(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 372 640**

(51) Int. CI.:
H04W 12/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08002827 .7**
(96) Fecha de presentación: **19.05.2006**
(97) Número de publicación de la solicitud: **1924117**
(97) Fecha de publicación de la solicitud: **21.05.2008**

(54) Título: **PROCEDIMIENTO Y SIMULADOR PARA EJECUTAR ACCESOS DE REGISTRO Y MANIPULACIÓN A UN TERMINAL MÓVIL.**

(30) Prioridad:
23.08.2005 DE 102005040002

(45) Fecha de publicación de la mención BOPI:
25.01.2012

(45) Fecha de la publicación del folleto de la patente:
25.01.2012

(73) Titular/es:
THALES DEFENCE DEUTSCHLAND GMBH
OSTENDSTRASSE 3
75117 PFORZHEIM, DE

(72) Inventor/es:
Kouadjo, Larisse Nana y
Gunzelmann, Georg

(74) Agente: **Carpintero López, Mario**

DESCRIPCIÓN

Procedimiento y simulador para ejecutar accesos de registro y manipulación a un terminal móvil

La presente invención se refiere a un procedimiento para ejecutar accesos de registro y manipulación a un terminal móvil en una red de telefonía móvil celular digital, en la que los datos se transmiten de acuerdo con un primer protocolo, mediante un simulador que está físicamente próximo al terminal. El terminal se identifica al obtenerse los parámetros de identificación del terminal. Toda la identificación se hace en el entorno de la red de telefonía móvil celular digital en la que los datos se transmiten de acuerdo con un primer protocolo.

La invención se refiere también a un simulador para ejecutar accesos de registro y manipulación a un terminal móvil que envía y recibe datos en una red de telefonía móvil celular digital de acuerdo con un primer protocolo. El simulador está dispuesto físicamente próximo al terminal móvil. El simulador presenta un sistema de medida para obtener los parámetros relevantes para la transmisión de datos de las estaciones base de la red de telefonía móvil físicamente próximas al simulador en el entorno del primer protocolo. Además el simulador presenta medios para hacer funcionar el simulador como una nueva estación base de la red de telefonía móvil en el entorno del primer protocolo teniendo en cuenta los parámetros obtenidos. Finalmente el simulador presenta medios para identificar el terminal en el marco del primer protocolo.

En las fuerzas del orden recae entre otras tareas, las de aclarar crímenes ya cometidos o prevenir los crímenes todavía no cometidos. Un aspecto importante a la hora de cumplir estas tareas es la posibilidad en casos excepcionales de poder identificar a una persona sospechosa en base a un teléfono móvil que utilice y poder escuchar, grabar y evaluar sus conversaciones telefónicas a través del teléfono móvil. Las fuerzas del orden gozan de la potestad para ello en base a una normativa legal y reglamentos relevantes. El objetivo es registrar las trazas de la comunicación de una persona sospechosa y evaluarlas para poder identificar así a la persona sospechosa o el teléfono móvil que utilice y para poder grabar y evaluar las conversaciones que se llevan a cabo.

Del estado de la técnica se conocen varias redes móviles para la transmisión de datos. Las redes de telefonía móvil GSM (Global System for Mobile communications) están ampliamente extendidas en lo que se refiere a la cobertura de red y también al número de terminales móviles existentes en uso. Desde hace unos años se puede tener acceso a las redes de telefonía móvil UMTS (Universal Mobile Telecommunications System) que están cada vez más extendidas. Estos dos estándares se diferencian, por ejemplo, en relación con la autentificación, la protección de la integridad y la encriptación. Mientras que en GSM sólo el terminal móvil se tiene que autentificar ante una estación base en el caso de UMTS también hay que hacer una autentificación de la estación base ante el terminal móvil. En el marco de la protección de la integridad en el caso de UMTS se protegen contra la falsificación los datos de control que hay que enviar a través de la red de telefonía móvil, por ejemplo, mediante firma. Para la encriptación de los datos que hay que enviar a través de la red de telefonía móvil se emplean en el caso de UMTS procedimientos de encriptación especiales como, por ejemplo, el procedimiento Kazumi. La encriptación en UMTS se refiere tanto a los datos útiles como a los datos de control. Mientras que en las redes de telefonía móvil GSM para transmitir datos se emplea una combinación de un procedimiento de multiplexación de frecuencia (FDMA - Frequency Divisional Multiple Access) y un procedimiento de multiplexación de tiempo (TDMA - Time Divisional Multiple Access) en la red de telefonía móvil UMTS se usa un procedimiento de multiplexación de códigos (Code Divisional Multiple Access) en el que los datos (señales) de varias fuentes o emisores se transmiten simultáneamente a la misma frecuencia. Se asigna a los datos ciertos patrones de código (llamados códigos de mezclado, “scrambling codes”).

Además se conoce, por ejemplo, por el documento DE 19920222 A1 un procedimiento para identificar y pinchar un terminal móvil en una red GSM de telefonía móvil celular digital. En base a la diferencia, reseñada antes a modo de ejemplo y no completamente, entre la red de telefonía móvil GSM y una red de telefonía móvil en la que los datos se transmitan según un procedimiento de multiplexación de códigos como, por ejemplo, una red de telefonía móvil UMTS no se pueden llevar los procedimientos conocidos para redes GSM a redes UMTS de telefonía móvil de forma sencilla.

Por la especificación técnica ETSI ·3GPP TS 33108 Versión 6.8.2, 6ª entrega, de enero de 2005, quedan definidos en términos generales los requisitos técnicos de una red de telefonía móvil UMTS para la llamada interceptación legal. La interceptación legal es la expresión técnica de una prestación que tienen que ofrecer todos los sistemas tecnológicos de las redes de comunicación públicas. La interceptación legal se refiere a la posibilidad que tienen que poder tener las autoridades públicas competentes de pinchar opcionalmente conexiones de comunicaciones determinadas y escuchar el tráfico de la comunicación que se da en ellas. Así tienen que diseñarse, por ejemplo, los puntos de acceso de las redes de telefonía móvil de tal manera que permitan esto. Esta especificación técnica se refiere por tanto a los diseños especiales de la estación base (Base Station, NodeB), al sistema de control de la red de telefonía móvil (Radio Network Controller RNC) y a la red troncal (Core Net) pero no a la interfaz de aire de una red de comunicaciones UMTS. Si no se cumplieran los requisitos que se describen en la especificación en una red de telefonía móvil UMTS, ya de antemano, quedaría excluida la escucha de terminales móviles en la zona del NodeB, RNC y Corenet por no darse los requisitos técnicos.

