(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 647 940**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **24.07.2008 PCT/EP2008/059733**

(87) Fecha y número de publicación internacional: **28.01.2010 WO10009766**

(96) Fecha de presentación y número de la solicitud europea: **24.07.2008 E 08775340 (6)**

(97) Fecha y número de publicación de la concesión europea: **06.09.2017 EP 2329631**

(54) Título: **Interceptación legal para equipos 2G/3G que interactúan con el sistema evolucionado de paquetes**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.12.2017

(73) Titular/es:

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

(72) Inventor/es:

IOVIENO, MAURIZIO y
DE SANTIS, RAFFAELE

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Interceptación legal para equipos 2G/3G que interactúan con el sistema evolucionado de paquetes

Campo técnico

La presente invención se refiere a métodos y disposiciones en un sistema de telecomunicaciones para proporcionar datos de interceptación o retención a las entidades solicitantes de interceptación legal, en particular en el caso de redes 2G/3G que interactúen con el Sistema Evolucionado de Paquetes

Antecedentes

En muchos países, los operadores de telecomunicaciones y los proveedores de servicios de Internet están actualmente obligados por requisitos legales a proporcionar a las Agencias de Aplicación de la Ley (LEA) los datos de tráfico almacenado generados desde las telecomunicaciones públicas con el fin de detectar, investigar y procesar delitos criminales.

Un sistema para acceder a datos relacionados con las comunicaciones es el conocido sistema de Interceptación Legal (LI). La arquitectura normalizada comprende Elementos de Control de Interceptación (ICEs) que proporcionan al equipo de usuario del usuario objetivo un acceso a la red de telecomunicaciones. Un Elemento de Control de Interceptación puede ser, por ejemplo, un Servidor de Central Telefónica del servicio Móvil 3G (MSC), un Servidor de Pasarela MSC 3G, un Nodo Servidor de Soporte de GPRS (SGSN) o una Pasarela GSN (GGSN).

La arquitectura puede comprender además uno o más Servicios de Supervisión de la Aplicación de la Ley (LEMFs) por medio de las cuales las respectivas Agencias de Aplicación de la Ley reciben información para la interceptación.

Una entidad de Función de Administración (ADMF) puede estar configurada para enviar la identidad objetivo y los datos de autorización de Interceptación Legal desde las Agencias de Aplicación de la Ley a los Elementos de Control de Interceptación.

Cada Elemento Físico de Control de Interceptación físico puede estar vinculado a la ADMF por medio de su propio interfaz X1_1. Por consiguiente, cada Elemento de Control de Interceptación puede realizar la interceptación, es decir, la activación, desactivación, interrogación e invocación, independientemente de otros Elementos de Control de Interceptación.

2G/GSM y 3G/UMTS son tecnologías clave de comunicaciones con móviles, utilizadas por más de dos mil millones de personas en todo el mundo. Con el fin de adaptarse a los nuevos servicios, la creciente demanda de ancho de banda por parte del usuario, calidad del servicio y requisitos para la convergencia de redes, evoluciones se introducen frecuentemente en la red 3G normalizada.

En este contexto, el Sistema Evolucionado de Paquetes (EPS) es una evolución importante de la norma 3G/UMTS introducida por el comité normalizador del Proyecto de Alianza de 3ª Generación (3GPP). El EPS viene definido por 3GPP en la Versión 8 como una red de núcleo enteramente nuevo con una arquitectura más plana toda IP lo que permite una mayor velocidad de datos y menor latencia del sistema optimizado de paquetes que soporta múltiples tecnologías de acceso por radio, centrándose en el dominio conmutado de paquetes.

A la vista de la difusión generalizada de las tecnologías 2G y 3G, las especificaciones 3GPP permiten que las redes 2G/3G interactúen con el Sistema Evolucionado de Paquetes, una situación que ocurre frecuentemente, por ejemplo, cuando se utiliza un terminal 2G/3G en una red cuyo operador también ha desplegado el Sistema Evolucionado de Paquetes.

Las especificaciones 3GPP incluyen los requisitos funcionales para la Interceptación Legal. La especificación técnica ETSI DTS/LI-00039 aporta una guía para la entrega y cuestiones asociadas con datos retenidos de las telecomunicaciones y de los abonados. En particular, dicha especificación proporciona un conjunto de requisitos relativos a Interfaces de Transferencia para los datos de tráfico retenidos y los datos de abonado por parte de las autoridades encargadas de la aplicación de la ley y otras autoridades solicitantes autorizadas. La Especificación Técnica ETSI DTS/LI-00033 contiene los requisitos de transferencia y una especificación de transferencia para los datos identificados en la Directiva de la UE 2006/24/EC sobre datos retenidos. En caso de interactuación entre 2G/3G y el Sistema Evolucionado de Paquetes, la Interceptación Legal debe realizarse en diferentes nodos, en particular en tres nodos diferentes donde, en algunos casos, dos nodos de cada tres pueden pertenecer a la misma red. Esta situación genera múltiples casos de productos de interceptación para el mismo abonado objetivo, situación que puede afectar negativamente al rendimiento de los nodos involucrados en la Interceptación Legal, tanto por parte del operador como de la Agencia de Aplicación de la Ley, en términos de ancho de banda y, en general, en términos del uso de los recursos.

Compendio

El objetivo de la presente invención es salvar los inconvenientes anteriormente mencionados, describiendo un método y un sistema que reducen el uso de recursos para satisfacer los requisitos de interceptación legal.

Este objetivo y otros objetos que resultarán más evidentes a continuación se logran mediante un método y un sistema que evitan la redundancia de las peticiones de interceptación y de los datos interceptados.

De acuerdo con un primer aspecto de la invención, la Interceptación Legal en un nodo se ignora cuando el nodo es capaz de determinar que la Interceptación Legal también se está realizando en otro nodo de la misma red.

