(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 449 223**

(51) Int. CI.:

H04W 12/06 (2009.01)
H04W 8/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **17.09.2009 E 09818221 (5)**

(97) Fecha y número de publicación de la concesión europea: **19.02.2014 EP 2332357**

(54) Título: **Método, estación móvil, sistema y procesador de red para utilizar en comunicaciones móviles**

(30) Prioridad:

02.10.2008 GB 0818027

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.03.2014

(73) Titular/es:

MOTOROLA SOLUTIONS, INC. (100.0%)
1303 East Algonquin Road
Schaumburg IL 60196, US

(72) Inventor/es:

HOFFMAN, TORBEN y
SORENSEN, LARS

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Método, estación móvil, sistema y procesador de red para utilizar en comunicaciones móviles

CAMPO DE LA INVENCIÓN

La presente invención se refiere a un método, una estación móvil, un sistema y un procesador de red para utilizar en comunicaciones móviles. En particular, la invención se refiere al establecimiento de suministro de servicios de comunicación a una estación móvil que puede migrar entre diferentes redes de comunicación.

ANTECEDENTES DE LA INVENCIÓN

Un sistema de comunicación celular o con concentración de enlaces es uno en el que los terminales de usuario móviles o portátiles, tales como teléfonos móviles, o radios portátiles o montadas en vehículos, en el presente documento denominados colectivamente 'estaciones móviles' o 'MSs', pueden comunicar mediante una infraestructura de sistema que incluye generalmente una o varias estaciones base fijas (estaciones base transceptoras) y otras instalaciones de encaminamiento y control. Cada estación base tiene uno o varios transceptores y da servicio a las MS en un área o región dada, conocida como 'celda', mediante comunicación inalámbrica. A menudo, las celdas de estaciones base vecinas están solapadas.

Puede considerarse que un sistema de comunicación móvil que proporciona cobertura de área extensa está formado por una serie de redes interconectadas. Cada red incluye normalmente un grupo de celdas denominado a menudo una 'zona'. La infraestructura de cada red comprende normalmente, además de las estaciones base que dan servicio a las estaciones móviles en las respectivas celdas de la zona, un encaminador (que puede denominarse asimismo un conmutador) que encamina comunicaciones hacia y desde la red, y dentro de la red. El encaminador puede estar asociado con, o formar parte de, un controlador de zona que puede proporcionar otras funciones de gestión dentro de la red, tal como proporcionar la administración de las estaciones base a nivel de red. La infraestructura puede incluir asimismo un procesador de autenticación que autentica y registra MSs para utilizar la red. Las redes de diferentes zonas, en particular los encaminadores y procesadores de autenticación de dichas redes, pueden comunicar mediante diversos medios conocidos, tal como comunicación por ondas de radio o microondas, comunicación eléctrica cableada u óptica, o internet.

Es habitual que una MS del usuario particular registrado con un operador del sistema móvil tenga una red 'propia' que proporciona normalmente un servicio de comunicación al usuario. Si el usuario se desplaza a otra región no cubierta por la red propia, por ejemplo a una parte diferente del país del usuario o a un país extranjero, el usuario puede recibir un servicio desde la red local, como una red visitada. Normalmente, es necesario completar satisfactoriamente un proceso de autenticación que involucra la red propia del usuario y la red visitada, junto con el registro de la MS visitante mediante la red visitada.

Por ejemplo, un tipo particular de sistema de comunicación móvil ampliamente utilizado en Europa y en otras partes para soportar comunicaciones dentro de organizaciones, tal como servicios públicos de seguridad y empresas, es un sistema TETRA. Dicho sistema está diseñado para funcionar de acuerdo con el 'protocolo' o procedimientos estándar TETRA (Terrestrial Trunked Radio, radio terrestre con concentración de enlaces) definido por el Instituto Europeo de Normas de Telecomunicaciones (ETSI, European Telecommunication Standards Institute). Generalmente, los sistemas TETRA soportan la migración de MS desde una red propia a una red visitada, y la provisión de servicios en la red visitada. Otro sistema que está diseñado para ser utilizado de manera similar es el sistema APCO 25, que es un sistema que funciona de acuerdo con el estándar APCO 25 definido por la Asociación de Funcionarios de Comunicaciones de Seguridad Pública - Internacional (APCO, Association of Public Safety Communications Officials International), estandarizado por la Asociación de la Industria de Telecomunicaciones (TIA, Telecommunications Industry Association) de EE.UU.

Normalmente, cuando una MS solicita su registro por una red visitada, los servicios específicos a proporcionar a la MS tienen que ser determinados por la red visitada durante el procedimiento de autenticación y registro. En los sistemas conocidos, los servicios a proporcionar son determinados por la red visitada obteniendo de la red propia un registro de servicios que proporciona detalles de los servicios que se permite proporcionar a la MS. Los servicios pueden variar de una MS a otra, en función, por ejemplo, de la implementación particular de la MS o del departamento de la organización, o la antigüedad dentro de la organización o departamento del usuario de la MS. Normalmente, la red visitada proporciona servicios que están en consonancia con los permitidos en la red propia y son especificados por la red propia cuando lo solicita la red visitada. Por lo tanto, en los sistemas conocidos se requiere una comunicación entre la red visitada y la red propia, de la información relativa a los servicios permitidos. La autenticación y el registro de la MS mediante una red visitada puede retardarse de manera no deseable debido a la necesidad de dicha comunicación, especialmente cuando una serie de MSs han migrado y solicitado información a la vez.

Además, no es posible ningún registro si hay un fallo en una conexión de comunicación entre las redes.

El documento de LONG M y otros, 'Localised Authentication for inter-network roaming across wireless LANs'-WLAN systems and interworking, IEE PROCEEDINGS: COMMUNICATIONS, INSTITUTION OF ELECTRICAL ENGINEERS, GB, volumen 151, número 5, 9 de junio de 2004 (09/07/2004), páginas 496 a 500, XP006022619, ISSN: 1350-2425, DOI:10.1049/IP-Com:20040661, describe una propuesta para un sistema que podría haberse desarrollado. Con dicha propuesta, se proporcionaría una autenticación manual inicial en un sistema de LANs inalámbricas. El objetivo era evitar el retardo implicado cuando una red propia tiene que adoptar una decisión de 'aceptar' o 'rechazar', en el momento en que un usuario intenta por primera vez acceder a una LAN diferente a la LAN doméstica. El enfoque propuesto hubiera evitado asimismo la vulnerabilidad a cualquier fallo de una red intermedia. Una red visitada validaría una firma proporcionada por un usuario que desea ser autenticado por la red visitada. La red visitada y el usuario podrían obtener a continuación un 'secreto compartido', que podría ser utilizado para la autenticación subsiguiente cuando el usuario itinera a continuación dentro de la red visitada.