En el documento WO 2005/011318 A1 con el objetivo de la escucha de un terminal móvil queda descrito cómo un simulador instalado en una celda de radio GSM, que se hace funcionar como una estación base virtual, puede

aceptar sólo el registro del terminal móvil a escuchar y rechazar el registro de otros terminales móviles. El objetivo de esto es disminuir la carga de la estación base virtual debida a otros terminales durante la escucha del terminal a pinchar. Para este fin la estación base virtual puede emitir señales de rechazo a los terminales móviles que intenten registrarse en la estación base virtual.

El documento WO 02/01902 A1 describe el principio del traspaso forzado entre sistemas ("forced inter-system handover") en el que se fuerza un traspaso entre dos redes diferentes de la red troncal, en particular, si la potencia de la señal en la primera red es más débil que en la segunda red.

El objetivo de la presente invención es crear la posibilidad de la forma más sencilla posible de acceder con fines de registro o manipulación a un teléfono móvil de una red de telefonía móvil en la que los datos se transmiten de acuerdo con un procedimiento de multiplexación de códigos, en particular, en una red de telefonía móvil UMTS, en particular rastrear la posición del teléfono móvil o localizarla y/o escuchar las conversaciones que se lleven a cabo a través del teléfono móvil.

Para la solución de este objetivo se propone, partiendo del procedimiento del tipo mencionado al principio, que tras la identificación del terminal móvil, para ejecutar el acceso de registro o manipulación se desvíe el terminal móvil a una red de telefonía móvil en la que los datos se transmiten según un segundo protocolo.

De acuerdo con la invención se propone entonces que la identificación del teléfono móvil en el entorno del primer protocolo, en particular, en un entorno UMTS. Esto resulta necesario ya que en cuanto a la autentificación, la protección de la integridad y la encriptación hay que considerar los mecanismos de seguridad específicos que dificultan claramente la identificación de los terminales móviles registrados en las estaciones base de la red UMTS. Para identificar el terminal móvil se emplea entonces un procedimiento ajustado especialmente al entorno UMTS. Tras haber hecho la identificación se puede desviar el terminal móvil a una red de telefonía móvil alternativa, por ejemplo, una red GSM. Esto tiene la ventaja de que se pueden ejecutar los accesos de registro o manipulación al teléfono móvil mediante procedimientos y dispositivos que se conocen per se. Esto tiene la ventaja de que, para la escucha de teléfonos móviles de nueva generación que, por ejemplo, funcionan en el entorno UMTS, se pueden seguir usando los aparatos que se emplean en la actualidad en las redes de telefonía móvil más antiguas, por ejemplo, en el entorno GSM, para la escucha, el rastreo o el posicionamiento del terminal móvil. No hace falta adquirir nuevos aparatos, no hace falta formar al personal otra vez etc. Los procedimientos y dispositivos correspondientes para la escucha de teléfonos móviles en un entorno GSM., se conocen por ejemplo por el documento DE 19920222 A1.

Un aspecto importante de la presente invención consiste por tanto en hacer la identificación de un terminal móvil en el entorno de un primer protocolo de transmisión de datos y desviar entonces el terminal identificado, para el acceso de registro o de manipulación de verdad, al entorno de un protocolo de transmisión de datos alternativo. Independientemente de las posibilidades legales de acceso descritas en la especificación técnica ETSI 3GPP TS 33108 Versión 6.8.2 6ª entrega, el procedimiento propuesto según la invención ofrece la posibilidad técnica de una interceptación legal en una interfaz Uu de aire.

Preferentemente se obtienen los parámetros relevantes para la transmisión de datos de las estaciones base de la red de telefonía móvil que estén físicamente próximas al simulador y se adoptan para la identificación del terminal. El simulador está físicamente próximo al terminal que hay que identificar, es decir, en la celda de radio en la que se ha registrado el terminal móvil o en una celda de radio vecina. Los parámetros obtenidos comprenden, en particular, los códigos de mezclado utilizados por la estación base dispuesta físicamente próxima al simulador y/o las potencias de emisión de las estaciones base. El código de mezclado es un patrón de códigos con el que se pueden codificar los diferentes emisores en el marco de un procedimiento de multiplexación de códigos para la transmisión de datos. Entonces se hace funcionar el simulador como una nueva estación con otro código de área local diferente al de la estación base original en la que el terminal a identificar se ha registrado originalmente o con el mismo código de área local. Para este fin el simulador dispone de medios adecuados, por ejemplo, una estación base que hace posible el funcionamiento del simulador como una estación base de la red de telefonía móvil, utilizando el primer protocolo.

Además el simulador envía información del sistema que si bien está en la misma banda de frecuencia de la estación base original preferentemente la envía con una potencia de emisión más alta que la de la estación base original. Al emitir otro código de área local (LAC) diferente se hace creer al terminal a identificar que entra en una nueva área a la que está asociado el otro código de área local. Así se obliga al terminal móvil a registrarse automáticamente en el simulador. Para este fin el terminal ejecuta la llamada actualización de localización ("localization update"). Puesto que el terminal se registra habitualmente en aquella estación base cuya señal se recibe más intensamente también se puede lograr un registro automático del terminal móvil si la estación base simulada del simulador envía el mismo código de área local aunque con una potencia de emisión más alta que la estación base de la red de telefonía móvil.

En base a los parámetros de identificación se puede hacer la identificación del teléfono móvil. Los parámetros de identificación comprenden, por ejemplo, un IMSI (International Mobile Subscriber Identity), un TMSI (Temporary Mobile Subscriber Identity), P-TMSI (Packet TMSI) y/o un TMEI (International Mobile Equipment Identity). Estos parámetros de identificación son suficientes para establecer una conexión del simulador al terminal identificado con

el fin de escuchar las conversaciones entrantes o salientes llevadas a cabo a través del terminal. Para este fin el simulador dispone de medios adecuados, por ejemplo, un terminal que permite que el simulador funcione como un terminal para el establecimiento de la conexión con el terminal identificado y para la monitorización de la conexión o de la conversación.

De acuerdo con una forma de realización preferida de la invención el sistema de medida está configurado como un terminal-monitor que puede ser parte del simulador. Como los terminales para la transmisión de datos de todas formas consiguen los parámetros relevantes para la transmisión de datos de las estaciones base de la red de telefonía móvil físicamente próximas al terminal se pueden emplear sin problema como sistemas de medida en el sentido de la invención.

