(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 795 699**

(51) Int. CI.:

H04W 12/12 (2009.01)
H04L 29/06 (2006.01)
H04Q 3/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **01.12.2015 E 15196421 (0)**

(97) Fecha y número de publicación de la concesión europea: **06.05.2020 EP 3029973**

(54) Título: **Procedimiento y un dispositivo para asegurar una interfaz de sistema de señalización nº 7**

(30) Prioridad:

02.12.2014 DE 102014117713

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.11.2020

(73) Titular/es:

GSMK GESELLSCHAFT FÜR SICHERE MOBILE KOMMUNIKATION MBH (100.0%)
Marienstrasse 11
10117 Berlin, DE

(72) Inventor/es:

ENGEL, TOBIAS y
FREYTHER, HOLGER

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento y un dispositivo para asegurar una interfaz de sistema de señalización nº 7

La invención se refiere a un procedimiento y a un dispositivo para asegurar una interfaz de sistema de señalización nº 7, interfaz SS7, que posibilita un acceso a una red de radiotelefonía móvil local, con respecto a un sistema externo.

Campo de la invención

El sistema de señalización nº 7 (designado en adelante como SS7) fue estandarizado en los años 70 por la UIT y sirve como protocolo de conmutación para el establecimiento de conexiones telefónicas.

El SS7 es una colección de protocolos y procedimientos para la señalización en redes de telecomunicaciones. Se utiliza en la red telefónica pública, en relación con RDSI, red de radiotelefonía fija y móvil, y desde aproximadamente el año 2000 también se ha intensificado el uso en redes VoIP. En las redes VoIP, el SS7 solo se utiliza en relación con *Media Gateway Controller* (Controladores de Pasarela de Medios). La colección de protocolos también se conoce, entre otras designaciones, como *Signalling System Number 7*, sistema de señalización nº 7, sistema de señalización central nº 7, SSC7, sistema de señalización CCITT nº 7, *Central Signalling System # 7* y C7.

La UIT-T (anteriormente CCITT) elabora propuestas detalladas para la implementación de redes de señalización nacionales e internacionales bajo la designación "ITU-T Recommendation Q.xxx" en las series Q.600 y Q.700. Organizaciones de normalización, como ETSI (*European Telecommunication Standarisation Institute* - Instituto Europeo de Normas de Telecomunicaciones) o ANSI (*American National Standarisation Institute* - Instituto Nacional Americano de Normalización) así como IETF (*Internet Engineering Task Force* - Grupo de Trabajo de Ingeniería de Internet), transforman las propuestas mediante RFC en normas vinculantes.

El SS7 es actualmente el sistema de señalización más común, y frecuentemente el único, en redes de telecomunicaciones nacionales e internacionales. Debido a esta popularidad se han especificado, desarrollado y utilizado diversos protocolos de la pila de SS7 para SS7oIP (*Signalling System Over Internet Protocol* - Sistema de Señalización Sobre Protocolo de Internet).

Los dispositivos de telecomunicaciones, como conmutadores o pasarelas, funcionan con pilas de protocolos SS7 que están adaptadas a las normas nacionales o especificaciones de los proveedores de servicios individuales. Como la mayoría de las recomendaciones UIT-T, las series Q.600 y Q.700 están estructuradas de forma muy variable y permiten numerosas variaciones. Por ello, a diferencia por ejemplo de IP, no existe ninguna pila de protocolos SS7 unificada, sino implementaciones específicas.

El SS7 es un sistema de señalización central o "*Common Channel Signalling System*" (Sistema de Señalización de Canal Común). Un único canal en un sistema de transmisión (normalmente un sistema múltiplex) transmite las informaciones de señalización para todos los canales de usuario (*bearer channels*) o canales de voz. Esta información de señalización puede incluir, por ejemplo, información sobre números llamados o llamantes, tasas, ocupado, número de llamada desconocido, etc.

El SS7 es un protocolo de alta eficiencia que, en comparación con otros tipos de comunicación, requiere cantidades de datos relativamente pequeñas.

En las redes de comunicaciones móviles, la proporción de señalización es muy alta debido a la movilidad y al uso de SMS. En la red fija, pero sobre todo en la red móvil, existen sistemas que solo presentan conexiones de señalización, como por ejemplo un centro de SMS (SMSC, por sus siglas en inglés).

