teclado 22, todos ellos conectados al controlador 18. El teclado 22 incluye las teclas 22a numéricas convencionales (0-9) y teclas relacionadas (#,*), y otras teclas 22b utilizadas para hacer operar la estación 10 móvil. Estas otras teclas 22b pueden incluir, por ejemplo, una tecla ENVIAR, varias teclas de desplazamiento de menú y programables, y una tecla de ENCENDIDO.

La estación 10 móvil incluye además una batería 26 extraíble para alimentar los diversos circuitos requeridos para hacer operar la estación móvil.

La estación 10 móvil incluye además varias memorias, mostradas colectivamente como la memoria 24, en las que se almacena una pluralidad de constantes y variables que se utilizan por el controlador 18 durante la operación de la estación móvil. Por ejemplo, la memoria 24 almacena los valores de parámetros de sistema inalámbrico y el módulo de asignación de número (NAM). Un programa operativo para controlar la operación del controlador 18 también está almacenado en la memoria 24 (normalmente en un dispositivo ROM). El programa operativo de la memoria 24 puede incluir rutinas para presentar al usuario mensajes y funciones relacionadas con mensajes en el dispositivo 20 de visualización, normalmente como varios elementos de menú. La memoria 24 también incluye rutinas para implementar los procedimientos ejecutados por la estación móvil descritos posteriormente.

Según un aspecto de la presente invención, la memoria 24 almacena un conjunto de contadores 24A de rendimiento de producto (PPC), donde cada contador individual indica un aspecto de la operación de la estación 10 móvil. En general, los contadores individuales de los PPC 24A pueden ser auténticos contadores, tal como un contador para registrar un número de llamadas interrumpidas, mientras que otros pueden considerarse más como registros para almacenar algún valor tal como, por ejemplo, la magnitud de la intensidad de señal recibida (RSS) en el momento en que se interrumpe una llamada particular. Cuando el almacenamiento se realiza en las posiciones de memoria de la memoria 24, puede apreciarse que el software utiliza las posiciones de memoria para emular la función de los contadores y de los registros (por ejemplo, incrementando una posición de memoria particular cada vez que se interrumpa una llamada).

En general, los PPC 24A proporcionan información relacionada con la calidad de la red inalámbrica, así como información relacionada con la operación de la estación 10 móvil. Según un aspecto adicional de la invención, el conjunto de PPC 24A, o un subconjunto del mismo, se transmite desde la estación móvil al sistema 32 de proveedor de red a través de una estación 30 base. Los PPC 24A pueden transmitirse en respuesta a una solicitud recibida desde el sistema 32 de proveedor de red o desde algún otro solicitante, bajo la orden de un usuario de la estación 10 móvil, de manera periódica según un intervalo de tiempo predeterminado o con la aparición de algún otro evento de activación (por ejemplo, alcanzar un número de umbral predeterminado de llamadas interrumpidas en un intervalo predeterminado de tiempo de funcionamiento).

La utilización de los PPC 24A puede ser especialmente ventajosa cuando se caracterizan nuevas características de especificación inalámbricas y nuevos servicios de aplicaciones de red, como cuando se utiliza un grupo o conjunto de prueba de estaciones móviles en el área de cobertura del sistema 32 de proveedor de red. Utilizando un grupo de prueba de estaciones móviles, el proveedor de servicios puede recopilar los PPC 24A de manera inalámbrica y, por lo tanto, caracterizar características de cobertura y otras características de interés. También puede proporcionarse retroalimentación a los usuarios de las estaciones 10 móviles, ya sea mediante transmisiones desde el proveedor de red para su presentación en el dispositivo 20 de visualización y/o mediante otros medios tales como publicar los resultados en una página web que pueda accederse mediante un PC convencional o de manera inalámbrica mediante las estaciones 10 móviles.

Durante una llamada, el conjunto o un subconjunto seleccionado de los PPC 24A puede transferirse por el controlador 18 a través del transmisor 14 utilizando, por ejemplo, una función de servicio de mensajes cortos (SMS), o mediante otra función relacionada con mensajes, tal como la función de servicio de datos suplementarios no estructurados de GSM, o como datos de paquete, tales como datos de paquete que se ajustan al formado TCP/IP enviados a través de Internet 37. También está dentro del alcance de la presente invención mostrar en el dispositivo 20 de visualización los PPC 24A que van a transmitirse y que después el usuario diga los resultados a operador humano o automatizado (reconocimiento de voz) del centro 33 de control de red. Los PPC 24A pueden analizarse en el centro 33 de control de red y/o en un centro 38 de diagnóstico remoto que esté conectado al sistema 32 de proveedor de red a través de líneas telefónicas convencionales (por ejemplo, la red 36 telefónica pública conmutada (PSTN)) o a través de otra red de comunicaciones. También puede utilizarse una conexión a Internet 37 para esta finalidad. El centro 38 de diagnóstico remoto puede estar situado en el emplazamiento de fabricación de la estación 10 móvil, en un centro de ventas o de servicios, en un centro de investigación y desarrollo o en cualquier ubicación adecuada o deseable.

Haciendo ahora referencia a la fig. 3, el centro 33 de control de red puede incluir un módulo 33A de análisis de fallos (FAM), tal como software que se ejecuta en un PC o en un ordenador central. El FAM 33A recibe como entradas el conjunto o subconjunto de los PPC 24A transmitidos, así como resultados de autoanálisis de estación móvil, o una parte de los PPC 24A, una entrada de datos del operador de red, tal como información obtenida del usuario de la estación 10 móvil, así como determinados parámetros de red, tales como la potencia de la estación base. También pueden proporcionarse otras entradas de datos, tales como las condiciones de propagación de RF en el área de servicio del sistema 32 de proveedor de red. El FAM 33A procesa estas entradas utilizando, por ejemplo, un sistema experto o una red neuronal, y transmite indicaciones apropiadas de la funcionalidad de la estación móvil/red. Estas indicaciones pueden incluir una indicación de un fallo de la estación 10 móvil, una indicación de un fallo del sistema 32 de proveedor de red o una indicación de ningún fallo encontrado (NFF). Está dentro del alcance de las enseñanzas de la presente invención transmitir la indicación de salida del FAM 33A a la estación 10 móvil, proporcionando de ese modo al usuario un análisis de fallos y una detección de errores en tiempo real o sustancialmente en tiempo real. Por ejemplo, puede informarse al usuario, mediante bucle cerrado en función de los PPC 24A transmitidos anteriormente y de la información obtenida a partir del operador de red, que con gran probabilidad la estación 10 móvil opera

correctamente (lo que implica que no hay ningún fallo o que el fallo radica en otro punto, tal como en el sistema 32 de proveedor de red), o que con gran probabilidad la estación 10 móvil experimenta algún fallo. En este último caso, el usuario puede llevar la estación 10 móvil a un centro de servicios local o a un comerciante para su devolución o para su reparación. Sin embargo, puede apreciarse que en este último caso ya se ha establecido que de manera muy probable la estación 10 móvil no opera correctamente, eliminando o reduciendo significativamente de ese modo que se produzca la situación de errores no encontrados (NFF) descrita anteriormente.