El verdadero nombre y los datos personales del usuario del terminal los guarda el operador de la red de telefonía móvil y se le pueden pedir, por ejemplo en el marco de una solicitud de las autoridades. Sólo el proveedor tiene listas de referencias cruzadas que hacen posible la asociación del IMSI a un usuario respectivamente a un número de teléfono. El TMSI, como su nombre ya indica, es sólo de naturaleza transitoria y no permite una asociación unívoca a un usuario determinado o a un número de teléfono determinado. Por este motivo es importante que el IMSI esté disponible y no sólo el TMSI.

En caso de que el terminal a identificar durante el registro en el simulador sólo transmita el TMSI (Temporary Mobile Subscriber Identity) como parámetro de identificación se puede empezar con un procedimiento de autentificación. En caso de que el terminal móvil a identificar espere sin embargo un procedimiento de autentificación se propone de acuerdo con un perfeccionamiento ventajoso de la invención que a continuación del registro del terminal móvil en el simulador:

- se empiece con un procedimiento de autentificación
- que el terminal a identificar rechace el procedimiento de autentificación por erróneo
- que el simulador empiece de nuevo un procedimiento de identificación y mientras transcurre, que el simulador le pida al terminal a identificar el IMSI (International Mobile Subscriber Identity) y/o IMEI (International Mobile Equipment Identity)
- el simulador obtenga el IMSI y/o IMEI del terminal a identificar

De acuerdo con este perfeccionamiento se empieza por un procedimiento de autentificación. Puesto que, sin embargo, el simulador o la nueva base estación base como parte del simulador no se puede identificar (lo que en la red UMTS sin embargo sí es necesario) el terminal a identificar rechaza el procedimiento de autentificación por erróneo, por ejemplo por un fallo MAC. Ahora el simulador empieza un procedimiento de identificación por el que se le hace creer al terminal a identificar que la nueva estación base (que en verdad es parte del simulador) necesitaría para fines de identificación los parámetros de identificación (IMSI o IMEI) del terminal a identificar. A partir de ahí el terminal le pasa su IMSI o IMEI al simulador en base al que resulta posible una identificación unívoca del terminal.

Al terminal a identificar después del rechazo del intento de registro en la primera red de telefonía móvil (por ejemplo UMTS) se le fuerza al registro en una estación base de la red de telefonía móvil alternativa (por ejemplo GSM). Las conversaciones telefónicas que se lleven a cabo a través del terminal identificado y la celda de radio GSM se escuchan preferentemente gracias a procedimientos de escucha tradicionales para las redes de telefonía móvil GSM.

Por tanto, tras haber hecho la identificación del terminal se remite a éste a una red de telefonía móvil GSM tradicional. Esto puede hacerse, por ejemplo, mediante elementos (IE) de información definidos, por interferencias (jamming) de la conexión UMTS o de otra forma adecuada. Al interrumpir o al interferir en la conexión UMTS, por el protocolo que utiliza para la transmisión de datos en la red de telefonía móvil, al teléfono móvil se le hace establecer una conexión a través de una red de telefonía móvil alternativa, en particular una red GSM. Esto sucede, por ejemplo, en el marco de un procedimiento llamado de reselección de celda (“Cell Reselection”).

Tras haber establecido la conexión a la red GSM se desarrolla toda la conversación a través del teléfono móvil de la forma habitual de acuerdo con el estándar GSM. Para la escucha de las conversaciones se pueden emplear procedimientos tradicionales como por ejemplo los que se conocen por el documento DE 19920222 A1. En cuanto a los procedimientos conocidos para la escucha de un terminal en una red GSM se remite expresamente a este documento.

Se propone en particular que tras la identificación del terminal móvil:

- mediante un terminal-monitor se pasen los parámetros obtenidos de identidad y las capacidades de seguridad del terminal móvil identificado a una estación base real de la red de telefonía móvil
- la estación base real le devuelva al terminal-monitor RAND (una cantidad aleatoria) y AUTN (token de autentificación)
- el simulador interrumpa la conexión con la estación base real de la red de telefonía móvil
- se haga funcionar el simulador como otra estación base de otra celda de radio de una red de telefonía móvil GSM y se establezca una conexión con el terminal móvil
- se empiece un procedimiento de autentificación entre el terminal identificado y el simulador y

- en caso de que el procedimiento de autentificación se concluya con éxito que el simulador haga que el terminal identificado no utilice encriptación en la subsiguiente transmisión de datos

Después de la interrupción de la conexión con la estación base real de la red de telefonía móvil el simulador establece la otra conexión con el terminal identificado a través de una estación base de una celda de radio GSM (Global System for Mobile Communication).

El terminal-monitor es preferentemente parte del simulador. Los conjuntos de números RAND y AUTN, que el simulador recibe de una estación base real de una red de telefonía móvil, son parámetros que hacen falta en una red UMTS para que una estación base se autentifique ante un terminal. Por tanto, el terminal-monitor hace creer a la estación base real su deseo de conexión y por tanto hace que la estación base real le pase los números RAND y AUTN al simulador. Desde el punto de vista de la estación base real el simulador es un terminal real. Sólo teniendo los parámetros RAND y AUTN resulta posible establecer una comunicación de voz entre una estación base y un terminal a escuchar identificado.

El establecimiento de la conexión con el terminal a escuchar se hace entonces en base a una estación base GSM simulada de una celda de radio GSM de una red de telefonía móvil GSM. La estación base GSM simulada es preferentemente parte del simulador. Hecha la autentificación, la estación base GSM simulada envía los parámetros de seguridad al terminal a escuchar. Los parámetros de seguridad comprenden entre otros una orden al terminal de no emplear encriptación (el llamado parámetro de no encriptación, “No encryption”), es decir, de transmitir los datos no encriptados.

El concepto propuesto funciona con dos redes de telefonía móvil diferentes concretamente las redes UMTS y GSM. Por esta razón el terminal a escuchar tiene que ser un terminal de modo de radio múltiple (Multi Radio Mode) que soporte varias redes de telefonía móvil diferentes, a saber, redes UMTS y GSM. El concepto comprende una estación base GSM simulada, una estación base UMTS simulada y un terminal-monitor. Los tiempos de retardo entre el acceso al parámetro de autentificación y la supresión de la encriptación debería ser el mínimo para evitar que se generen por parte de la red UMTS real nuevos números RAND y AUTN antes de suprimir la encriptación. Los tiempos de retardo deberían estar en el intervalo de pocos segundos hasta, como mucho, minutos.

