(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 427 798**

(51) Int. CI.:

***H04W 48/04*** (2009.01)
*H04W 48/02* (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **26.04.2004 E 04729418 (6)**

(97) Fecha y número de publicación de la concesión europea: **24.07.2013 EP 1741306**

(54) Título: **Validación de estaciones de telefonía móvil en redes de acceso de radio sin licencia**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**04.11.2013**

(73) Titular/es:

**TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)**
**164 83 Stockholm, SE**

(72) Inventor/es:

**NYLANDER, THOMAS;**
**HALLENSTÅL, MAGNUS;**
**LÜPPERT, BO;**
**ÖHMAN, L. PETER y**
**VIKBERG, JARI**

(74) Agente/Representante:

**DE ELZABURU MÁRQUEZ, Alberto**

## DESCRIPCIÓN

Validación de estaciones de telefonía móvil en redes de acceso de radio sin licencia

**Campo de la invención**

La presente invención se refiere a la autenticación de estaciones de telefonía móvil que acceden a un sistema de comunicación celular a través de una red de acceso de radio sin licencia.

**Antecedentes de la técnica**

En las redes celulares convencionales, tales como GSM, por ejemplo, la identidad de una estación de telefonía móvil se comprueba y su operación y derecho de acceso a la red es autenticada utilizando varios elementos dentro de la porción de red de núcleo, tal como el Registro de Ubicación Local (HLR – Home Location Register, en inglés), el Registro de Identidad de Equipo (EIR – Equipment Identity Register, en inglés) y el centro de autenticación (AUC – AUthentication Centre, en inglés).

Las redes celulares convencionales pueden ser extendidas mediante la provisión de redes de acceso de radio sin licencia, que incluyen un controlador de red de acceso para interactuar con la porción de red de núcleo de un sistema celular convencional y para controlar una pluralidad de puntos de acceso adaptados para comunicarse con estaciones de telefonía móvil sobre una interfaz de radio sin licencia. Tal red de acceso de radio sin licencia se describe en el documento EP-A-1 207 708. Otros ejemplos pueden encontrarse en el documento US 6.167.279 ó en el WO 03/085992 ó en “Seamless Roaming Services in Hybrid Networks”, Seong Soo Park et al. La interfaz de radio sin licencia puede utilizar cualquier tecnología de radio que no requiera una licencia de operación de una autoridad de suministro de licencias y en particular puede utilizar la LAN inalámbrica (WLAN – Wireless LAN, en inglés), Bluetooth o tecnologías de radio de DECT. Aunque una estación de telefonía móvil que utiliza una red de acceso de radio sin licencia para acceder a un sistema celular puede ser autenticada de la misma manera que para una red de acceso convencional, no obstante, las estaciones de telefonía móvil defectuosas pueden suponer una pesada carga de operación tanto en la red de acceso como en la red de núcleo, por ejemplo cuando generan Actualizaciones de Ubicación u otra información en un bucle. También, puesto que las estaciones de telefonía móvil capaces de acceder a una red de acceso de radio sin licencia requerirán alguna modificación sobre las estaciones de telefonía móvil convencionales, resulta necesario un nivel de validación adicional, específicamente tal como si una estación de telefonía móvil está autorizada a utilizar tal red de acceso y si esta estación de telefonía móvil está autorizada a acceder a la porción de red de núcleo a través de esta red de acceso de radio sin licencia.

**Compendio de la invención**

Es así un objeto de la presente invención permitir la autenticación y la validación de estaciones de telefonía móvil utilizando una red de acceso de radio sin licencia que minimiza la carga tanto en la red de acceso como en la red de núcleo a la cual se conecta.

Otro objeto de la presente invención es permitir la autenticación y validación de estaciones de telefonía móvil para su uso con una red de acceso sin licencia.

Estos y otros objetos se consiguen en una red de acceso de radio sin licencia y un método de validación de una estación de telefonía móvil en una red de acceso de radio sin licencia de acuerdo con las reivindicaciones adjuntas.

Específicamente, la red de acceso de radio sin licencia de acuerdo con la presente invención incluye un controlador de acceso que está adaptado para comunicarse con la porción de red de núcleo de una red de comunicación de telefonía móvil pública y está conectada a una red de paquetes conmutados de banda ancha. El controlador de acceso está adaptado para recibir mensajes de estaciones de telefonía móvil que se comunican a través de una interfaz de radio sin licencia con puntos de acceso conectados a la red de paquetes conmutados de banda ancha. El controlador de acceso comprende un módulo de apantallamiento para monitorizar la información recibida de una estación de telefonía móvil y un controlador de conexión acoplado al módulo de apantallamiento para controlar la conexión entre la estación de telefonía móvil y el controlador de acceso. En particular, el módulo de apantallamiento está adaptado para determinar si a una estación de telefonía móvil le está permitido conectarse al citado controlador de acceso, y el citado controlador de acceso está adaptado para terminar una conexión con la estación de telefonía móvil si el módulo de apantallamiento determina que la estación de telefonía móvil no está autorizada a conectarse al controlador de acceso.

La provisión de una función de apantallamiento dentro de la red de acceso asegura que el acceso a los recursos de la red de núcleo para móviles sea denegado lo antes posible para usuarios y equipos no autorizados.

Preferiblemente, el módulo de apantallamiento incluye un módulo para extraer al menos parte de una identidad de abonado de la información recibida de la citada estación de telefonía móvil para obtener una identidad de operador de red para la citada estación de telefonía móvil. Una tabla que contiene identidades de operador de red permitidas y/o bloqueadas está acoplada al módulo extractor de identidad del abonado, y el módulo extractor de identidad de

abonado está adaptado para comparar una identidad de operador de red extraída con las identidades de operador de red almacenadas en la tabla para determinar si la identidad del operador de red extraída es válida y consecuentemente si la estación de telefonía móvil debería ser autorizada a conectarse al controlador de acceso y, a través de éste, a la porción de red de núcleo. De esta manera sólo aquellas estaciones de telefonía móvil que pertenecen a una red que está autorizada a utilizar la red de núcleo estarán autorizadas a registrarse con la red de acceso y subsiguientemente a conectarse a la porción de red de núcleo.

De acuerdo con otra realización de la invención, el módulo de apantallamiento incluye un módulo para extraer al menos parte de una identidad de equipo de la información recibida de la citada estación de telefonía móvil. Este módulo compara la identidad de equipo extraída con una lista de identidades de equipo permitidas y/o bloqueadas para determinar si la citada identidad de equipo extraída está autorizada.

El módulo de apantallamiento puede, adicional alternativamente, incluir un módulo para monitorizar el tráfico entre la estación de telefonía móvil y el controlador de acceso y desde la estación de telefonía móvil a la porción de red de núcleo. Este módulo de monitorización está adaptado para señalar al controlador de conexión que termine la conexión con la estación de telefonía móvil si determina que el patrón de transacciones iniciadas en la citada estación de telefonía móvil es anormal. Tal módulo sirve como una protección adicional a la porción de red de núcleo y también al controlador de acceso identificando un comportamiento defectuoso y posiblemente malicioso que amenaza con minar la operación de la red de núcleo, y terminando la comunicación rápida y limpiamente.

Esta monitorización de tráfico o de transacciones es llevada a cabo de una manera particularmente simple, cuando la comunicación entre una estación de telefonía móvil y el controlador de acceso tiene lugar en una conexión abierta. El módulo de monitorización está entonces adaptado para monitorizar una conexión abierta entre una estación de telefonía móvil y el controlador de acceso. Esto se consigue, por ejemplo, cuando la comunicación sobre la red de banda ancha utiliza un protocolo que mantiene un estado de conexión en una red de banda ancha entre la controlador y el controlador de acceso.

