(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 950 147**

(51) Int. CI.:

H04W 48/04 (2009.01)
H04L 9/40 (2012.01)
H04W 12/126 (2011.01)
H04W 8/18 (2009.01)
H04W 48/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **25.06.2012 PCT/FR2012/051446**

(87) Fecha y número de publicación internacional: **03.01.2013 WO13001220**

(96) Fecha de presentación y número de la solicitud europea: **25.06.2012 E 12738524 (3)**

(97) Fecha y número de publicación de la concesión europea: **26.04.2023 EP 2735196**

(54) Título: **Método de inhibición de la comunicación de un equipo con una red**

(30) Prioridad:

27.06.2011 FR 1155689

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.10.2023

(73) Titular/es:

ORANGE (100.0%)
111, quai du Président Roosevelt
92130 Issy-les-Moulineaux, FR

(72) Inventor/es:

COUDOUX, AURÉLIE y
ALIX, CYRIL

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método de inhibición de la comunicación de un equipo con una red

Campo técnico

La invención hace referencia en general a las comunicaciones y más concretamente a las comunicaciones por radio entre un equipo y una red, en particular a un método de inhibición de una comunicación de un equipo con una red.

La invención se aplica más particularmente a un equipo móvil que se puede desplazar en una red celular

El equipo en cuestión es un equipo móvil equipado con recursos físicos y de software, que incluyen un módulo de identidad de abonado. Por módulo de identidad de abonado se entiende un módulo físico o de software de un abonado de la red que le permite comunicarse en esta red. Para ello, el módulo de identidad de abonado memoriza al menos un identificador que puede identificar de manera única al abonado. El módulo de identidad de abonado se ilustra en el siguiente ejemplo de forma de realización mediante una tarjeta de tipo SIM (del inglés *Subscriber Identification Module*) o USIM (del inglés *Universal Subscriber Identification Module*).

Técnica anterior

Una red móvil celular de comunicaciones por radio, en particular de acuerdo con la norma GSM (del inglés *Global System for Mobile communications),* utiliza tecnologías de radio para permitir que un equipo móvil de un abonado establezca una comunicación con otros equipos móviles conectados a la red. El enlace de radio entre el equipo y una red móvil debe ser de calidad suficiente, lo que requiere la instalación en la red de un conjunto de estaciones intermedias, denominadas estaciones de base, o BTS (del inglés *Base Transceiver Station*), en todo el territorio objetivo. De este modo, una célula es la superficie en la que el teléfono móvil puede establecer un enlace con una estación base determinada.

La movilidad de los abonados en una red móvil supone saber en qué célula se encuentra el abonado. Para ello, el equipo del abonado se identifica en la red por medio de un método de autentificación que también informa a la red de su localización. La red puede entonces aceptar o rechazar la comunicación. De este modo, la red puede restringir la comunicación de un equipo móvil a un conjunto de células. Una restricción de este tipo es necesaria cuando el abonado tiene, por ejemplo, derecho a comunicarse sólo en una zona geográfica limitada.

Sin embargo, sería deseable que el propio terminal pudiera restringir sus comunicaciones a un conjunto de células sin intervención de la red y, en particular, sin sobrecargarlo con engorrosos y a veces innecesarios métodos de localización y autentificación.

La red también puede, en caso extremo de pérdida o robo, por ejemplo, bloquear el equipo móvil. Este método se realiza bajo el control de un operador de red. No es simplemente reversible, en la medida de que el abonado cuyo equipo móvil ha sido bloqueado debe ponerse de nuevo en contacto con el operador para volver a utilizarlo. Sin embargo, sería deseable que, por ejemplo, si el abonado encontrara el equipo que había perdido, pudiera liberarse de la red y de su operador. La publicación WO00/18156 (Telia AB) de 30 de marzo de 2000 muestra un método en el que la información de posicionamiento se almacena en la tarjeta SIM. Esta información se compara con la información de posición actual del equipo para determinar si el usuario tiene derecho a comunicarse con la red en esa posición.

La invención ofrece una solución que no presenta las desventajas de la técnica anterior.

La invención

Para ello, de acuerdo con un aspecto funcional, la invención tiene por objetivo un método de inhibición de una comunicación de una red de comunicaciones con un equipo que tiene al menos un identificador de abonado que se puede transmitir a la red con el fin de verificar un derecho de comunicación en la red, caracterizado por que tiene las siguientes etapas:

Obtención de una primera información de posicionamiento relacionada con el equipo;

Obtención de una primera información denominada información de posicionamiento del equipo, representativa de su localización geográfica, de su localización temporal, o de la pertenencia a un grupo autorizado en esta red;

Comparación de la primera información de posicionamiento con al menos una segunda información de posicionamiento;

Modificación total o parcial de los identificadores de abonado que se deben emitir para la verificación, en función de los resultados de la comparación.

De este modo, la invención ofrece la ventaja de no imponer a la red la gestión de la inhibición del equipo, ya que es un identificador del propio equipo el que se modifica con el objetivo de prohibir su reconocimiento por la red, y por tanto el establecimiento de una comunicación. De este modo, la red se ve de forma ventajosa liberada de tareas que pueden resultar engorrosas e innecesarias. Si la identidad no es correcta, el abonado cuyo equipo está inhibido ya no puede establecer comunicación con otro abonado de la red móvil por medio de la red. La identidad comprobada puede ser la del abonado, o la de todo o parte del equipo.

En una forma de realización particular de la invención, la modificación es reversible.

De esta forma, esta inhibición es de forma ventajosa temporal. De este modo, de acuerdo con esta forma de realización, la comunicación se puede restablecer, por ejemplo, con referencia a la etapa de comparación, en cuanto vuelva a cumplirse una condición relativa a la información de posicionamiento. De este modo, el abonado se puede liberar del operador de su red para recuperar el uso de su equipo.

De acuerdo con una segunda forma de realización particular de la invención, un equipo tal como el descrito anteriormente es un terminal móvil equipado con un módulo de identidad de abonado en el que se ejecuta el método.