De acuerdo con un segundo aspecto de la invención, los datos interceptados de un nodo se descartan

Con más detalle, el propósito y los objetivos de la invención se logran mediante un método para reducir el consumo de recursos para la Interceptación Legal o la retención de datos relativos al tráfico concerniente a un móvil objetivo 2G/3G conectado a una red de telecomunicaciones que interactúa con el Sistema Evolucionado de Paquetes, que comprende las etapas de: en un primer nodo, detectar al menos un valor de parámetro en los datos para los cuales se ha activado la Interceptación Legal o la retención de datos; basándose en dicho al menos primer valor de parámetro, evaluar si dicho tráfico es interceptado o retenido en un segundo nodo cruzado por dicho tráfico en la misma red; filtrar las peticiones de interceptación legales o los datos interceptados si dicho segundo nodo está situado aguas abajo de dicho primer nodo.

Este objetivo y los anteriores también se logran mediante un sistema de Interceptación Legal para la interceptación o retención de datos relacionados con el tráfico asociado a un equipo de usuario objetivo en una red de telecomunicaciones 2G/3G interactuando con el Sistema Evolucionado de Paquetes, en el que al menos un primer nodo y al menos un segundo nodo están configurados para operar como Elementos de Control de Interceptación o fuentes de Retención de Datos, en el que dicho primer nodo está configurado para detectar al menos un valor de parámetro en los datos, cuya Interceptación Legal o retención de datos ha sido activada y, basándose en dicho valor de parámetro, filtrar las peticiones de Interceptación Legal o datos interceptados si dicho segundo nodo está situado aguas abajo de dicho primer nodo.

La presente invención también concierne a programas informáticos que comprenden porciones de códigos de software con el fin de realizar el método de acuerdo con la invención cuando se opera en un procesador de un Elemento de Control de Interceptación o de una fuente de Retención de Datos. Un programa de ordenador puede cargarse en al menos uno de un Nodo Servidor de Soporte de GPRS o una Pasarela Servidora para configurar dicho Nodo Servidor de Soporte de GPRS o Pasarela Servidora como Elemento de Control de Interceptación o fuente de Retención de Datos operable en un sistema de Interceptación Legal de acuerdo con la invención.

Dicho programa de ordenador puede almacenarse en un medio interpretable por ordenador, que puede ser una memoria permanente o regrabable dentro del Elemento de Control de Interceptación o de la fuente de Retención de Datos o puede estar situado externamente. El programa de ordenador respectivo también se puede transferir al Elemento de Control de Interceptación o a la fuente de Retención de Datos, por ejemplo por medio de un cable o un enlace inalámbrico como una secuencia de señales.

Breve descripción de los dibujos

Otras características y ventajas de la invención se harán más evidentes a partir de la descripción detallada de las realizaciones en particular pero no exclusivas, ilustradas a modo de ejemplos no limitativos en los dibujos adjuntos, en los que:

La figura 1 es un diagrama de bloques de la arquitectura del Sistema Evolucionado de Paquetes en un escenario como no transeúnte.

La figura 2 es una disposición de un sistema de Interceptación Legal, en el que uno o más de un Nodo Servidor de Soporte de GPRS, una Pasarela Servidora y una Pasarela de Red de Datos en Paquetes (PDN-GW) pueden funcionar como Elementos de Control de Interceptación.

La figura 3 es una disposición de un sistema de Interceptación Legal, en el que uno o más de un Nodo Servidor de Soporte de GPRS, una Pasarela Servidora y una Pasarela de Red de Datos en Paquetes pueden actuar como fuentes de Retención de Datos.

La figura 4 es un diagrama de flujo que muestra un método para ignorar la Interceptación Legal de acuerdo con un aspecto de la presente invención.

La figura 5 es un diagrama de flujo que muestra un método para descartar los datos interceptados de acuerdo con otro aspecto de la presente invención.

Descripción detallada

En la figura 1 se representa una arquitectura del Sistema Evolucionado de Paquetes en el caso de un escenario no transeúnte. La arquitectura comprende un móvil objetivo o Equipo de usuario (UE) 1, UTRAN mejorada (E-UTRAN) 110, Redes Terrestres Universales de Acceso por Radio (UTRAN) 120 y Red de Acceso por Radio GSM EDGE (GERAN) 130, Nodo Servidor de Soporte de GPRS (SGSN) 3, Entidad de Gestión de la Movilidad (MME) 140, Servidor de Abonado Doméstico (HSS) 150, Pasarela Servidora (S-GW) 4, Pasarela de Red de Datos en Paquetes (PDN) **5**, Función de Política de Reglas de Cargos (PCRF) 170 y servicios IP del Operador 180.

Algunos de los nodos representados en la figura 1 pueden operar como Elementos de Control de Interceptación de un Sistema de Interceptación Legal, particularmente el Nodo Servidor de Soporte de GPRS 3, la Pasarela Servidora 4 y la Pasarela de Red de Datos en Paquetes 5.

El Nodo Servidor de Soporte de GPRS **3** es responsable de la entrega de paquetes de datos desde y hacia las estaciones móviles dentro de su área geográfica de servicio. La Interceptación Legal puede ser necesaria en el Nodo Servidor de Soporte de GPRS **3**, ya que maneja los eventos de Gestión de la Movilidad y también está en posición en la red para interceptar abonados en la Red Móvil Terrestre Pública Visitada (VPLMN) en caso de que se utilice el interfaz Gp entre diferentes países.

La Pasarela Servidora 4 es la pasarela que termina el interfaz hacia E-UTRAN. Para cada Equipo de Usuario 1 asociado al Sistema Evolucionado de Paquetes, una única Pasarela Servidora 4 está activa en un momento dado. Se requiere una Interceptación Legal en la Pasarela Servidora 4 para interceptar abonados conectados a E-UTRAN.

La Pasarela de Red de Datos en Paquetes 5 es la pasarela que termina el interfaz SGi hacia la Red de Datos en Paquetes. Si un Equipo de Usuario 1 accede a múltiples Redes de Datos en Paquetes, puede haber activa más de una Pasarela de Red de Datos en Paquetes para ese Equipo de Usuario 1. En los escenarios descritos por 3GPP TS 23.401, se requiere Interceptación Legal en la Pasarela de Red de Datos en Paquetes 5 para interceptar los abonados de la Red Móvil Terrestre Pública Doméstica (HPLMN) que transitan por una Red Móvil Terrestre Pública Visitada diferente.