Con el fin de evitar tener que procesar intentos repetidos de registro por parte de una estación de telefonía móvil a la que se le ha denegado el acceso debido a un comportamiento anormal, se proporciona un registro asociado con una estación de telefonía móvil. Este registro está controlado por medio del controlador de acceso, y es establecido por el controlador de conexión cuando la conexión con la estación de telefonía móvil ha terminado. El controlador de conexión deniega entonces el acceso a esta estación de telefonía móvil mientras que el citado registro es establecido. Adicionalmente puede proporcionarse un temporizador que está adaptado para reiniciar el registro después de un periodo de tiempo predeterminado.

**Breve descripción de los dibujos**

Otros objetos y ventajas de la presente invención resultarán evidentes a partir de la siguiente descripción de las realizaciones preferidas que están dadas a modo de ejemplo con referencia a los dibujos que se acompañan. En las figuras:

la Fig. 1 representa esquemáticamente partes de una red de GSM con una red de acceso por radio sin licencia,

la Fig. 2 es un diagrama de bloques que representa esquemáticamente la disposición funcional del controlador de acceso de radio sin licencia de acuerdo con la presente invención,

la Fig. 3 es un diagrama de flujo que ilustra la función de parte del controlador de acceso de radio sin licencia de acuerdo con la presente invención, y

la Fig. 4 es un diagrama de flujo que ilustra la función de otra parte del controlador de acceso de radio sin licencia de acuerdo con la presente invención.

**Descripción detallada de los dibujos**

La figura 1 representa esquemáticamente partes de una red de GSM convencional. Esta red está esencialmente dividida en una porción de red de núcleo 20 y una porción de acceso también conocida como subsistema de estación de base BSS (Base Station Subsystem, en inglés) 10. Los elementos de la red de núcleo 20 ilustrados en la figura incluyen los centros de conmutación de telefonía móvil o MSCs (Mobile Switching Centers, en inglés) 202, un registro de ubicación local HLR (Home Location Register, en inglés) 201 asociado y el registro de ubicación de visitante VLR (Visitor Location Register, en inglés) 204. La función y estructura de estos elementos de GSM convencionales son conocidas para los expertos en la materia y no serán descritas con más detalle en esta memoria. Aunque no se muestra en la figura, resultará evidente para los expertos en la materia que la porción de red de núcleo puede incluir el acceso a otras redes de telefonía móvil y de línea fija, tales como las redes ISDN y PSTN, las redes de paquetes y de circuitos conmutados tales como las intranets, extranets y la Internet a través de uno o más nodos de puerta de enlace. También ilustrado en la figura está el Registro de Identidad de Equipo EIR (Equipment Identity Register, en inglés) 205, que es una base de datos que almacena la identidad de los equipos de

telefonía móvil en forma de Identidad de Equipo de Telefonía Móvil Internacional IMEI (International Mobile Equipment Identity, en inglés) y se utiliza principalmente para evitar llamadas de estaciones de telefonía móvil robadas, no autorizadas o defectuosas.

La porción de acceso esencialmente consiste en subsistemas de estación de base BSS (Base Station Subsystems, en inglés) 10, uno de los cuales se ilustra en la Fig. 1, que se comunica a través de las interfaces A del estándar de telefonía fija con los MSCs 202 en la porción de la red de núcleo 20. Cada subsistema de estación de base BSS (Base Station Subsystem, en inglés) 10 incluye un controlador de estación de base BSC (Base Station Controller, en inglés) 103 que comunica con una o más estaciones transceptoras de base BTS (Base Transceiver Stations, en inglés) 101 a través de la interfaz aérea $A_{bis}$ 102 definida. Las estaciones transceptoras de base 101 se comunican con las estaciones de telefonía móvil MS (Mobile Station, en inglés) 1 sobre la interfaz aérea de radio $U_m$ de estándar GSM. Se comprenderá que aunque la BTS 101 y el BSC 103 se representan como formando una única entidad en el BSS 10, el BSC 103 está a menudo separado de las BTSs 101 y puede incluso estar situado en el centro de conmutación de servicios de telefonía móvil MSC 202.

Además de la porción de red de acceso estándar proporcionada por los BSSs 10 la red representada en la Fig. 1 incluye también una porción de la red de acceso modificada 30 mostrada en la mitad inferior de la figura. En lo que sigue en esta memoria esto se describirá como una porción de red de acceso de radio sin licencia.

Los componentes que conforman esta porción de red de acceso de radio sin licencia 30 también permiten que la estación de telefonía móvil 1 acceda a la porción de red de núcleo de GSM, y a través de ésta, a otras redes de comunicación a través de una interfaz de radio sin licencia X, representada en la Fig. 1 por la flecha 13 bidireccional. Por radio sin licencia se entiende cualquier protocolo de radio que no requiere que el operador ejecute la red de telefonía móvil para haber obtenido una licencia del cuerpo regulatorio apropiado. En general, tales tecnologías de radio sin licencia deben ser de baja potencia y así de alcance limitado en comparación con los servicios de radio de telefonía móvil con licencia. Esto significa que la vida útil de la batería de las estaciones de telefonía móvil será mayor. Además, debido a que el alcance es bajo, la radio sin licencia puede ser una radio de banda ancha, proporcionando así una mejor calidad de voz. La interfaz de radio puede utilizar cualquier protocolo de radio sin licencia adecuado, por ejemplo, un protocolo de LAN inalámbrica (WLAN – Wireless LAN, en inglés) o Telecomunicaciones Inalámbricas Mejoradas Digitales (DECT – Digital Enhanced Cordless Telecommunications, en inglés). Preferiblemente, no obstante, se utiliza la radio de Bluetooth, que tiene un elevado ancho de banda y un menor consumo de energía que la radio de red de telefonía móvil pública.

El estándar Bluetooth especifica un enlace de radio digital bidireccional para conexiones de corto alcance entre diferentes dispositivos. Los dispositivos están equipados con un transceptor que transmite y recibe en una banda de frecuencia de aproximadamente 2,45 GHz. Esta banda está disponible globalmente con alguna variación de ancho de banda dependiendo del país. Además del de datos, hasta tres canales de voz están disponibles. Cada dispositivo tiene una única dirección de 48 bits del estándar 802 del IEEE. También están disponibles codificación y verificación incluidas.

A la porción de la red de acceso 30 se accede a través de puntos de acceso AP (Access Point, en inglés) 301 que están adaptados para comunicarse a través de la interfaz Bluetooth. Sólo se muestra un punto de acceso AP (Access Point, en inglés) 301 en la Fig. 1, pero resulta evidente que muchos cientos de estos elementos pueden estar incluidos en la red de acceso de radio sin licencia 30. Este elemento maneja los protocolos del enlace de radio con la estación de telefonía móvil MS (Mobile Station, en inglés) 1 y contiene transceptores de radio que definen una celda de una manera similar a la operación de un transceptor de estación de base BTS (Base Station Transceiver, en inglés) 101 de GSM convencional. Toda la comunicación a través de los puntos de acceso AP (Access Point, en inglés) 301 está controlada por medio de un controlador de acceso AC (Access Controller, en inglés) 303, que se comunica con un centro de conmutación de servicios de telefonía móvil MSC (Mobile Serving Switching Centre, en inglés) 202 sobre la interfaz A del estándar de GSM. El controlador de acceso AC (Access Controller, en inglés) 303 proporciona la conexión entre el MSC 202 y la estación de telefonía móvil 1. La función de conexión del punto de acceso AP 301 y el controlador de acceso AC 303 emula la operación del BSS (Base Station Subsystem, en inglés) 10 hacia el MSC 202. En otras palabras, cuando se ve desde los elementos de la red de núcleo 20 tal como el centro de conmutación de servicio de telefonía móvil MSC (Mobile Service Switching Centre, en inglés) 202, la porción de la red de acceso 30 constituida por los puntos de acceso AP (Access Points, en inglés) 301 y el controlador de acceso AC (Access Controller, en inglés) 303 parece una porción de la red de acceso 10 convencional.

