(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 314 913**

(51) Int. Cl.:
H04Q 7/38 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06753729 .0**
(96) Fecha de presentación : **19.05.2006**
(97) Número de publicación de la solicitud: **1917821**
(97) Fecha de publicación de la solicitud: **07.05.2008**

(54) Título: **Procedimiento y dispositivo para la identificación de un terminal móvil en una red de telefonía móvil celular digital.**

(30) Prioridad: **23.08.2005 DE 10 2005 040 002**

(45) Fecha de publicación de la mención BOPI:
16.03.2009

(45) Fecha de la publicación del folleto de la patente:
16.03.2009

(73) Titular/es: **Thales Defence Deutschland GmbH**
Ostendstrasse 3
75175 Pforzheim, DE

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

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

DESCRIPCIÓN

Procedimiento y dispositivo para la identificación de un terminal móvil en una red de telefonía móvil celular digital.

La presente invención se refiere a un procedimiento para la identificación de un terminal móvil en una red de telefonía móvil celular digital en el que los datos se transmiten según un primer protocolo. Además, la invención se refiere a un simulador dispuesto en la cercanía espacial de un terminal móvil a identificar para identificar el terminal móvil en una red de telefonía móvil celular digital en la que se transmiten datos según un primer protocolo.

Las fuerzas de seguridad tienen entre otras cosas la tarea de clarificar delitos ya cometidos o bien prevenir delitos aún no cometidos. Un aspecto importante en el cumplimiento de estas tareas es la posibilidad de identificar en casos excepcionales una persona sospechosa con la ayuda de un móvil utilizado por ella y poder escuchar llamadas telefónicas llevadas por la persona a través del teléfono móvil utilizado, grabarlas y evaluarlas. Las fuerzas de seguridad están autorizadas para ello mediante códigos jurídicos pertinentes y reglamentos. El objetivo en este caso es captar y evaluar las huellas de comunicación de una persona sospechosa, para así poder identificar la persona sospechosa o bien el teléfono móvil usado por ella y poder grabar y evaluar las conversaciones mantenidas.

Del estado de la técnica se conocen diferentes redes de telefonía móvil para la transmisión de datos. De uso muy amplio tanto referente a la cobertura de la red como también referente el número de los terminales móviles en uso son las redes de telefonía móvil GSM (Global System for Mobile Communications). Disponibles desde hace unos años y cada vez de mayor uso son las redes de telefonía móvil UMTS (Universal Mobile Telecommunications Systems). Estos dos estándares se distinguen por ejemplo con respecto a la autentificación, la protección de la integridad y la codificación. Mientras que en el caso del GSM el terminal móvil solamente tiene que identificarse frente una estación base, en el caso de UMTS también está prevista un autentificación de la estación base en los terminales móviles. En el marco de la protección de integridad en el caso de UMTS, los datos de control a transmitir a través de la red de telefonía móvil se protegen contra falsificación, por ejemplo, mediante firmas. Para la codificación de los datos a transmitir a través de la red de telefonía móvil en UMTS se aplican procedimientos de codificación especiales, como por ejemplo el procedimiento Kazumi. La codificación en el caso de UMTS afecta tanto los datos útiles como también los datos de control. Mientras que en una red de telefonía móvil GSM para la transmisión de datos se aplica una combinación del procedimiento de acceso múltiple por división de frecuencia (FDMA-Frequency Divisional Multiple Access) y del procedimiento de acceso múltiple por división de tiempo (TDMA-Time Divisional Multiple Access), en una red de telefonía móvil UMTS tiene aplicación un procedimiento de acceso múltiple por división del código (CDMA-Code Divisional Multiple Access) en el que los datos (señales) de varias fuentes o emisores se transmiten al mismo tiempo en la misma frecuencia. En este caso a los datos se les asignan determinados patrones de código (el llamado “scrambling code”).

Además, se conoce por ejemplo del documento DE 199 20 222 A1 un procedimiento para identificar y escuchar un terminal móvil en una red de telefonía móvil GSM celular digital. Debido a las diferencias indicadas a modo de ejemplo y no completas anteriormente entre una red de telefonía móvil GSM y una red de telefonía móvil en la que los datos de transmiten según un procedimiento de acceso múltiple por división de código, tal como por ejemplo en una red de telefonía móvil UMTS, los procedimientos conocidos para redes GMS no se pueden aplicar sencillamente a las redes UMTS.

En el documento Technical Specification ETSI 3GPP TS 33 108 versión 6.8.2 edición 6 de Enero del 2005 se describe de forma muy general la interfaz handover (interfaz de traspaso) UMTS en el caso de la llamada “lawful interception” (interceptación legal). “Lawful interception” es el termino técnico para una característica que todas las instalaciones técnicas de redes de comunicación públicas tienen que ofrecer. La “lawful interception” se refiere a la posibilidad de que organismos estatales autorizados se conectan de forma optativa a determinadas conexiones de comunicación debiendo poder escuchar el tráfico de comunicación que transcurre allí. De este modo, por ejemplo, las centrales telefónicas de redes de telefonía móvil deben está configuradas de tal manera que posibiliten esto. En la Technical Specification por lo tanto están descritas las condiciones técnicas que deben cumplir las interfaces handover de UMTS para permitir la “lawful interception”. Si no se cumplieran las condiciones descritas allí en una red de telefonía móvil UMTS, estaría descartada de antemano la identificación o escucha de terminales móviles debido a la falta de las condiciones técnicas.

En el documento WO 2005/011 318 A1 se describe como un simulador insertado en una célula de teléfono móvil GSM con el fin de escuchar un terminal móvil que es operado como estación base virtual puede aceptar sólo la solicitud de registro del terminal móvil a escuchar y rechazar las solicitudes de otros terminales móviles. En este caso el fin es reducir la carga de la estación base virtual por otros terminales durante la escucha del terminal a escuchar. Para este fin la estación base virtual es capaz de enviar señales de rechazo a los terminales que intentan registrarse en la estación base virtual.