De este modo, de forma ventajosa, una utilización fraudulenta del módulo de identidad de abonado, por ejemplo, una tarjeta de tipo SIM (del inglés *Subscriber Identification Module*) o USIM (del inglés *Universal Subscriber Identification Module)*, no es posible de acuerdo con esta forma de realización de la invención. Es conocido, de acuerdo con la técnica anterior, el bloqueo del equipo en caso de robo. Sin embargo, un bloqueo de este tipo no impide en absoluto que el módulo de identidad de abonado sea robado y reinsertado con éxito en otro equipo. Por el contrario, en el contexto de la invención, dado que el método se realiza en el propio módulo de identidad de abonado, la inhibición sigue siendo efectiva, aunque el módulo de identidad de abonado se inserte en otro equipo. Además, la invención no bloquea el terminal móvil del usuario, que puede por lo tanto seguir jugando, escuchando música o utilizando su móvil para cualquier otra función independiente de la comunicación con la red móvil.

Además, de forma ventajosa, es posible utilizar los recursos de software y hardware del módulo de identidad de abonado para facilitar la implementación del método. En particular, en el contexto de la norma GSM, la recomendación 11.14 del ETSI propone un entorno de desarrollo denominado *SIM Application Toolkit* para definir aplicaciones en el módulo de identidad de abonado que puedan interactuar con el equipo y la red. La utilización juiciosa de este entorno permite desarrollar rápidamente el método de la invención y descargarlo fácilmente en cualquier módulo de identidad de abonado de acuerdo con la norma GSM.

De acuerdo con una variante de esta segunda forma de realización, el al menos un identificador de abonado de acuerdo con la invención es su número de identificación internacional.

Esta variante de aplicación de la invención permite una utilización juiciosa del número de identidad internacional del abonado móvil (en inglés IMSI de *International Mobile Subscriber Identity*) memorizado en el módulo de identidad de abonado, por ejemplo, la tarjeta SIM de acuerdo con la norma GSM. Este identificador, que se transmite a la red con vistas a la autentificación del equipo, se puede obtener fácilmente ya que está memorizado de manera permanente en la memoria del módulo de identidad de abonado. La modificación temporal del identificador es sencilla y transparente para la red y conlleva la desactivación del módulo de identidad de abonado y, por tanto, del equipo. Su restauración a partir de la memoria del módulo de identificación del abonado hace que el método sea reversible de forma muy sencilla.

De acuerdo con una segunda variante de esta segunda forma de realización, que se puede llevar a cabo de forma alternativa o acumulativa con la anterior, el al menos un identificador de abonado es el número de identificación temporal del abonado.

Esta variante de aplicación de la invención permite garantizar la inhibición del equipo en el caso de que el identificador temporal atribuido por la red al abonado (en inglés TMSI de *Temporary Mobile Subscriber Identity*) se utilice para sustituir al Identificador Internacional del Abonado (IMSI). Este método de sustitución es utilizado por la norma GSM para evitar la interceptación y una utilización fraudulenta del IMSI. Este identificador temporal también se memoriza en el módulo de identidad de abonado de acuerdo con la norma GSM. Su modificación cumple de forma ventajosa las mismas funciones que la modificación del IMSI comentada anteriormente.

De acuerdo con una tercera forma de realización particular de la invención, que se puede llevar a cabo de forma alternativa o acumulativa con las anteriores, un método tal como el descrito anteriormente se caracteriza además porque la primera información de posicionamiento es una localización geográfica.

Esta forma de realización de la invención permite inhibir de forma ventajosa el equipo en cuanto abandona una zona geográfica determinada. En un sistema celular, tal como el definido por ejemplo por la norma GSM, una información relativa a la localización del móvil está disponible a petición del equipo a su estación base (BTS). El método de la invención compara este identificador de localización con un conjunto de informaciones de localización, y puede decidir

o no, en función del resultado de la comparación, modificar un identificador de abonado con el objetivo de inhibir el equipo. En particular, si la célula a la que está conectado el equipo no se encuentra dentro de un conjunto de zonas geográficas, o células, autorizadas, se inhibirá hasta que regrese a una zona autorizada.

De acuerdo con otra forma de realización particular más de la invención, que se puede llevar a cabo de forma alternativa o acumulativa con las anteriores, un método tal como el descrito anteriormente se caracteriza además porque la primera información de posicionamiento es una localización temporal.

Esta forma de realización de la invención permite inhibir de forma ventajosa el equipo en cuanto sale de una determinada una franja horaria. El método de la invención compara la hora actual, que se puede recuperar fácilmente del equipo, con un conjunto de informaciones horarias, y puede decidir si, de acuerdo con el resultado de la comparación, modificar o no un identificador de abonado con el objetivo de inhibir el equipo. De este modo, si el equipo no se encuentra en una franja horaria permitida, por ejemplo, después de la hora de acostarse de un niño, se inhibirá hasta la siguiente franja horaria permitida.

De acuerdo con otra forma de realización particular más de la invención, que se puede llevar a cabo de forma alternativa o acumulativa con las anteriores, un método tal como el descrito anteriormente se caracteriza además porque la primera información de posicionamiento es una pertenencia a un grupo.

Esta forma de realización de la invención permite inhibir de forma ventajosa el equipo si no está autorizado por un operador. El método de la invención compara un identificador del terminal al que está acoplado, por ejemplo, su IMEI (*International Mobile Equipment Identity*), que permite identificar un terminal móvil de manera única, independientemente de un módulo de identificación del abonado SIM, con un conjunto de terminales autorizados por el operador. El método puede decidir o no, en función del resultado de la comparación, modificar un identificador de abonado, por ejemplo, IMSI o TMSI, para inhabilitar el equipo. De este modo, si el terminal en el que se ha insertado el módulo de identificación del abonado está prohibido por el operador, se inhibirá.

De acuerdo con otra forma de realización particular de la invención, que se puede llevar a cabo de forma alternativa o acumulativa con las anteriores, la segunda información de posicionamiento se memoriza en el módulo de identidad de abonado.