El conjunto de PPC 24A puede incluir una pluralidad de diferentes indicaciones de funcionalidad de estación móvil incluyendo, además del número de llamadas interrumpidas y/o de intentos fallidos de establecimiento de llamada (así como indicaciones de intensidad de señal), otras indicaciones tales como el resultado de programas de autoanálisis internos (por ejemplo, errores de memoria, estados y terminaciones de programa anormales, etc.), y también datos recopilados periódicamente durante periodos de funcionamiento aparentemente normal. Esta última indicación es útil para establecer una línea de base con la que comparar otras indicaciones. Los PPC 24A también pueden incluir indicaciones de tasas de error de trama, tasas de error de símbolo, un número de solicitudes de retransmisión que se producen durante un intervalo de tiempo, etc.

Haciendo referencia al procedimiento descrito en la fig. 4, en la etapa A la estación 10 móvil almacena el conjunto de PPC 24A. Esta etapa puede producirse durante un periodo de tiempo considerable durante la operación de la estación 10 móvil. En la etapa B se determina si se ha producido un evento de activación. El evento de activación puede ser, por ejemplo, la recepción de un mensaje que solicita a la estación 10 móvil que transmita el conjunto o subconjunto de PPC 24A, una entrada de datos del usuario de la estación 10 móvil o la expiración de un temporizador. Si no se ha producido el evento de activación, el control vuelve a la etapa A para seguir almacenando y/o actualizando el conjunto de PPC 24A. Si se ha producido el evento de activación, entonces el conjunto o el subconjunto de PPC 24A se transmite desde la estación 10 móvil al sistema 32 de proveedor de red a través de la estación 30 base. Está dentro del alcance de la presente invención transmitir de manera selectiva los PPC 24A, tal como transmitiendo solamente los PPC 24A solicitados (por ejemplo, solicitados en un mensaje transmitido a la estación 10 móvil), o transmitiendo solamente un subconjunto de los PPC 24A al centro 33 de control de red, transmitiendo al mismo tiempo el conjunto completo de PPC 24A al centro 38 de diagnóstico remoto. Los PPC 24A transmitidos pueden cifrarse antes de su transmisión y descifrarse posteriormente en la ubicación de recepción, garantizando de ese modo la privacidad de la información PPC transmitida.

En una realización actualmente preferida de la presente invención, el mensaje de evento de activación recibido desde la red 32 inalámbrica está cifrado, tal y como se describirá posteriormente en gran detalle, y se descifra mediante la estación 10 móvil después de su recepción. Los datos de respuesta PPC pueden cifrarse o no por la estación 10 móvil antes de transmitirse a la red 32 inalámbrica.

En cualquier caso, en la etapa C, el FAM 33A o un sistema equivalente en el centro 38 de diagnóstico remoto analiza los PPC 24A, preferentemente junto con la otra información descrita anteriormente tal como información relacionada con la red y/o información obtenida por un operador con relación al usuario de la estación 10 móvil. En la etapa D se determina si los PPC 24A (y otra información opcional) indican un fallo de estación móvil. Si es así, el control pasa a la etapa G, mientras que si no se indica ningún fallo de estación móvil, en la etapa E se determina si se indica un fallo de red. Si es así, el control pasa a la etapa G, mientras que si no se indica ningún fallo de red, en la etapa F se determina que no se ha encontrado ningún error o fallo (NFF). Después, el control pasa a la etapa G donde un mensaje puede formatearse y enviarse a la estación 10 móvil para indicar al usuario el resultado del análisis PPC.

Aunque se describe en el contexto de realizaciones preferidas, debe observarse que un experto en la técnica puede concebir una pluralidad de modificaciones en estas enseñanzas. Por ejemplo, puede apreciarse que diferentes tipos de estaciones 10 móviles pueden almacenar diferentes tipos de PPC 24A. Por ejemplo, una estación 10 móvil TDMA puede almacenar uno o más PPC relacionados con funciones de sincronización de tramas y de ranuras de tiempo, mientras que una estación móvil CDMA puede almacenar uno o más PPC relacionados con funciones de correlación de código de ensanchamiento de seudorruido (PN).

Debe observarse además que los PPC 24A pueden utilizarse por el operador de red y/o por el fabricante de la estación móvil para obtener datos estadísticos relacionados con la operación de un grupo de estaciones 10 móviles. Por ejemplo, información estadística relacionada con una pluralidad de llamadas interrumpidas en un área geográfica determinada (por ejemplo, en un conjunto predeterminado de células adyacentes), como una función de la intensidad de señal recibida en el momento en que se interrumpen las llamadas, así como con tasas de error de trama que están experimentándose, puede recopilarse y analizarse por el tipo de teléfono móvil (por ejemplo, la operación de una estación móvil de un modelo nuevo puede contrastarse con la operación de una estación móvil de un modelo antiguo).

Además, este ejemplo puede ampliarse para cubrir también la determinación de la ubicación del error. Por ejemplo, si los datos 24A PPC indican que la estación 10 móvil ha interrumpido tres llamadas en los últimos diez minutos y si las indicaciones de intensidad de señal asociadas muestran una cantidad adecuada de intensidad de señal, entonces el FAM 33A puede determinar que el error puede estar en la estación 10 móvil. Sin embargo, si se observa que una pluralidad de estaciones móviles interrumpen llamadas y si a partir de los datos 24A PPC o de los datos de parámetro relacionados con la red se determina que gran parte de las mismas están situadas en la misma célula, entonces el error puede estar en cambio en la estación 30 base y no en las estaciones 10 móviles. Esto es especialmente cierto si los resultados de autoanálisis de estación móvil no indican un fallo de estación móvil.

Como otro ejemplo, si los datos 24A PPC indican que la estación 10 móvil está interrumpiendo llamadas y si las indicaciones de intensidad de señal asociadas no muestran una cantidad adecuada de intensidad de señal (señal recibida débil), entonces el FAM 33A puede indicar también que es muy probable que el fallo esté en la estación 10 móvil si los resultados de autoanálisis de estación móvil indican un fallo de estación móvil.