La presente invención se basa en el objetivo de crear una posibilidad de identificar un teléfono móvil dentro de una red de telefonía móvil en la que los datos se transmiten según el procedimiento de acceso múltiple por división de código, especialmente en una red de telefonía móvil UMTS, y -si deseado- escuchar también conversaciones llevadas a través del teléfono móvil.

Para conseguir este objetivo se propone partiendo del procedimiento de tipo mencionado anteriormente que

- en cercanía espacial del terminal a identificar esté dispuesto un simulador;
- desde un sistema de medición se determinen los parámetros relevantes para la transmisión de datos de las estaciones base de la red de telefonía móvil en cercanía espacial del simulador y se traspasen al simulador;
- el simulador considerando los parámetros determinados se opere como una nueva estación base;
- el terminal a identificar detecte al simulador como nueva estación base y se registre allí,
  - iniciándose un procedimiento de autentificación, rechazandoel terminal a identificar como erróneo el procedimiento de autentificación, iniciando el simulador un procedimiento de autentificación en cuyo transcurso el simulador pregunta el terminal a identificar por los parámetros de identificación y recibiendo el simulador los parámetros de identificación del terminal a identificar; e
  - identificándose el terminal en el entorno del primer protocolo mediante los parámetros de identificación trasmitidos.

Según la invención se proponen procedimientos con los que se pueden determinar parámetros relevantes para la transmisión de datos desde estaciones base de la red de telefonía móvil en cercanía espacial del simulador y se pueden utilizar para la identificación del terminal. El simulador en este caso está dispuesto en cercanía espacial del terminal a identificar, es decir, en la célula en la que el terminal está registrado. Los parámetros determinados comprenden especialmente los "scrambling codes" utilizado por las estaciones base dispuestas en cercanía espacial de los simuladores y/o las potencias de transmisión de las estaciones base. El "scrambling code" es un patrón de código con el que se codifican los distintos emisores en el marco del procedimiento de acceso múltiple por división de código para la transmisión de datos. Entonces se opera el simulador como nueva estación base, aunque con un código de área de localización distinto al de la estación base original en la que el terminal a identificar se ha registrado originalmente. Para este fin el simulador dispone de medios apropiados, por ejemplo, una estación base que posibilita el funcionamiento del simulador como estación base dentro de la red de telefonía móvil.

Además, el simulador si envía información del sistema en la misma banda de frecuencia como la estación base original, aunque con una potencia de transmisión mayor que la estación base original. Mediante la emisión de otro código de área de localización (LAC) se simula al terminal a identificar un movimiento del terminal a una zona espacial nueva a la que está asociado el otro LAC. De este modo se obliga al terminal a registrarse automáticamente en el simulador. Para este fin el terminal lleva a cabo una llamada actualización de localización.

Con la ayuda de los parámetros de identificación se puede realizar una identificación del terminal. Los parámetros de identificación comprenden por ejemplo una IMSI (International Mobile Subscriber Identity o identidad internacional de usuario de móvil), una TMSI (Temporary Mobile Subscriber Identity o identidad temporal de usuario de móvil), P-TMSI (Packet TMSI o TMSI paquete) y/o una IMEI (International Mobile Equipment Identity o identidad internacional de equipo móvil). Estos parámetros de identificación son suficientes para establecer una conexión desde el simulador al terminal identificado con el fin de escuchar las conversaciones entrantes o salientes del terminal. Para este fin el simulador dispone de medios apropiados, por ejemplo, un terminal que permite el funcionamiento del simulador como terminal para el establecimiento de la conexión con el terminal identificado y para vigilar la conexión o bien la conversación.

Según una forma de realización preferida de la invención, el sistema de medición está configurado como un terminal con monitor que puede ser parte del simulador. Dado que los terminales, de cualquier forma determinan los parámetros relevantes para la transmisión de datos de estaciones base de la red de telefonía móvil en cercanía del terminal, se pueden aplicar sin problemas como sistemas de medición en el sentido de la invención.

El nombre propio y los datos personales del usuario del terminal están archivados en el operador (el denominado "provider") de la red de telefonía móvil y por ejemplo se pueden consultar allí en el marco de un requerimiento de la administración. Solamente en el operador están disponibles listas de referencias cruzadas que posibilitan la asignación de la IMSI a un usuario o bien de la IMSI a un número de teléfono. La TMSI -tal como dice el nombre- solamente tiene una naturaleza temporal y no permite una asignación inequívoca a un determinado usuario o a un número de teléfono determinado. Por esta razón es importante que esté disponible la IMSI y no solo la TMSI.

Si el terminal a identificar al registrarse en el simulador solamente transmite la TMSI (Temporary Mobile Subscriber Identity) como parámetros de identificación, se puede iniciar el procedimiento de autentificación. Sin embargo, si el terminal a identificar espera un procedimiento de autentificación, se propone según una variante ventajosa de la invención que a continuación del registro del terminal en el simulador

- se inicie un procedimiento de autentificación;
- el terminal a identificar rechace como erróneo el procedimiento de autentificación;

- se inicie de nuevo un procedimiento de identificación por el simulador en cuyo transcurso el simulador pregunta al terminal a identificar por su IMSI (International Mobile Subscriber Identity) o IMEI (International Mobile Equipment Identity); y

- el simulador reciba la IMSI o la IMEI del terminal a identificar.

Según esta variante primeramente se inicia un procedimiento de autentificación. No obstante, dado que el simulador o bien la nueva estación base como parte del simulador no se puede identificar (lo que en redes UMTS, sin embargo, es necesario), el terminal a identificar rechaza como erróneo el procedimiento de autentificación, por ejemplo, debido a un error MAC. Ahora el simulador inicia un procedimiento de identificación por el que se simula al terminal a identificar que la nueva estación base (que realmente es parte del simulador) requiera para fines de identificación los parámetros de identificación (IMSI o IMEI) del terminal a identificar. A continuación, el terminal transmite su IMSI o IMEI al simulador, con ayuda de la cual es posible una identificación inequívoca del terminal.