Esta forma de realización ofrece la ventaja de poder modificar fácilmente todas las posiciones, por ejemplo, localizaciones geográficas, autorizadas para el equipo. El protocolo SMS (del inglés Short Message Service) definido por la norma GSM en sus recomendaciones ETSI 3.40 y 3.48, permite en particular a las aplicaciones del módulo de identidad de abonado SIM dialogar con el terminal y la red utilizando el servicio de mensajes cortos. En el marco de la invención, es posible de este modo actualizar fácilmente en la tarjeta SIM, mediante el envío de un SMS al equipo, toda la información de posicionamiento autorizada, por ejemplo, una lista de estaciones base en cuyas células puede operar el equipo. De este modo, la etapa de comparación del método se puede realizar en la tarjeta SIM, sin tener que recurrir al terminal móvil o a la red.

De acuerdo con un aspecto material, la invención también hace referencia a un módulo de identificación del abonado que comprende medios para transmitir al menos un identificador de un abonado con el fin de verificar un derecho de un equipo a comunicarse en la red, caracterizado por que tiene:

- Medios para recibir del equipo una primera información denominada información de posicionamiento, representativa de su localización geográfica, de su localización temporal o de la pertenencia a un grupo autorizado en esta red;

- Medios para comparar la primera información de posicionamiento con al menos una segunda información de posicionamiento;

- Medios para modificar total o parcialmente los identificadores de abonado que deben emitir para la verificación, en función de los resultados de la comparación.

De acuerdo con otro aspecto material, la invención también hace referencia a un equipo que se puede comunicar con una red, caracterizado por que comprende un módulo tal como el definido anteriormente y por que comprende un terminal acoplado al módulo.

En uno de los ejemplos de formas de realización descritos a continuación, el terminal transmitirá al módulo de identificación del abonado la primera información de posicionamiento objetivo del método de la invención.

De acuerdo con otro aspecto material, la invención hace referencia a un programa informático que se puede llevar a cabo en el módulo de identidad de abonado tal como el descrito anteriormente, comprendiendo el programa instrucciones de código que, cuando el programa es ejecutado por un procesador, lleva a cabo las etapas del método descrito anteriormente.

La invención se comprenderá mejor con la lectura de la siguiente descripción, dada a modo de ejemplo y hecha con referencia a los dibujos adjuntos.

Las figuras:

La figura 1 muestra una red móvil celular de comunicaciones por radio de acuerdo con la técnica anterior.

La figura 2 muestra una arquitectura de un equipo equipado con un módulo de identidad de abonado, que puede llevar a cabo una forma de realización preferida de la invención.

La figura 3 muestra un método de identificación entre un equipo móvil y la red móvil de acuerdo con la técnica anterior.

La figura 4 muestra un método de identificación entre un teléfono móvil y la red de acuerdo con la forma de realización preferida de la invención.

Descripción detallada de un ejemplo de forma de realización que ilustra la invención

La figura 1 muestra un sistema que comprende una red móvil celular de comunicaciones por radio, por ejemplo, del tipo GSM, de acuerdo con la técnica anterior y un equipo (1).

Por supuesto, la invención no se limita a este tipo de redes y también es aplicable a las denominadas redes móviles de tercera generación, o a cualquier otro tipo de red de comunicaciones por radio.

En nuestro ejemplo, el equipo 1 es móvil. Suele estar compuesto por un módulo de identidad de abonado en forma de tarjeta SIM (del inglés *Subscriber Identification Module*), que permite identificar de forma única al usuario, y de un terminal móvil, es decir, el aparato del abonado. Como se describirá con más detalle con la ayuda de la figura 2, la tarjeta SIM contiene los datos del abonado, así como un procedimiento para autentificarlo a través de la red. De acuerdo con la norma GSM, un equipo sin módulo de identidad de abonado no puede, por tanto, comunicarse con la red, salvo para comunicaciones de emergencia.

Por supuesto, no hay ninguna limitación en cuanto al tipo de terminal utilizado, ni en cuanto a la definición de un equipo. El terminal móvil puede ser, por ejemplo, un teléfono móvil, una tableta, un contador eléctrico, etc. o cualquier otro medio de comunicación, fijo o móvil, que puede permitir la comunicación entre el equipo y la red móvil. En particular, el equipo se puede limitar a sólo el módulo de identificación del abonado (por ejemplo, una tarjeta SIM). El equipo también se puede limitar al terminal móvil y el módulo de identificación del abonado se puede reducir a un programa informático que se ejecuta en este terminal. En lo sucesivo, se entenderá por equipo el conjunto formado por el terminal, fijo o móvil, y su módulo de identidad de abonado.

Con el fin de establecer la comunicación con la red 5, el equipo móvil 1 se tiene que identificar ante los equipos de la red 4 y el operador de red en el curso de un procedimiento que se detallará más adelante con la ayuda de la figura 3.

En nuestro ejemplo, la comunicación entre el equipo 1 y una estación base 2 se realiza a través de un enlace de radio. Este enlace de radio entre el equipo y la estación base debe ser de calidad suficiente, lo que requiere la instalación de un conjunto de estaciones base, también denominadas BTS (del inglés *Base Transceiver Stations*), en todo el territorio objetivo. De este modo, en la figura 1, el terminal 1 se comunica con la estación base 2 que le es geográficamente más próxima. De forma más general, cualquier equipo móvil o fijo situado en las zonas A1, A2 o A3 se puede comunicar con la estación base 2. El conjunto de las zonas A1, A2 y A3 constituye la llamada célula de la estación base, identificada unívocamente por su identificador (BTS_ID). Sin embargo, los equipos situados en una de las zonas A4, A5 o A6 están demasiado lejos de la BTS 2 para poder comunicarse con ella.