Como otra solución del objetivo de la presente invención, a partir del simulador para ejecutar accesos de registro o manipulación a un terminal móvil del tipo mencionado al principio se propone que:

- el simulador presente medios para desviar el terminal identificado en el entorno del primer protocolo a una red de telefonía móvil celular digital alternativa en la que los datos se transmitan de acuerdo con un segundo protocolo que difiera del primer protocolo
- el simulador presente medios (por ejemplo, un estación base simulada, una funcionalidad BSC y/o un computador de control y servicio) para hacer funcionar el simulador como una nueva estación base de la red de telefonía móvil alternativa en la que los datos se transmiten de acuerdo con un segundo protocolo y
- el simulador presente medios (por ejemplo, la estación base simulada, la funcionalidad BSC y/o el computador de operación y servicio) para ejecutar accesos de registro o manipulación al terminal móvil identificado en la red de telefonía móvil alternativa en la que los datos se transmiten de acuerdo con un segundo protocolo.

Ventajosamente, el sistema de medida comprende un terminal-monitor para la red de telefonía móvil celular digital en la que los datos se transmiten de acuerdo con un primer protocolo.

De acuerdo con un perfeccionamiento ventajoso de la invención se propone que los medios para desviar a otra red de telefonía móvil alternativa un terminal identificado en el entorno de un primer protocolo rechacen un intento de registro del terminal identificado en el simulador o que los medios interrumpan la conexión entre el terminal móvil y la nueva estación base y/o de otra forma interfieran en la conexión y que el simulador fuerce al terminal (en base al protocolo UMTS estandarizado) a que se registre automáticamente en otra estación base de otra celda de radio de la red de telefonía móvil alternativa en la que los datos se transmiten de acuerdo con un segundo protocolo.

A continuación, se detallará más un ejemplo de realización preferido de la invención en base a las figuras. Muestran:

la figura 1: un simulador según la invención para identificar un terminal móvil en una red de telefonía móvil celular digital de acuerdo con una forma de realización preferida

la figura 2: una representación de celdas de radio de una red de telefonía UMTS con diferentes códigos de área de localización

la figura 3: un diagrama de flujo de un procedimiento según la invención para identificar un terminal de acuerdo con una primera forma de realización

la figura 4: un diagrama de flujo de un procedimiento según la invención para identificar un terminal móvil de acuerdo con una segunda forma de realización

la figura 5: un diagrama de flujo de un procedimiento según la invención para la escucha de un terminal de acuerdo con una forma de realización preferida

En las fuerzas del orden recae entre otras la tarea de aclarar los crímenes ya cometidos o prevenir los crímenes aún no cometidos. Un aspecto importante en el cumplimiento de estas tareas es la posibilidad de poder identificar, en casos excepcionales bien fundados, a una persona sospechosa en base al teléfono móvil que utiliza y poder escuchar, grabar y evaluar las conversaciones telefónicas que lleva a cabo esa persona a través de su teléfono móvil.

Hay diferentes redes de telefonía móvil para la transmisión de datos. Las redes de telefonía móvil GSM (Global System for Mobile Communication) están muy extendidas, tanto en lo que se refiere a la cobertura de red como en lo que se refiere al número de terminales móviles existentes en uso. Desde hace unos años se encuentran disponibles las redes de telefonía móvil UMTS (Universal Mobile Telecommunication System) y cada vez están más extendidas. Estos dos estándares se diferencian, por ejemplo, en cuanto a la autentificación, la protección de la integridad y la encriptación. Otra diferencia consiste en que la red UMTS emplea el llamado procedimiento de acceso múltiple por división de códigos (CDMA) mientras que GSM se recurre a una combinación de acceso por múltiple por división de frecuencia y de acceso múltiple por división de tiempo (FDMA/TDMA). Debido a estas diferencias tan marcadas los procedimientos y dispositivos empleados en las redes GSM para la identificación y escucha de un terminal móvil no se pueden llevar a las redes UMTS.

La presente invención propone en primer lugar un procedimiento con el que se puedan identificar también los terminales móviles sobre el terreno en redes de telefonía móvil UMTS de personas sospechosas y eventualmente poder pincharlos.

En la figura 1 está marcado con el número de referencia 1, en su conjunto, un dispositivo para la ejecución del procedimiento según la invención, un dispositivo según la invención, llamado simulador UTRAN (UMTS Terrestrial Radio Access Network). El simulador comprende una estación 2 base simulada, que se denomina NodeB y un terminal-monitor 3 simulado que funciona según el estándar UMTS y que se designa como monitor-UE (UE: user equipment, equipo de usuario). Además el simulador 1 comprende una funcionalidad 4 RNC (Radio Network Controller, controlador de red de radio). Entre el nodeB 2 simulado y la funcionalidad 4 RNC hay una denominada interfaz-lub 5. Además está previsto un computador 10 de control y servicio que controla la secuencia del procedimiento según la invención.

El simulador 1 además comprende una estación 12 base GSM simulada que se denomina estación base (BS) y un terminal 13 GSM simulado que funciona de acuerdo con el estándar GSM. El terminal 3 UMTS simulado y el terminal 13 GSM simulado se pueden combinar en una única unidad. Es posible sin más que el terminal UMTS, habitualmente, de todas formas presente una funcionalidad GSM para poder garantizar una conexión de voz segura y fiable incluso en las zonas en las que no exista suficiente cobertura UMTS. Además el simulador 1 presenta una funcionalidad 14 BSC (Base Station Controller, controlador de estación base). Entre la BS 12 simulada y la funcionalidad 14 BSC está prevista una interfaz 15.

Además está previsto un sistema 11 de medida externo que mide los parámetros relevantes para UMTS de las estaciones base que rodean al simulador 1. Naturalmente el sistema 11 de medida puede estar integrado en el simulador 1. Como sistema 11 de medida se utiliza preferentemente el terminal-monitor 3 UMTS de modo que no sea necesario ya un sistema de medida adicional. El sistema 3 de medida respectivamente el sistema 11 de medida ofrece una visión global del entorno UMTS celular que luego se le pasa al simulador 1.