RESUMEN DE LA INVENCIÓN

De acuerdo con la presente invención, en un primer aspecto se da conocer un método de funcionamiento en un sistema de comunicación móvil, siendo el método tal como se define en la reivindicación 1 de las reivindicaciones adjuntas.

De acuerdo a la presente invención, en un segundo aspecto se da a conocer una estación móvil tal como la definida en la reivindicación 13 de las reivindicaciones adjuntas.

De acuerdo con la presente invención, en un tercer aspecto se da a conocer un procesador para utilizar como un procesador de autenticación en una red propia de un sistema de comunicación móvil, siendo el procesador tal como se define en la reivindicación 14 de las reivindicaciones adjuntas.

De acuerdo con la presente invención, en un cuarto aspecto se da conocer un procesador para utilizar como un procesador de autenticación en una red visitada de un sistema de comunicación móvil, siendo el procesador tal como se define el la reivindicación 15 de las reivindicaciones adjuntas.

Se definen características adicionales de la invención en las reivindicaciones dependientes adjuntas, y se dan a conocer en la descripción de realizaciones de la invención proporcionada más adelante en este documento.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La figura 1 es un diagrama esquemático de bloques de un sistema de comunicación móvil en el que pueden aplicarse realizaciones de la invención.

La figura 2 es un diagrama de flujo de un método que realiza la presente invención para su utilización en el sistema de la figura 1.

DESCRIPCIÓN DE REALIZACIONES DE INVENCIÓN

La figura 1 es un diagrama de bloques que muestra un sistema de comunicación móvil 100 ilustrativo, en el que pueden aplicarse realizaciones de la invención. Para mayor simplicidad, en la figura 1 se muestran solamente componentes básicos del sistema 100. El sistema 100 incluye una MS (estación móvil) 101 y dos redes 102, 103. El sistema 100 puede incluir otras MSs y otras redes (no mostradas). La red 102 es la red propia de la MS 101 y la red 103 es una red visitada, es decir, otra red desde la cual la MS 101 es capaz de obtener servicios de comunicación cuando se encuentra en la proximidad de la red 103 y cuando ha tenido lugar un procedimiento de autenticación y registro entre la red 103 y la MS 101.

La MS 101 incluye como componentes principales (junto con otros componentes no mostrados) un transceptor de RF 104 y un procesador 105 que controla las opciones funcionales en la MS 101 y está acoplado operativamente al transceptor 104. La MS 101 incluye asimismo una memoria 106 acoplada operativamente al procesador 105 y al transceptor 104. La memoria 106 incluye datos y programas almacenados necesarios, en funcionamiento, para el procesador 105 y el transceptor 104.

La red propia 102 incluye una estación base 107 que incluye uno o varios transceptores que proporcionan comunicación inalámbrica con el transceptor 104 de la MS 101, cuando la MS 101 está dentro del alcance de la estación base 107. La red propia 102 incluye asimismo: (i) un encaminador 108 para encaminar comunicaciones hacia y desde la red 102 y dentro de la red 102; (ii) un procesador de autenticación 109 que lleva a cabo funciones de autenticación y registro de la red propia 102; y (iii) una memoria 110 que almacena datos y programas

requeridos, en funcionamiento, por la red propia 102, especialmente por el procesador de autenticación 109. El procesador de autenticación 109 está acoplado operativamente a un registro de posiciones propias 111, que es la base de datos que contiene datos relativos a estaciones móviles servidas normalmente por la red 102 como red propia. El procesador 109 está asimismo acoplado operativamente a un registro de posiciones de visitantes 112, que es una base de datos que contiene datos relativos a estaciones móviles servidas normalmente por otras redes diferentes a la red 102 como red propia, y que han visitado la red 102.

Los registros 111 y 112 se muestran en la figura 1 estando dentro de la red propia 102, aunque alternativamente podrían estar fuera de la red propia 102 pero conectados operativamente con la red propia 102.

El procesador de autenticación 109 y/o el encaminador 108 pueden estar asociados con, o incorporados dentro de, un controlador de zona (no mostrado) de la red propia 102.

Tal como será evidente para los expertos en la materia, la red propia 102 puede incluir otros componentes interconectados (no mostrados), tales como otras estaciones base y otros encaminadores.

La red visitada 103 incluye una estación base 113 que incluye uno o varios transceptores que proporcionan comunicación inalámbrica con el transceptor 104 de la MS 101, cuando la MS 101 está dentro del alcance de la estación base 113 y la autenticación y el registro de la MS 101 mediante la red 103 se ha completado satisfactoriamente, tal como se describe más adelante. La red visitada 103 incluye asimismo: (i) un encaminador 118 para encaminar comunicaciones hacia y desde la red 103 y dentro de la red 103; (ii) un procesador de autenticación 119 que lleva a cabo funciones de autenticación y registro de la red visitada 103; y (iii) una memoria 120 que almacena datos y programas necesarios, en funcionamiento, para la red 103, especialmente para el procesador de autenticación 119.

El procesador de autenticación 119 está acoplado operativamente de un registro de posiciones propias 121, que es una base de datos que contiene datos relativos a estaciones móviles servidas normalmente por la red 103 como red propia. El procesador 119 está asimismo acoplado operativamente a un registro de posiciones de visitantes 122, que es una base de datos que contiene datos relativos a estaciones móviles servidas normalmente por otras redes diferentes a la red 103 como red propia, y que han visitado la red 103.

Los registros 121 y 122 se muestran en la figura 1 estando dentro de la red visitada 103, aunque podrían estar alternativamente fuera de la red visitada 103 y acoplados operativamente a la red 103.

El procesador de autenticación 119 y/o el encaminador 118 pueden estar asociados con, o incorporados dentro de, un controlador de zona (no mostrado) de la red visitada 103.

Tal como resultará evidente para los expertos en la materia, la red visitada 103 puede incluir otros componentes interconectados (no mostrados), tales como otras estaciones base y otros encaminadores.

Puede existir una conexión bidireccional 115 entre la red propia 102 y la red visitada 103 para permitir que se realicen comunicaciones entre las dos redes cuando es necesario. La conexión 115 puede formarse de una de las maneras conocidas en la técnica, que se han mencionado anteriormente. Por lo tanto, ésta puede ser una conexión cableada o de cable o una conexión inalámbrica.