El conjunto de estaciones base (2,3) de una red celular se conecta a los equipos de red de un operador de red (4). En particular, cada estación base está vinculada a un controlador de estaciones (BSC, del inglés *Base Station Controllet*), que a su vez está vinculado a un conjunto de dispositivos denominado subsistema de red (en inglés NSS de *Network Station Subsystem)*, encargado de gestionar las identidades de los usuarios, su localización y el establecimiento de la comunicación con otros abonados, y los vincula a la red 5. Esta red 5 puede ser una red telefónica pública y/o una red de Internet.

Describiremos a continuación, con la ayuda de la figura 2, la arquitectura del equipo 1 introducido en la figura 1, que puede llevan a cabo una comunicación de tipo GSM y una forma de realización de la invención. El equipo 1 está constituido clásicamente, de acuerdo con la norma GSM, por un teléfono móvil 20 equipado con un módulo de identidad de abonado 10, por ejemplo, una tarjeta SIM. La función de la tarjeta SIM 10 es almacenar información y procedimientos específicos del abonado que permiten al equipo autenticarse en la red. La tarjeta SIM 10 tiene tres tipos de memoria construidos alrededor de un procesador (CPU) 14. La ROM 11 (del inglés *Read Only Memory*) contiene, en particular, el sistema de explotación del módulo de identidad de abonado y los programas que llevan a cabo los mecanismos de seguridad, entre otros el algoritmo de autentificación A3 que se describirá más adelante con

la ayuda de la figura 3. La EEPROM 12 (del inglés *Electrically Erasable Programmable Read Only Memory*) contiene de manera permanente directorios y datos definidos por la norma GSM, en particular el IMSI (del inglés *International Mobile Subscriber Identity*) que es el número de identificación único del módulo de identidad de abonado y la clave de autentificación Ki, así como aplicaciones específicas (AP1, AP2) denominadas *applets.* Los applets son programas informáticos especificados por medio de la *SIM Application Toolkit* de acuerdo con la recomendación 11.14 del ETSI, que permiten controlar determinadas funciones del teléfono móvil, por ejemplo, hablar con el abonado por medio de la interfaz de comunicación 15 entre el módulo de identidad de abonado SIM 10 y el teléfono móvil 20, normalizada por el ETSI con el número 11.11. En la figura 2 se muestran dos applets: la AP1 es, por ejemplo, una aplicación de mensajes cortos (SMS del inglés *Short Message Service*) y la AP2, o applet de inhibición, lleva a cabo el método de acuerdo con esta forma de realización de la invención. La RAM 13 (del inglés Random Access Memory) permite, en particular, efectuar cálculos o cargar instrucciones de programa relativas, por ejemplo, a los applets AP1 y AP2 y para ejecutarlas bajo el control del procesador 14.

Con la ayuda de la figura 3, se describe ahora un procedimiento de identificación, más concretamente un procedimiento de autentificación, de acuerdo con la técnica anterior, entre un equipo móvil 1 y los equipos de red y del operador 4 presentado anteriormente con ayuda de la figura 1. En este ejemplo de forma de realización, se recuerda que el equipo 1 consta de un teléfono móvil 20 equipado con un módulo de identidad de abonado SIM 10. El módulo de identidad de abonado SIM, como se ha mencionado anteriormente, contiene tradicionalmente un identificador IMSI (*International Mobile Subscriber Identity*) y también, cuando el equipo está encendido, un identificador TMSI *(Temporary Mobile Subscriber Identity*) que, en particular, permite identificar temporalmente a un usuario durante las interacciones entre el equipo móvil y la red. Cuando el equipo disponga de un TMSI, el IMSI dejará de utilizarse, para evitar que se pueda escuchar en la interfaz de radio y se pueda utilizar con fines deshonestos.

Se supone que el equipo, al principio del algoritmo, busca ser identificado, o autenticado, por la red, por ejemplo, porque desea iniciar una comunicación.

El equipo transmite a la red, en una etapa E1, su identificador temporal TMSI o su identificador internacional IMSI. El equipo comienza transmitiendo el TMSI si dispone de él. Si la red no reconoce el TMSI, o si el equipo no tiene el TMSI, transmite su identificador IMSI. Al final de esta etapa, el equipo ha transmitido por lo tanto a la red o bien el IMSI o bien el TMSI. En lo sucesivo, se hará referencia de forma indiferente a cualquiera de estos identificadores con la denominación genérica MSI.

A continuación, se entra en una etapa E2 en la que la red determina la clave de autentificación Ki específica para cada abonado. Existen distintas variantes de cálculo de acuerdo con la naturaleza de la red y de la norma soportada, pero en todos los casos la clave Ki es calculada o recuperada por la red con la ayuda del identificador MSI (TMSI o IMSI), operación que se puede expresar en forma más compacta: Ki = f(MSI).

En la etapa posterior, anterior o simultánea a E3, la red genera un número aleatorio (RAND) que se transmite al equipo.

A su vez, el equipo extrae, en una etapa E4, la clave Ki que necesita para la autentificación. Esta clave se almacena en la EEPROM 12 del módulo de identidad de abonado SIM, según se describe en la figura 2.

A continuación, en dos etapas similares, denominadas respectivamente E5 en el lado de la red y E6 en el lado del equipo, se ejecuta el algoritmo denominado "A3" de la norma GSM. El algoritmo A3 suministra un número SRES (del inglés *Signed RESponse calculado por una tarjeta SIM*) a partir de las entradas RAND y Ki. La etapa E6 calcula un número SRES_sm para el móvil y la etapa E5 un número SRES_re para la red. El equipo 1 transmite el resultado SRES_sm a la red.

Finalmente, en una etapa E7, la red compara los dos números generados por el algoritmo A3, sRES_re y sRES_sm. Si son iguales, la autentificación del equipo se ha realizado correctamente y el equipo se puede comunicar con la red a partir de la etapa E8, es decir, por ejemplo, transmitir o recibir datos o voz hacia o desde otro equipo. En caso contrario, la autentificación del equipo ha fallado. Se puede iniciar una nueva fase de autentificación volviendo a la etapa E1 y describiendo de nuevo las etapas E1 a E7.