Según una forma de realización preferida de la invención se propone que

- el intento de registro del terminal a identificar en el simulador se rechace una vez que el terminal haya identificado el simulador como nueva estación base o que se interrumpa o se perturbe la conexión entre el terminal y la nueva estación base de otra manera; y

- en base a un protocolo utilizado para la transmisión de datos en la red de telefonía móvil se obligue al terminal a registrarse de forma automática en otra estación base de otra célula de otra red de telefonía móvil para la transmisión de datos según otro protocolo.

Ventajosamente se obliga al terminal a identificar después del rechazo del intento de registro en la red de telefonía móvil para el registro automático en una estación base de una célula GSM (Global System for Mobile Communications). Preferentemente las conversaciones telefónicas llevadas a través del terminal a identificar y la célula GSM se escuchan mediante procesos de escucha convencionales para redes de telefonía móvil GSM.

Después de haberse realizado la identificación del terminal, éste se remite a una red de telefonía móvil GSM convencional. Esto se puede realizar, por ejemplo, mediante elementos de información (IE) definidos, mediante perturbación (llamado jamming) de la conexión UMTS o mediante otra manera apropiada. En el caso de interrupción o perturbación de la conexión UMTS, debido al protocolo utilizado para la transmisión de datos en la red de telefonía móvil se incita al terminal a establecer la conexión a través de una red de telefonía móvil alternativa, especialmente a través de la red GSM. Esto se realiza, por ejemplo, en el marco de un procedimiento denominado “Cell Reselection”.

Después de establecer la conexión con la red GSM, se realiza la tramitación completa de la conversación en el terminal de forma convencional según el estándar GSM. Para escuchar las conversaciones se pueden aplicar procedimientos convencionales, como se conocen, por ejemplo, del documento DE 199 20 222 A1. Con respecto a los procedimientos conocidos para escuchar un terminal en una red GSM se remite expresamente a este documento.

Según otra variante ventajosa de la presente invención a continuación de la identificación del terminal se propone que

- mediante un terminal con monitor se transmitan los parámetros de identificación y las capacidades de seguridad (security capabilities) del terminal identificado a una estación base auténtica de la red de telefonía móvil;

- la estación base real re-transmita RAND (número aleatorio) y AUTN (stoken de autentificación) al terminal con monitor;

- el simulador interrumpa la conexión con la estación base real de la red de telefonía móvil;

- el simulador sea operado como otra estación base de otra célula de la red de telefonía móvil GSM y establezca una conexión con el terminal a identificar;

- se inicie un procedimiento de autentificación entre el terminal a identificar y el simulador; y

- si el procedimiento de autentificación se termina con éxito, el simulador incite al terminal identificado a no utilizar ninguna codificación en la transmisión de datos subsiguiente.

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 célula GSM (Global System for Mobile Communications).

El terminal con monitor preferentemente es parte del simulador. Los grupos de números RAND y AUTN que el simulador recibe de una estación base real de la red de telefonía móvil son parámetros que se requieren en UMTS para la autentificación de una estación base frente un terminal. El terminal con monitor simula, por consiguiente, un

deseo de conexión a la estación base real y por lo tanto se incita a la estación base real a transmitir RAND y AUTN al simulador. Desde el punto de vista de la estación base real, el simulador es un terminal real. Solamente con la ayuda de los parámetros RAND y AUTN es posible escuchar una conexión de conversación entre una estación base y un terminal identificado a escuchar.

El establecimiento de conexión con el terminal a escuchar se realiza entonces con la ayuda de una estación base GSM simulada de una célula GSM de una red de telefonía móvil GSM. La estación base GSM simulada preferentemente es parte de un simulador. Una vez realizada la autentificación, la estación base GSM simulada envía parámetros de seguridad al terminal a escuchar. Los parámetros de seguridad comprenden entre otras cosas una orden para el terminal de trabajar sin codificación (llamados parámetros "No Encryption"), es decir, de transmitir datos no codificados.

El concepto propuesto según esta variante trabaja con dos redes de telefonía móvil diferentes, concretamente con redes UMTS y GSM. Por esta razón el terminal a escuchar tiene que ser un terminal con modo multi-radio que soporta varias diferentes redes de telefonía móvil, concretamente redes UMTS y redes GSM. El concepto comprende una estación base GSM simulada, una estación base UMTS simulada y un terminal con monitor. Los tiempos de retardo entre el acceso a los parámetros de autentificación y la supresión de la codificación deberían ser lo más cortos posibles para evitar que se generen nuevas RAND y AUTN por la red UMTS auténtica antes de la supresión de la codificación. Los tiempos de retardo deberían situarse en el intervalo de pocos segundos, y como máximo en el intervalo de minutos.

Como otra solución del objetivo de la presente invención, partiendo de un simulador para identificar un terminal móvil en una red de telefonía móvil celular digital del tipo mencionado más atrás se propone que el simulador esté caracterizado por

- un sistema de medición para la determinación de los parámetros relevantes para la transmisión de datos de estaciones bases de la red de telefonía móvil en cercanía espacial del simulador;

- medios para operar el simulador como una nueva estación base de la red de telefonía móvil bajo la consideración de los parámetros determinados;

- medios para la recepción de parámetros de identificación del terminal a identificar durante el registro del terminal en el simulador,

- iniciándose un procedimiento de autentificación, rechazandoel terminal a identificar como erróneo el procedimiento de autentificación, iniciando el simulador un procedimiento de identificación en cuyo transcurso el simulador pregunta el terminal a identificar por sus parámetros de identificación del terminal a identificar y recibiendo el simulador los parámetros de identificación del terminal a identificar; y

- Medios para identificar el terminal en el entorno de primer protocolo con la ayuda de los parámetros de identificación transmitidos.

De forma preferente, el simulador presenta medios para rechazar el intento de registro del terminal a identificar en el simulador después del procedimiento de identificación o interrumpir la conexión entre el terminal y la estación base nueva de otra manera y/o de perturbarla, obligándose de este modo el terminal a registrarse de forma automática en otra estación base de otra célula de una red de telefonía móvil alternativa en la que se transmiten datos según un segundo protocolo que difiere del primer protocolo, transmitiendo el terminal a identificar en el entorno del segundo protocolo sus parámetros de identificación en el marco del registro y presentando el simulador medios para la recepción de los parámetros de identificación del terminal a identificar.