Como alternativa, si los datos 24A PPC indican que la estación 10 móvil está interrumpiendo llamadas y si las indicaciones de intensidad de señal asociadas indican una intensidad de campo débil (señal recibida débil), pero los resultados de autoanálisis de estación móvil no indican ningún fallo de estación móvil, entonces puede indicarse que el fallo radica con gran probabilidad en el sistema 32 de proveedor de red.

Como alternativa, si los datos 24A PPC indican que la estación 10 móvil está interrumpiendo llamadas, si las indicaciones de intensidad de señal asociadas indican lecturas de intensidad de campo adecuadas o correctas y si los resultados de autoanálisis de estación móvil no indican ningún fallo de estación móvil, entonces puede indicarse de nuevo que el fallo radica con gran probabilidad en el sistema 32 de proveedor de red (por ejemplo, la red puede estar demasiado sobrecargada o alguna unidad electrónica de red es marginal o intermitente).

También debe observarse que determinadas etapas del procedimiento mostrado en la fig. 4 pueden ejecutarse en otro orden diferente al mostrado y que pueden añadirse etapas adicionales obteniendo también el resultado deseado. Por ejemplo, el orden de ejecución de las etapas D y E puede invertirse, y la etapa G puede omitirse total o selectivamente (por ejemplo, solo se informa al usuario cuando se determina que el fallo radica en la estación 10 móvil).

También debe observarse que no es necesario que los PPC 24A se transmitan desde la estación 10 móvil transmitiéndose solamente a través del transmisor 14 inalámbrico. Por ejemplo, y haciendo de nuevo referencia a la fig. 1, una interfaz 28 de datos de estación móvil puede utilizarse para transmitir o enviar los PPC 24A a través de un cable o de un enlace IR a un ordenador 29 local (mostrado en la fig. 2) que contenga un programa de diagnóstico adecuado similar o idéntico al programa que se ejecuta en el centro 33 de control de red o en el centro 38 de diagnóstico remoto. En este caso, el ordenador 29 local puede instalarse en un punto de ubicación de venta o en un centro de servicios, o en cualquier otra ubicación adecuada, y puede proporcionar una rápida retroalimentación al usuario con relación a un posible origen de un problema que esté experimentando el usuario. También en este caso, el evento de activación que provoca que el controlador 18 transmita los PPC 24A puede ser la recepción por parte del controlador 18, a través de la interfaz 28 de datos, de una señal de interrogación enviada desde el ordenador 29 local.

Tal y como se ha comentado anteriormente de manera breve, está dentro del alcance de estas enseñanzas requerir que la red 32 inalámbrica cifre o "firme" el mensaje de solicitud PPC antes de transmitir el mensaje a la estación 10 móvil. De esta manera, la estructura del mensaje de solicitud PPC no puede determinarse fácilmente por terceras partes y, por lo tanto, es menos probable que la estación 10 móvil responda a un mensaje de solicitud PPC enviado desde una fuente no autorizada de mensajes de solicitud PPC. Esto puede ser importante si la estación 10 móvil responde al solicitante utilizando, por ejemplo, un mensaje SMS, donde el usuario de estación móvil debe pagar una tasa por el envío del mensaje SMS. Un algoritmo de cifrado actualmente preferido, pero en absoluto limitativo, es uno basado en RSA.

Brevemente, RSA es un sistema criptográfico de clave pública desarrollado por el MIT en 1977 en un intento por ayudar a garantizar la seguridad entre redes. Un sistema criptográfico puede considerarse como un algoritmo que puede convertir datos de entrada en algo irreconocible (cifrado), y convertir de nuevo los datos irreconocibles a su forma original (descifrado). Para cifrar los datos se introducen los datos ("texto normal") y una clave de cifrado en la parte de cifrado del algoritmo. Para descifrar el "texto cifrado" se utiliza una clave de descifrado adecuada en la parte de descifrado del algoritmo. Estas claves se denominan como una clave pública y como una clave privada, respectivamente. Por ejemplo, para enviar datos desde A a B, A busca o conoce la clave pública de B y después cifra los datos utilizando la clave pública de B. Sin embargo, la clave pública no descifrará el texto cifrado. Para que B descifre el texto cifrado recibido, B debe utilizar su clave privada. Si B desea responder a A utilizando una respuesta cifrada, B debe cifrar la respuesta utilizando la clave pública de A.

En un sistema criptográfico de clave pública, tal como RSA, es importante que no pueda determinarse la clave privada de un usuario. Esto se consigue utilizando una función unidireccional. Con una función unidireccional es sencillo calcular un resultado dados determinados valores de entrada. Sin embargo, es extremadamente difícil, preferentemente casi imposible, determinar los valores originales si se empieza por el resultado. La función unidireccional utilizada en RSA es la multiplicación de números primos. En general, es relativamente sencillo multiplicar dos números primos elevados, pero para la mayoría de números primos elevados su factorización requiere mucho tiempo. La criptografía de clave pública crea por tanto un sistema criptográfico que utiliza dos números primos elevados para formar la clave privada y el producto de los números primos para formar la clave pública.

Según un aspecto de la presente invención, una clave 35A privada y secreta (ClvPrvd) está almacenada en la red 32, tal como en el centro 33 de control de red o en el centro 38 de diagnóstico remoto, junto con una clave 35B pública general (CPG) de estaciones móviles asociadas con un servicio específico que, en este caso, es el servicio PPC. La estación 10 móvil almacena la clave pública general ClavePública, por ejemplo, en una posición 24B de la memoria 24. Cuando el mensaje cifrado llega desde la red 32 inalámbrica, se descifra mediante el procesador 18 de datos de la estación 10 móvil utilizando la clave pública asociada almacenada en la posición 24B. La estación 10 móvil sólo transmite el conjunto o el subconjunto de datos PPC a la red 32 inalámbrica en respuesta al descifrado de una solicitud

válida de datos PPC (etapa B de la fig. 4). La estación 10 móvil puede cifrar la respuesta, aunque esto no es un requisito para la mayoría de tipos de respuesta, tal como la respuesta de datos PPC, ya que normalmente no hay nada secreto o confidencial en los datos de respuesta o no es reconocible para una tercera parte.