Para la realización del procedimiento el simulador 1 se coloca en el entorno de una red UMTS real que comprende una estación 6 base (nodeB) real y un terminal 7 (UE) real. Naturalmente el entorno UMTS puede comprender más estaciones base que la estación 6 base representada y más terminales que el terminal 7 representado. El terminal 7 es el terminal a identificar y eventualmente a pinchar y se llama también equipo de usuario objetivo. Un terminal UMTS arbitrario, de acuerdo con la terminología que se emplea en este documento, es un equipo 7 de usuario objetivo cuando se ha registrado, dando sus parámetros individuales, en el simulador 1 UTRAN (por ejemplo, IMSI y/o IMEI). Entre el terminal 7 real y el nodeB 2 simulado está prevista una interfaz 8 Uu de aire. Entre el terminal 3 simulado y el nodeB 6 real está previsto otra interfaz 9 de aire.

En la figura 2 está representada una red de telefonía móvil UMTS celular que comprende una multiplicidad de celdas 120- 128, 130-133 de radio. Varias de las celdas 120-128 de radio pertenecen a una primera área de localización, así llamada, estando asociadas a todas las celdas 120-128 de radio el mismo código de área de localización (LAC), por ejemplo LAC=1000. Otras celdas 130-133 de radio pertenecen a una segunda área de localización estando asociado el mismo código de área de localización, por ejemplo LAC=2000, a todas ellas y que es distinto del primer código de área de localización. Las estaciones base (NodeB) cubren una o varias de las celdas 120-128, 130-133 de radio. Las estaciones base no se representan en la figura 2 para una mejor visión global.

En la figura 3 está representado un diagrama de flujo del procedimiento según la invención para la identificación del terminal 7. El procedimiento empieza en un bloque 20. El simulador 1 se dispone físicamente próximo a un terminal 7 UMTS a identificar en la red UMTS (bloque 21). El simulador 1 UTRAN se hace funcionar en una celda 120-128,

130-133 de radio geográfica en cuya estación base está registrado el terminal 7 a identificar. Posiblemente el terminal 7 está registrado junto con otros terminales en la estación base. Con el sistema 3, 11 de medida, en un bloque 22, se miden, o se registran de otra manera, los parámetros relevantes para UMTS de las estaciones base que rodean al simulador 1 y se pasan al simulador 1. Estos parámetros comprenden, por ejemplo, los llamados códigos de mezclado (Scrambling Codes) de las celdas 120-128, 130-133 de radio, las potencias de emisión de las estaciones base, los parámetros de identidad de los nodeB e información del sistema.

En otro bloque 23 el simulador 1 UTRAN envía por su parte información del sistema en la misma banda de frecuencias que las estaciones base vecinas aunque a una potencia de emisión superior de modo que los terminales dispuestos físicamente próximos al simulador 1 (y por tanto el terminal 7 a identificar) reconocen al simulador 1 como nueva (simulada) estación base. Además el simulador 1 emite con otro código de área de localización, por ejemplo LAC=3000, para que los terminales dispuestos físicamente próximos al simulador 1 (y, por tanto, el terminal 7 a identificar) tengan la impresión de haberse movido espacialmente hacia una nueva zona con un nuevo código de área de localización, es decir, hacia una nueva área de localización. El código de área de localización de la estación 2 base simulada se elige de modo que no se esté usando por las estaciones 6 base comunes del entorno del simulador 1.

Así se inicia en estos terminales (y, por tanto en el terminal 7 a identificar) un procedimiento de actualización de localización, así llamado, en cuyo marco los terminales se registran, dando sus parámetros de identificación, en la estación 2 base simulada (bloque 24). Los parámetros de identificación comprenden, por ejemplo, un IMSI (International Mobile Subscriber Identity), un TMSI (Temporary Mobile Subscriber Identity) y/o un IMEI (International Mobile Equipment Identity). En base a estos parámetros de identificación se hace entonces, en un bloque 25, una identificación de terminal 7. En el bloque 26 se termina el procedimiento de identificación del terminal 7. La zona geográfica simulada con un nuevo LAC se designa en la figura 2 con el número de referencia 140.

El nombre verdadero y los datos personales del usuario del terminal 7 están en posesión del operador de la red de telefonía móvil y se le pueden pedir, por ejemplo, en el marco de una solicitud de las autoridades o por otras vías. Sólo para el proveedor están disponibles las listas de referencias cruzadas que hacen posible la asociación de un IMSI a un usuario o del IMSI a un número de teléfono. El TMSI es, como su nombre ya indica, de naturaleza transitoria y no permite una asociación unívoca un usuario determinado o a un número de teléfono determinado. Por esta razón es importante que esté disponible el IMSI o el IMEI y no sólo el TMSI.

En caso de que el terminal 7 a identificar a la hora de registrarse en el simulador 1, bloque 24, sólo transmita el TMSI (Temporary Mobile Subscriber Identity) como parámetro de identificación y espere un procedimiento de autentificación la invención se puede completar siguiendo con el diagrama de flujo de la figura 4 para que a continuación del registro del terminal 7 en el simulador 1 en un bloque 27 se empiece el procedimiento de autentificación. Sin embargo ya que el simulador 1 o la estación base 2 simulada como parte del simulador 1 no se puede identificar ante el terminal 7 (lo que sí es necesario en redes UMTS) a identificar, el terminal 7 rechaza en un bloque 28 el proceso de autentificación por erróneo, por ejemplo, por un error MAC. Por su parte, ahora el simulador 1 empieza, en un bloque 29, un procedimiento de identificación haciendo creer al terminal 7 a identificar que la estación 2 base simulada necesita, para fines de identificación, el IMSI del terminal 7 a identificar. Entonces el terminal 7 en un bloque 30 le pasa su IMSI al simulador 1 en base al que, en un bloque 25 resulta posible una identificación unívoca del terminal 7. En el bloque 26 el procedimiento termina.

Tras la identificación del terminal 7 objetivo de acuerdo con el procedimiento de la figura 3 y la figura 4 se pueden escuchar las conversaciones entrantes o salientes realizadas a través del terminal 7 de distintas maneras. De acuerdo con una primera forma de realización cuyo diagrama de flujo se representa en la figura 5, el procedimiento de escucha del terminal 7 empieza en un bloque 40. En el bloque 41 se hace la identificación del terminal 7. El bloque 41 comprende, por tanto, todos los pasos de procedimiento 20-26 de la figura 3 o 20-30 de la figura 4. A continuación en un bloque 42 se rechaza el procedimiento de actualización de localización del terminal 7 por parte del simulador 1 o de la estación 2 base simulada.