Según una variante ventajosa de la invención se propone que el simulador presente medios para la realización del procedimiento según la invención.

Un ejemplo de realización preferido de la invención se describe más en detalle a continuación con la ayuda de las Figuras. Muestran:

Figura 1 un simulador según la invención para identificar un terminal móvil dentro de una red de telefonía móvil celular digital, según una forma de realización preferida;

Figura 2 una representación de células UMTS con diferentes códigos de área de localización

Figura 3 un diagrama de flujo de un procedimiento según la invención para la identificación de un terminal según una primera forma de realización;

Figura 4 un diagrama de flujo de un procedimiento según la invención para la identificación de un terminal según una segunda forma de realización; y

Figura 5 un diagrama de flujo de un procedimiento según la invención para escuchar un terminal según una forma de realización preferida.

Las fuerzas de seguridad entre otras cosas tienen la tarea de resolver crímenes ya cometidos o bien prevenir crímenes no cometidos aún. Un aspecto importante en el cumplimiento de estas tareas es la posibilidad de identificar en casos excepcionales justificados una persona sospechosa con la ayuda de un teléfono móvil utilizado por ella y de escuchar, grabar y evaluar las llamadas telefónicas realizadas por la persona a través del teléfono móvil.

Existen diferentes redes de telefonía móvil para la transmisión de datos. De uso extendido, tanto referente a la cobertura de red como también respecto al número de los terminales móviles que se encuentran en función, son las redes de telefonía móvil GSM (Global System for Mobile Communications). Disponibles desde hace algunos años y cada vez de mayor uso son las redes de telefonía móvil UMTS (Universal Mobile Telecommunications System). Estos dos estándares se distinguen, por ejemplo, en vista a la autentificación, la protección de integridad y la codificación. Otra diferencia consiste en que en UMTS se aplica un llamado procedimiento de acceso múltiple de división de código (CDMA) mientras que GSM recurre a una combinación de procedimientos de acceso múltiple de división de frecuencia y acceso múltiple de división de tiempo (FDMA/TDMA). Debido a estas diferencias marcadas no se pueden traspasar a las redes UMTS los procedimientos y dispositivos aplicados en las redes GMS para identificar y escuchar un terminal móvil.

La presente invención por primera vez propone un procedimiento con el que también en redes de telefonía móvil UMTS se pueden identificar *in situ* y, en su caso, escuchar terminales de personas sospechosas.

En la Figura 1 se denomina con 1 en su totalidad un dispositivo para la realización del procedimiento según la invención, un dispositivo según la invención, un denominado simulador UTRAN (UMTS Terrestrial Radio Access Networks). El simulador 1 comprende una estación base 2 UMTS simulada que se denomina como NodeB y un terminal con monitor 3 simulado que trabaja según el estándar UMTS y se denomina Monitor UE (User Equipment). Además, el simulador 1 comprende una funcionalidad RNC (Radio Network Controller) 4. Entre el NodeB 2 simulado y la funcionalidad RNC 4 está prevista una denominada interfaz Iub 5. Además, está previsto un ordenador 10 de control y de manejo que controla el transcurso del procedimiento según la invención.

Además de esto, el simulador 1 comprende una estación base 12 GSM simulada que se denomina estación base (BS) y un terminal GSM 13 simulado que trabaja según el estándar GSM. El terminal UMTS 3 simulado y el terminal GSM 13 simulado también pueden ser unidos en una unidad. Esto es posible sin más, dado que los terminales UMTS normalmente presentan de cualquier modo una funcionalidad GSM para poder asegurar una conexión de conversación segura y fiable también en regiones con una cobertura UMTS insuficiente. Además, el simulador 1 presenta un funcionalidad BSC 14 (Base Station Controller). Entre la BS 12 simulada y la funcionalidad BSC 14 está prevista una interfaz 15.

Además, está previsto un sistema de medición 11 externo que mide los parámetros relevantes para UMTS de las estaciones base que rodean el simulador 1. Naturalmente, el sistema de medición 11 también puede estar integrado en el simulador 1. Como sistema de medición 11 se utiliza de forma preferente el terminal con monitor 3 UMTS, de manera que no sea necesario ningún sistema de medición adicional. El sistema de medición 3 u 11 proporciona una visión global del entorno UMTS celular que luego se transmite al simulador UTRAN 1.

El simulador 1 se introduce para la realización del procedimiento en un entorno UMTS real que comprende una estación base real (NodeB) 6 y un terminal real (UE) 7. Naturalmente, el entorno UMTS puede comprender más estaciones base que la estación base 6 representada y más terminales que el terminal 7 representado. El terminal 7 es el terminal a identificar y en su caso a escuchar y se denomina también UE-objetivo. Según la terminología utilizada aquí, un terminal UMTS cualquiera se convierte en un UE-objetivo 7 cuando ha solicitado el registro (también parcialmente) o se ha registrado en el simulador UTRAN 1. Entre el terminal 7 real y el NodeB 2 simulado está prevista una interfaz aérea Uu 8. Entre el terminal 3 simulado y el NodeB 6 real está prevista otra interfaz aérea 9.

En la Figura 2 se representa una red de telefonía móvil UMTS celular que comprende una multitud de células 120-128, 130-133. Algunas de estas células 120-128 pertenecen a una primera llamada Location Area, estando asignado a todas las células 120-128 el mismo código de área de localización (LAC) (por ejemplo, LAC=1000). Otras células 130-133 pertenecen a una segunda Local Area, estando asignado a todas las células 130-133 el mismo código de área de localización (por ejemplo, LAC=2000) que se distingue del primer código de área de localización. Las estaciones base (NodeBs) cubren una o varias células 120-128, 130-133. Las estaciones base, no obstante, por razones de mayor claridad no están representadas en la Figura 2.