En esta técnica puede apreciarse que sólo es necesario almacenar la(s) clave(s) pública(s) general(es) en las estaciones 10 móviles, mientras que la clave 35A secreta o privada está almacenada de manera segura en un servidor principal mantenido por el proveedor 32 de servicios inalámbricos. De esta manera, también se protegen el conjunto de instrucciones y/o los datos que se envían a la estación 10 móvil, manteniendo secreta de ese modo la estructura de la aplicación e impidiendo que terceras partes no autorizadas intenten utilizar la aplicación y las partes asociadas del sistema.

Debe observarse que cuando se utiliza esta técnica, la estación 10 móvil puede almacenar *n* claves públicas diferentes correspondientes a un conjunto de *n* aplicaciones diferentes. De esta manera, la estación 10 móvil responde a una aplicación dada iniciada por la red 32 inalámbrica solamente si el evento de activación, por ejemplo, la recepción de un mensaje válido y de un conjunto de datos opcional, puede descifrarse de manera precisa utilizando una de las *n* claves públicas almacenadas.

En otras realizaciones de la presente invención pueden utilizarse otros sistemas criptográficos distintos al RSA.

La fig. 5 muestra un diagrama de niveles de sistema que incluye un sistema de activación inalámbrico (OTA) según un aspecto de estas enseñanzas. En este sistema hay una capa 60 de servicio, una capa 62 de servidores web y una capa 64 de clientes. La capa 60 de servicio incluye un servidor OTA que ejecuta software 66 (SW) OTA que se comunica con una base 68 de datos global de servicios de sistema. La capa 62 de servidores web está formada por servidores 70 web y la capa 64 de clientes está formada por una pluralidad de PC y/o de estaciones de trabajo, denominados genéricamente como terminales 72, que están ubicados, por ejemplo, en instalaciones de investigación y desarrollo (R&D), ubicaciones de soporte a clientes y ubicaciones de punto de venta (POS). Los terminales 72 se comunican con el servidor 66 OTA mediante Internet u otra red a través de la capa 62 de servidores web. Según estas enseñanzas, los datos PPC enviados se obtienen de la estación 10 móvil utilizando un mensaje de solicitud PPC cifrado enviado desde el servidor 66 OTA. Después, la información recuperada puede almacenarse en la base 68 de datos global y/o puede proporcionarse a uno o más de los terminales 72 de la capa 64 de clientes para su revisión y análisis.

La fig. 6 muestra un diagrama de flujo lógico de un procedimiento de recuperación PPC a modo de ejemplo según estas enseñanzas. En la etapa A, el cliente llama a una línea de asistencia para informar sobre un problema detectado en la estación 10 móvil del cliente. Esta llamada del cliente también puede realizarse a través de Internet 37 y no necesita ser una llamada de voz. En las etapas B y C se produce un diálogo con el cliente en relación al supuesto fallo en la estación 10 móvil del cliente. En la etapa D se envía un mensaje SMS de activación a la estación 10 móvil del cliente para solicitar el envío de los datos PPC. Todo o parte del mensaje SMS de activación puede cifrarse, utilizando por ejemplo la técnica de cifrado RSA descrita anteriormente. En la etapa E se determina si los datos se transmitirán preguntando al cliente si los datos PPC deben transmitirse. El envío de los datos PPC puede realizarse sin coste alguno para el cliente o puede solicitarse una tasa. Si el cliente elige no transmitir los datos PPC, el control vuelve a la etapa B para seguir el diálogo con el cliente. Si el cliente indica que los datos PPC van a transmitirse, el control pasa a la etapa F para transmitir todos o un subconjunto de los datos PPC desde la estación 10 móvil, a través del SW 66 OTA, y los datos se almacenan en una base de datos PPC de la red 32 inalámbrica. La base de datos PPC puede ser la base 68 de datos global mostrada en la fig. 5. En las etapas G y H, la base de datos PPC se requiere para los datos PPC de la estación 10 móvil y los datos se analizan. Los resultados de los análisis pueden devolverse a la línea de asistencia utilizando una herramienta web en la etapa I para informar verbalmente al cliente del resultado, o los resultados pueden enviarse al cliente mediante Internet 37 a través de la capa 62 de servidores web de la fig. 5. Si fuera necesario, la herramienta web de la etapa I puede consultar directamente la base de datos PPC en la etapa J.

El resultado final es una mejora en el diagnóstico de los fallos detectados en la estación móvil del cliente, una reducción en los costes para el operador 32 de red y posiblemente también para el fabricante de la estación 10 móvil, y mayor satisfacción del cliente.

Aunque en la presente invención se ha mostrado y descrito específicamente con respecto a realizaciones preferidas de la misma, los expertos en la técnica entenderán que pueden realizarse cambios en la forma y en los detalles de la misma sin apartarse del alcance de la invención.

REIVINDICACIONES

1. Un procedimiento de operación de una estación (10) móvil, que comprende:

durante la operación de la estación móvil en una red, determinar y almacenar un conjunto de datos (24A) relacionados con el rendimiento en la estación móvil, comprendiendo dichos datos relacionados con el rendimiento información que representa estados normales y anormales en la red y en la estación móvil;

en respuesta a la aparición de un evento de activación, transmitir el conjunto o un subconjunto de los datos relacionados con el rendimiento a un ordenador (33A) para su análisis; y

recibir en la estación móvil un mensaje para informar a un usuario con relación al análisis;

caracterizado porque el evento de activación comprende recibir en la estación móvil un mensaje cifrado para transmitir el conjunto o subconjunto de los datos relacionados con el rendimiento, y comprende además descifrar el mensaje recibido utilizando una clave pública asociada almacenada en la estación móvil y transmitir el conjunto o el subconjunto de los datos relacionados con el rendimiento solamente en respuesta a un descifrado correcto del mensaje cifrado,

en el que además la clave pública almacenada en la estación móvil es una clave de un conjunto de claves públicas almacenadas en la estación móvil, donde los elementos individuales del conjunto de claves públicas están asociados con aplicaciones que pueden ejecutarse por la estación móvil en cooperación con al menos uno de entre un comando cifrado y un conjunto de datos cifrados recibidos desde la red inalámbrica que se descifran por la estación móvil utilizando una clave del conjunto de claves públicas.

2. Un procedimiento según la reivindicación 1, en el que los datos relacionados con el rendimiento se almacenan en contadores y en registros.

3. Un procedimiento según la reivindicación 1 ó 2, en el que los datos relacionados con el rendimiento comprenden un cómputo de llamas interrumpidas.

4. Un procedimiento según la reivindicación 1 ó 2, en el que los datos relacionados con el rendimiento comprenden una indicación de un resultado del modo de funcionamiento de autoanálisis de la estación móvil.