A partir de ahí el terminal 7 se registra, en un bloque 43, de acuerdo con el procedimiento llamado de reselección de celda (“Cell reselection”) a través de la estación 12 base GSM simulada de una celda de radio de una red GSM. Los terminales UMTS, de acuerdo con el estándar, tienen que poder funcionar también en la red GSM. El desvío del terminal 7 objetivo de la red UMTS a la red GSM puede hacerse de una forma arbitraria. Así se puede hacer el desvío, por ejemplo, mediante un comando (una información fijada) que se emita por el llamado BCCH (broadcast control channel, canal de control de difusión).

Alternativamente el desvío se puede hacer también a través de un aviso arbitrario que se pueda emitir por el llamado FACH (Forward Access Channel, canal de acceso de envío de enlace descendente) o por el DCCH (Dedicated Control Channel, canal de control dedicado). Los terminales UMTS que se encuentran en la celda 140 del simulador 1 UTRAN obtienen este comando (esta información) y se registran en una red GSM que haya. También es concebible perturbar la conexión con una red UMTS, por ejemplo, mediante interferencias (“jamming”) y en último extremo terminar la conexión.

Todas las conversaciones entrantes o salientes que se hacen a través del terminal 7 objetivo ya no se hacen a

través de la red UMTS sino a través de la red GSM. Más exactamente las conversaciones se conducen a través de la estación 12 base GSM simulada, el terminal 13 GSM simulado continuando hasta una estación 16 base GSM real. En un bloque 44 se pueden escuchar entonces las conversaciones llevadas a cabo a través del terminal 7 objetivo en el entorno de la red GSM mediante procedimientos tradicionales como los conocidos, por ejemplo, por el documento DE 19920222 A1. Después, en un bloque 45, se termina el procedimiento.

Los accesos de registro o manipulación al terminal 7 móvil pueden comprender también una transmisión de la información relativa al terminal 7 al simulador 1. En el marco de la transmisión de información se pueden pasar, por ejemplo, las informaciones relativas a la posición actual del terminal. Esto permite una localización particularmente precisa del terminal móvil, en particular, en el entorno urbano y/o en edificios. Alternativamente o adicionalmente se pueden pasar también valores de la intensidad de campo con la que el terminal recibe las señales de la estación base visible de la red de telefonía móvil. También resulta concebible que el terminal 7 disponga de un sistema de localización de la posición vía satélite que pueda obtener información de la posición actual del terminal 7. Esta información de posición se puede transmitir también al simulador 1.

También es posible de acuerdo con la presente invención, escuchar las conversaciones telefónicas llevadas a cabo a través del terminal 7 objetivo mediante el llamado proceso cuasitransparente. Para ello es necesario que el simulador 1 en primer lugar consiga la información de seguridad de la estación 6 base UMTS real y con esta información establezca una conexión de la estación 12 base GSM simulada al terminal 7. También tiene que establecer, gracias a los parámetros de identificación obtenidos antes en el marco de la identificación del terminal 7, una conexión del terminal 13 GSM a la estación 16 base GSM real. Las comunicaciones de voz desde o hacia el terminal 7 objetivo ahora no se pasan directamente a la estación 6, 16 base real sino sólo indirectamente a través del simulador 1 UTRAN. En el simulador 1 se pueden grabar las conversaciones escuchadas al completo o parcialmente, por ejemplo, para una evaluación posterior o un aseguramiento de una prueba. Además las conversaciones se realizan a la fuerza a través de la red GSM y no a través de la red UMTS incluso aunque hubiera cobertura de red UMTS suficiente.

REIVINDICACIONES

1. Procedimiento para ejecutar accesos de registro o manipulación a un terminal (7) móvil en una red de telefonía móvil celular digital en la que los datos se transmiten según un primer protocolo mediante un simulador (1) que está dispuesto físicamente próximo al terminal (7)

- identificándose el terminal (7) al obtener los parámetros de identificación (7) del terminal y
- haciéndose la identificación completa en el entorno de la red de telefonía móvil celular digital en la que los datos se transmiten de acuerdo con un primer protocolo

caracterizado por que tras la identificación del terminal (7) móvil para la ejecución del acceso de registro o manipulación se desvía el terminal (7) móvil hacia otra red de telefonía móvil en la que los datos se transmiten según un segundo protocolo.

2. Procedimiento de acuerdo con la reivindicación 1 **caracterizado por que** el primer protocolo es un protocolo UMTS (Universal Mobile Telecommunications System, sistema de telecomunicaciones móvil universal).

3. Procedimiento de acuerdo con la reivindicación 1 ó 2 **caracterizado por que** el segundo protocolo es un protocolo GSM (Global System for Mobile Communication, sistema global para comunicaciones móviles).

4. Procedimiento de acuerdo con una de las reivindicaciones 1-3 **caracterizado por que** los accesos de registro o manipulación al terminal (7) móvil comprenden un rastreo o una localización del terminal (7)

5. Procedimiento de acuerdo con una de las reivindicaciones 1-3 **caracterizado por que** los accesos de registro o manipulación al terminal (7) móvil comprenden una escucha de las conversaciones que se llevan a cabo a través del terminal (7).

6. Procedimiento de acuerdo con una de las reivindicaciones 1-5 **caracterizado por que** para la identificación del terminal (7) móvil en la red de telefonía móvil celular digital en la que los datos se transmiten según un primer protocolo se ejecutan los siguientes pasos en el entorno del primer protocolo:

- un sistema (11) de medida obtiene los parámetros relevantes para la transmisión de datos de estaciones (6) base de la red telefonía móvil físicamente próximas al simulador (1) y se pasan al simulador (1)
- el simulador (1) se hace funcionar teniendo en cuenta los parámetros obtenidos como una nueva estación (2) base
-el terminal (7) a identificar reconoce el simulador (1) como nueva estación (2) base y se registra en él
- se inicia un procedimiento de autentificación, el terminal (7) a identificar rechaza el procedimiento de autentificación por erróneo, el simulador (1) inicia un procedimiento de identificación durante el que el simulador (1) le pide al terminal (7) a identificar sus parámetros de identificación y el simulador (1) recibe los parámetros de identificación del terminal (7) a identificar y
- se identifica el terminal (7) en el marco del primer protocolo en base a los parámetros de identificación transmitidos

7. Procedimiento de acuerdo con la reivindicación 6 **caracterizado por que** tras el procedimiento de identificación se rechaza el intento de registro del terminal (7) a identificar en el simulador (1) o la conexión entre el terminal (7) y la nueva estación (2) base se interrumpe otra manera y/o se interfiere, se fuerza al terminal (7) a registrarse automáticamente en otra estación base de otra celda de radio de una red de telefonía móvil alternativa en la que los datos se transmiten según un segundo protocolo que difiere del primer protocolo, en el entorno del segundo protocolo el terminal (7) identificar, en el marco del registro envía sus parámetros de identificación y el simulador (1) recibe los parámetros de identificación del terminal (7).