En la Figura 3 está representado un diagrama de flujo del procedimiento según la invención para la identificación del terminal 7. El procedimiento comienza en un bloque de función 20. El simulador 1 está dispuesto en la red UMTS en cercanía espacial del terminal UMTS 7 a identificar (bloque de función 21). El simulador UTRAN 1 se opera dentro de una de las células geográficas 120-128, 130-133 en cuya estación base está registrado el terminal 7 a identificar. Posiblemente el terminal 7 está registrada conjuntamente con otros terminales en la estación base. Con el sistema de medición 3; 11 se miden en un bloque de función 22 los parámetros relevantes para UMTS de las estaciones base que rodean el simulador 1 o bien se detectan de otro modo y se traspasan al simulador 1. Estos parámetros comprenden, por ejemplo, los llamados “scrambling codes” de las células 120-128, 130-133, las potencias de transmisión de las estaciones base, los parámetros de identificación de los NodeBs e información del sistema.

En un bloque de función 23, el simulador UTRAN 1 a sus vez transmite informaciones de sistema en la misma banda de frecuencia que las estaciones base contiguas, no obstante, con una potencia de transmisión más elevada, de manera que los terminales (y con ello también el terminal 7 a identificar) dispuestos en cercanía espacial del simulador 1 reconocen el simulador 1 como nueva estación base (simulada). Además, el simulador 1 emite con otro código de área de localización (por ejemplo, LAC=3000), para que los terminales (y con ello también el terminal a identificar 7) dispuestos en cercanía espacial del simulador 1 tengan la impresión de que se hayan movido a una nueva área con un nuevo LAC, es decir, a un nuevo área de localización. El LAC de la estación base 2 simulada se elige de tal manera que no es usado por las estaciones base regulares 6 en la cercanía del simulador.

Por ello en estos terminales (y con ello también en el terminal 7 a identificar) se inicia un procedimiento denominado actualización de localización en cuyo marco los terminales se registran con sus parámetros de identificación en la estación base 2 simulada (bloque de función 24). Los parámetros de identificación comprenden, por ejemplo, una IMSI (International Mobile Subscriber Identity), una TMSI (Temporary Mobile Subscriber Identity) y/o una IMEI (International Mobile Equipment Identity). Con la ayuda de estos parámetros de identificación se realiza entonces en un bloque de función 25 una identificación del terminal 7. En un bloque de función 26 se termina el procedimiento para la identificación del terminal 7. La zona espacial simulada con un LAC nuevo está referenciada en la Figura 2 con la referencia 140.

El nombre propio y los datos personales del usuario del terminal 7 están archivados con el operador (denominado provider) de la red de telefonía móvil y allí se pueden consultar, por ejemplo, en el marco de una consulta por parte de la administración o de otra manera. Solo en el operador están disponibles denominadas listas de referencias cruzadas que posibilitan una asignación de la IMSI a un usuario o bien de la IMSI a un número de teléfono. La TMSI es -tal como ya indica el nombre- solamente de naturaleza temporal y no permite ninguna asignación inequívoca a un usuario determinado o a un teléfono determinado. Por esta razón es importante que esté disponible la IMSI o la IMEI y no solo la TMSI.

Si el terminal 7 a identificar en el registro en el simulador 1 en el bloque de función 24 solamente transmite la TMSI (Temporary Mobile Subscriber Indentity) como parámetro de identificación y espera un procedimiento de autentificación, se puede completar la invención según el diagrama de flujo de la Figura 4 de tal manera que a continuación al registro del terminal 7 en el simulador 1 se inicia en un bloque de función 27 el procedimiento de autentificación. Dado que el simulador 1 o bien la estación base 2 simulada como parte del simulador 2, sin embargo, no se puede identificar frente al terminal 7 (lo que es necesario, no obstante, en redes UMTS) el terminal 7 a identificar en un bloque de función 28 rechaza el procedimiento de autentificación como erróneo, por ejemplo, debido a un error MAC. Ahora el simulador 1 comienza a su vez en un bloque de función 29 un procedimiento de identificación por lo que al terminal 7 a identificar se simula la impresión de que la estación base 2 simulada necesite para fines de identificación la IMSI del terminal 7 a identificar. Después de esto el terminal 7 transmite su IMSI al simulador 1 en un bloque de función 30 con la ayuda de la cual en el bloque de función 25 es posible una identificación inequívoca del terminal 7. En el bloque de función 26 se termina el procedimiento.

A continuación a la identificación del terminal 7 objetivo según el procedimiento según la Figura 3 y la Figura 4 se pueden escuchar a través del terminal 7 llamadas entrantes y salientes de diferentes maneras. Según una primera forma de realización cuyo diagrama de flujo está representado en la Figura 5, el procedimiento para escuchar el terminal 7 comienza en un bloque de función 40. En un bloque de función 41 tiene lugar la identificación del terminal 7. El bloque 41 de este modo comprende todos los pasos del procedimiento 20 a 26 de la Figura 3 o bien 20 a 30 de la Figura 4. A continuación, en un bloque de función 42 se rechaza el procedimiento de actualización de localización del terminal 7 por el simulador 1 o bien por la estación base 2 simulada.

A continuación, el terminal 7 se registra en un bloque de función 43 después de un procedimiento denominado reselección de celda a través de la estación base GSM 12 simulada en una célula GSM de una red GSM. Los terminales UMTS según el estándar tienen que ser capaces de ser operados también en la red GSM. El rechazo de un terminal 7 objetivo por la red UMTS desviándolo a la red GSM se puede realizar de cualquier manera. Así, el rechazo se puede realizar, por ejemplo, mediante un comando (una información definida) que se transmite a través del denominado BCCH (Broadcast Control Channel). De forma alternativa el rechazo también se puede realizar a través de un mensaje cualquiera que se transmite a través del denominado FACH (Forward Access Channel) o el denominado DDCH (Dedicated Control Channel). Los terminales UMTS que se encuentran en la celda 140 del simulador 1 UTRAN reciben este comando (esta información) y se registran en una red GSM existente. También se puede imaginar perturbar la conexión con la red UMTS de otra manera, por ejemplo, mediante perturbación (el llamado jamming) y terminarla finalmente.