La interfaz entre el punto de acceso AP (Access Point, en inglés) 301 es proporcionada por una red de banda ancha de paquetes conmutados, la cual puede ser una red fija. El punto de acceso 301 está previsto para ser un dispositivo pequeño que un abonado puede comprar e instalar en una ubicación deseada tal como el hogar o un entorno de oficina para obtener un acceso fijo a la red de telefonía móvil. No obstante, también podrían ser instalados por operadores en puntos de acceso de tráfico. Para reducir los costes de instalación en la parte del operador, la interfaz entre el punto de acceso 301 y el controlador de acceso 303 aprovecha preferiblemente una conexión proporcionada por una red 302 ya existente. Redes adecuadas podrían incluir las basadas en ADSL, Ethernet, LMDS o similares. Algunas conexiones a tales redes están cada vez más disponibles para abonados mientras que los puntos de

acceso a tales redes resultan cada ved más extendidas en edificios públicos y comerciales. Aunque no se muestra en la Fig. 1, el punto de acceso AP (Access Point, en inglés) 301 estará conectado a un terminal de red dando acceso a la red 302, mientras que el controlador de acceso AC (Access Controller, en inglés) 303 puede estar conectado a un encaminador de borde ER (Edge Router, en inglés) de la red 302 que también conecta la red 302 a otras redes tales como intranets y la internet. El protocolo de Internet, IP (Internet Protocol, en inglés), se utiliza para comunicación sobre la red 302 para hacer el transporte de datos independiente del tipo de red.

El punto de acceso AP (Access Point, en inglés) 301 puede servir como un punto de acceso dedicado a la red de acceso de radio sin licencia. En este caso el punto de acceso AP (Access Point, en inglés) 301 es capaz de comunicarse de manera independiente con la estación de telefonía móvil 10 sobre la interfaz de radio sin licencia X o con el controlador de acceso 303 sobre la interfaz de red de banda ancha 302. El punto de acceso AP (Access Point, en inglés) 301 utiliza los protocolos y funciones estándar para establecer a qué controlador de acceso AC (Access Controller, en inglés) 303 debería conectarse, y también para establecer una conexión y registro con este controlador de acceso AC (Access Controller, en inglés) 303.

En una realización alternativa, el punto de acceso 301 sirve como un punto de acceso esencialmente transparente cuando se ve tanto desde el controlador de acceso 303 como desde la estación de telefonía móvil 1. En otras palabras, este punto de acceso transmite toda la información en el nivel de IP y por encima entre la estación de telefonía móvil 1 y el controlador de acceso 303. Simplemente afecta a la conversión entre servicios de radio sin licencia de capa 1 y 2 del modelo de referencia de OSI y de capa de acceso terrestre. De acuerdo con esto, la estación de telefonía móvil 1 establece una conexión con el controlador de acceso 303 sin reconocer al punto de acceso como un nodo de la conexión. De manera similar el controlador de acceso 303 podría establecer una conexión con la estación de telefonía móvil 1 directamente.

El enlace entre la estación de telefonía móvil MS (Mobile Station, en inglés) 1 y el controlador de acceso AC (Access Controller, en inglés) 303 sobre la red de IP de banda ancha 302 está siempre abierto, de manera que esta conexión siempre está disponible sin la necesidad de reservar un canal. Específicamente, se utiliza un protocolo de transporte que mantiene un estado de conexión entre una estación de telefonía móvil MS (Mobile Station, en inglés) 1 y el controlador de acceso AC (Access Controller, en inglés) 303. Un protocolo de transporte adecuado es el Protocolo de Control de transmisión (TCP – Transmission Control Protocol, en inglés), no obstante, podrían utilizarse otros protocolos tales como el Protocolo de Diagrama de Datos de Usuario (UDP – User Datagram Protocol, en inglés) o el Protocolo de Transferencia de Control de Señalización. Aunque la red 302 es preferiblemente una red basada en IP, también podrían utilizarse redes basadas en ATM. En particular cuando se utilizan tecnologías de DSL en esta red, podrían ser utilizadas directamente sobre la capa de ATM, puesto que están basadas en ATM. Naturalmente, una red basada en ATM también podría ser utilizada para transportar IP, sirviendo como capa de base.

Las aplicaciones que son ejecutadas sobre la estación de telefonía móvil MS (Mobile Station, en inglés) 1 sobre las interfaces de radio de red de telefonía móvil pública también son ejecutadas sobre radio Bluetooth entre la estación de telefonía móvil 1 y el punto de acceso AP 301.

El punto de acceso AP (Access Point, en inglés) 301 se instala conectándolo en un puerto de un modem adecuado, tal como un modem de ADSL o de CATV, para acceder a la red fija 302. Alternativamente, el punto de acceso AP (Access Point, en inglés) 301 podría ser integrado en tal modem. El puerto está en contacto con una intranet que es conectada o encaminada en el nivel de IP.

En una red de GSM convencional o en otra red de telefonía móvil con licencia pública PLMN (Public Licensed Mobile Network, en inglés), tal como CDMA2000 ó UMTS, una estación de telefonía móvil es autenticada y validada cuando se registra con una red. En un sistema de GSM el Registro de Identidad de Equipo EIR (Equipment Identity Register, en inglés) típicamente contiene tres listas de Identidades de Equipo de Telefonía Móvil IMEI (International Mobile Equipment Identities, en inglés) para estaciones de telefonía móvil que están vetadas, que deben ser rastreadas y que son válidas. El centro de conmutación de servicios de telefonía móvil MSC (Mobile services Switching Center, en inglés) pregunta al EIR cuándo se registra una estación de telefonía móvil con la red para determinar si el móvil puede ser autorizado a utilizar el servicio. Otro nivel de seguridad es proporcionado por un centro de autenticación AUC. Éste liga la Identidad de Abonado de Telefonía Móvil Internacional IMSI (International Mobile Subscriber Identity, en inglés) a parámetros de autenticación y codificación para verificar la identidad de un usuario y asegurar la confidencialidad de cada llamada. En ambos casos, la estación de telefonía móvil es autenticada y verificada en la porción de red de núcleo de la red.

De acuerdo con la presente invención, se proporciona un nivel de seguridad adicional en la red de acceso sin licencia de manera que a estaciones de telefonía móvil no autorizadas pueda impedírseles el acceso a la porción de red de núcleo. Además, las estaciones de telefonía móvil que se comportan de una manera inusual pueden ser identificadas y vetadas de la red. Filtrando las estaciones de telefonía móvil en la red de acceso de radio sin licencia la red de núcleo resulta protegida. Además, esto permite el derecho de acceso a la propia red de acceso de radio sin licencia para ser verificada.

La Fig. 2 muestra un diagrama de bloques funcional de aquellas partes del controlador de acceso AC (Access Controller, en inglés) 303 de la red de acceso de radio sin licencia que permiten este nivel adicional de seguridad de acuerdo con la presente invención. Como se muestra en la Fig. 2, el controlador de acceso AC (Access Controller, en inglés) 303 está conectado a la red de IP 302 de banda ancha y todas las comunicaciones hacia y desde las estaciones de telefonía móvil MS (Mobile Station, en inglés) 1 ocurren a través de esta red de IP 302. El controlador de acceso AC (Access Controller, en inglés) 303 está también conectado a un centro de conmutación de servicios de telefonía móvil MSC (Mobile services Switching Center, en inglés) 202 en la porción de red de núcleo de la PLMN. Aunque no se ilustra en las figuras, el controlador de acceso AC (Access Controller, en inglés) 303 podría también proporcionar acceso al Servicio de Radio en paquetes General GPRS (General Packet Radio Service, en inglés) que comprende una interfaz Gb a un nodo de soporte de GPRS (SGSN – GPRS Support Node, en inglés).