El tráfico que implica a un abonado 1 conectado a 2G/3G puede ser manejado en un Nodo Servidor de Soporte de GPRS 3 usando la denominada "pista doble". El interfaz Gn/Gp se puede utilizar hacia una GGSN mientras que los interfaces S4/S12 se pueden utilizar con una Pasarela Servidora 4.

De acuerdo con la norma 3GPP, un Nodo Servidor de Soporte de GPRS 3 que soporte ambos interfaces Gn/Gp y S4/S12 deberá, para todas las conexiones activas de Red de Datos en Paquetes para un determinado Equipo de Usuario 1, utilizar S4 o Gn/Gp. Por lo tanto, cada Nodo Servidor de Soporte de GPRS 3 está rechazando una activación de contexto de PDP violando esto de la siguiente manera. Si el Equipo de Usuario 1 envía una petición de contexto del Protocolo Activado de Datos en Paquetes para un Nombre de Punto de Acceso utilizando Gn, la activación es rechazada por el Nodo Servidor de Soporte de GPRS 3 si ya existe un contexto PDP que está ya utilizando S4 para el Equipo de Usuario 1.

Si el Equipo de Usuario 1 está enviando una petición de contexto de Activar PDP para un Nombre de Punto de Acceso utilizando S4, la activación es rechazada por el Nodo Servidor de Soporte de GPRS 3 si ya existe un contexto PDP que está utilizando Gn para este Equipo de Usuario 1.

Un método para optimizar el consumo de recursos para la Interceptación Legal o retención de datos de acuerdo con un primer aspecto de la presente invención se describe ahora con respecto al flujo de datos de la figura 4.

La figura 4 muestra dos elementos de red, denominados, un Equipo de Usuario 1 y un nodo de red 200, que puede ser un Nodo Servidor de Soporte de GPRS 3 o una Pasarela Servidora 4.

Cuando un Equipo de Usuario 1 envía un mensaje al Nodo Servidor de Soporte de GPRS 3 o a la Pasarela Servidora 4, se envía en el mensaje un valor de parámetro desde el cual se puede determinar una ruta del tráfico del usuario.

Tal valor de parámetro puede ser, por ejemplo, un Nombre del Punto de Acceso (APN), que se utilizará en la siguiente descripción.

En la etapa 210, el Nodo Servidor de Soporte de GPRS 3 comprueba el Nombre del Punto de Acceso y, en la etapa 211, el Nodo Servidor de Soporte de GPRS 3 evalúa si el Nombre del Punto de Acceso está solicitando el uso de una pista S4.

Si este es el caso, en la etapa 212, se ignora la Interceptación Legal, puesto que una solicitud de una pista S4 implica necesariamente que el tráfico procedente del Equipo de Usuario 1 atraviese la Pasarela Servidora 4, en la que se ha activado la Interceptación Legal.

De manera similar, en la etapa 210, se comprueba el Nombre del Punto de Acceso por la Pasarela Servidora 4 que, en la etapa 211, evalúa si el Nombre del Punto de Acceso está relacionado con una Pasarela de Red de Datos en Paquetes 5 en la misma Red Pública Móvil Terrestre. En este caso, la Interceptación Legal es igualmente ignorada, ya que esto implica que el tráfico del Equipo de Usuario 1 cruce la Pasarela de Red de Datos en Paquetes 5, en la cual se ha activado la Interceptación Legal.

De acuerdo con un primer aspecto de la invención, la optimización del uso de recursos para la Interceptación Legal se logra, por tanto, ignorando las peticiones de Interceptación Legal cuando las mismas se están solicitando en un nodo diferente situado en la misma red, particularmente en un nodo diferente situado aguas abajo del nodo que está ignorando la Interceptación legal.

De acuerdo con un segundo aspecto de la invención, la optimización del uso de recursos para la Interceptación Legal se logra descartando datos redundantes.

Con referencia a la figura 2, se describe una arquitectura para el acceso a las comunicaciones en un sistema 10 de Interceptación Legal de acuerdo con dicho segundo aspecto de la invención.

Un sistema de Interceptación Legal 10 puede comprender Elementos de Control de Interceptación 11 que proporcionan al equipo de usuario 1 del usuario objetivo acceso a la red de telecomunicaciones.

Uno o más del Nodo Servidor de Soporte de GPRS 3, Pasarela Servidora 4 y Pasarela de Red de Datos en Paquetes 5 pueden ser definidos como Elementos de Control de Interceptación 11, con el fin de interceptar la señalización y el contenido de comunicación para un nodo móvil 1 que es objetivo de una Interceptación Legal.

El sistema de Interceptación Legal 10 puede comprender además uno o más Servicios de Supervisión de Aplicación de la Ley (LEMFs) 12, por medio de los cuales las respectivas Agencias de Aplicación de la Ley (LEAs) pueden recibir información sobre interceptación.

Una entidad de Función de Administración (ADMF) 13 puede configurarse adicionalmente para enviar la identidad del objetivo y los datos de autorización para la Interceptación Legal recibidos de las respectivas Agencias de Aplicación de la Ley a los Elementos de Control de Interceptación 11.

La Función de Administración 13 puede conectar por medio de un primer Interfaz de Transferencia 14 (HI1) con todas las Agencias de Aplicación de la Ley que puedan solicitar la interceptación en la red de interceptación y puede mantener separadas las actividades de interceptación de cada una de las Agencias de Aplicación de la Ley y conectarlas a la red de interceptación. La Función de Administración 13 también puede usarse para ocultar de los Elementos de Control de Interceptación 11 que pueden haber sido activadas múltiples activaciones por diferentes Agencias de Aplicación de la Ley sobre el mismo objetivo. Además, la Función de Administración 13 puede dividirse para asegurar la separación de los datos de aprovisionamiento de las diferentes agencias.