El sistema 100 incluye asimismo un terminal de emisión de claves 123. Un objetivo del terminal 123 es emitir una clave MAC (código de autenticación de mensaje) a las redes 102 y 103. El terminal 123 puede emitir asimismo una clave MAC a otras redes (no mostradas) y/o puede emitir otras claves, tales como claves requeridas en comunicaciones cifradas hacia y desde estaciones móviles, a las redes 102 y 103 (y a otras redes). La clave MAC emitida por el terminal 123 permite que un código de certificado, que se denomina 'MAC' (código de autenticación de mensaje) en el presente documento, sea calculado y aplicado en relación con un registro de servicios emitido por la red propia 102 para la MS 101 (o para cualquier otra MS para la que la red 102 es la red propia), tal como se describe más adelante. El registro de servicios certificado que incluye el MAC calculado utilizando el registro de servicios, es proporcionado a la MS relevante, por ejemplo la MS 101, y almacenado por la misma. El registro de servicios certificado puede ser comunicado posteriormente a la red visitada 103 mediante la MS 101 y, tal como se escribe más adelante, un código de autenticación, un MAC que se prevé sea el mismo que el calculado por la red propia 102, puede ser calculado por la red visitada 103 utilizando la misma clave MAC y el procedimiento de cálculo que se utilizan por la red propia 102 para autenticar el registro de servicios.

La clave MAC emitida por el terminal de emisión de claves 123 a diferentes redes puede ser convenientemente la misma, aunque pueden emitirse diferentes claves MAC para diferentes redes como redes propias. Cada red, tal como la red 102, puede utilizar convenientemente la misma clave MAC, para su utilización en relación con la certificación de los registros de servicios de todas las MS servidas por la red como red propia. Sin embargo, cada

red podría recibir del terminal de emisión de claves 123, y utilizar, diferentes claves MAC para los registros de servicios de diferentes MS, o diferentes grupos de MS, servidos por la red, como red propia.

El terminal de emisión de claves 123 puede emitir una clave MAC nueva a la red propia 102 y a la red 103 periódicamente, por ejemplo después de un cierto período de tiempo, por ejemplo un número fijo de semanas, desde la emisión de la clave MAC anterior. Alternativa o adicionalmente, el terminal de emisión de claves 123 puede emitir una clave MAC nueva después de un evento desencadenante, por ejemplo después de que se ha restablecido el funcionamiento a continuación de un periodo de avería, de parte o la totalidad del sistema 100, o de una de las conexiones en el sistema 100, por ejemplo la conexión 115.

El terminal de emisión de claves 123 está conectado a la red propia 102 mediante una conexión 125 y a la red visitada 103 mediante una conexión 127. Cada una de las conexiones 125 y 127 puede ser una conexión cableada o de cable, o una conexión inalámbrica. La clave MAC es enviada a las redes 102 y 103 mediante las conexiones 125 y 127, respectivamente.

Cuando la red propia 102 recibe la clave MAC desde el terminal de emisión de claves 123 a través de la conexión 125, almacena dicha clave en su memoria 110. Cuando la red visitada 103 recibe la clave MAC desde el terminal de emisión de claves 123 a través de la conexión 127, almacena dicha clave en su memoria 120.

Cuando cada una de las redes 102 y 103 recibe y almacena cada clave MAC nueva, preferentemente retiene almacenada en su memoria la clave o claves anteriores a las que sustituye la clave nueva, de tal modo que la red es capaz de llevar a cabo el procedimiento de cálculo necesario utilizando la clave anterior si se requiere, por ejemplo tal como se describe más adelante haciendo referencia a la figura 2. Preferentemente, la red 102 actualiza asimismo el código MAC del registro de servicios para cada una de las MS a las que da servicio como red propia, en cuanto puede después de la recepción de la clave MAC nueva.

El terminal de emisión de claves 123 se muestra en la figura 1 estando fuera de las redes 102 y 103, si bien el terminal 103 podría alternativamente estar incorporado dentro de una de las redes, por ejemplo dentro de la red propia 102, o distribuido entre las redes 102 y 103.

La figura 2 es un diagrama de flujo que muestra un método 200 que realiza la invención, que puede ser utilizado en el sistema 100.

En la etapa 201 del método 200, la red propia 102 recibe a través de la conexión 125 la última clave MAC emitida por el terminal de emisión de claves 123 y almacena la clave en su memoria 110.

En la etapa 202, la red propia 102 produce un registro de servicios de la MS 101 y añade un MAC (código de certificado) al registro de servicios. El procesador de autenticación 109 puede producir el registro de servicios mediante la utilización de datos actuales de registro de servicios obtenidos del registro de posiciones propias 111. El registro de servicios puede producirse como un registro actualizado siempre que el registro de servicios mantenido en el registro de posiciones propias 111 esté actualizado y/o siempre que haya transcurrido un cierto período de tiempo, por ejemplo un número fijo de semanas, desde la emisión anterior del registro de servicios, y/o siempre que se produzca un evento desencadenante, por ejemplo siempre que la MS 101 se registre con la red propia 102. Además, el MAC del registro de servicios puede actualizarse por recálculo siempre que se haya recibido una nueva clave MAC desde el terminal de emisión de claves 123. Por lo tanto, el registro de servicios puede actualizarse siempre que recalcule el MAC.

El registro de servicios producido en la etapa 202 incluye datos relativos a detalles de los servicios que se permite recibir a la MS en el sistema 100 desde redes del sistema 100, incluida la red propia 102 y la red visitada 103. Ejemplos de dichos datos incluidos en el registro de servicios pueden incluir:

(i) Permiso de acceso al sistema: indica que se permite a la MS 101 y/o a su usuario autorizado actual utilizar el sistema 100 para comunicaciones móviles;

(ii) Capacidad de interconexión individual: indica si se permite a la MS 101 participar en llamadas integradas interconectadas que tienen lugar dentro del sistema 100;

(iii) Capacidad semidúplex/dúplex: indica si se permite a la MS 101 participar en llamadas dúplex o semidúplex dentro del sistema 100;

(iv) Capacidad de cifrado: indica si se permite a la MS 101 transmitir o recibir comunicaciones inalámbricas cifradas, y el nivel o tipo de seguridad de cifrado a aplicar;

(v) Nivel de prioridad: indica qué nivel de prioridad se permite para realizar o recibir llamadas por la MS 101, por ejemplo en base a la antigüedad o función laboral de la persona que utiliza la MS 101;

(vi) Capacidad de transferencia de datos: indica la capacidad o caudal de datos, por ejemplo datos de texto, numéricos, de imagen o de video, que se permite enviar a o recibir desde la MS 101;

(vii) Autorización de redes: indica la identidad de la red o redes del sistema 100 con las que se permite a la MS 101 registrarse como red visitada o redes visitadas;

(viii) Pertenencias a grupos: indica la identidad del grupo o grupos ('grupo o grupos de llamada') de MSs, de los que la MS 101 es miembro, y a los que se le permite unirse cuando está establecida o estableciéndose una llamada entre el grupo.