De acuerdo con la estructura de bloques simplificada del controlador de acceso AC (Access Controller, en inglés) 303 tal como se representa en la Fig. 2, las comunicaciones que se originan en una estación de telefonía móvil MS (Mobile Station, en inglés) 1 se pasan a la porción de red de núcleo 20 a través de un controlador de interfaz de red de núcleo 3035, el cual pasa mensajes convirtiéndolos a la interfaz de estándar A (o Gb) o bloquea el acceso a la porción de red de núcleo 20. Tres bloques funcionales más se muestran conectados a este controlador de interfaz de red de núcleo 3035. Dependiendo de la información recibida de estos tres bloques, el controlador de interfaz de red de núcleo 3035 bien permite o bien deniega el acceso a la red de núcleo 20. Un primer bloque 3031 extrae la Identidad de Abonado de Telefonía Móvil Internacional IMSI (International Mobile Subscriber Identity, en inglés) de una solicitud de registro recibida de una estación de telefonía móvil MS (Mobile Station, en inglés) 1 a través de la red de IP 302. La IMSI está compuesta por tres partes: un código de país para móviles MCC (Mobile Country Code, en inglés), que consiste en tres dígitos e identifica de manera única el país del domicilio del abonado de telefonía móvil; un código de red de telefonía móvil MNC (Mobile Network Code, en inglés), que consiste en dos o tres dígitos para aplicaciones de GSM y que identifica la red de GSM local (es decir, el operador de red) del abonado de telefonía móvil; y un número de identificación de abonado de telefonía móvil MSIN (Mobile Subscriber Identification Number, en inglés), que identifica al abonado de telefonía móvil dentro de una PLMN de GSM. Las dos primeras partes de la IMSI, a saber el MCC y el MNC, sirven para identificar a un operador de telefonía móvil o PLMN. El extractor de la IMSI 3031 está conectado a una base de datos o memoria 3032 que contiene una tabla de PLMNs. Esta base de datos 3032 puede incluir una lista de PLMNs a la cual la red de acceso de radio sin licencia le está permitido proporcionar acceso, o a una llamada “lista blanca”. En otras palabras, la tabla listará todas las PLMNs que tengan un acuerdo de itinerancia o similar, que acceden a la red de núcleo a través de la red de acceso de radio sin licencia. Alternativamente, o además de, la base de datos 3032 puede incluir una lista negra de PLMNs que lista a aquellas PLMNs para las cuales no puede obtenerse ningún acceso a través de la red de acceso de radio sin licencia. Tras obtener la IMSI de la estación de telefonía móvil, el extractor de IMSI obtiene las porciones de MCC y de MNC para obtener un identificador de PLMN, que compara con los identificadores de la PLMN contenidos en la tabla o tablas 3032. Si el identificador de la PLMN corresponde a una PLMN permitida, la estación de telefonía móvil MS (Mobile Station, en inglés) 1 es autorizada a registrarse y a obtener acceso tanto a los recursos de la red de acceso como de la red de núcleo. A la inversa si el identificador de PLMN no corresponde a una PLMN permitida el registro de la estación de telefonía móvil es rechazado y el acceso a la red de núcleo es bloqueado.

Un segundo bloque opcional es un extractor de Identificador de Equipo de telefonía móvil Internacional IMEI 3033 (International Mobile Equipment Identifier, en inglés). Si la estación de telefonía móvil incluye una IMEI en su solicitud de registro o se solicita hacerlo mediante las redes de acceso o de núcleo, este bloque extrae la IMEI del mensaje de registro. Este bloque envía a continuación una pregunta que contiene la IMEI recibida al Registro de Identidad del Equipo EIR (Equipment Identity Register, en inglés) 205 a través del centro de conmutación de servicios de telefonía móvil MSC (Mobile services Switching Center, en inglés) 202 en la porción de red de núcleo. Como se ha mencionado anteriormente, el Registro de Identidad de Equipo EIR (Equipment Identity Register, en inglés) 205 lista las Identidades de Equipo de Telefonía Móvil Internacionales IMEI (International Mobile Equipment Identities, en inglés) de las estaciones de telefonía móvil que están vetadas, que deben ser rastreadas y que son válidas. Dependiendo de la respuesta a la pregunta, el bloque extractor de IMEI 3033 señala al controlador de interfaz de red de núcleo 3035 que permita o que deniegue el registro de la estación de telefonía móvil. En una realización alternativa, el extractor de IMEI 3033 es capaz de interactuar con el Registro de Identidad de Equipo EIR (Equipment Identity Register, en inglés) 205 directamente sin tener que pasar la pregunta a través del centro de conmutación de servicios de telefonía móvil MSC (Mobile services Switching Center, en inglés) 202. Esto se ilustra en la figura mediante una flecha de doble cabeza de trazo y punto entre estos dos elementos. En otra realización más, no ilustrada en la Fig. 2, la funcionalidad de EIR se incorpora en el controlador de acceso 303, por ejemplo como una tabla o base de datos separada, y es actualizada a partir del EIR 205 en la red de núcleo periódicamente.

El tercer bloque que intercepta la comunicación entre las estaciones de telefonía móvil MS (Mobile Stations, en inglés) 1 y la porción de la red de núcleo 20 es un monitor de transacción 3034. Este bloque opera sólo tras el registro de una estación de telefonía móvil MS (Mobile Station, en inglés) 1 con la red de acceso y la red de núcleo y sirve para monitorizar el comportamiento de una estación de telefonía móvil. Como se ha mencionado anteriormente, una vez que una estación de telefonía móvil se ha registrado con el controlador de acceso AC (Access Controller, en inglés) 303, la conexión a través de la red de IP 302 entre una estación de telefonía móvil MS (Mobile Station, en inglés) 1 y el controlador de acceso AC (Access Controller, en inglés) 303 está siempre abierto,

incluso cuando una estación de telefonía móvil está en reposo. No hay necesidad de reservar canales, ni es necesario identificar cada comunicación separadamente, puesto que todo el tráfico en una conexión abierta designada se originará desde la misma estación de telefonía móvil MS (Mobile Station, en inglés) 1. De acuerdo con esto, el monitor de transacción 3034 es capaz de monitorizar todo el tráfico que se origina en una sola estación de telefonía móvil MS (Mobile Station, en inglés) 1. Si el número de transacciones iniciadas por la estación de telefonía móvil es demasiado elevado, indicando una operación defectuosa o un intento malicioso de desestabilizar la red de núcleo, el monitor de transacción 3034 señalará al controlador de la interfaz de la red de núcleo 3035 que termine el acceso para esta estación de telefonía móvil a la red de núcleo. Éste podría ser el caso, por ejemplo, si una estación de telefonía móvil está generando mensajes de actualización de ubicación con demasiada frecuencia como resultado de un bucle. Tal transacción podría inutilizar el centro de conmutación de servicios de telefonía móvil 202. Al mismo tiempo que fuerza a la estación de telefonía móvil MS (Mobile Station, en inglés) 1 a que salga del sistema, el controlador de la interfaz de la red de núcleo 3035 también establece un registro indicando que a la estación de telefonía móvil se le debería denegar el acceso en el futuro. Este registro está preferiblemente ligado a un temporizador, de manera que tras un periodo de tiempo predeterminado, tal como un número de días, por ejemplo, el registro es reiniciado y la estación de telefonía móvil MS (Mobile Station, en inglés) 1 puede reintentar el registro al controlador de acceso AC (Access Controller, en inglés) 303.

La estructura de bloques separados ilustrada en la Fig. 2 se da a modo de ejemplo solamente. Resultará evidente para los expertos en la materia que la función de los tres elementos podría alternativamente ser realizada mediante un único procesador o grupos de procesadores con la memoria apropiada.