Todas las llamadas entrantes y salientes a través del terminal 7 objetivo ahora no se realizan a través de la red UMTS, sino a través de la red GSM. Dicho más exactamente las llamadas se realizan a través de la estación base 12 simulada, el terminal GSM 13 simulado y más allá hacia una estación base GSM auténtica. En un bloque de función 44, las llamadas realizadas a través del terminal 7 objetivo en el ambiente GSM se pueden escuchar con procedimientos convencionales, como se conocen, por ejemplo, por el documento DE 199 20 222 A1. En un bloque de función 45 se termina el procedimiento.

Naturalmente también es posible realizar no sólo el escuchar las llamadas realizadas a través del terminal 7 objetivo, sino ya la identificación del terminal 7 en el ambiente GSM con medios convencionales. Para ello se le rechaza en la

red UMTS desviándose a la red GSM aún antes de que se termine el procedimiento de actualización de localización y allí en el ambiente GSM se captan sus parámetros de identificación IMSI y IMEI mediante procedimientos conocidos. Además, allí también es posible una manipulación posterior del terminal 7 objetivo.

Asimismo, según la presenta invención es posible escuchar las llamadas realizadas a través del terminal 7 objetivo mediante un proceso denominado casi transparente. Para ello es necesario que el simulador 1 primeramente consiga informaciones de seguridad de la estación base UMTS 6 real y luego establezca una conexión con esta información desde la estación base GSM 12 simulada al terminal 7. Asimismo, con la ayuda de los parámetros de identificación del terminal 7 conseguidos anteriormente en el marco de la identificación hay que establecer una conexión del terminal GSM 13 a la estación base GSM 16 real. Las llamadas del y al terminal 7 objetivo ahora no se llevan de forma directa a través de la estación base 6 ó 16 real, sino solamente de forma indirecta a través del simulador UTRAN 1. En el simulador 1 las llamadas escuchadas se pueden grabar por completo o parcialmente, por ejemplo, para una evaluación posterior o para asegurar pruebas. Además, las llamadas se llevan de forma obligatoria a través de la red GSM y no a través de la red UMTS, incluso si existiera una cobertura UMTS suficiente.

REIVINDICACIONES

1. Procedimiento para la identificación de un terminal móvil (7) en una red de telefonía móvil celular digital en el que se transmiten datos según un primer protocolo, que comprende los siguientes pasos realizados en el entorno del primer protocolo:

- en cercanía espacial del terminal (7) a identificar se dispone un simulador (1);
- de un sistema de medición (11) se determinan los parámetros relevantes para la transmisión de datos de estaciones base (6) de la red de telefonía móvil en cercanía espacial del simulador (1) y se traspasan al simulador (1);
- el simulador (1) se opera como estación base (2) nueva teniendo en cuenta los parámetros determinados;
- el terminal (7) a identificar reconoce al simulador (1) como estación base (2) nueva y se registra en el,
  - iniciándose un procedimiento de autentificación, rechazando el terminal (7) a identificar como erróneo el procedimiento de autentificación, iniciando el simulador (1) un procedimiento de identificación en cuyo transcurso el simulador (1) pregunta el terminal (7) a identificar por sus parámetros de identificación y recibiendo el simulador (1) los parámetros de identificación del terminal (7) a identificar; y
  - identificándose el terminal (7) en el entorno del primer protocolo con la ayuda de los parámetros de identificación transmitidos.

2. Procedimiento según la reivindicación 1, **caracterizado** porque el intento de registro del terminal (7) a identificar en el simulador (1) se rechaza después del procedimiento de identificación o la conexión entre el terminal (7) y la nueva estación base (2) se interrumpe y/o perturba de otra manera, se obliga al terminal (7) a registrarse de forma automática en otra estación base de otra célula 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) a identificar transmite en el marco del registro sus parámetros de identificación y el simulador (1) recibe los parámetros de identificación del terminal (7).

3. Procedimiento según la reivindicación 1 o 2, **caracterizado** porque para el fin de una escucha, una determinación de la posición y/o una localización,el terminal (7) se rechaza después de la identificación hacia la red de telefonía móvil alternativa, en la que los datos se transmiten según el segundo protocolo que difiere del primer protocolo.

4. Procedimiento según una de las reivindicaciones 1 a 3, **caracterizado** porque en la red de telefonía móvil se utiliza como primer protocolo un protocolo UMTS.

5. Procedimiento según una de las reivindicaciones 1 a 4, **caracterizado** porque en la red de telefonía móvil alternativa se utiliza como segundo protocolo un protocolo GSM.

6. Procedimiento según una de las reivindicaciones 1 a 5, **caracterizado** porque el sistema de medición (11) determina como parámetros relevantes para la transmisión de datos los “scrambling codes”, frecuencias de funcionamiento y/o potencias de transmisión utilizados por las estaciones base del entorno.

7. Procedimiento según una de las reivindicaciones 1 a 6, **caracterizado** porque el terminal (7) a identificar al registrarse en le simulador (1) o bien en el marco del procedimiento de identificación traspasa al menos uno de los parámetros de identificación siguientes al simulador (1): IMSI, TMSI, P-TMSI e IMEI.

8. Procedimiento según la reivindicación 7, **caracterizado** porque si el terminal (7) a identificar al registrarse en el simulador (1) solamente traspasa los TMSI como parámetros de identificación

- en caso de rechazo del procedimiento de identificación por el terminal (7) a identificar:
  - se inicia un procedimiento de autentificación;
  - el terminal (7) a identificar rechaza como erróneo al procedimiento de autentificación;
  - se inicia de nuevo un procedimiento de identificación por el simulador (1) en cuyo trascurso el simulador (1) pregunta al terminal (7) a identificar por su IMSI y/o su IMEI; y
  - el simulador (7) recibe la IMSI y/o la IMEI del terminal (7) a identificar.