De este modo, para que la red pueda identificar al equipo de acuerdo con la técnica anterior, es evidente que necesita conocer el identificador MSI (TMSI o IMSI), con el fin de obtener la clave Ki y ejecutar correctamente el algoritmo A3, garantizando de este modo el éxito de la autentificación. De acuerdo con el estado de la técnica, si se roba el equipo (1), o simplemente su módulo de identidad de abonado (SIM, 10) con vistas a insertarlo en otro equipo, sigue siendo posible el establecimiento de una comunicación con la red, y por tanto una utilización fraudulenta del módulo de identidad de abonado. El principio de la forma de realización de la invención que se describirá a continuación es, por lo tanto, modificar, o corromper, los identificadores TMSI e IMSI con el fin de que la red no pueda restablecer la clave Ki y, por lo tanto, falle en su procedimiento de autentificación.

La figura 4 muestra un procedimiento de autentificación o identificación entre un equipo consistente en un terminal móvil 20 y un módulo de identificación del abonado 10, y los equipos de red 4 de acuerdo con una forma de realización de la invención. Dado que las principales etapas del procedimiento de autentificación descrito en la figura 3 con la

ayuda de las etapas E2 a E7 permanecen inalteradas, sólo se muestra en este caso una etapa E'1 para generar el identificador de abonado MSI o MSI' de acuerdo con esta forma de realización, prevista para sustituir a la etapa E1 del estado de la técnica de la figura 3 y desglosada en las subetapas E10 a E14. El principio básico consiste en corromper el MSI (IMSI o TMSI) que el equipo transmite a la red, con el fin de que éste no pueda encontrar la clave Ki correspondiente y, por tanto, falle la autentificación en caso de que el equipo móvil no se encuentre en una zona geográfica autorizada. El programa o *applet* inhibidor AP2 que se ejecuta en el módulo de identidad de abonado SIM 10, tal y como se describe con la ayuda de la figura 2, utiliza para ello herramientas especificadas por el *SIM Application Toolkit* de acuerdo con la Recomendación ETSI 11.14 de la norma GSM para comunicarse con el terminal móvil por medio de un conjunto de mensajes que tienen comandos y datos. Por ejemplo, el comando *PROFILE_DOWNLOAD* permite al terminal móvil informar al módulo de identidad de abonado sobre sus capacidades. En esta forma de realización, el módulo de identidad de abonado SIM es proactivo, es decir, puede iniciar intercambios con la red enviando comandos al terminal móvil, a diferencia de los módulos de identidad de abonado de primera generación, que sólo son pasivos.

En una etapa E10 inicial, que suele tener lugar al encender el equipo 1, el programa de inhibición (*applet*) AP2 es activado por el mensaje *PROFILE_DOWNLOAD* transmitido desde el terminal al módulo de identidad de abonado. En primer lugar, el applet restaura el identificador IMSI a partir de la EEPROM 13 del módulo de identidad de abonado SIM. En efecto, si el IMSI se ha corrompido durante una ejecución anterior del método de esta forma de realización de la invención, es importante restaurarla para garantizar el buen funcionamiento del equipo.

Después de esta etapa E10, el teléfono móvil envía periódicamente un comando *STATUS* al módulo de identidad de abonado SIM para informarse sobre su estado. En la etapa E11, el *applet* AP2 también se activa periódicamente por la recepción de este evento *STATUS.* El applet recupera una información de posicionamiento del móvil enviando un comando *PROVIDE_LOCAL_INFORMATION* al terminal móvil. A cambio, el terminal le transmite la información de localización P1 del equipo, que contiene, por ejemplo, la identificación del país, la red, la zona y la estación base (BTS) en la que se encuentra el equipo. El terminal puede o no haber interrogado a la red para disponer de esta información.

Cuando el applet AP2 ha recibido y memorizado esta información, lee en una etapa E12 la información de localización P2, que se almacena de acuerdo con esta forma de realización en la SIM, por ejemplo, en un archivo. Esta información P2 puede adoptar la forma de una lista de células autorizadas en una zona, red y país determinados. Se puede modificarse en cualquier momento, por ejemplo, mediante un mensaje de tipo SMS (del inglés *Short Message Service)* de la red. El protocolo SMS definido por la norma GSM en sus recomendaciones ETSI 3.40 y 3.48, permite en efecto a las aplicaciones del módulo de identidad de abonado dialogar con el equipo terminal y la red con la ayuda del servicio de mensajes cortos.

El *applet* efectúa en la etapa E13 una comparación entre la información de posicionamiento local P1 obtenida en la etapa E11 y esta información de posicionamiento autorizada P2 obtenida en la etapa E12. Si la etapa E13 tiene éxito, es decir, si se ha encontrado una correspondencia entre las dos informaciones de posicionamiento P1 y P2, entonces el equipo está autorizado en esa zona y el *applet* permite que el terminal móvil se autentique en la red transmitiendo su identificador MSI (IMSI o TMSI) de acuerdo con la técnica anterior descrita con la ayuda de la figura 3.

Si, por el contrario, no se ha encontrado ninguna coincidencia durante la comparación entre P1 y P2, el applet corrompe la información necesaria para esta autentificación (IMSI, TMSI) durante una etapa E14 que da lugar a la emisión de un identificador MSI' modificado. Una modificación de este tipo puede consistir, por ejemplo, en fijar el MSI en un valor predeterminado (MSI' = 0), o en cualquier operación sobre el identificador MSI (TMSI o IMSI) que dé lugar a un identificador MSI' modificado que sea una función del MSI de acuerdo con cualquier función f2 (MSI'=f2(MSI)). La red no puede recuperar la clave Ki a partir del identificador MSI' modificado, es decir, no puede realizar la operación Ki = f(MSI) en la etapa E2 de la figura 3 y no autentifica el equipo móvil, que por lo tanto no se puede comunicar.