La función del controlador de acceso 303 se ilustra en los diagramas de flujo de las Figs. 3 y 4. Volviendo a la Fig. 3, el diagrama de flujo se inicia en la etapa 400 con la recepción por parte del controlador de acceso AC (Access Controller, en inglés) 303 de una solicitud de registro de una estación de telefonía móvil MS (Mobile Station, en inglés) 1. En la etapa 410 el extractor de IMSI 3031 obtiene la IMSI del mensaje de registro y en la etapa 420 extrae el MCC y el MNC de la IMSI para formar un identificador de PLM PLMD-Id. En la etapa 430, el PLMN-Id es comparado con la lista o listas presente o presentes en la memoria 3032 para determinar si la estación de telefonía móvil pertenece a un operador permitido. Si la respuesta es sí, el método continúa hacia el bloque 440. Si, por otro lado, la respuesta es no, el método pasa al bloque 490, el extractor de IMSI informa al controlador de la interfaz de la red de núcleo 3035 que deniega la solicitud de registro. El método termina entonces hasta que se recibe otra solicitud de registro. En el bloque 440, el extractor de IMEI obtiene la Identidad de Equipo de telefonía móvil Internacional a partir del mensaje de registro, o a partir de un mensaje separado que forma parte de la solicitud de registro. La IMEI formula a continuación una solicitud de validación que contiene esta IMEI y la envía al Registro de Identidad del Equipo, bien a través del centro de conmutación de servicios de telefonía móvil MSC (Mobile Services Switching Center, en inglés) 202 ó del EIR 205 en la red de núcleo directamente. De acuerdo con otra variación, el extractor de IMEI consulta un registro o una tabla local proporcionado en el controlador de acceso AC (Access Controller, en inglés) 303 y determina si la IMEI de la estación de telefonía móvil está permitida. Si la respuesta a la pregunta o la determinación dentro del extractor de IMEI resulta negativa en la etapa 460, el método se mueve al bloque 490 y el registro es denegado a la estación de telefonía móvil. Si la respuesta es positiva, el método se mueve a continuación a la etapa 470, donde el controlador de la interfaz de la red de núcleo 3035 comprueba para ver si el registro para estaciones de telefonía móvil vetadas ha sido establecido. Si el registro es establecido en la etapa 480, el método se mueve a la etapa 490 y el registro se deniega. Si, a la inversa, el registro no se ha establecido, el método pasa a la etapa 500 y la estación de telefonía móvil es registrada con el controlador de acceso 303.

Volviendo ahora a la Fig. 4, el método continúa tras el registro de la estación de telefonía móvil. En la etapa 510 el monitor de transacción 3034 observa la conexión utilizada entre una única estación de telefonía móvil MS (Mobile Station, en inglés) 1 y el controlador de acceso AC (Access Controller, en inglés) 303. Esta etapa también incluye la monitorización de la comunicación entre la estación de telefonía móvil y el centro de conmutación de servicios de telefonía móvil 202 de la red de núcleo que es transmitida por el controlador de acceso 303. Todas las transacciones iniciadas en la estación de telefonía móvil MS (Mobile Station, en inglés) 1 son reportadas en la etapa 520. En la etapa 530, se determina si la incidencia de transacciones iniciadas por la estación de telefonía móvil es demasiado alta, en otras palabras si la frecuencia con la cual la estación de telefonía móvil genera algunas transacciones es inusual o si la información generada por la estación de telefonía móvil MS (Mobile Station, en inglés) es de otro modo anormal. Un ejemplo de comportamiento anormal podría ser si la IMSI o la Identidad de Abonado de telefonía móvil Temporal de Paquetes P-IMSI (Packet – Temporary Mobile Subscriber Identity, en inglés) contenida en una Solicitud de Actualización de Ubicación difieren del valor recibido durante el registro o el acoplamiento. Si la respuesta es no, el método vuelve hacia atrás en el bucle a la etapa 510 y la monitorización continúa. Si, a la inversa, se determina que la incidencia de las transacciones de la estación de telefonía móvil es anormalmente alta o suficientemente alta para crear una rotura en la red de núcleo, el método pasa a la etapa 540 y el monitor de transacción informa al controlador de la interfaz de la red de núcleo 3035. En la etapa 550, el controlador de la interfaz de la red de núcleo 3035 termina la conexión con la estación de telefonía móvil y en la etapa 560 el controlador de la interfaz de la red de núcleo 305 establece el registro, opcionalmente con el temporizador. El registro puede ser un área de memoria ligada de alguna manera con la identificación de la estación de telefonía móvil, es decir, bien la IMSI o la IMEI. Alternativamente, el registro puede ser una forma de tabla de búsqueda que

contiene un identificador de estación de telefonía móvil, en el cual se borran entradas individuales tras un periodo de tiempo predeterminado. El registro puede incluir una lista de estaciones de telefonía móvil, por ejemplo, identificadas por la IMSI, por una combinación de la IMSI con la IMEI, por algún derivado de éstas o por un identificador separado que está ligado al menos a la IMSI. En este caso, el registro podría ser utilizado por el extractor de IMSI – y el extractor de IMEI en aquellos casos en los que no se proporciona ningún extractor, o cuál de la IMEI se verifica primero – de manera que el identificador obtenido es almacenado en el registro comprobando también que para esta estación de telefonía móvil no es llevado a cabo, pero el registro es denegado inmediatamente. En el método ilustrado en la Fig. 3 esto significaría que la etapa 470 debería ser realizada entre las etapas 410 y 420, es decir, entre la obtención de la IMSI y la verificación de la validez de esta IMSI en la etapa 420.

Resultará evidente que aunque se muestran tres bloques funcionales en el controlador de acceso 303 y se describen con referencia a los diagramas de flujo en las Figs. 3 y 4, cualquiera de estas funciones puede ser proporcionada independientemente de las otras. Por ejemplo, un controlador de acceso AC (Access Controller, en inglés) 303 puede apantallar estaciones de telefonía móvil de acuerdo con la PLMN, pero ser soportado por la red de núcleo para proporcione el necesario apantallamiento de la identidad del equipo utilizando el Registro de Identidad de Equipo EIR (Equipment Identity Register, en inglés) de acuerdo con una operación de PLMN convencional. En este caso, el método de la Fig. 3 pasaría de la etapa 430 a la etapa 470 ó posiblemente directamente a la etapa 500. De manera similar, la monitorización del comportamiento de las estaciones de telefonía móvil tras el registro con la red de acceso sólo puede ser el control de validación proporcionado en el controlador de acceso AC (Access Controller, en inglés) 303, o puede ser combinado con sólo uno o con las demás de las funciones de apantallamiento proporcionadas por los bloques funcionales 3031 y 3033.

Resultará evidente que la disposición descrita anteriormente aplica también al uso de la red de acceso para proporcionar el Servicio de Radio en Paquetes General GPRS (General Packet Radio Service, en inglés) a la estación de telefonía móvil. En tal disposición, el controlador de acceso AC (Access Controller, en inglés) está conectado a través de una interfaz Gb a un nodo de soporte de GPRS (SGSN – GPRS Support Node, en inglés) y extraerá los identificadores del abonado y/o del equipo y/o monitorizará el tráfico del servicio de paquetes al controlador de acceso y al nodo de red de núcleo de la misma manera que se ha descrito anteriormente.

Aunque las disposiciones y el método anteriores se han descrito con referencia específica a un sistema de GSM resultará evidente que la presente invención puede ser igualmente aplicada a otros sistemas celulares, tales como UMTS o CDMA2000, por ejemplo. En todos los casos puede utilizarse un identificador de abonado equivalente capaz de indicar al operador a qué estación de telefonía móvil pertenece en lugar de la IMSI, mientras que un identificador de equipo puede ser utilizado en lugar de la IMEI.