El registro de servicios producido en la etapa 202 puede incluir datos en campos relativos a un gran número de parámetros de servicio, por ejemplo hasta cien o más de dichos parámetros.

El registro de servicios puede incluir asimismo detalles básicos, tales como la identidad de la red 102 que como red propia ha producido el registro de servicios, un número de serie de la emisión del registro de servicios y la fecha de la emisión del registro de servicios.

Tal como se ha indicado anteriormente, un MAC de certificado es producido por la red propia 101, por ejemplo por el procesador de autenticación 109. El MAC de certificado se produce llevando a cabo un procedimiento de cálculo en el que los datos que comprenden el registro de servicios, por ejemplo los contenidos completos del registro de servicios, o por lo menos los contenidos principales del registro de servicios, y la clave MAC proporcionan conjuntamente entradas al procedimiento de cálculo. El MAC de certificado es una salida del procedimiento de cálculo. Existen muchas formas conocidas de algoritmos o procedimientos de cálculo de MAC, que se conocen por sí mismas, y dichos procedimientos conocidos pueden utilizarse en el método 200. Habitualmente, dichos procedimientos aplican una operación matemática definida para combinar los datos del registro de servicios con los datos de la clave MAC. La operación matemática puede incluir, por ejemplo, varias etapas de multiplicación y reorganización de los datos. El procedimiento matemático puede ser, por ejemplo, un algoritmo MAC estándar publicado, tal como el algoritmo SHA 256 o un algoritmo MAC estándar similar. El MAC resultante producido por el cálculo es diferente para cualquier diferencia en los datos del registro de servicios, incluso si se trata de una diferencia insignificante. Convenientemente, la clave MAC utilizada en el procedimiento de cálculo es un número que ha sido generado de manera aleatoria o pseudoaleatoria por el terminal de emisión de claves 123.

El MAC de certificado calculado por la red propia 102 tiene por lo tanto un valor que protege tanto la integridad como la autenticidad de los datos del registro de servicios a partir del cual se ha calculado. Por lo tanto, el registro de servicios puede ser autenticado permitiendo a cualquier verificador, en particular la red visitada 103, que posee asimismo la clave MAC y el procedimiento de cálculo utilizado por la red propia 102, calcular asimismo el MAC como un MAC de autenticación y cotejar el MAC de autenticación con el MAC de certificado aplicado por la red propia 102. El verificador será capaz de detectar cualesquiera cambios no autorizados en el contenido de datos del registro de servicios, mediante detectar que el MAC de autenticación y el MAC de certificado no se corresponden.

Opcionalmente, el propio registro de servicios puede cifrarse utilizando una clave de cifrado y un algoritmo de cifrado, de forma conocida. La clave de cifrado puede comprender la clave MAC u otra clave, por ejemplo emitida por el terminal de emisión de claves 123.

El MAC de certificado producido por el procedimiento de cálculo se añade al registro de servicios a partir del cual se ha calculado, en la etapa 202 del método 200.

En la etapa 203 del método 200, la red propia 102 envía a la MS 101 el registro de servicios certificado, que incluye el registro de servicios y el MAC de certificado calculado a partir de éste, obtenido en la etapa 202. El registro de servicios certificado puede ser enviado a la MS 101 en la etapa 203, cuando la MS tiene a continuación una conexión inalámbrica normal con la red 102, mediante registro de manera convencional a través de la estación base 107. La MS 101 recibe el registro de servicios certificado mediante comunicación inalámbrica desde la estación base 107 al transceptor 104 de la MS.

En la etapa 204, la MS 101, controlada por el procesador 105, almacena en su memoria 106 el registro de servicios certificado enviado en la etapa 203. Cuando la MS 101 tiene una versión previa del registro de servicios almacenada ya en su memoria 106, la versión posterior enviada en la etapa 203 puede sustituir la que ya hay almacenada.

Preferentemente, la propia MS 101 no tiene la clave MAC emitida por el terminal 123, de tal modo que no puede hacer funcionar por sí misma el procedimiento de cálculo de MAC.

En la etapa 208, normalmente al mismo tiempo que la etapa 201, la red visitada 103 recibe a través de la conexión 127, y almacena en la memoria 120, la última versión de la clave MAC utilizada por el terminal de emisión de claves 123. Se prevé que la clave MAC recibida en la etapa 208 sea la misma clave que ha sido utilizada por la red propia 102 en la etapa 202 para calcular el MAC de certificado. La etapa 208 puede llevarse a cabo al mismo tiempo que la recepción de la última versión de la clave MAC mediante la red propia 102. Sin embargo, en algunos casos, la clave MAC contenida por la red visitada 103 puede ser una versión anterior o posterior de la clave MAC, en comparación con la utilizada por la red propia 102 para hacer funcionar el procedimiento de cálculo a efectos de producir el código de certificado en la etapa 202.

Algún tiempo después de la etapa 204, la MS 101 está en una zona cubierta por la red visitada 103. En la etapa 205, la MS 101 solicita el registro mediante la red visitada 103. La comunicación entre la MS 101 y la red visitada 103 se lleva a cabo entre el transceptor 104 de la MS 101 y la estación base 113 de la red visitada 103.

En la etapa 207, la MS 101 recupera de la memoria 106 su registro de servicios certificado almacenado en la etapa 203, y envía a la red visitada 103 el registro de servicios certificado recuperado, que comprende el registro de servicios y el MAC de certificado calculado a partir del mismo mediante la red propia 102. La etapa 207 puede seguir a la etapa 205, tal como se muestra en la figura 2, aunque podría formar parte de la etapa 205, o incluso preceder a la etapa 205.

En la etapa 209, que se lleva a cabo por medio de la red visitada 103 en respuesta a la recepción del registro de servicios certificado en la etapa 207, la red visitada 103 recupera la última versión de la clave MAC almacenada en su memoria 120. La última versión de la clave MAC es la que se ha recibido y almacenado en la etapa 208.