9. Procedimiento según una de las reivindicaciones 1 a 8, **caracterizado** porque el simulador (1) emite en la misma banda de frecuencia, aunque con mayor potencia que las estaciones base (6) que rodean al simulador (1).

10. Procedimiento según una de las reivindicaciones 1 a 9, **caracterizado** porque el simulador (1) se opera en la misma célula geográfica (120-128, 130-133) o en una que se encuentra en cercanía espacial en cuya estación base (6) está registrada originalmente el terminal (7) a identificar.

11. Procedimiento según una de las reivindicaciones 1 a 10, **caracterizado** porque al terminal (7) a identificar se simula mediante la presencia del simulador (1) operado como nueva estación base (2) un movimiento del terminal (7) a un área espacial nueva a la que está asignado un nuevo código de área de localización y debido al primer protocolo utilizado para la transmisión de datos en la red de telefonía móvil se le obliga al terminal (7) a registrarse de forma automática en el simulador (1).

12. Procedimiento según una de las reivindicaciones 1 a 11, **caracterizado** porque

- mediante un terminal (3) con monitor se transmiten los parámetros de identificación determinados y la capacidad de seguridad del terminal (7) identificado a una estación base (6) real de la red de telefonía móvil;
- la estación base (6) real reenvía un número aleatorio y un token de autentificación al terminal (3) con monitor;
- el simulador (1) interrumpe la conexión con la estación base (6) real de la red de telefonía móvil;
- el simulador (1) se opera como otra estación base (12) de otra célula de una red de telefonía móvil GSM y establece otra conexión con el terminal (7) a identificar;
- se inicia un procedimiento de autentificación entre el terminal (7) identificado y el simulador (1); y
- si el procedimiento de autentificación termina con éxito, el simulador (1) incita al terminal (7) identificado a no utilizar ninguna codificación en la transmisión de datos subsiguiente.

13. Simulador (1) para identificar el terminal (7) móvil en una red de telefonía móvil celular digital que está dispuesto en cercanía espacial de un terminal (7) móvil a identificar, transmitiéndose en la red de telefonía móvil datos según un primer protocolo que comprende:

- un sistema de medición (11) para determinar los parámetros relevantes para la transmisión de datos de estaciones base (6) de la red de telefonía móvil en cercanía espacial del simulador (1);
- medios (2) para operar el simulador (1) como una nueva estación base de la red de telefonía móvil teniendo en cuenta los parámetros determinados;
- medios (2) para la recepción de parámetros de identificación del terminal (7) a identificar durante el registro del terminal (7) en el simulador (1),
  - presentando el terminal (7) a identificar medios para rechazar como erróneo un procedimiento de autentificación,
  - presentando el simulador (1) medios para iniciar un procedimiento de identificación a continuación del rechazo del procedimiento de autentificación y medios para preguntar al terminal (7) a identificar por sus parámetros de identificación; y
  - medios (10) para identificar el terminal (7) en el entorno del primer protocolo con la ayuda de los parámetros de identificación transmitidos.

14. Simulador (1) según la reivindicación 13, **caracterizado** porque el simulador (1) presenta medios para rechazar el intento de registro del terminal (7) a identificar en el simulador (1) después del procedimiento de identificación o para interrumpir y/o perturbar de otra manera la conexión entre el terminal (7) y la nueva estación base (2) y el simulador (1) por ello obliga al terminal (7) a registrarse de forma automática en otra estación base de otra célula de una red de telefonía móvil alternativa en la que los datos se transmiten según un segundo protocolo que difiere del primer protocolo y porque el simulador (1) presenta medios (12) para recibir los parámetros de identificación del terminal (7) transmitidos en el entorno del segundo protocolo en el marco del registro del terminal (7) a identificar.

15. Simulador (1) según la reivindicación 13 o 14, **caracterizado** porque el simulador (1) presenta medios para la realización de un procedimiento según una de las reivindicaciones 3 a 12.