En esta forma de realización, esta operación es reversible. En efecto, el usuario cuyo equipo ha sido inhibido puede posteriormente apagar y volver a encender el equipo móvil cuando se encuentre en una zona autorizada para realizar de nuevo las etapas E'1 a E7 y restablecer una comunicación.

Alternativamente, las informaciones de posicionamiento P1 y P2 pueden corresponder a informaciones horarias, por ejemplo, franjas horarias autorizadas. De este modo, por ejemplo, P2 podría contener las franjas horarias 10:00-12:00 y 18:00-20:00, permitiendo inhibir la comunicación si la información horaria actual P1 del equipo no pertenece a una de estas dos franjas horarias.

Huelga decir que la forma de realización descrita anteriormente se ha dado a título puramente indicativo y en modo alguno restrictivo, y que el experto en la técnica puede realizar fácilmente numerosas modificaciones sin salirse del ámbito de la invención.

Por ejemplo, de acuerdo con una variante, la etapa E'1 se puede completar con una subetapa adicional de modificación de un identificador que indica a qué operador de red (4) está permitido conectarse la estación. Por ejemplo, el identificador FPLMN (del inglés *Forbidden Public Land Mobile Network*) de la norma GSM indica a qué red no está permitido conectarse un equipo móvil. Una modificación de estos datos constituye una seguridad adicional con

respecto a la que consiste en modificar únicamente uno o varios identificadores de la tarjeta de identidad de abonado (IMSI, TMSI), como se ha explicado en la descripción anterior. Naturalmente, estos datos FPLMN se deberán restablecer después del encendido del equipo, de la misma manera que los demás identificadores (TMSI, IMSI) que se hayan podido modificar.

La modificación de los datos de identificación con el objetivo de inhibir un equipo también se puede producir cuando un usuario de un equipo intenta utilizar un módulo de identificación del abonado en un terminal móvil que no está autorizado por el operador (4). De acuerdo con una forma de realización de este tipo, el terminal móvil del equipo tiene un IMEI (del inglés *International Mobile Equipment Identity*) que permite identificarlo de manera única, independientemente de un módulo de identificación del abonado SIM. Si el IMEI del terminal no es reconocido por el operador de la red (4), es decir, si este terminal no está autorizado en esta red, la realización de la subetapa E14 de la etapa E'1 de la figura 4 permitirá modificar, o corromper, al menos uno de los identificadores (MSI', FPMLN) de manera que el terminal no pueda comunicar en la red de este operador.

REIVINDICACIONES

1. Método de inhibición de una comunicación de una red de comunicaciones (5) con un equipo (1) que tiene al menos un identificador de abonado (MSI) que se puede transmitir a la red con el fin de verificar un derecho de comunicación en la red, **caracterizado por que** tiene las etapas siguientes:
- Obtención (E11) de una primera información denominada información de posicionamiento (P1) del equipo (1), representativa de su localización geográfica, de su localización temporal, o de la pertenencia a un grupo autorizado en esta red;
- Comparación (E13) de la primera información de posicionamiento (P1) con al menos una segunda información de posicionamiento (P2);
- Modificación (E14) de todos o parte de los identificadores de abonado (MSI, MSI') que se deben emitir para la verificación, en función de los resultados de la comparación.

2. Método de inhibición de acuerdo con la reivindicación 1, **caracterizado por que** la modificación es reversible.

3. Método de inhibición de acuerdo con la reivindicación 1, **caracterizado por que** el equipo (1) es un terminal móvil (20) equipado con un módulo de identidad de abonado (SIM, 10) y **por que** dicho método se ejecuta en el módulo de identidad de abonado (SIM, 10).

4. Método de inhibición de acuerdo con la reivindicación 3 **caracterizado por que** el al menos un identificador de abonado (MSI) es el número internacional de identificación del abonado (IMSI).

5. Método de inhibición de acuerdo con la reivindicación 3 **caracterizado por que** el al menos un identificador de abonado (MSI) es el número de identificación temporal del abonado (TMSI).

6. Método de inhibición de acuerdo con la reivindicación 1, **caracterizado por que** dicha al menos una segunda información de posicionamiento (P2) se memoriza en el módulo de identidad de abonado (SIM, 10).

7. Método de inhibición de acuerdo con la reivindicación 1, **caracterizado por que** comprende la obtención de un conjunto de identificadores de terminales autorizados en dicha red de comunicación.

8. Módulo de identificación del abonado (SIM, 10) que comprende medios para transmitir al menos un identificador de un abonado (MSI) con el fin de verificar un derecho de un equipo a comunicarse en la red, **caracterizado por que** tiene:
- Medios (AP2) para recibir una primera información de posicionamiento (P1) del equipo, representativa de su localización geográfica, de su localización temporal o de su pertenencia a un grupo autorizado en esta red;
- Medios (AP2) para comparar la primera información de posicionamiento (P1) con al menos una segunda información de posicionamiento (P2);
- Medios (AP2) para modificar total o parcialmente los identificadores de abonado (MSI, MSI') que se deben emitir para la verificación, en función de los resultados de la comparación.

9. Equipo (1) que se puede comunicar con una red, **caracterizado por que** comprende un módulo de identificación del abonado (SIM, 10) tal como el definido en la reivindicación 8 y un terminal (20) acoplado al módulo.

10. Programa informático (AP2) que se puede llevar a cabo en el módulo de identidad de abonado (10) tal como se define en la reivindicación 8, comprendiendo el programa instrucciones de código que, cuando el programa es ejecutado por un procesador (CPU, 14), llevan a cabo las etapas del método (E'1, E10-E14) de la reivindicación 1.