El SS7 ofrece procedimientos para corregir errores lo más rápidamente posible y para encontrar vías alternativas. Los tiempos de conmutación en caso de error o en caso de fallo de un nodo son en general del orden de unos milisegundos.

Los componentes más importantes del SS7 son recomendaciones que describen diferentes aspectos parciales del modelo de comunicación complejo (véase la figura 10).

MTP - Partes de Transferencia de Mensajes

La MTP (por sus siglas en inglés) o Parte de Transferencia de Mensajes describe cómo se transmiten informaciones de señalización. A ello pertenecen definiciones de las interfaces eléctricas u ópticas, detalles sobre cómo se separan los mensajes individuales entre sí y cómo se direccionan comunicaciones individuales o mejor, en la jerga de la UIT-T, *signalling points* (puntos de señalización).

El nivel 1 de MTP establece los parámetros físicos, eléctricos y funcionales para una ruta de señalización. A ello pertenecen especificaciones como frecuencia de reloj, tensiones, procedimientos de codificación así como dimensiones y forma de los conectores. Habitualmente se trata de interfaces que corresponden a las recomendaciones V.35 o G.703. El nivel 1 representa la capa física para una ruta de señalización, que en una red digital consiste normalmente en un canal de 64 kbit/s.

El nivel 2 de MTP establece los procedimientos para un intercambio sin errores de mensajes a través de una ruta de señalización. A ello pertenecen funciones para activar o finalizar la conexión de mensajes, examinar la misma en busca de errores y en caso dado corregir los mismos. Los mensajes se separan entre sí mediante marcas. El nivel 2 es similar en su estructura a procedimiento HDLC frecuentemente utilizado, pero ampliado en algunas funciones.

El nivel 3 de MTP define la cooperación de varias rutas de señalización individuales. Todos los aspectos que son comunes en un plano lógico para el intercambio de mensajes entre dos puntos de señalización a través de varias rutas de señalización se regulan. A ello pertenece el encaminamiento de mensajes entrantes a la ruta de señalización deseada. La separación de estas funciones en un nivel 3 propio sirve también para la administración de la red de señalización: se pueden añadir rutas de señalización o, en caso de fallo, se puede conmutar a una ruta alternativa, sin que sea necesario cambiar la configuración en planos superiores más abstractos.

Conexiones E1 LSL y HSL: Los E1 LSL se han utilizado desde la introducción del SS7. LSL (*Low Speed Link* - Enlace de Baja Velocidad) designa las conexiones en las que se utilizan intervalos de tiempo de 64 kbit/s. Dado que por cada conjunto de enlaces solo se pueden conectar 16 intervalos de tiempo, el ancho de banda está correspondientemente limitado. Esto da como resultado un ancho de banda de solo 1 Mbit/s por cada conjunto de enlaces. Desde hace algún tiempo se han especificado los HSL (*High Speed Link* - Enlace de Alta Velocidad). Los HSL permiten un ancho de banda de 2 Mbit/s por cada intervalo de tiempo, lo que para un conjunto de enlaces daría como resultado un ancho de banda teórico de 32 Mbit/s. Los HSL se utilizan cuando el ancho de banda con LSL es demasiado pequeño. Sin embargo, dado que el HSL es muy caro, el HSL solo se utiliza por ejemplo cuando el SS7oIP, la alternativa más económica, (todavía) no es factible debido a la falta de posibilidades de conexión en la red.

Conjunto de enlaces designa la conexión lógica entre dos *Signalling Point Codes* (SPC) (Códigos de Puntos de Señalización). Los conjuntos de enlaces se utilizan únicamente en conexiones E1, pero no en SS7oIP. La limitación a 16 intervalos de tiempo por conjunto de enlaces se debe a la falta de bits para el SLC en UIT, dado que el SLC (*Signalling Link Code* - Código de Enlace de Señalización) solo presenta 4 bits. Sin embargo, en la norma ANSI hay 8 bits disponibles para el SLC, lo que entonces posibilita 256 intervalos de tiempo. Sin embargo, cuando entre dos códigos de puntos ha de haber disponibles más intervalos de tiempo (ancho de banda) y no es posible el HSL, se ha de establecer un segundo conjunto de enlaces. Para que esto sea posible, en el *Signalling Transfer Point* (STP) (Punto de Transferencia de Señalización) se ha de configurar *Capability Pointcode* (Código de Puntos de Capacidad), que permite definir otro conjunto de enlaces.