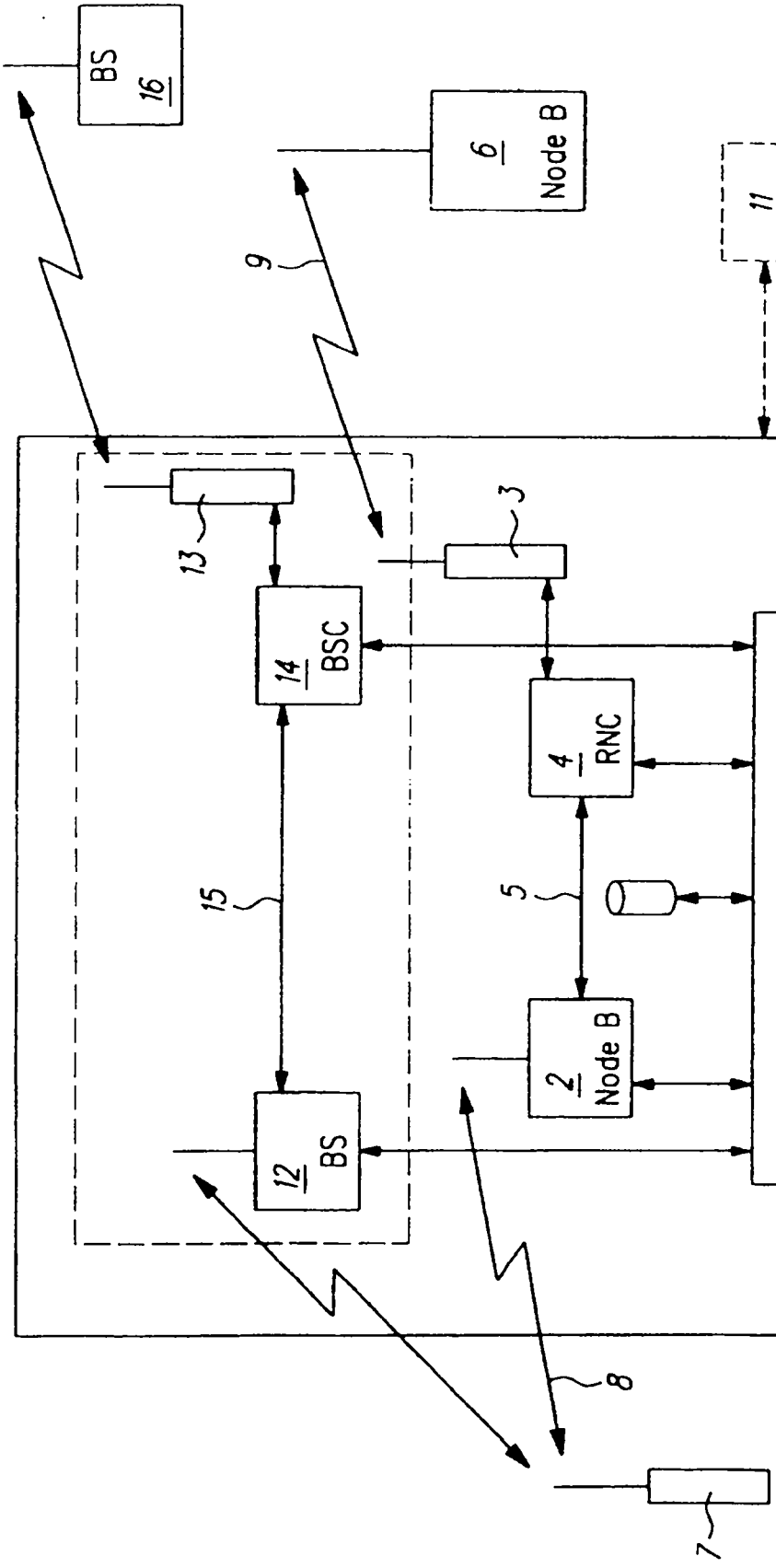

Fig. 1

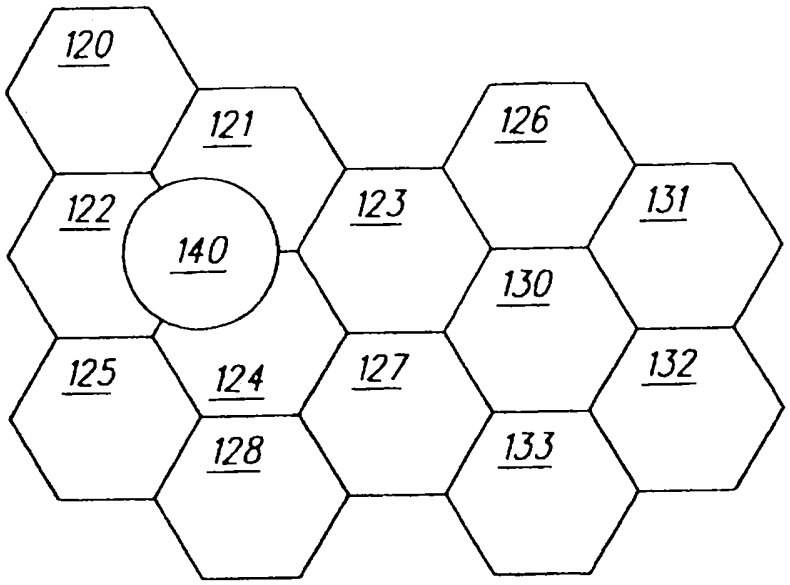
120
121
126
122
140
123
131
130
125
124
127
132
128
133

Fig. 2

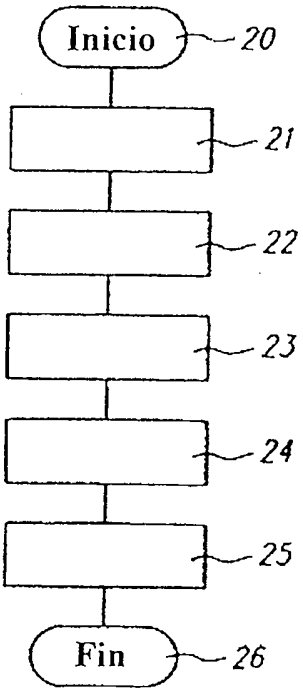
Inicio
20
21
22
23
24
25
Fin
26

Fig. 3

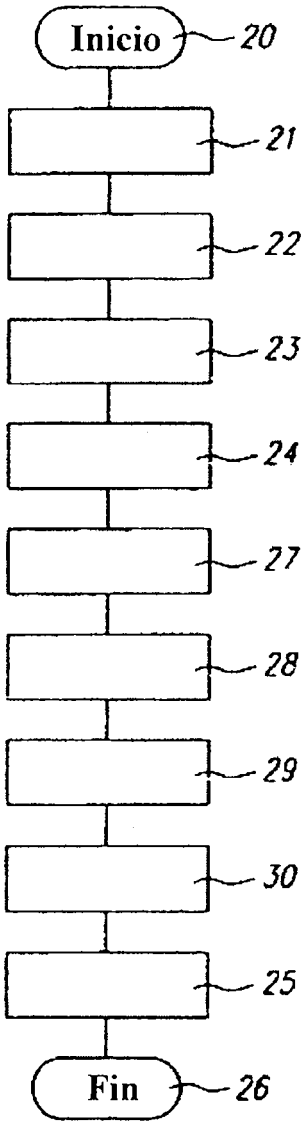
Inicio
20
21
22
23
24
27
28
29
30
25
Fin
26

Fig. 4

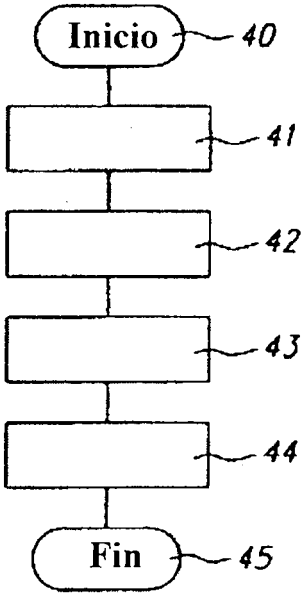
Inicio
40
41
42
43
44
Fin
45

Fig. 5