Todo Elemento de Control de Interceptación físico 11 puede estar vinculado a la Función de Administración 13 mediante su propio interfaz X1_1. Por consiguiente, cada Elemento de Control de Interceptación único 11 puede realizar la interceptación, es decir, la activación, desactivación, interrogación e invocación, independientemente de otros Elementos de Control de Interceptación 11.

Con el fin de entregar la información interceptada a las Agencias de Aplicación de la Ley, se pueden proporcionar dos entidades de Funciones de Entrega (DF), intercambiando cada una porciones respectivas de información con la Función de Administración 13, por medio de los interfaces X1_2 y X1_3, y del Servicio de Supervisión de la Aplicación de la Ley 12.

En particular, una entidad de Función de Entrega 15 DF2 puede estar configurada para recibir la Información Interceptada Relacionada (IRI) del Elemento de Control de Interceptación 11, por medio de un interfaz X2, y para convertir y distribuir la Información de Interceptación Relacionada a las Agencias de Aplicación de la Ley pertinentes mediante un segundo Interfaz de Transferencia 16 (HI2) por medio de una función de mediación (MF) 17.

La Información de Interceptación Relacionada puede ser una colección de información o datos asociados con servicios de telecomunicaciones que implican la identidad objetivo, tal como información o datos asociados a llamadas, por ejemplo, intentos fallidos de llamada, información o datos asociados con el servicio, por ejemplo, gestión del perfil del servicio por parte del abonado, e información sobre la localización.

Una entidad de Función de Entrega 18 DF3 puede estar configurada para recibir información del Contenido de las Comunicaciones (CC) de los Elementos de Control de Interceptación 11 por medio de un interfaz X3, y para convertir y distribuir dicha información a la Agencia de Aplicación de la Ley por medio de la Función de Mediación 19 y de un tercer Interfaz de Transferencia 20 (HI3).

El Contenido de las Comunicaciones puede ser una información diferente de la Información Interceptada Relacionada, la cual es intercambiada entre dos o más usuarios de un servicio de telecomunicaciones y, más en

general, puede incluir información que, como parte de algún servicio de telecomunicaciones, podría ser almacenada por un usuario para su posterior recuperación por otro usuario.

Toda la información del tráfico puede utilizarse para el almacenamiento adecuado a fin de satisfacer los posibles requisitos legales relativos a la retención de datos.

A este respecto, la figura 3 representa una disposición para retener datos en un Proveedor de Servicios de Comunicación 21 (CSP). Concretamente, el Proveedor de Servicios de Comunicación 21 puede estar provisto de un Sistema de Retención de Datos 23 (DRS) para intercambiar datos retenidos que relacionan la información con una Autoridad Solicitante 24, que puede ser una Agencia de Aplicación de la Ley (LEA).

El Proveedor de Servicios de Comunicación 21 puede incluir un Nodo Servidor de Soporte de GPRS 3, una Pasarela Servidora 4 y una Pasarela de Red de Datos en Paquetes 5, configurados para funcionar como fuentes de Retención de Datos.

Los datos intercambiados entre el Proveedor de Servicios de Comunicación 21 y la Autoridad Solicitante 24 pueden comprender solicitudes de la Autoridad Solicitante 24, las respuestas correspondientes del Sistema de Retención de Datos 23 y otra información de retención de datos, tal como resultados de las solicitudes y acuses de recibo. Las interfaces a través de las cuales el Proveedor de Servicios de Comunicación 21 y el Sistema de Retención de Datos 23 intercambian los datos anteriores con la Autoridad Solicitante se designan como Interfaces de Transferencia.

El Interfaz de Transferencia genérico adopta una estructura de dos puertos en los que se separan lógicamente la información administrativa de solicitud/respuesta y la información de Datos Retenidos. En particular, un primer puerto de Interfaz de Transferencia HI-A 25 puede estar configurado para transportar varios tipos de información administrativa, de solicitud y respuesta de/a la Autoridad Solicitante 24 y una organización en el Proveedor de Servicios de Comunicación 21 que es responsable de los asuntos de Datos Retenidos, identificados por una Función de Administración 27.

Un segundo Interfaz de Transferencia HI-B 26 puede estar configurado para transportar la información de datos retenidos almacenada en un depósito 29 del Proveedor de Servicios de Comunicación 21 a la Autoridad Solicitante 24. Los parámetros individuales de los datos retenidos deben ser enviados a la Autoridad Solicitante 24 al menos una vez, si están disponibles. Con este fin, se puede proporcionar una función de Mediación/Entrega 28, para recuperar del depósito 29 los datos retenidos y enviar dichos datos a la Autoridad Solicitante 24 en un formato adecuado por medio del HI-B 26.

Un segundo aspecto de la presente invención se describe ahora con respecto al diagrama de flujo de datos de la figura 5.

La figura 5 muestra tres elementos de red: el nodo 200, que puede ser un Nodo Servidor de Soporte de GPRS 3 o una Pasarela Servidora 4, una Función de Entrega 2 (DF2) 15 y una Función de Entrega 3 (DF3) 18.

El nodo 200 puede enviar Información Relativa a la Interceptación (IRI) por medio de un interfaz X2 a DF2 15. La Información Relativa a la Interceptación puede incluir un valor de parámetro a partir del cual se puede determinar una ruta del tráfico del usuario.

Tal valor de parámetro puede ser, por ejemplo, un Nombre del Punto de Acceso (APN) que se utilizará en la siguiente descripción.

En la etapa 300, la DF2 15 comprueba el Nombre del Punto de Acceso, que en la etapa 310 evalúa si el Nombre del Punto de Acceso está relacionado con una Pasarela de Red de Datos en Paquetes en la misma Red Pública Móvil Terrestre.

En este caso, en la etapa 320 la DF2 15 descarta los datos de la Información Relativa a la Interceptación. Además, la DF2 15 envía un mensaje a la DF3 18 que ordena filtrar los correspondientes el Contenido de los datos de la Comunicación (CC).

En la etapa 330, los datos del Contenido de la Comunicación son entonces filtrados por la DF3 18.