En la etapa 211, la red visitada 103, por ejemplo mediante el procesador de autenticación 119, calcula un MAC de autenticación para el registro de servicios recibido desde la MS 101. Para proporcionar autenticación del registro de servicios, está previsto que el MAC de autenticación sea el mismo que el MAC de certificado del registro de servicios recibido desde la MS 101. Por lo tanto, para producir el MAC de autenticación, la red visitada 103 lleva a cabo el mismo procedimiento de cálculo que fue llevado a cabo por la red propia 103 para producir el MAC de certificado. Para el procedimiento de cálculo, la red visitada 103 utiliza como entradas la clave MAC recuperada en la etapa 209, y el registro de servicios enviado por la MS 101 en la etapa 207. Cuando el registro de servicios ha sido cifrado, la red visitada 103 descifra el registro de servicios (utilizando la misma clave de cifrado y un algoritmo de desciframiento correspondiente al algoritmo de cifrado utilizado por la red 102) antes de llevar a cabo la etapa 211.

En la etapa 212, la red visitada 103, por ejemplo mediante el procesador de autenticación 119, compara el MAC de autenticación del registro de servicios que ha sido calculado en la etapa 211, con el MAC de certificado que ha sido recibido con el registro de servicios desde la MS 101. Verificando la correspondencia del MAC de autenticación calculado, con el MAC de certificado recibido desde la MS 101, la red visitada 103, por ejemplo mediante el procesador de autenticación 119, es capaz de determinar que el registro de servicios recibido desde la MS 101 es auténtico y está actualizado. En respuesta a un cotejo satisfactorio de los MACs en la etapa 212 para proporcionar autenticación del registro de servicios a partir del cual se calcularon los MAC, la red visitada 103, por ejemplo mediante el procesador de autenticación 119, registra, en la etapa 213, la MS 101 y almacena detalles del registro de servicios autenticado de la MS 101 en el registro de posiciones de visitantes 122. Finalmente, en la etapa 215, la red visitada 103 proporciona servicios de comunicación a la MS 101, de acuerdo con el registro de servicios autenticado. La comunicación entre la MS 101 y la red 103 tiene lugar entre el transceptor 104 y la estación base 113 (u otra estación base de la red visitada 103), mientras la MS 101 esté en la zona de la red visitada 103 y esté registrada con la red visitada 103.

Cuando la red visitada 103 calcula el MAC de autenticación en la etapa 211, puede ocurrir que la red visitada 103 sea incapaz de comprobar la correspondencia del MAC de autenticación calculado, con el MAC de certificado recibido desde la MS 101, tal como se indica en la etapa 217 que sigue la etapa 211. En respuesta a la etapa 217, la red visitada 103, por ejemplo mediante el procesador de autenticación 119, recupera de la memoria 120 en la etapa 219 una versión anterior de la clave MAC, es decir la versión recibida antes de la que se recibe en la etapa 209.

La versión anterior de la clave MAC recuperada en la etapa 219 puede ser la misma que la clave MAC utilizada por la red propia 102 en la etapa 201 para calcular el MAC proporcionado a la MS 101, y por la MS 101 a la red 103. En tal caso, pueden sucederse satisfactoriamente las etapas 212, 213 y 215.

Si después de la etapa 219 sigue sin obtenerse una correspondencia para el MAC de autenticación calculado, la etapa 219 puede repetirse una o varias veces utilizando otras claves MAC almacenadas incluso antes.

Si aún así la red visitada 103 sigue sin ser capaz de obtener una correspondencia para el MAC de autenticación calculado, tal como se indica en la etapa 221, puede considerarse que el registro de la MS 101 ha fallado, tal como se indica mediante la etapa 223.

Después de su solicitud de registro en la etapa 205, la MS 101 es capaz de obtener autenticación y registro mediante la red visitada 103 y servicios de comunicación de la red visitada 103, mediante la disposición de información en forma del registro de servicios certificado, de la MS 101 a la red visitada 103. Por lo tanto, la utilización del método 200 en el sistema 100 permite beneficiosamente la autenticación y el registro de la MS 101 por la red visitada 103, o cualquier otra MS con una red visitada, sin comunicación directa entre la red visitada, por ejemplo la red 103, y la red propia, por ejemplo la red 102, en el momento en que la MS 101 u otra MS solicita el registro.

Aunque la comunicación entre la red propia 102 y la red visitada 103 a través de la conexión 115 puede ser necesaria para algunos propósitos, el método 200 da a conocer una manera segura y fiable mediante la cual la red visitada 103 puede determinar qué servicios de comunicación debería proporcionar a la MS 101, y proporcionar dichos servicios a la MS 101 sin la necesidad inmediata de comunicación con la red propia 102. El método 200 puede ser particularmente útil, por ejemplo, si la conexión 115 entre las redes 102 y 103 no está disponible debido a un fallo o avería, o está congestionado debido a un volumen elevado de tráfico sobre la conexión 115.

Además, evitando la comunicación entre la red visitada 103 y la red propia 102 cuando la MS 101 envía una solicitud de registro a la red visitada 101, es posible proporcionar el registro más rápidamente (que cuando se utiliza dicha comunicación, tal como en la técnica anterior). Esto puede ser importante en una operación de emergencia en la que es esencial para la MS 101 obtener el registro y la provisión de servicios de comunicación lo antes posible.

Además, mediante evitar la comunicación entre la red visitada 103 y la red propia 102 cuando la MS 101 u otra MS envía una solicitud de registro, es posible reducir beneficiosamente el volumen de tráfico de control del sistema, enviado entre las dos redes.

El sistema 100 en el que se aplica el método 200 puede ser un sistema en el que es necesario controlar cuidadosamente los servicios de comunicación proporcionados a estaciones móviles, por ejemplo debido a que los usuarios operan en una organización en la que es necesario mantener la seguridad de las comunicaciones. La organización de los usuarios del sistema 100 puede ser, por ejemplo, la policía u otra organización pública de servicios de seguridad. El sistema 100 puede ser un sistema TETRA, un sistema APCO 25 u otro sistema diseñado para su utilización en dicho tipo de organización.

REIVINDICACIONES

1. Un método (200) de funcionamiento en un sistema de comunicación móvil (100), que incluye las etapas de:

una estación móvil (101) enviando (207) a una red visitada (103) un registro de servicios certificado, proporcionado por una red propia (102), de servicios de comunicación cuya prestación se permite para la estación móvil (101), estando acompañado del registro de servicios por, o incluyendo, un código de certificado aplicado por la red propia (102) mediante un procedimiento de cálculo aplicado a contenidos del registro de servicios utilizando una clave de autenticación;

la red visitada (103) calculando (211) un código de autenticación para el registro de servicios recibido desde la estación móvil (101) utilizando una clave de autenticación contenida por la red visitada (103);

la red visitada (103) autenticando (212) el registro de servicios recibido, mediante la determinación de que el código de autenticación calculado se corresponde con el código de certificado recibido desde la estación móvil (101); y

la red visitada (103) proporcionando (215) servicios de comunicación a la estación móvil (101) basándose en el registro de servicios autenticado.