5. Un procedimiento según cualquier reivindicación anterior, en el que el ordenador está en un centro de control asociado con un proveedor de servicios de red, y en el que el ordenador determina, para la estación móvil, una indicación de la aparición de al menos uno de entre un fallo en la estación móvil, un fallo en un sistema del proveedor de servicios de red o ningún estado de fallo.

6. Un procedimiento según la reivindicación 5, en el que la recepción comprende además hacer que la indicación esté disponible para un usuario de la estación móvil.

7. Un procedimiento según cualquiera de las reivindicaciones 1 a 4, en el que el ordenador está en un centro de diagnóstico remoto, y en el que el ordenador determina, para la estación móvil, una indicación de la aparición de al menos uno de entre un fallo en la estación móvil, un fallo en un sistema del proveedor de servicios de red o ningún estado de fallo.

8. Un procedimiento según la reivindicación 7, en el que la recepción comprende además hacer que la indicación esté disponible para un usuario de la estación móvil individual.

9. Una estación (10) móvil que comprende un transceptor (14, 16) inalámbrico para llevar a cabo comunicaciones bidireccionales con una red (32) inalámbrica, comprendiendo además dicha estación móvil una memoria (24) y un controlador (18) acoplado a dicha memoria y a dicho transceptor, estando dispuesto dicho controlador para determinar, durante la operación de dicha estación móvil, un conjunto de datos relacionados con el rendimiento y para almacenar dicho conjunto determinado de datos (24A) relacionados con el rendimiento en dicha memoria, donde dichos datos relacionados con el rendimiento comprenden información que representa estados normales y anormales en la red y en la estación móvil, siendo sensible dicho controlador a la aparición de un evento de activación para transmitir dicho conjunto o un subconjunto de dichos datos relacionados con el rendimiento a un ordenador (33A) para su análisis;

caracterizada porque el evento de activación comprende recibir en la estación móvil un mensaje cifrado para transmitir el conjunto o subconjunto de los datos relacionados con el rendimiento, y siendo sensible dicho controlador a la recepción del mensaje para descifrar el mensaje recibido utilizando una clave (24B) pública asociada almacenada en la estación móvil y para transmitir el conjunto o el subconjunto de los datos relacionados con el rendimiento solamente en respuesta a un descifrado correcto del mensaje cifrado,

en la que además la clave pública almacenada en la estación móvil es una clave de un conjunto de claves públicas almacenadas en la estación móvil, donde los elementos individuales del conjunto de claves públicas están asociados

con aplicaciones que pueden ejecutarse por la estación móvil en cooperación con al menos uno de entre un comando cifrado y un conjunto de datos cifrados recibidos desde la red inalámbrica, descifrándose el comando cifrado y el conjunto de datos por la estación móvil utilizando la clave asociada del conjunto de claves públicas.

10. Una estación móvil según la reivindicación 9, en la que dichos datos relacionados con el rendimiento están almacenados en al menos uno de entre contadores y registros de hardware y en posiciones de memoria que operan como contadores y como registros.

11. Una estación móvil según la reivindicación 9 ó 10, en la que dichos datos relacionados con el rendimiento comprenden al menos uno de entre un contador de llamadas interrumpidas y una indicación de un resultado de un modo de funcionamiento de autoanálisis de la estación móvil.

12. Una estación móvil según cualquiera de las reivindicaciones 9 a 11, en la que dicho ordenador comprende una parte de un centro (33) de control asociado con un proveedor (32) de servicios de red, y en la que el ordenador está dispuesto para determinar, para la estación móvil, una indicación de la aparición de al menos uno de entre un fallo en dicha estación móvil, un fallo en un sistema de dicho proveedor de servicios de red o ningún estado de fallo.

13. Una estación móvil según la reivindicación 12, en la que dicho centro de control está dispuesto para transmitir dicha indicación a dicho controlador de estación móvil a través de dicho transceptor de estación móvil.

14. Una estación móvil según cualquiera de las reivindicaciones 9 a 11, en la que dicho ordenador está en un centro (38) de diagnóstico remoto, y en la que el ordenador está dispuesto para determinar, para la estación móvil, una indicación de la aparición de al menos uno de entre un fallo en dicha estación móvil, un fallo en un sistema de dicho proveedor de servicios de red o ningún estado de fallo.

15. Una estación móvil según la reivindicación 14, en la que dicho centro de diagnóstico está dispuesto para transmitir dicha indicación a dicho controlador de estación móvil a través de dicho transceptor de estación móvil.