De acuerdo con este segundo aspecto de la invención, los datos interceptados procedentes del nodo se descartan cuando los mismos datos han sido interceptados o retenidos en un nodo diferente cruzado por el mismo tráfico del Equipo de Usuario 1.

Se ha mostrado que la invención consigue totalmente el objeto propuesto y el resto de objetivos, puesto que evita activar, mantener o entregar múltiples casos de productos de interceptación para el mismo abonado objetivo, lo que mejora el rendimiento de los nodos implicados en la Interceptación Legal, tanto en el lado del operador como en el de la Agencia de Cumplimiento de la Ley, en términos de utilización de los recursos, incluyendo el ancho de banda y el tamaño del almacenamiento.

En particular la invención permite ahorrar capacidad de Interceptación Legal en los Nodos Servidores de Soporte de GPRS 3 y en los Nodos de Pasarelas Servidoras 4.

El ahorro en la capacidad de la Interceptación Legal se logra también en el procesamiento en las DF/MF, lo mismo que el filtrado se puede realizar en el Nodo Servidor de Soporte de GPRS directamente, sin implicar a las DF/MF en el filtrado. El ahorro de capacidad de Interceptación Legal se obtendrá consecuentemente en la LEMF.

Además la invención permite el ahorro del ancho de banda en los interfaces de Interceptación Legal entre un Nodo Servidor de Soporte de GPRS y las DF/MF (interfaces X), puesto que el filtrado se hace en el elemento de la red y, en consecuencia, en los interfaces HI entre las DF/MF y la LEMF.

Los ahorros de la capacidad y del ancho de banda dan lugar a reducir los costos de transmisión para la aplicación de la Ley, lo cual, también es muy conveniente para las Agencias de Aplicación de la Ley.

Claramente, diversas modificaciones serán evidentes y las podrán realizar fácilmente los expertos en la técnica sin apartarse del alcance de la presente invención.

Donde las características técnicas mencionadas en cualquier reivindicación son seguidas por signos de referencia, esos signos de referencia se han incluido con el propósito de aumentar la inteligibilidad de las reivindicaciones, y de acuerdo con ello, tales signos de referencia no tienen ningún efecto limitante en la interpretación de cada elemento identificado a modo de ejemplo por tales signos de referencia.

REIVINDICACIONES

1. Un método para reducir el consumo de recursos para la interceptación legal o retención de datos relativos al tráfico relacionado con un móvil objetivo 2G/3G conectado a una red de telecomunicaciones que interactúa con el Sistema Evolucionado de Paquetes, comprende las etapas de:

- en un primer nodo, detectar (200, 300) al menos un valor de parámetro en los datos para los cuales se ha activado la Interceptación Legal o la retención de datos basándose en dicho al menos valor de parámetro, evaluando (211, 310) si dicho tráfico es interceptado o retenido en un segundo nodo cruzado por dicho tráfico en la misma red;

- filtrar (212, 320) las solicitudes legales de interceptación o los datos interceptados si dicho segundo nodo está situado aguas abajo de dicho primer nodo.

2. El método de acuerdo con la reivindicación 1, en el que dicho valor de parámetro es un Nombre del Punto de Acceso.

3. El método de acuerdo con las reivindicaciones 1 ó 2, en el que dicho primer nodo es un Nodo Servidor de Soporte de GPRS (3) y dicho segundo nodo es una Pasarela Servidora (4).

4. El método de acuerdo con las reivindicaciones 1 ó 2, en el que dicho primer nodo es una Pasarela Servidora (4) y dicho segundo nodo es una Pasarela de Red de Datos en Paquetes (5)

5. El método de acuerdo con las reivindicaciones 1 ó 2, en el que dicho primer nodo es un Nodo Servidor de Soporte de GPRS (3) y dicho segundo nodo es una Pasarela de Red de Datos en Paquetes (5).

6. El método de acuerdo con las reivindicaciones 4 ó 5, en el que dicha Pasarela de Red de Datos en Paquetes (5) está situada en la misma red y en el mismo país que dicho primer nodo.

7. El método de acuerdo con cualquiera de las reivindicaciones 1 a 6, en el que dicha etapa de filtrar (212, 320) las solicitudes de interceptación legal incluye descartar las peticiones de interceptación legal antes de aplicar la interceptación o la retención de datos.

8. El método de acuerdo con las reivindicaciones 2 y 7, en el que dicha etapa de descartar las solicitudes de interceptación legal antes de aplicar la interceptación o la retención de datos se basa en si dicho Nombre del Punto de Acceso solicita el uso de una pista S4.

9. El método de acuerdo con cualquiera de las reivindicaciones 1 a 6, en el que dicha etapa de filtrar (212, 320) las solicitudes de interceptación legal incluye descartar los datos interceptados.

10. El método de acuerdo con la reivindicación 9, en el que dicha etapa de descartarlos datos interceptados incluye:

-verificar la Información Relativa Interceptada recibida en una función DF2/MF2;

- si dicho tráfico es interceptado o retenido en el segundo nodo cruzado por dicho tráfico en la misma red: descartando dichos IRIs y descartando la correspondiente Comunicación del Contenido recibida en una función DF3/MF3.

11. Un sistema de Interceptación Legal (10) para la interceptación o retención de datos relativos al tráfico asociado con un equipo de usuario objetivo (1) en una red de telecomunicaciones 2G/3G que interactúa con el Sistema Evolucionado de Paquetes, en el que al menos un primer nodo y al menos un segundo nodo están configurados para operar como Elementos de Control de Interceptación (11) o como fuentes de Retención de Datos (22), en el que dicho primer nodo está configurado para detectar al menos un valor de parámetro en los datos para los cuales se ha activado la interceptación legal o la retención de datos y, basándose en dicho valor de parámetro, filtrar las solicitudes de interceptación legal o los datos interceptados si dicho segundo nodo está situado aguas abajo de dicho primer nodo.

12. El sistema de Interceptación Legal (10) de acuerdo con la reivindicación 11, en el que dicho valor de parámetro es un Nombre del Punto de Acceso.