**REIVINDICACIONES**

1. Una red de acceso de radio sin licencia que incluye un controlador de acceso (303) adaptado para comunicarse con la porción de red de núcleo (20) de una red de comunicación de telefonía móvil pública y conectada a una red de paquetes conmutados de banda ancha (302), estando el citado controlador de acceso (303) adaptado para recibir mensajes desde estaciones de telefonía móvil (1) que se comunican a través de una interfaz de radio sin licencia con puntos de acceso (301) conectada, a la citada red de paquetes conmutados de banda ancha (302), **caracterizada porque** el citado controlador de acceso (303) comprende un módulo de apantallamiento (3031; 3033; 3034) para monitorizar la información recibida desde una estación de telefonía móvil y un controlador de acceso (3035) acoplado al citado módulo de apantallamiento para controlar la conexión entre la estación de telefonía móvil y el controlador de acceso (303), donde el citado módulo de apantallamiento está adaptado para determinar si una estación de telefonía móvil está autorizada a conectarse al citado controlador de acceso y el citado controlador de acceso (3035) está adaptado para terminar una conexión con la estación de telefonía móvil si el módulo de apantallamiento determina que la estación de telefonía móvil no está autorizada a conectarse al controlador de acceso.

2. Una red de acceso de radio sin licencia de acuerdo con la reivindicación 1, **caracterizada porque** el citado módulo de apantallamiento incluye un módulo (3031) para extraer al menos parte de una identidad de usuario de la información recibida de la citada estación de telefonía móvil para obtener una identidad de operador de red para la citada estación de telefonía móvil, y una tabla (3032) que contiene identidades de operador de red permitidas y/o vetadas acopladas al citado módulo extractor de identidad de abonado, estando el citado módulo extractor de identidad de abonado (3031) adaptado para comparar una identidad de operador de red extraída con las identidades de operador de red almacenadas en la citada tabla para determinar si la citada identidad de operador de red extraída es válida.

3. Una red de acceso de radio sin licencia de acuerdo con la reivindicación 2, **caracterizada porque** el citado módulo extractor de identidad de abonado (3031) está adaptado para extraer al menos parte de una identidad de abonado de una solicitud de registro recibida de la citada estación de telefonía móvil.

4. Una red de acceso de radio sin licencia de acuerdo con cualquiera de las reivindicaciones previas, **caracterizada porque** el citado módulo de apantallamiento incluye un módulo para extraer al menos parte de una identidad de equipo de la información recibida de la citada estación de telefonía móvil y para comparar la citada identidad de equipo extraída con una lista de identidades de equipo permitidas y/o vetadas para determinar si la citada identidad de equipo extraída está autorizada.

5. Una red de acceso de radio sin licencia de acuerdo con la reivindicación 2, **caracterizada porque** el citado módulo extractor de identidad de equipo (3031) está adaptado para extraer al menos parte de una identidad de abonado de una solicitud de registro recibida desde la citada estación de telefonía móvil.

6. Una red de acceso de radio sin licencia de acuerdo con cualquiera de las reivindicaciones previas, **caracterizada porque** el citado módulo de apantallamiento incluye un módulo (3034) para monitorizar el tráfico entre la citada estación de telefonía móvil (1) y el citado controlador de acceso (303) y la citada estación de telefonía móvil y la porción de red de núcleo, estando el citado módulo de monitorización (3034) adaptado para señalar al citado controlador de acceso (3035) que termine la conexión con la citada estación de telefonía móvil si el citado módulo de monitorización determina que el patrón o naturaleza de las transacciones iniciadas en la citada estación de telefonía móvil es anormal.

7. Una red de acceso de radio sin licencia de acuerdo con la reivindicación 6, **caracterizada porque** la comunicación entre una estación de telefonía móvil y el citado controlador de acceso tiene lugar en una conexión abierta, y **porque** el citado módulo de monitorización (3034) está adaptado para monitorizar una conexión abierta entre una estación de telefonía móvil y el citado controlador de acceso (303).

8. Una red de acceso de radio sin licencia de acuerdo con la reivindicación 6 ó 7, también **caracterizada por** un registro asociado con una estación de telefonía móvil y controlado por el citado controlador de conexión (3035), donde el citado controlador de conexión está adaptado para establecer el citado registro cuando la conexión con la citada estación de telefonía móvil ha terminado y para denegar el acceso a la citada estación de telefonía móvil mientras que el citado registro es establecido.

9. Una red de acceso de radio sin licencia de acuerdo con la reivindicación 8, también **caracterizada por** un temporizador adaptado para reiniciar el citado registro tras un periodo de tiempo predeterminado.

10. Un método de validar una estación de telefonía móvil en una red de acceso de radio sin licencia, donde la red de acceso de radio sin licencia incluye un controlador de acceso (303) adaptado para comunicarse con la porción de red de núcleo (20) de una red de comunicación de telefonía móvil pública y conectada a una red de paquetes conmutados de banda ancha (302), estando el citado controlador de acceso (303) adaptado para recibir mensajes de estaciones de telefonía móvil (1) que se comunican a través de una interfaz de radio sin licencia con

puntos de acceso (301) conectados a la citada red de paquetes conmutados de banda ancha (302), **caracterizada porque** el citado método comprende las etapas de:

que el citado controlador de acceso monitorice la información recibida de una estación de telefonía móvil para determinar si una estación de telefonía móvil está autorizada a conectarse al citado controlador de acceso, y

que el citado controlador de acceso termine una conexión con la estación de telefonía móvil si se determina que la estación de telefonía móvil no está autorizada a conectarse al controlador de acceso.

11. Un método de acuerdo con la reivindicación 10, **caracterizado por** la etapa de

monitorizar la información, lo que incluye extraer al menos parte de una identidad de abonado de la citada información recibida para obtener una identidad de operador de red para la citada estación de telefonía móvil, y

comparar la citada identidad extraída con identidades de operador de red permitido y/o vetado para determinar si la citada identidad de operador de red extraída es válida.

12. Un método de acuerdo con la reivindicación 10 u 11, **caracterizado porque** la etapa de monitorizar la información incluye extraer al menos parte de una identidad de equipo de la información recibida de la citada estación de telefonía móvil, y comparar la citada identidad de equipo extraída con una lista de identidades de equipo permitidas y/o vetadas para determinar si la citada identidad de equipo extraída está autorizada.

13. Un método de acuerdo con cualquiera de las reivindicaciones 10 a 12, **caracterizado por** la etapa de

monitorizar información, lo que incluye monitorizar el tráfico entre la citada estación de telefonía móvil y el citado controlador de acceso y entre la citada estación de telefonía móvil y la porción de red de núcleo,

y la citada etapa de terminación incluye terminar la conexión con la citada estación de telefonía móvil si se determina que el patrón o naturaleza de las transacciones iniciadas en la citada estación de telefonía móvil es anormal.