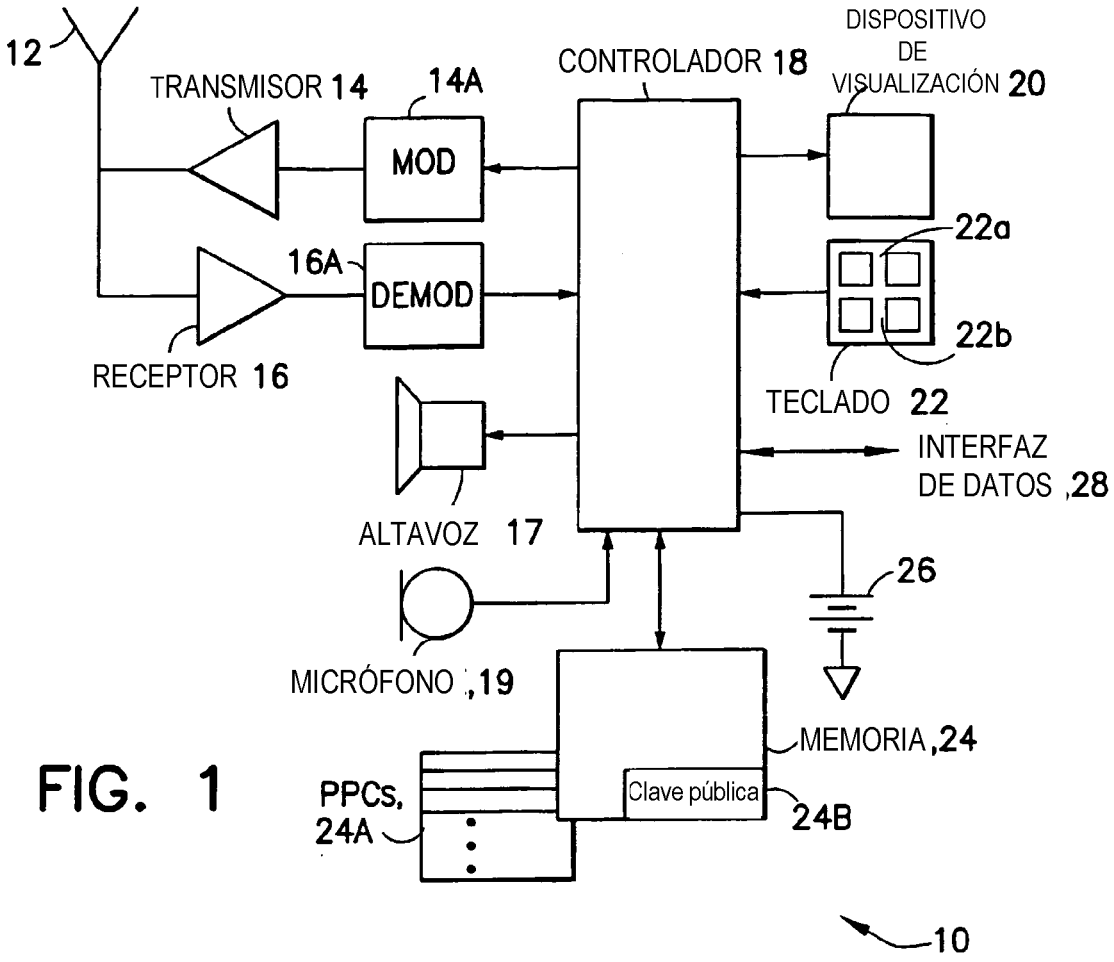

12
TRANSMISOR 14
14A
MOD
CONTROLADOR 18
DISPOSITIVO DE VISUALIZACIÓN 20
16A
DEMOD
22a
22b
RECEPTOR 16
TECLADO 22
INTERFAZ DE DATOS ,28
ALTAVOZ 17
26
MICRÓFONO ,19
MEMORIA ,24
PPCs, 24A
Clave pública
24B
10

FIG. 1

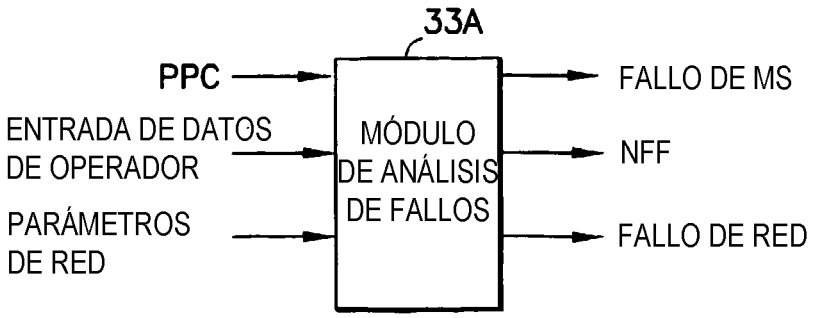
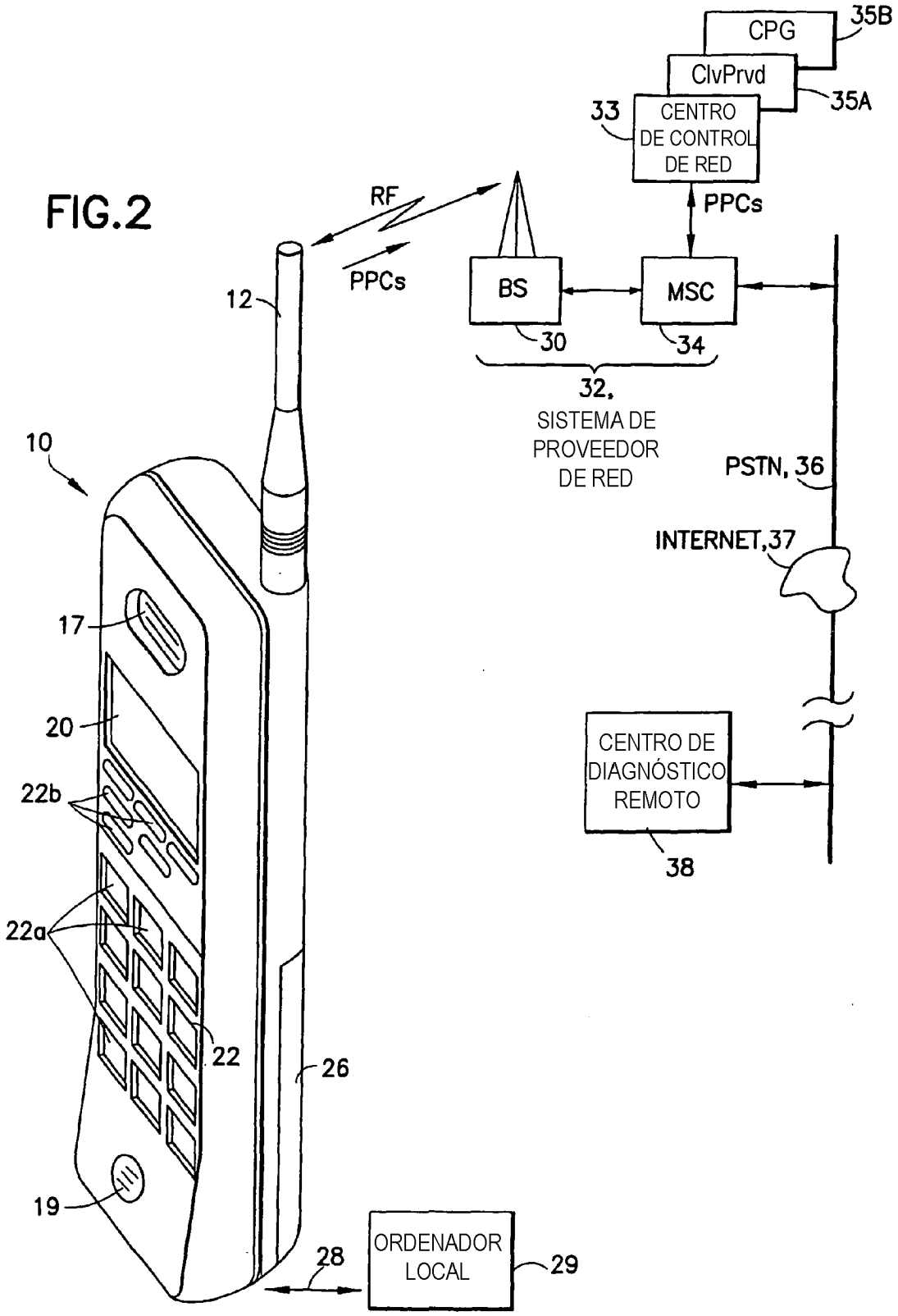