8. Procedimiento de acuerdo con la reivindicación 6 ó 7 **caracterizado por que** el sistema (11) de medida obtiene como parámetros relevantes para la transmisión de datos los códigos de mezclado (Scrambling codes) empleados por las estaciones (6) base de su entorno, frecuencias de funcionamiento y/o las potencias de emisión.

9. Procedimiento de acuerdo con la una de las reivindicaciones 6-8 **caracterizado por que** el terminal (7) a identificar cuando se registra en el simulador (1) o en el marco del procedimiento de identificación le pasa al simulador (1) al menos uno de los siguientes parámetros de identificación: IMSI, TMSI, P-TMSI, IMEI.

10. Procedimiento de acuerdo con una de las reivindicaciones 1-8 **caracterizado por que** el simulador (1) emite en la misma banda de frecuencias aunque a una potencia más alta que las estaciones (6) base que rodean al simulador (1).

11. Procedimiento de acuerdo con una de las reivindicaciones 1-9 **caracterizado por que** el simulador (1) funciona en la misma u otra celda (120-128, 130-133) de radio geográfica físicamente próxima en cuya estación (6) base el terminal (7) móvil está registrado originalmente.

12. Simulador (1) para ejecutar accesos de registro o manipulación a un terminal (7) móvil que envía o recibe datos de acuerdo con un primer protocolo en una red de telefonía móvil celular digital,

- estando dispuesto el simulador (1) físicamente próximo al terminal (7) móvil
- presentando el simulador (1) un sistema (11) de medida para obtener los parámetros relevantes para la transmisión de datos de las estaciones (6) base de la red de telefonía móvil físicamente próximas al simulador (1) en el marco del primer protocolo
- presentando el simulador (1) medios (2, 4, 10) para hacer funcionar el simulador (1) como una nueva estación base de la red de telefonía móvil en el entorno del primer protocolo teniendo en cuenta los parámetros obtenidos
- presentando el simulador (1) medios (2, 4, 10) para la identificación del terminal (7) en el entorno del primer protocolo

caracterizado por que:

- el simulador (1) presenta medios (10) para desviar el terminal (7) identificado en el entorno del primer protocolo a una red de telefonía móvil celular digital alternativa en la que los datos se transmiten según un segundo protocolo que difiere del primer protocolo
- el simulador (1) presenta medios (12, 14, 10) para hacer funcionar el simulador (1) como una nueva estación base de la red de telefonía móvil alternativa en la que los datos se transmiten según un segundo protocolo y que
- el simulador (1) presenta medios (12, 14, 10) para ejecutar accesos de registro o manipulación al terminal (7) móvil identificado en la red de telefonía móvil alternativa en la que los datos se transmiten según un segundo protocolo.

13. Simulador (1) de acuerdo con la reivindicación 12 **caracterizado por que** el sistema (11) de medida comprende un terminal-monitor (3) para la red de telefonía móvil celular digital en la que los datos se transmiten según un primer protocolo.

14. Simulador (1) de acuerdo con la reivindicación 12 ó 13 **caracterizado por que** los medios (10) para desviar el terminal (7) identificado en el marco del primer protocolo a la red de telefonía móvil alternativa están configurados de modo que los medios (10) rechazan un intento de registro del terminal (7) identificado en el simulador (1) o que los medios (10) interrumpen la conexión entre el terminal (7) y la nueva estación (2) base y/o de otra forma interfieren y que el simulador (1) está configurado de tal forma que fuerza así al terminal (7) móvil a que se registre automáticamente en otra estación base (12) de otra celda de radio de la red de telefonía móvil alternativa en la que los datos se transmiten según un segundo protocolo.