13. El sistema de Interceptación Legal (10) de acuerdo con las reivindicaciones 11 ó 12, en el que dicho primer nodo es un Nodo Servidor de Soporte de GPRS (3) y dicho segundo nodo es una Pasarela Servidora (4).

14. El sistema de Interceptación Legal (10) de acuerdo con las reivindicaciones 11 ó 12, en el que dicho primer nodo es una Pasarela Servidora (4) y dicho segundo nodo es una Pasarela de Red de Datos en Paquetes (5).

15. El sistema de Interceptación Legal (10) de acuerdo con las reivindicaciones 11 ó 12, en el que dicho primer nodo es un Nodo Servidor de Soporte de GPRS (3) y dicho segundo nodo es una Pasarela de Red de Datos en Paquetes (5).

16. El sistema de Interceptación Legal (10) de acuerdo con las reivindicaciones 11 ó 12, en el que dicha Pasarela de Red de Datos en Paquetes (5) está situada en la misma red y en el mismo país que dicho primer nodo.

17. Un Nodo Servidor de Soporte de GPRS (3) configurado para funcionar como Elemento de Control de Interceptación (11) o como fuente de Retención de Datos (22) para un sistema de Interceptación Legal (10), en el que dicho Nodo Servidor de Soporte de GPRS (3) está configurado para:

- detectar (200, 300) al menos un valor de parámetro en los datos para los cuales se ha activado la interceptación legal o la retención de datos,

- basándose en dicho valor de parámetro, evaluar (211, 310) si dicho tráfico es interceptado o retenido en un segundo nodo cruzado por dicho tráfico en la misma red y filtrar (212,320) las solicitudes de interceptación legal o los datos interceptados si dicho segundo nodo está situado aguas abajo de dicho Nodo Servidor de Soporte de GPRS (3)

18. Una Pasarela servidora (4) configurada para operar como Elemento de Control de Interceptación (11) o como fuente de Retención de Datos (22) para un sistema de Interceptación Legal (10), en el que dicha Pasarela Servidora (4) está configurada para:

- detectar (200, 300) al menos un valor del parámetro en los datos para los cuales se ha activado la Interceptación Legal o la retención de datos,

- basándose en dicho valor del parámetro, evaluar (211, 310) si dicho tráfico es interceptado o retenido en un segundo nodo cruzado por dicho tráfico en la misma red y filtrar (212, 320) las solicitudes de interceptación legal o los datos interceptados si dicho segundo nodo está situado aguas abajo de dicha Pasarela Servidora (4)

19. Una red de telecomunicaciones que comprenda el sistema de Interceptación Legal (10) de acuerdo con la reivindicación 11.

20. Un programa de ordenador cargable en un Nodo Servidor de Soporte de GPRS(3) para configurar dicho Nodo Servidor de Soporte de GPRS (3) como Elemento de Control de Interceptación (11) o fuente de retención de Datos (22) operable en un sistema de Interceptación Legal (10), de modo que dicho Nodo de Soporte de GPRS de Servicio (3) está adaptado para llevar a cabo las etapas de:

- detectar (200, 300) al menos un valor de parámetro en los datos para los cuales se ha activado la Interceptación Legal o la retención de datos

- basándose en dicho valor de parámetro, evaluar (211, 310) si dicho tráfico es interceptado o retenido en un segundo nodo cruzado por dicho tráfico en la misma red y filtrar (212, 320) las solicitudes de interceptación legal o datos interceptados si dicho segundo nodo está situado aguas abajo de dicho Nodo Servidor de Soporte de GPRS (3).

21. Un programa de ordenador cargable en una Pasarela Servidora (4) para configurar dicha Pasarela Servidora (4) como Elemento de Control de Interceptación (11) o como fuente de Retención de Datos (22) operable en un Sistema de Interceptación Legal (10), de manera que dicha Pasarela Servidora (4) está adaptada para realizar las etapas de:

- detectar (200, 300) al menos un valor de parámetro en los datos para los cuales se ha activado la Interceptación Legal o la retención de datos,

- basándose en dicho valor de parámetro, evaluar (211, 310) si dicho tráfico es interceptado o retenido en un segundo nodo cruzado por dicho tráfico en la misma red y filtrar (212, 320) las solicitudes de interceptación legal los datos interceptados si dicho segundo nodo está situado aguas abajo de dicha Pasarela Servidora (4).

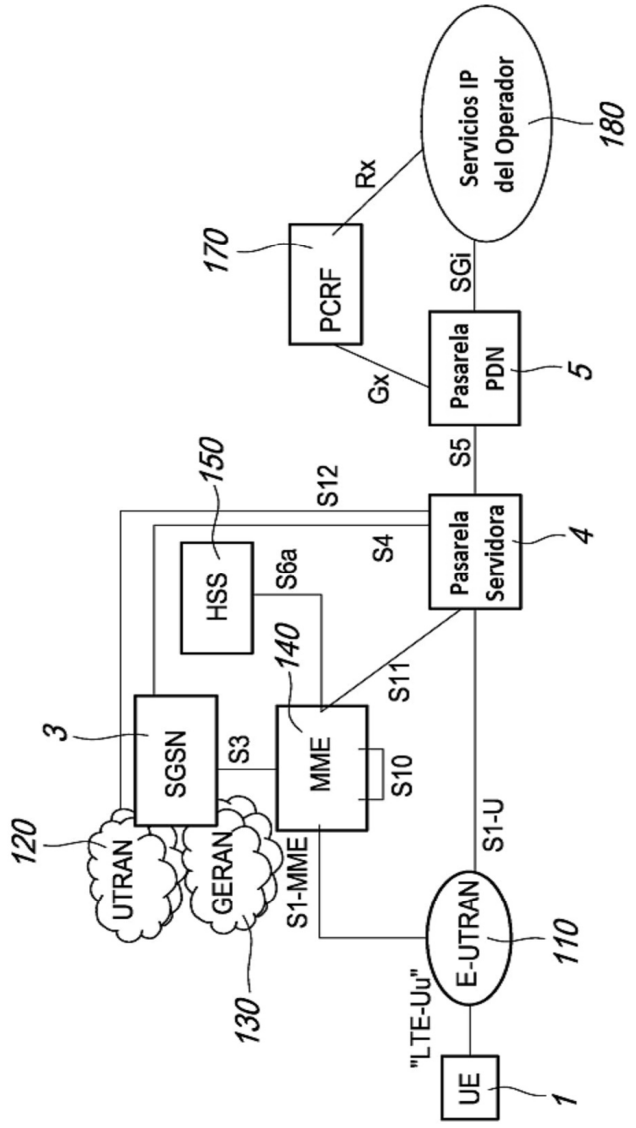
Servicios IP del Operador
180
Rx
PCRF
170
SGi
Gx
Pasarela PDN
5
S5
150
S12
Pasarela Servidora
4
S4
HSS
S6a
140
S11
3
SGSN
S3
MME
S10
120
UTRAN
GERAN
S1-MME
S1-U
130
E-UTRAN
110
"LTE-Uu"
UE
1