33A
PPC
ENTRADA DE DATOS DE OPERADOR
PARÁMETROS DE RED
MÓDULO DE ANÁLISIS DE FALLOS
FALLO DE MS
NFF
FALLO DE RED

FIG.3

FIG.2


CPG
35B
ClvPrvd
35A
33
CENTRO DE CONTROL DE RED
PPCs
RF
PPCs
12
BS
MSC
30
34
32,
SISTEMA DE PROVEEDOR DE RED
PSTN, 36
INTERNET,37
10
17
20
22b
22a
22
26
19
CENTRO DE DIAGNÓSTICO REMOTO
38
ORDENADOR LOCAL
28
29

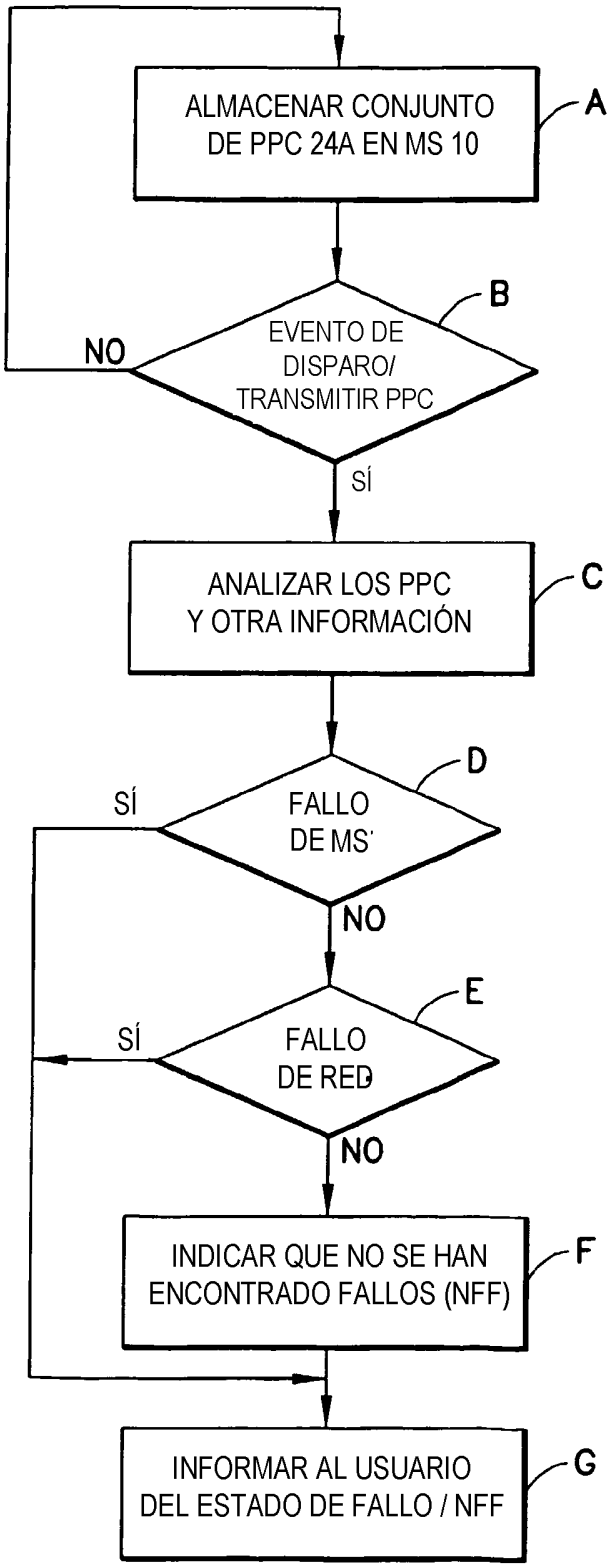

ALMACENAR CONJUNTO DE PPC 24A EN MS 10
A
B
EVENTO DE DISPARO/ TRANSMITIR PPC
NO
SÍ
ANALIZAR LOS PPC Y OTRA INFORMACIÓN
C
D
FALLO DE MS
SÍ
NO
E
FALLO DE RED
SÍ
NO
INDICAR QUE NO SE HAN ENCONTRADO FALLOS (NFF)
F
INFORMAR AL USUARIO DEL ESTADO DE FALLO / NFF
G