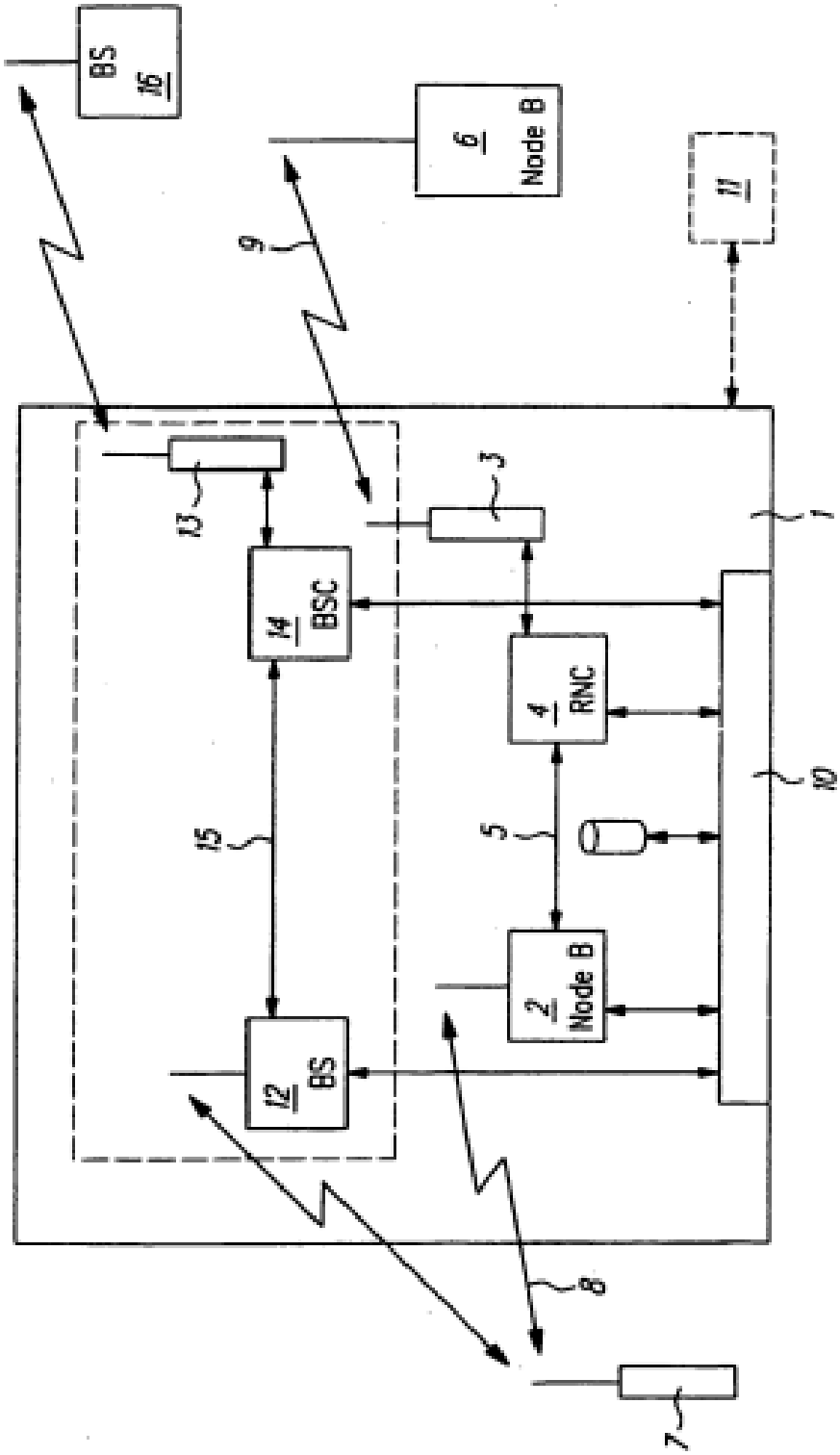

Fig. 1

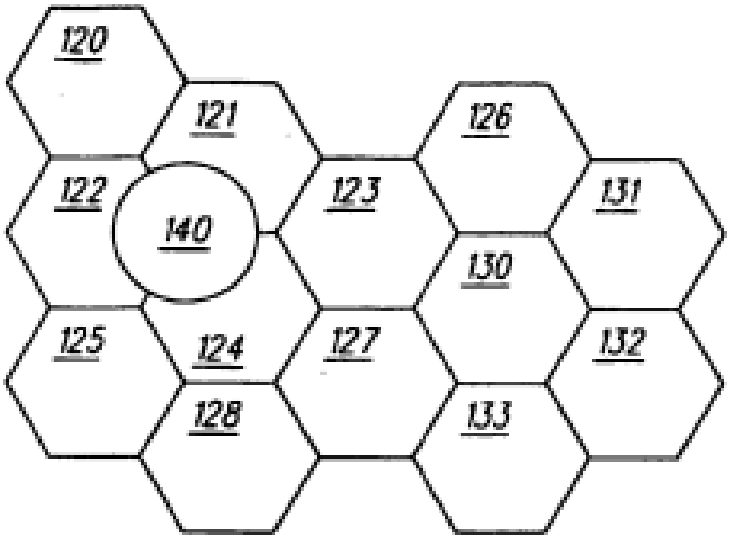
120
121
126
122
140
123
131
130
125
124
127
132
128
133

Fig. 2

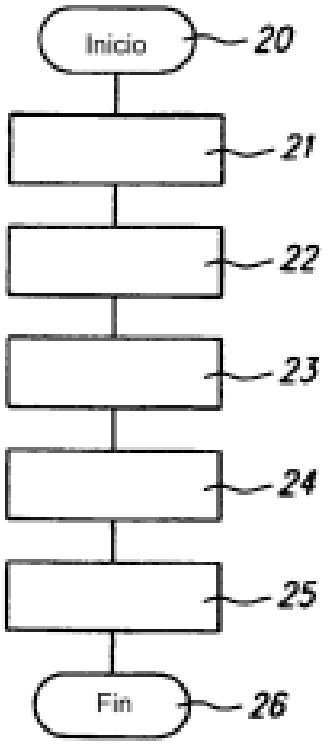
Inicio
20
21
22
23
24
25
Fin
26

Fig. 3

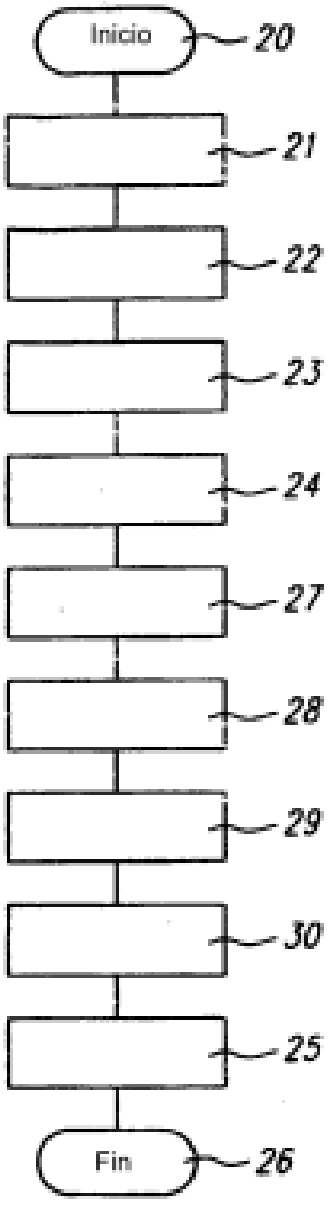
Inicio
20
21
22
23
24
27
28
29
30
25
Fin
26

Fig. 4

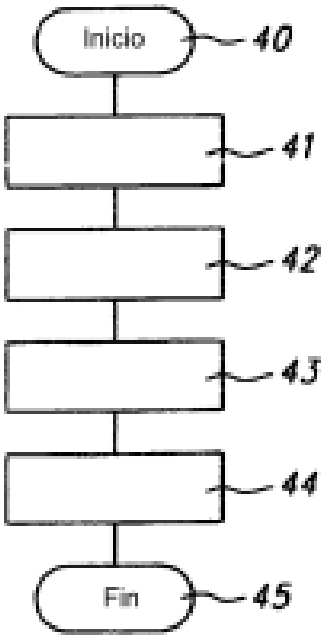
Inicio
40
41
42
43
44
Fin
45

Fig. 5