2. Un método (200) acorde con la reivindicación 1, en el que:

la estación móvil (101) recupera (207) de su memoria (106) el registro de servicios certificado y envía el registro de servicios certificado en asociación con una solicitud de servicios de comunicación por parte de la red visitada (103).

3. Un método (200) acorde con la reivindicación 1 ó 2, en el que:

la red visitada (103) recupera (209) de su memoria (120) la clave de autenticación.

4. Un método (200) acorde con cualquiera de las reivindicaciones anteriores, que incluye:

la red visitada (103) obteniendo la clave de autenticación desde un terminal de emisión de claves (123); y

la red propia (102) obteniendo la misma clave desde el terminal de emisión de claves (123) para su utilización en el cálculo del código de certificado por la red propia (102).

5. Un método (200) acorde con la reivindicación 4, en el que:

el terminal de emisión de claves (123) está en la red propia (102).

6. Un método (200) acorde con cualquiera de las reivindicaciones anteriores 2 a 5, que incluye la red visitada (103) recibiendo (208) y almacenando el código de autenticación antes de la solicitud procedente de la estación base (101), y a continuación:

(i) recuperar (209) la clave de autenticación almacenada;

(ii) llevar a cabo el procedimiento de cálculo (211) para calcular el código de autenticación utilizando la clave recuperada y el mensaje de servicio recibido;

(iii) comparar (212) el código de autenticación calculado, con el código de certificado recibido desde la estación base (101) a efectos de autenticar el registro de servicios recibido desde la estación base (101); y

(iv) cuando el código de autenticación calculado y el código de certificado se corresponden proporcionando autenticación al registro de servicios recibido, proporcionar (215) servicios de comunicación a la estación móvil (101) de acuerdo con el registro de servicios autenticado; sin comunicar con la red propia (102) después de la solicitud procedente de la estación móvil (101).

7. Un método (200) acorde con la reivindicación 6, en el que:

cuando la red visitada (103) es incapaz de encontrar una correspondencia entre el código de certificado recibido desde la estación móvil (101) y el código de autenticación que ha calculado utilizando la última clave de autenticación almacenada por la red visitada (103), la red visitada (103) recupera (219) por lo menos una clave de autenticación almacenada recibida antes que la última clave; y lleva a cabo por lo menos un procedimiento de

autenticación (212) adicional utilizando dicha por lo menos una clave anterior recuperada, a efectos de encontrar un código de autenticación calculado que se corresponda con el código de certificado recibido desde la estación móvil (101).

8. Un método (200) acorde con cualquiera de las reivindicaciones anteriores, que incluye:

una red propia (102) que produce un código de certificado del registro de servicios, mediante llevar a cabo un procedimiento de cálculo utilizando la última clave de autenticación recibida y contenidos del registro de servicios;

añadir (202) el código de certificado utilizado en el cálculo del registro de servicios de la estación móvil (101) al registro de servicios, para producir un registro de servicios certificado; y

enviar (203) el registro de servicios certificado a la estación móvil (101) mediante comunicación inalámbrica; y

la estación móvil (101) almacena en una memoria (106) el registro de servicios certificado.

9. Un método (200) acorde con la reivindicación 8, en el que:

el código de certificado se produce a partir de datos que forman los contenidos completos del registro de servicios.

10. Un método (200) acorde con cualquiera de las reivindicaciones anteriores, en el que el registro de servicios de la estación móvil (101) incluye uno o varios de los siguientes:

(i) Un permiso de acceso al sistema, que indica que se permite a la estación móvil (101) o a su actual usuario autorizado, utilizar el sistema para comunicaciones móviles;

(ii) Capacidad de interconexión individual, que indica si se permite a la estación móvil (101) participar en llamadas interconectadas que tienen lugar dentro del sistema;

(iii) Capacidad semidúplex/dúplex, que indica si se permite a la estación móvil (101) participar en llamadas semidúplex o dúplex dentro del sistema;

(iv) Capacidad de cifrado, que indica si se permite a la estación móvil (101) transmitir o recibir comunicaciones inalámbricas cifradas, y el nivel o tipo de seguridad de cifrado a aplicar;

(v) Nivel de prioridad, que indica qué nivel de prioridad se permite para realizar o recibir llamadas por la estación móvil (101);

(vi) Capacidad de transferencia de datos, que indica la capacidad o caudal de datos que se permite enviar hacia o desde la estación móvil (101);

(vii) Autorización de redes, que indica la identidad de una o varias redes del sistema con las que se permite a la estación móvil (101) registrarse como red visitada (103);

(viii) Pertenencias a grupos, que indican la identidad del grupo o grupos de estaciones móviles, de los que la estación móvil (101) es miembro, y a los que le está permitido unirse cuando está establecida o estableciéndose una llamada entre el grupo.

11. Un método (200) acorde con cualquiera de las reivindicaciones anteriores, en el que el registro de servicios producido por la red propia (102) incluye uno o varios de los siguientes:

(i) un número de serie del registro de servicios de la estación móvil (101);

(ii) una fecha de emisión del registro de servicios de la estación móvil (101);

(iii) una identidad de la red propia (102) que emite el registro de servicios de la estación móvil (101).

12. Un método (200) acorde con cualquiera de las reivindicaciones anteriores, en el que el registro de servicios está cifrado.

13. Un estación móvil (101) operativa para:

recibir (203) desde una red que es su red propia (102), un registro de servicios certificado de servicios de comunicación que se permite proporcionar a la estación móvil (101), estando acompañado de, o incluyendo, un registro de servicios un código de certificado calculado por la red propia (102) utilizando un procedimiento de cálculo que utiliza una clave de autenticación y contenidos del registro de servicios;

almacenar el registro de servicios certificado en su memoria (106);

recuperar (207) de su memoria (106) el registro de servicios certificado y comunicar a una red visitada (103) el registro de servicios certificado incluyendo el código de certificado calculado; y

obtener servicios de comunicación desde la red visitada (103) en respuesta a que la red visitada (103) reciba el registro de servicios certificado y autentique el registro de servicios mediante calcular un código de autenticación utilizando el registro de servicios recibido y una clave de autenticación mantenida por la red visitada (103) y compruebe la correspondencia (212) del código de autenticación calculado, con el código de certificado enviado por la estación móvil (101), basándose los servicios de comunicación en el registro de servicios autenticado.