FIG.4

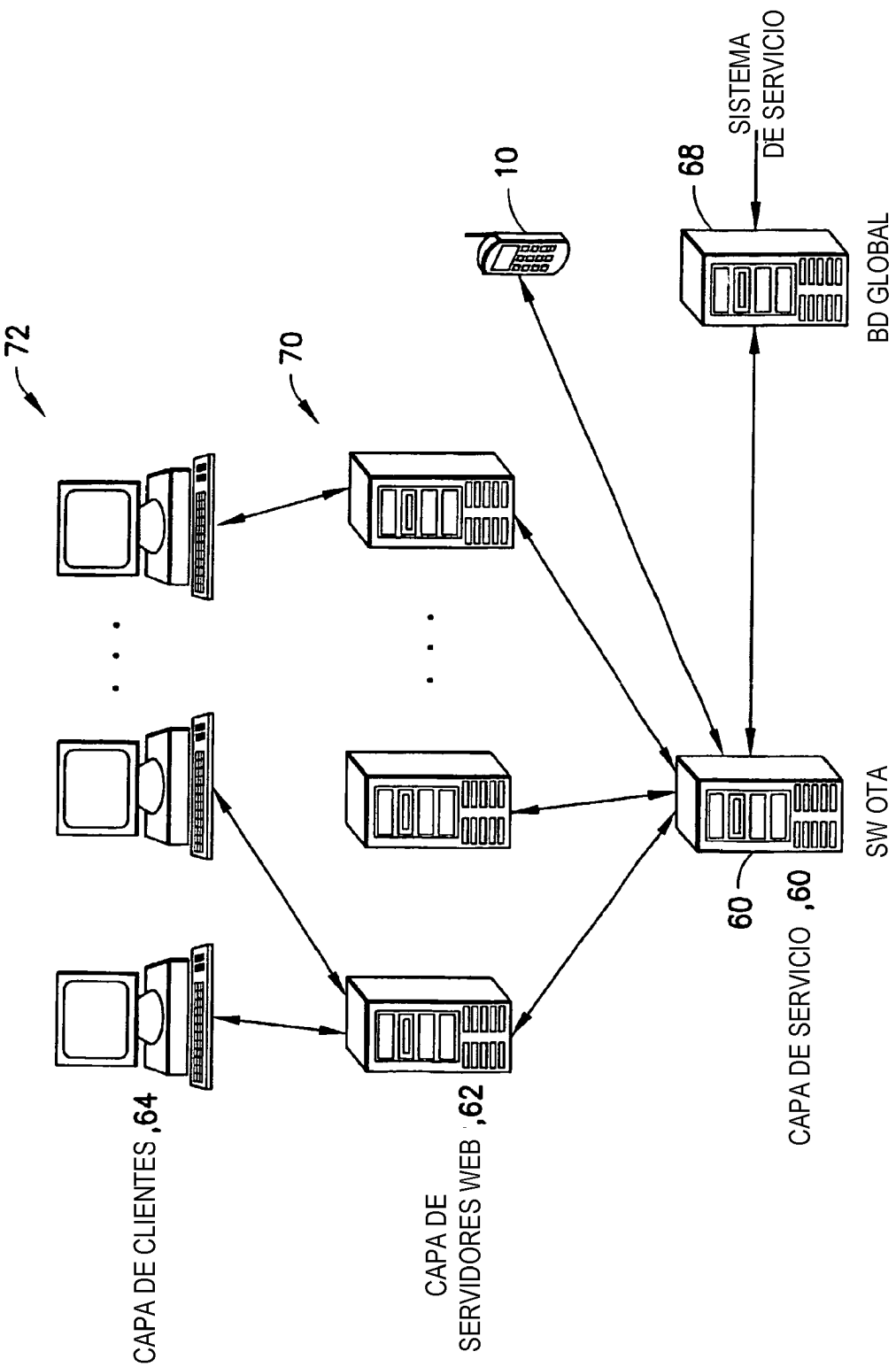

72
70
10
68
SISTEMA
DE SERVICIO
BD GLOBAL
CAPA DE CLIENTES ,64
CAPA DE
SERVIDORES WEB ,62
CAPA DE SERVICIO ,60
60
SW OTA

FIG.5

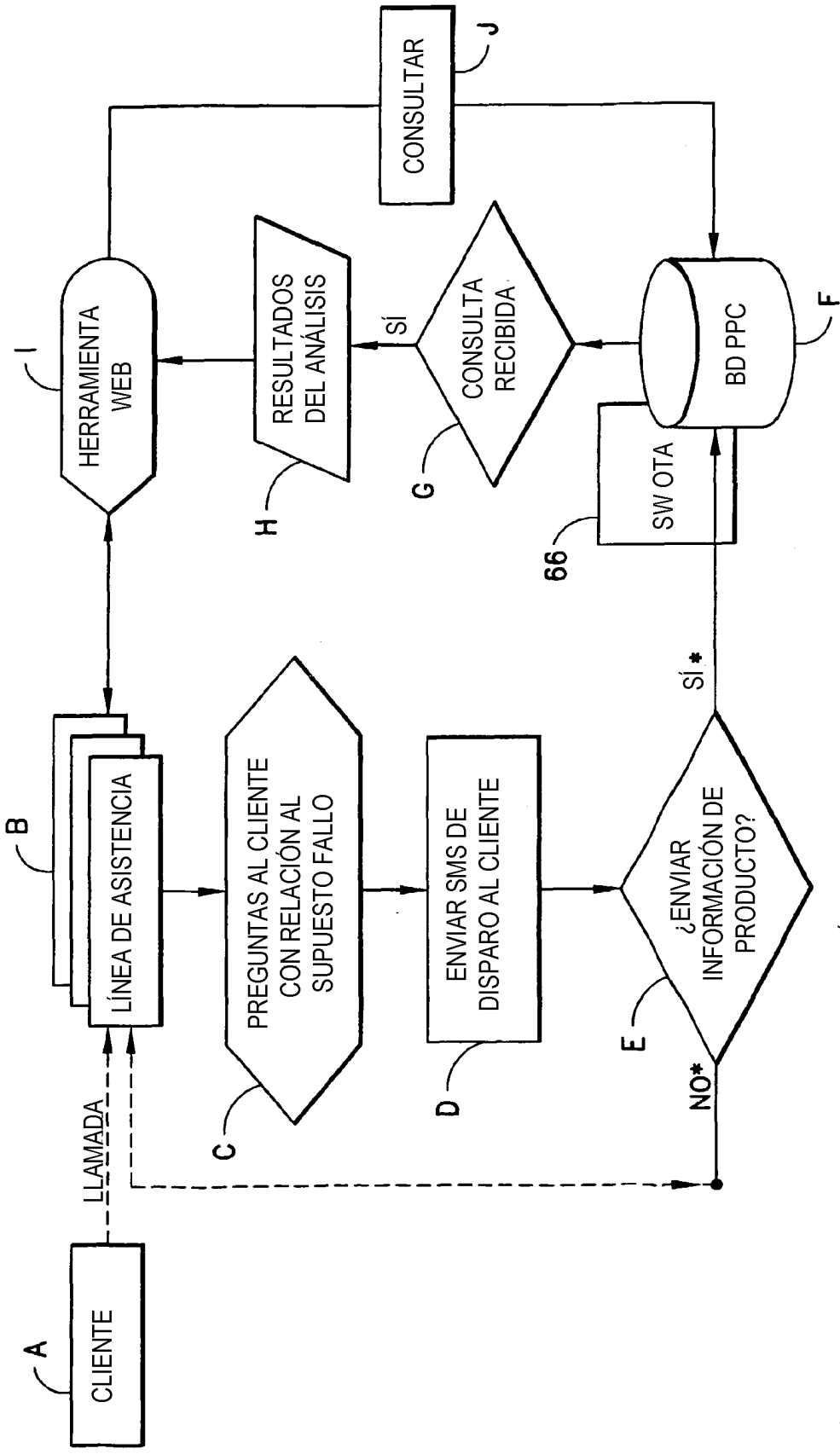

CLIENTE
A
LLAMADA
B
LÍNEA DE ASISTENCIA
PREGUNTAS AL CLIENTE CON RELACIÓN AL SUPUESTO FALLO
C
ENVIAR SMS DE DISPARO AL CLIENTE
D
¿ENVIAR INFORMACIÓN DE PRODUCTO?
E
NO*
SÍ *
SW OTA
66
BD PPC
F
CONSULTA RECIBIDA
G
SÍ
RESULTADOS DEL ANÁLISIS
H
HERRAMIENTA WEB
I
CONSULTAR
J
* ENTRADA DE DATOS DE USUARIO A TRAVÉS DE LA INTERAZ DE USUARIO DEL TELÉFONO

FIG.6