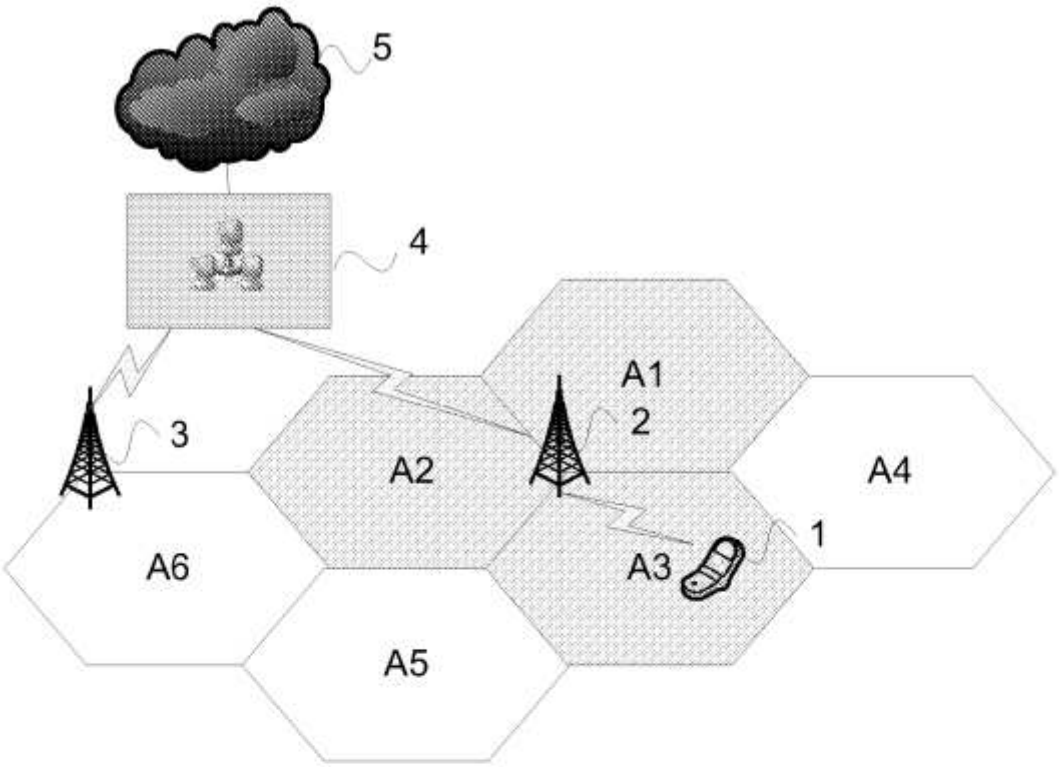

FIGURA 1

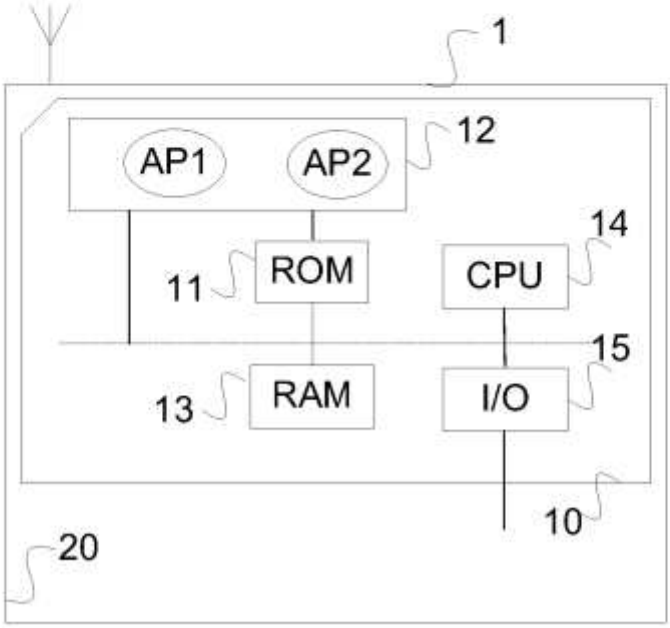

FIGURA 2

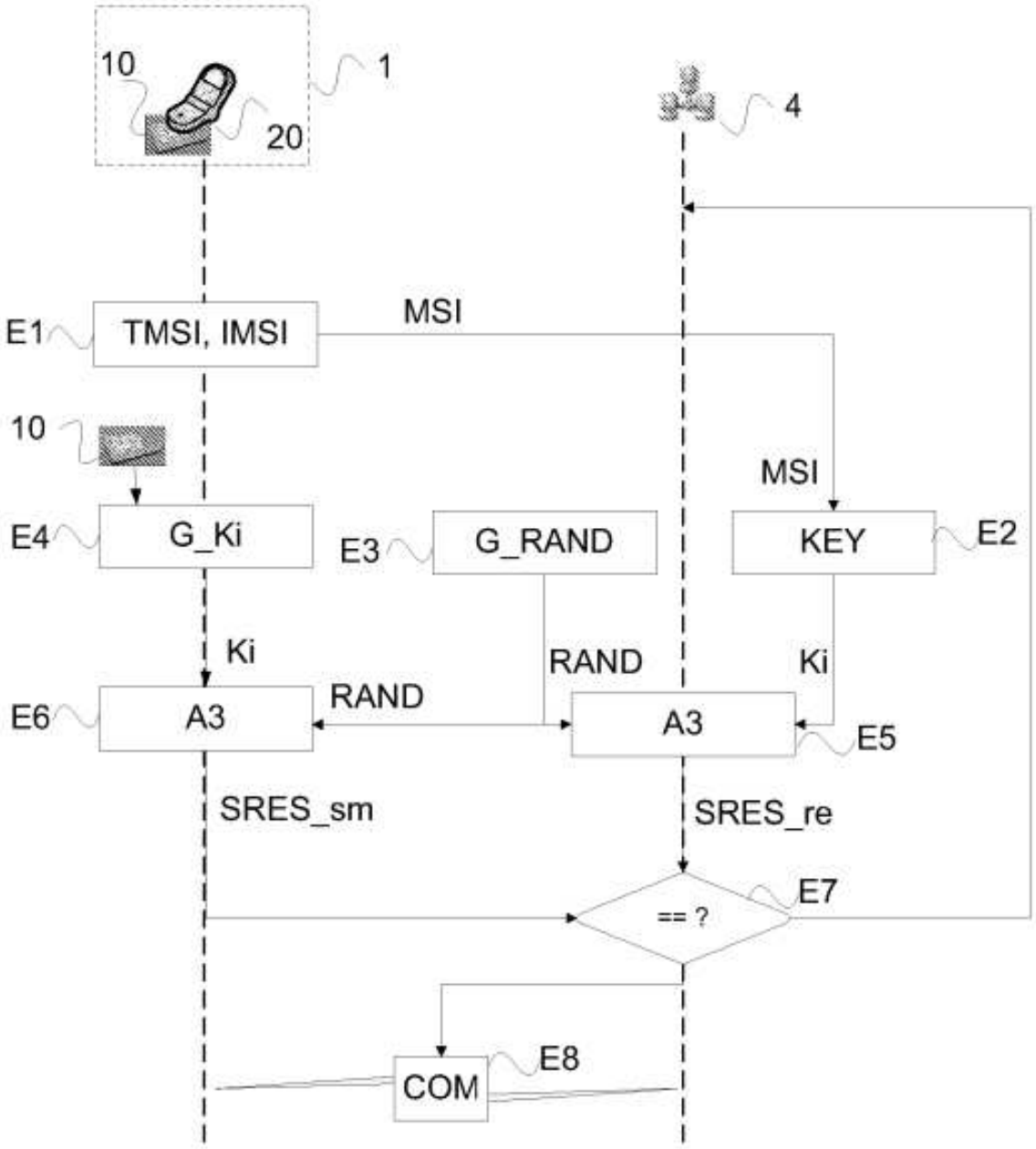
10
1
20
4
E1
TMSI, IMSI
MSI
10
MSI
E4
G_Ki
E3
G_RAND
KEY
E2
Ki
RAND
Ki
E6
A3
RAND
A3
E5
SRES_sm
SRES_re
E7
== ?
E8
COM