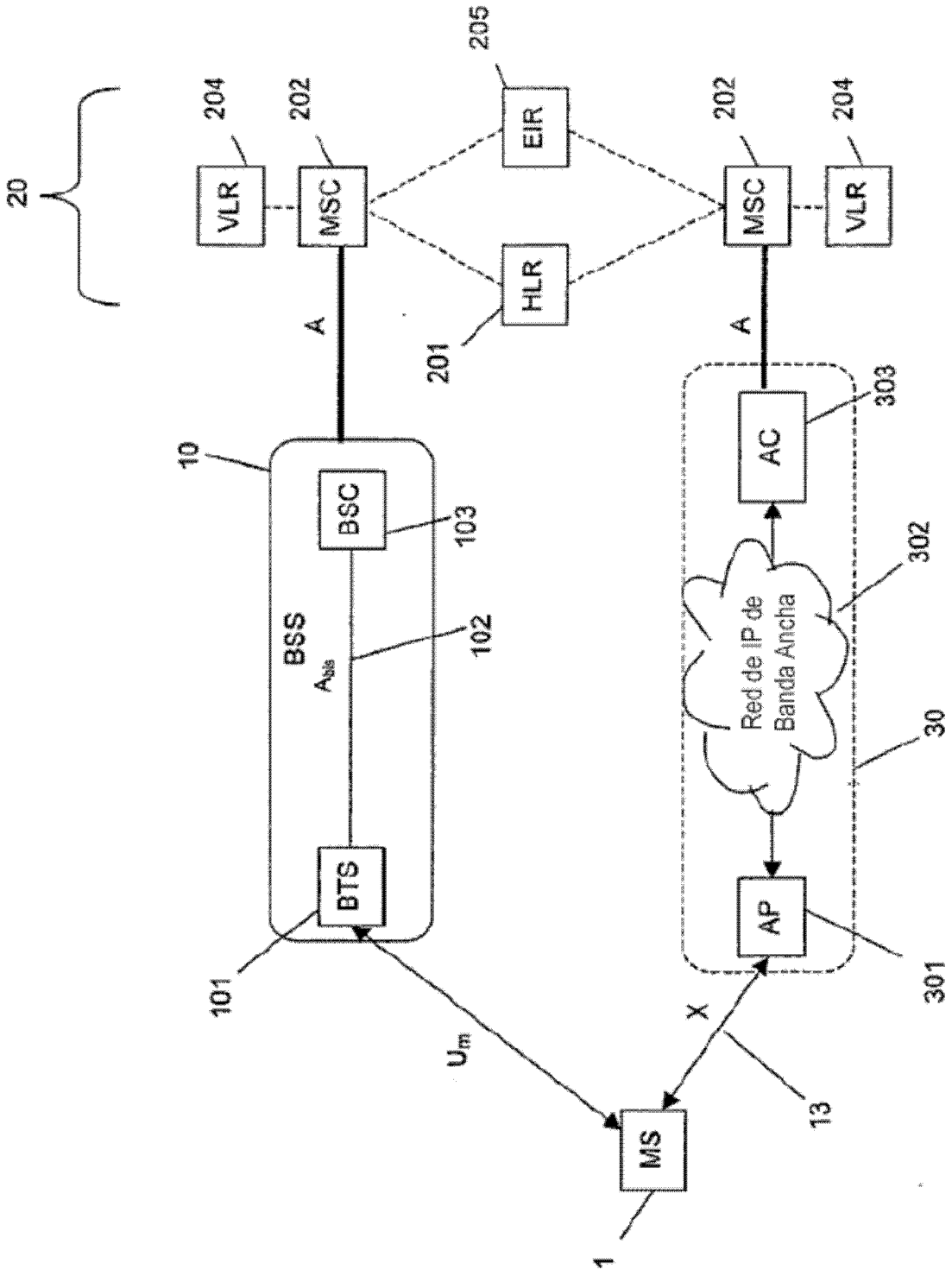
20
204
202
205
VLR
MSC
EIR
HLR
202
204
MSC
VLR
A
A
201
10
BSC
103
BSS
Abis
102
BTS
101
AC
303
302
Red de IP de Banda Ancha
30
AP
301
X
13
Um
MS
1

Fig. 1

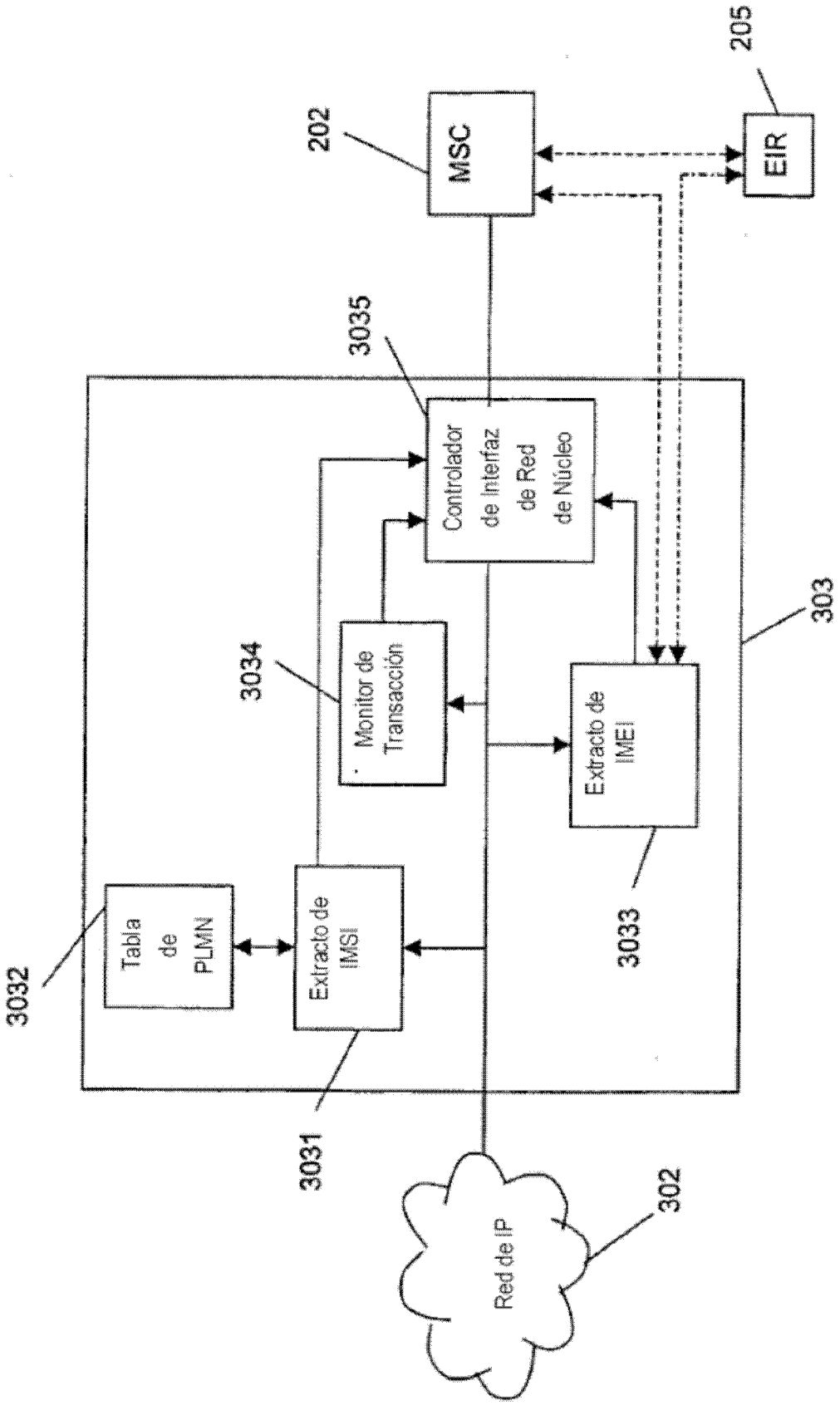
205
EIR
202
MSC
3035
Controlador de Interfaz de Red de Núcleo
303
3034
Monitor de Transacción
Extracto de IMEI
3033
3032
Tabla de PLMN
Extracto de IMSI
3031
302
Red de IP