Fig. 1

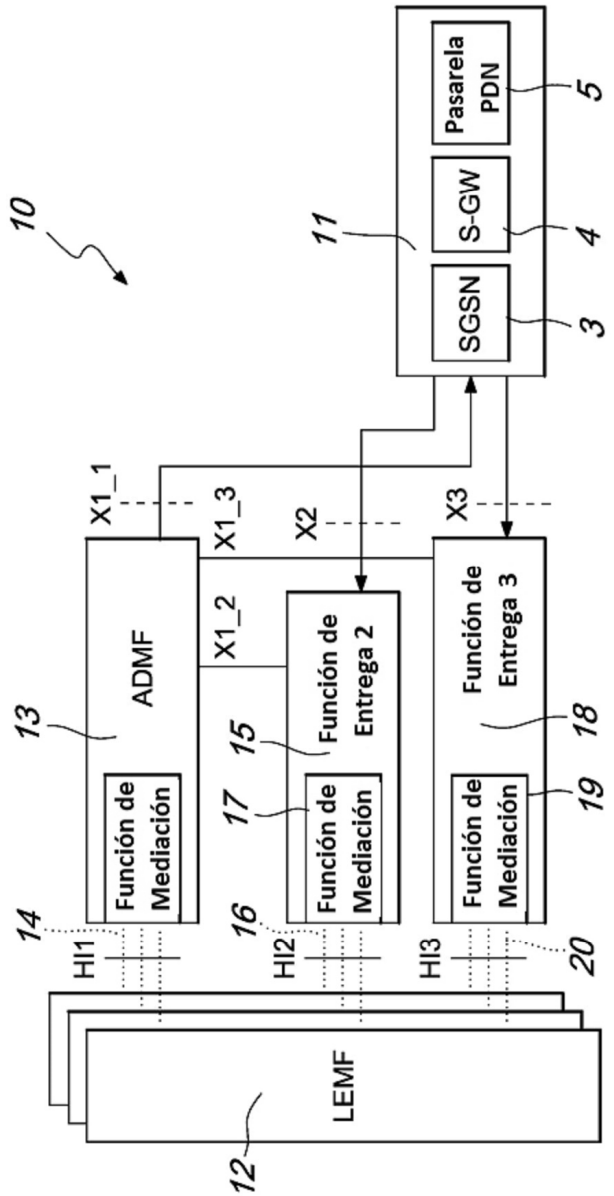
10
11
Pasarela PDN
5
S-GW
4
SGSN
3
X1_1
X1_3
X2
X3
X1_2
ADMF
13
Función de Mediación
14
Función de Entrega 2
15
Función de Mediación
17
16
Función de Entrega 3
18
Función de Mediación
19
20
HI1
HI2
HI3
LEMF
12

Fig. 2

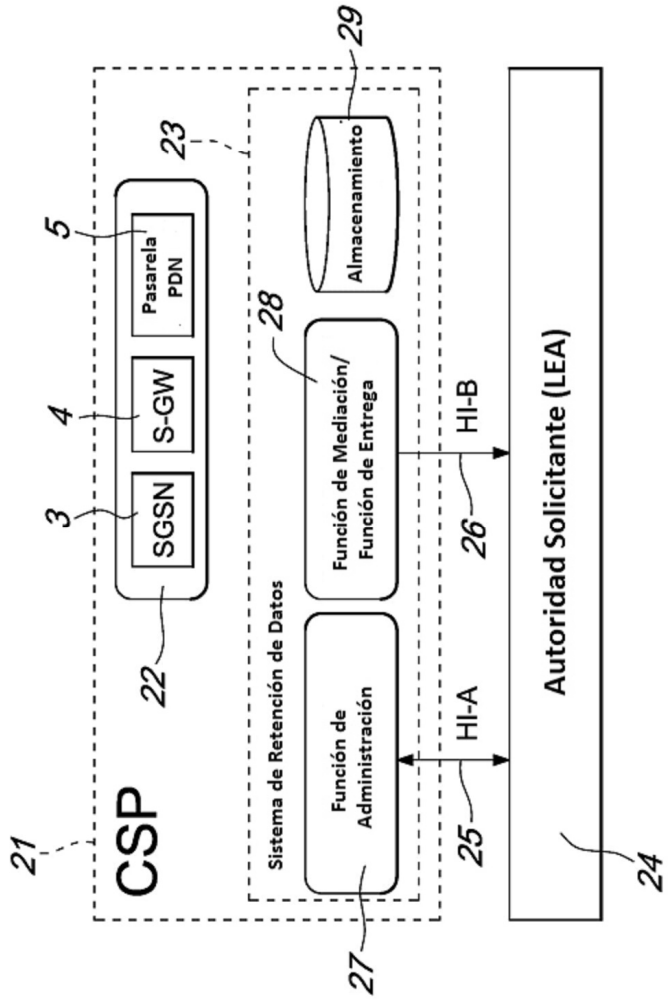
21
CSP
22
23
3
SGSN
4
S-GW
5
Pasarela PDN
Sistema de Retención de Datos
Función de Administración
27
28
Función de Mediación/ Función de Entrega
29
Almacenamiento
HI-A
25
HI-B
26
Autoridad Solicitante (LEA)
24