FIGURA 3

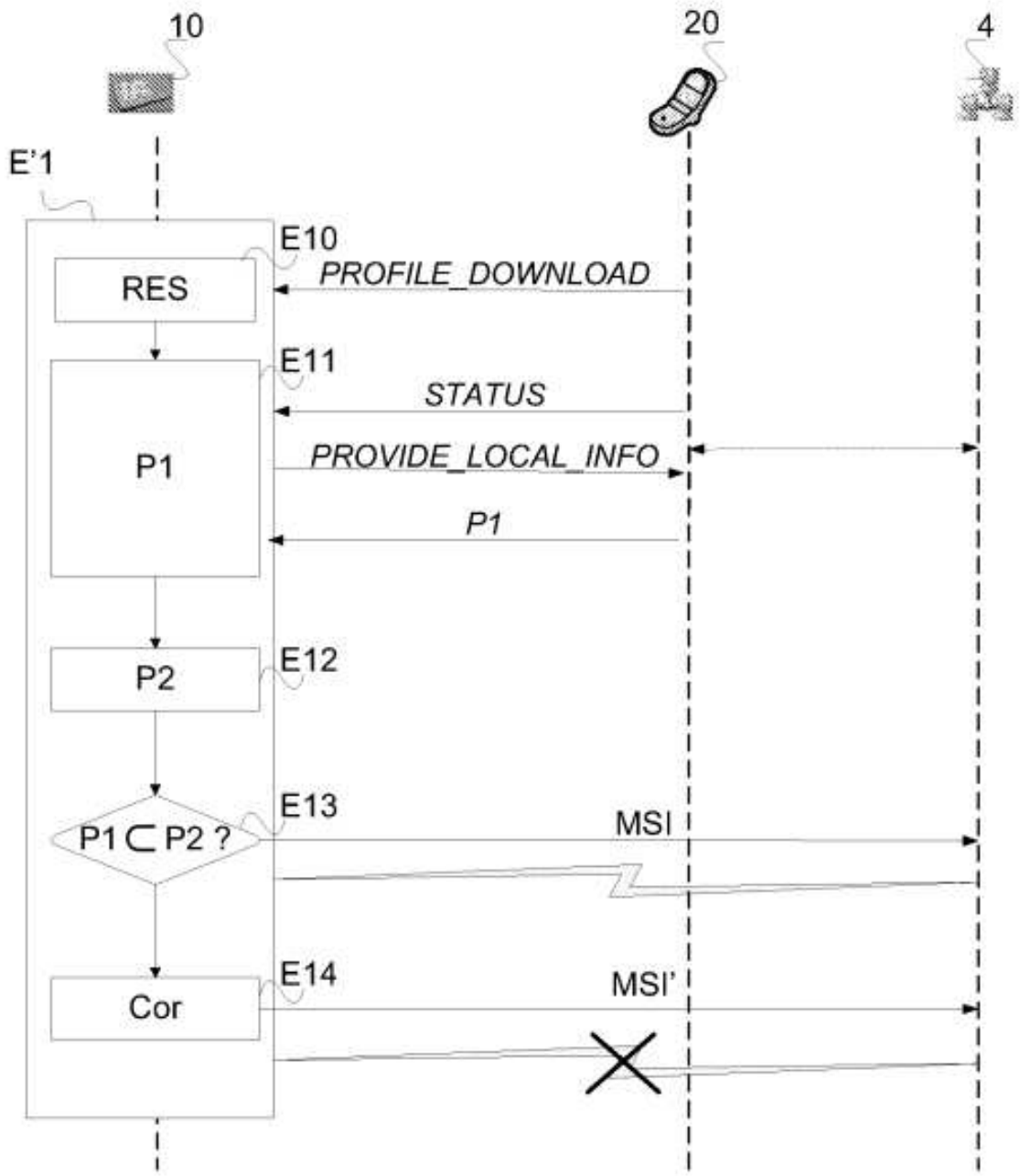
10
20
4
E'1
E10
RES
PROFILE_DOWNLOAD
E11
STATUS
P1
PROVIDE_LOCAL_INFO
P1
P2
E12
E13
P1 ⊂ P2 ?
MSI
E14
Cor
MSI'

FIGURA 4