14. Un procesador (109) para utilizar como un procesador de autenticación en una red (100) de un sistema de comunicación móvil (100) que incluye asimismo una estación móvil (101), siendo la red una red propia (102) de la estación móvil (101), el procesador (109) siendo operativo para:

recibir (201) una clave de autenticación procedente de un terminal de emisión de claves (123);

producir (202) un registro de servicios para la estación móvil (101), el registro de servicios siendo de servicios de comunicación que se permite proporcionar a la estación móvil (101),

producir un código de certificado relativo al registro de servicios mediante llevar a cabo un procedimiento de cálculo aplicado al registro de servicios utilizando la clave de autenticación;

añadir el código de certificado al registro de servicios para formar un registro de servicios certificado; y

enviar (203) el registro de servicios certificado a la estación móvil (101) mediante comunicación inalámbrica desde una estación base (107) de la red propia (102) para su almacenamiento por la estación móvil (101).

15. Un procesador (119) para su utilización como procesador de autenticación en una red (100) de un sistema de comunicación móvil (100) que incluye asimismo una estación móvil (101), la red siendo una red (103) visitada por la estación móvil (101) cuando la estación móvil (101) no está siendo servida por su red propia (102), el procesador (119) siendo operativo para:

recibir (208) una clave de autenticación procedente de un terminal de emisión de claves (123);

recibir (207) desde la estación móvil (101) un registro de servicios certificado, proporcionado por una red propia (102) de la estación móvil (101), de servicios de comunicación que se permite proporcionar a la estación móvil (101), el registro de servicios estando acompañado de, o incluyendo, un código de certificado aplicado por la red propia (102), siendo el código de certificado un código producido mediante un procedimiento de cálculo que utiliza contenidos del registro de servicios y una clave de autenticación;

calcular (211) un código de autenticación para el registro de servicios recibido, mediante un procedimiento de cálculo que utiliza contenidos del registro de servicios recibido y la clave de autenticación recibida;

autenticar (212) el registro de servicios recibido mediante comprobar la correspondencia del código de certificado recibido con el código de autenticación calculado; y

proporcionar (215) servicios de comunicación a la estación móvil (101) en base al registro de servicios autenticado.

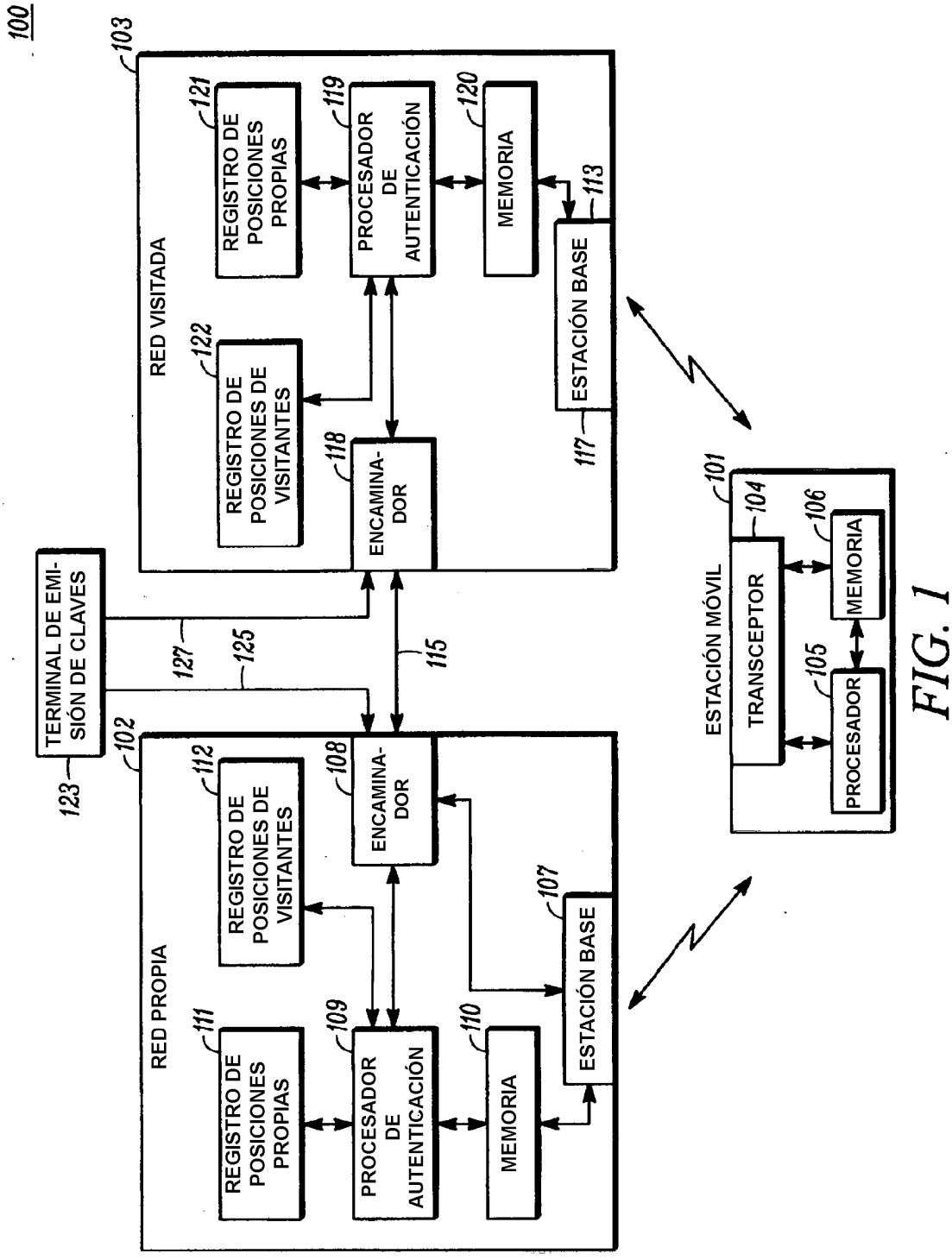
100
103
RED VISITADA
121
REGISTRO DE POSICIONES PROPIAS
119
PROCESADOR DE AUTENTICACIÓN
120
MEMORIA
113
ESTACIÓN BASE
122
REGISTRO DE POSICIONES DE VISITANTES
118
ENCAMINA-DOR
117
TERMINAL DE EMI-SIÓN DE CLAVES
123
127
125
115
102
RED PROPIA
112
REGISTRO DE POSICIONES DE VISITANTES
108
ENCAMINA-DOR
107
ESTACIÓN BASE
111
REGISTRO DE POSICIONES PROPIAS
109
PROCESADOR DE AUTENTICACIÓN
110
MEMORIA
101
ESTACIÓN MÓVIL
104
TRANSCEPTOR
106
MEMORIA
105
PROCESADOR