Fig. 3

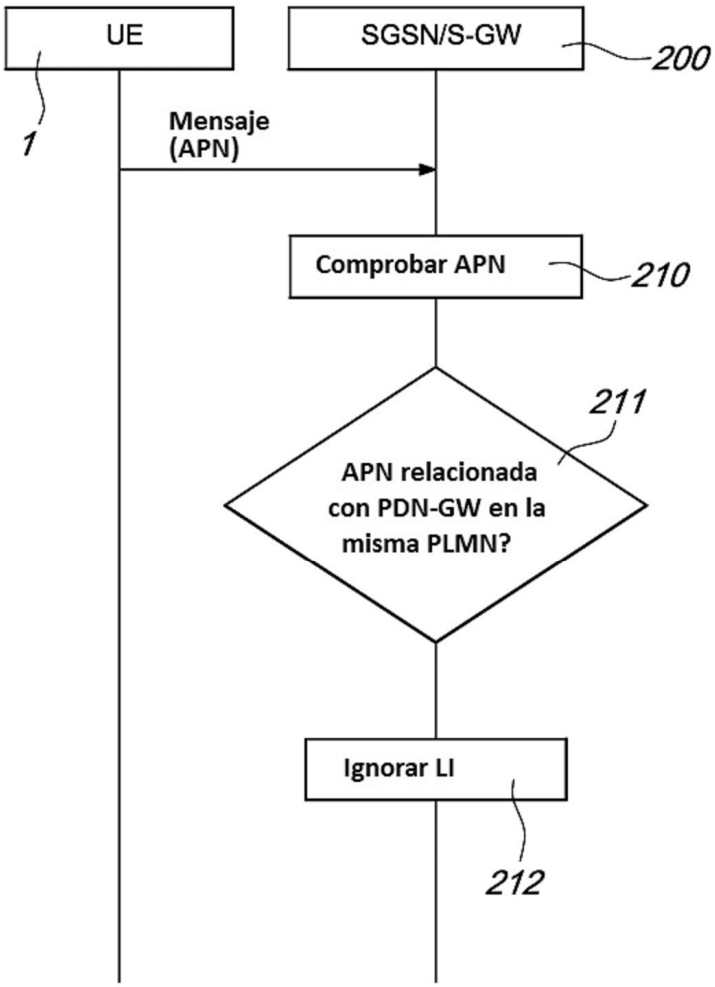
UE
SGSN/S-GW
200
1
Mensaje
(APN)
Comprobar APN
210
211
APN relacionada
con PDN-GW en la
misma PLMN?
Ignorar LI
212

Fig. 4

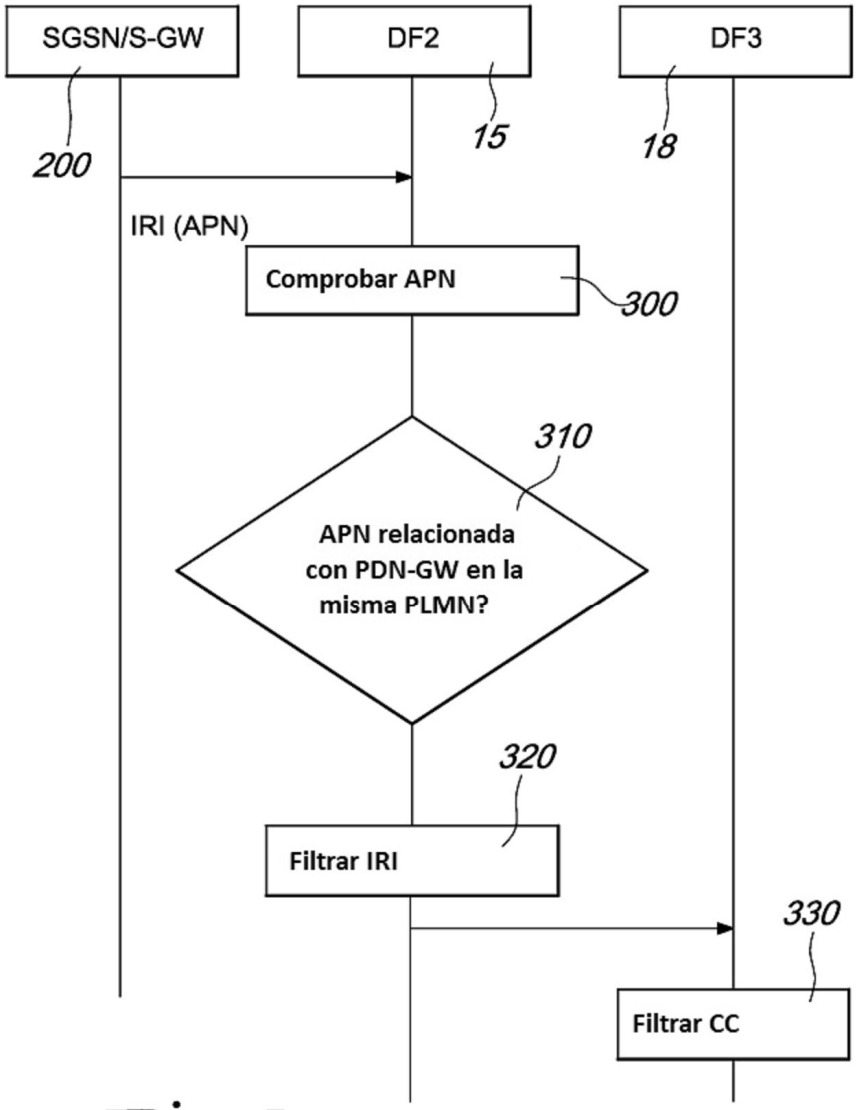
SGSN/S-GW
DF2
DF3
200
15
18
IRI (APN)
Comprobar APN
300
310
APN relacionada con PDN-GW en la misma PLMN?
320
Filtrar IRI
330
Filtrar CC

Fig. 5