Fig. 2

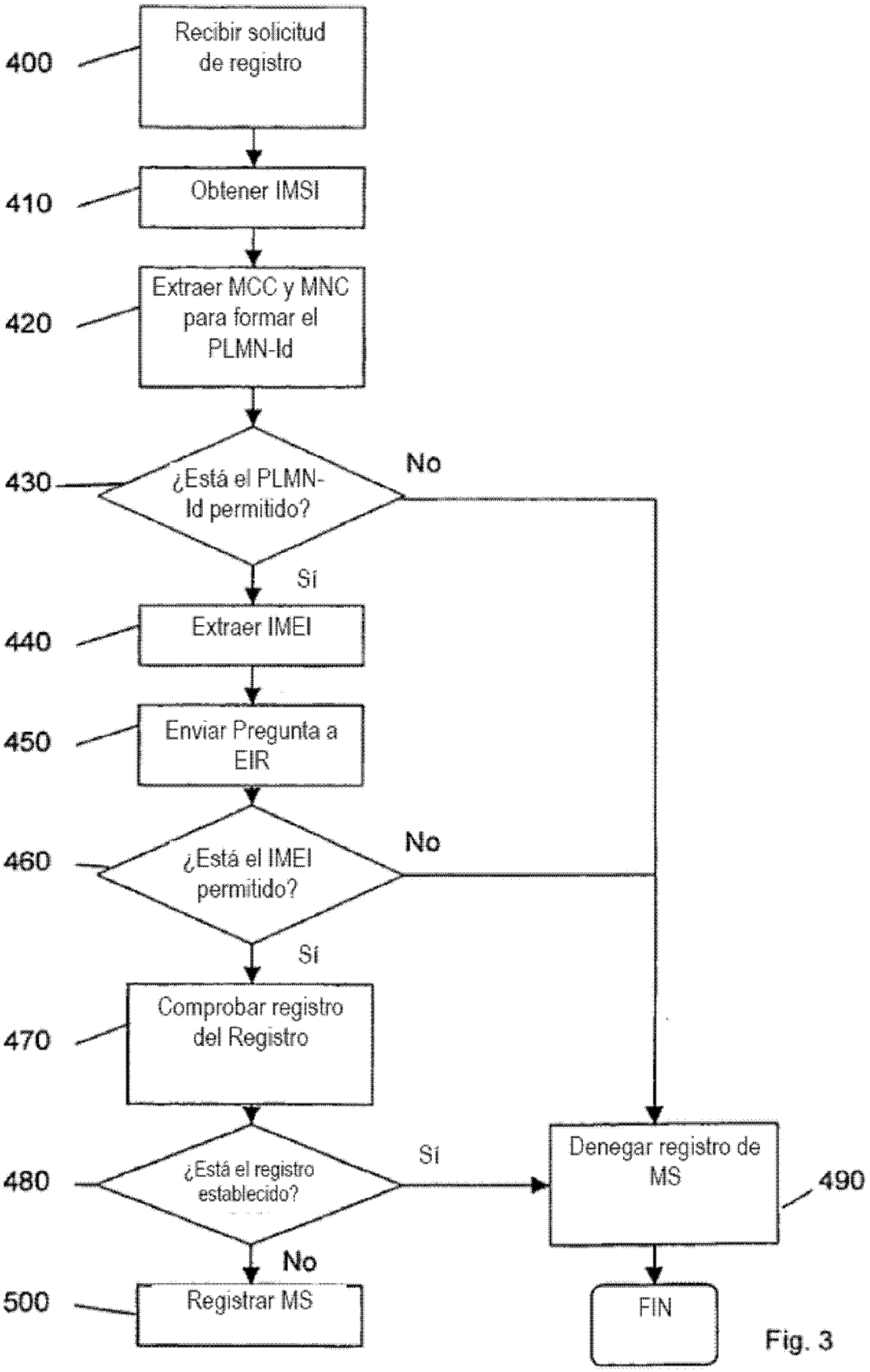
400
Recibir solicitud de registro
410
Obtener IMSI
420
Extraer MCC y MNC para formar el PLMN-Id
430
¿Está el PLMN-Id permitido?
No
Sí
440
Extraer IMEI
450
Enviar Pregunta a EIR
460
¿Está el IMEI permitido?
No
Sí
470
Comprobar registro del Registro
480
¿Está el registro establecido?
Sí
490
Denegar registro de MS
No
500
Registrar MS
FIN

Fig. 3

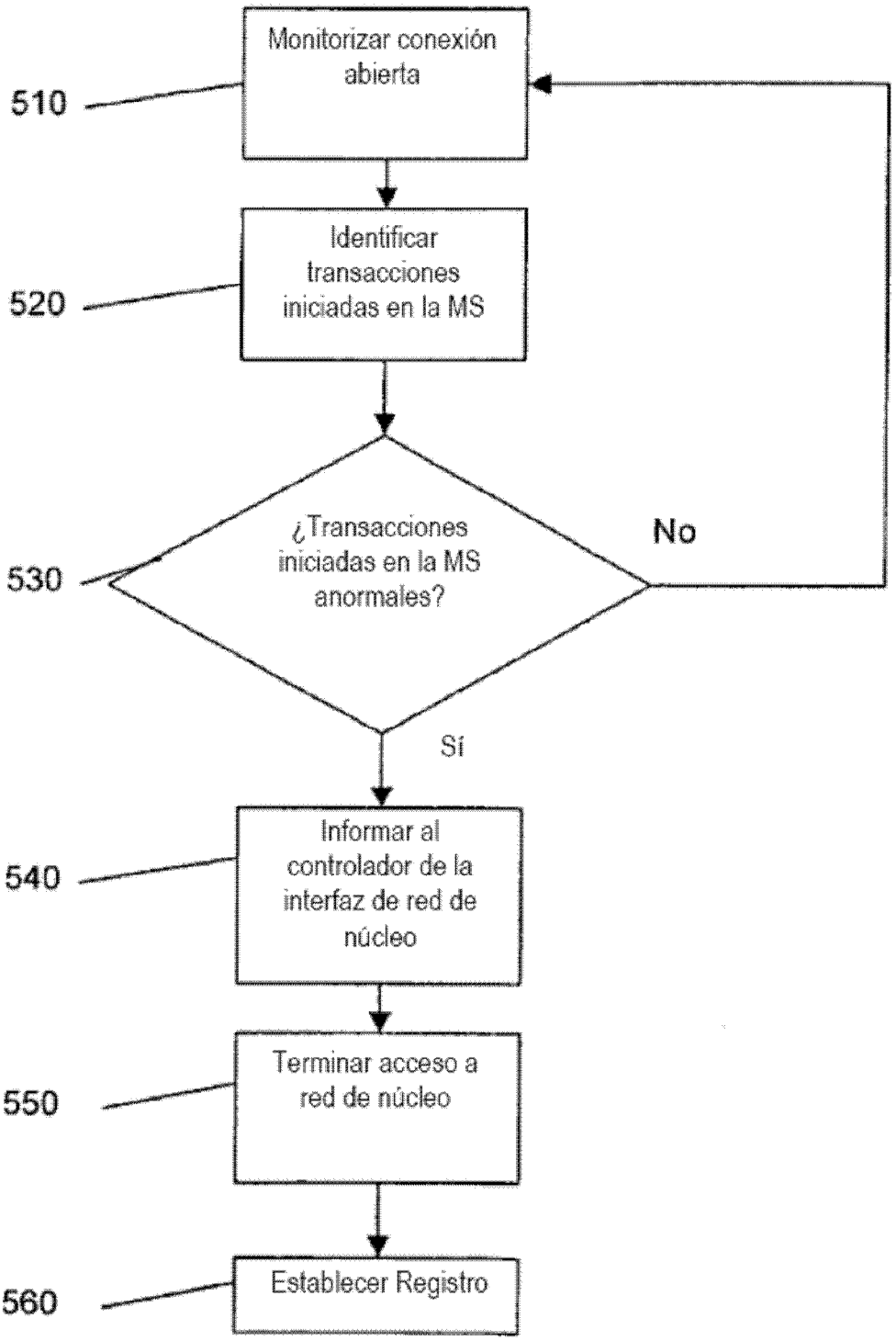
Monitorizar conexión abierta
510
Identificar transacciones iniciadas en la MS
520
¿Transacciones iniciadas en la MS anormales?
530
No
Sí
Informar al controlador de la interfaz de red de núcleo
540
Terminar acceso a red de núcleo
550
Establecer Registro
560

Fig. 4