FIG. 1

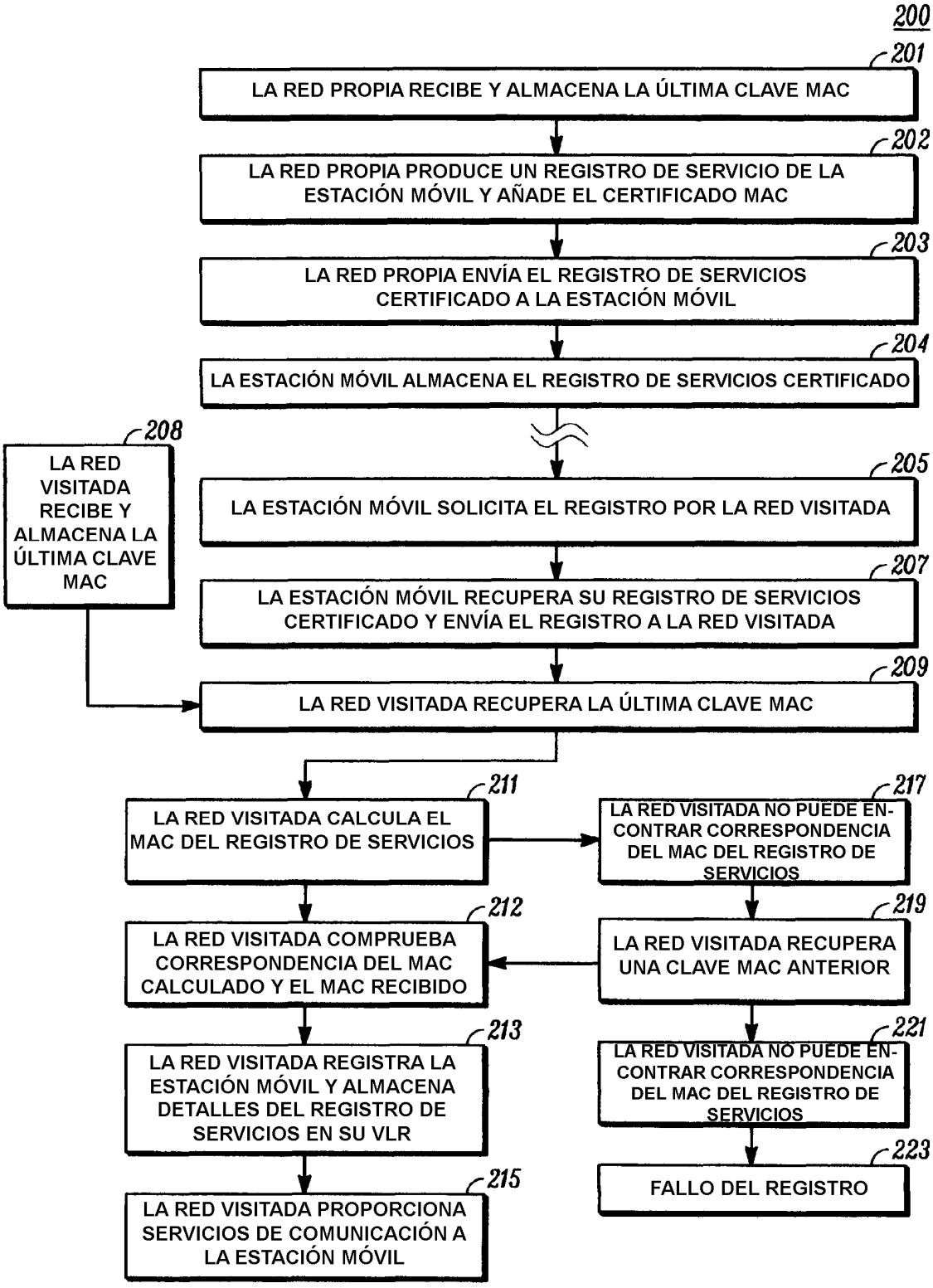
200
201
LA RED PROPIA RECIBE Y ALMACENA LA ÚLTIMA CLAVE MAC
202
LA RED PROPIA PRODUCE UN REGISTRO DE SERVICIO DE LA ESTACIÓN MÓVIL Y AÑADE EL CERTIFICADO MAC
203
LA RED PROPIA ENVÍA EL REGISTRO DE SERVICIOS CERTIFICADO A LA ESTACIÓN MÓVIL
204
LA ESTACIÓN MÓVIL ALMACENA EL REGISTRO DE SERVICIOS CERTIFICADO
208
LA RED VISITADA RECIBE Y ALMACENA LA ÚLTIMA CLAVE MAC
205
LA ESTACIÓN MÓVIL SOLICITA EL REGISTRO POR LA RED VISITADA
207
LA ESTACIÓN MÓVIL RECUPERA SU REGISTRO DE SERVICIOS CERTIFICADO Y ENVÍA EL REGISTRO A LA RED VISITADA
209
LA RED VISITADA RECUPERA LA ÚLTIMA CLAVE MAC
211
LA RED VISITADA CALCULA EL MAC DEL REGISTRO DE SERVICIOS
217
LA RED VISITADA NO PUEDE ENCONTRAR CORRESPONDENCIA DEL MAC DEL REGISTRO DE SERVICIOS
212
LA RED VISITADA COMPRUEBA CORRESPONDENCIA DEL MAC CALCULADO Y EL MAC RECIBIDO
219
LA RED VISITADA RECUPERA UNA CLAVE MAC ANTERIOR
213
LA RED VISITADA REGISTRA LA ESTACIÓN MÓVIL Y ALMACENA DETALLES DEL REGISTRO DE SERVICIOS EN SU VLR
221
LA RED VISITADA NO PUEDE ENCONTRAR CORRESPONDENCIA DEL MAC DEL REGISTRO DE SERVICIOS
223
FALLO DEL REGISTRO
215
LA RED VISITADA PROPORCIONA SERVICIOS DE COMUNICACIÓN A LA ESTACIÓN MÓVIL

FIG. 2