En las Partes de Usuario se describen las funciones que están disponibles para un usuario. Estas funciones pueden depender del servicio utilizado (RDSI, teléfono analógico, radiotelefonía móvil) y, por lo tanto, se describen por separado. Las Partes de Usuario más importantes son:

La TUP (por sus siglas en inglés) - Parte de Usuario de Telefonía es la Parte de Usuario más sencilla, que solo describe funciones básicas. A ello pertenecen informaciones como establecimiento de conexión (llamar), corte de conexión (colgar), ocupado o número de llamada desconocido.

La ISUP (por sus siglas en inglés) - Parte de Usuario de RDSI describe las funciones que están disponibles para los usuarios de RDSI. A ello pertenece como elemento más importante la descripción del servicio o capacidad portadora. La RDSI permite operar diferentes terminales, como teléfono, fax u ordenador, en la misma conexión. En caso de una conexión en la RDSI siempre se envía conjuntamente una descripción del tipo de servicio para que solo responda el terminal que soporta el servicio deseado. De este modo se evita, por ejemplo, que un aparato de fax intente aceptar una conexión de voz cuando los dos terminales tienen capacidad RDSI.

La DUP (por sus siglas en inglés) - Parte de Usuario de Datos está concebida para transmitir informaciones especiales para conexiones de datos.

La parte más utilizada actualmente es ISUP.

La Parte de Control de Conexión de Señalización (SCCP, por sus siglas en inglés) es una capa que se apoya en el nivel 3 de MTP y permite una señalización de extremo a extremo en la red de señalización. En la SCCP se ponen a disposición cuatro clases de servicio:

Clase 0: Servicio básico sin conexión: Los mensajes más largos se pueden dividir. La composición correcta de estas partes tiene lugar entonces en capas superiores.

Clase 1: Servicio sin conexión con números secuenciales: Este número (código SLS) tiene una longitud de 4 u 8 bits (norma UIT-T o ANSI). Los mensajes pertenecientes al mismo grupo utilizan el mismo código SLS. Si se utilizan varias conexiones (conjunto de enlaces) para un mensaje, el número secuencia se diferencia en los bits de menor valor.

Clase 2: Servicio básico orientado a la conexión: La conexión de señalización se ha de establecer y cortar.

Clase 3: Servicio básico orientado a la conexión con control de flujo.

La Parte de Aplicación de Capacidades de Transacción (TCAP, por sus siglas en inglés) se apoya en la SCCP y permite que los protocolos suprayacentes, como por ejemplo INAP, CAP, MAP y PAOM, comuniquen en todo el mundo a través de la red SS7. Éstos se explican a continuación.

A través de la Parte de Aplicación de Red Inteligente (INAP, por sus siglas en inglés) se desarrollan las funciones para redes inteligentes (IN, por sus siglas en inglés). A ello pertenecen, entre otros, la Portabilidad del Número Local (LNP - *Local Number Portability*) o los números 0800, que son transmitidos a la central más próxima en función de la ubicación de la persona que llama.

La Parte de Aplicación CAMEL (CAP, por sus siglas en inglés) se utiliza en redes de radiotelefonía móvil y sirve para las *Customised Applications for Mobile networks Enhanced Logic* (CAMEL) (Aplicaciones Personalizadas para Lógica Mejorada de redes Móviles).

La MAP (por sus siglas en inglés) (Parte de Aplicación de Móviles) sirve para la comunicación entre los diferentes componentes de la red de radiotelefonía móvil (entre otros, HLR, VLR, SMSC). El estándar también puede ser utilizado para la comunicación entre redes de radiotelefonía móvil de diferentes proveedores y, por lo tanto, es una de las condiciones para la funcionalidad de itinerancia (*roaming*). Por medio de la itinerancia, un abonado de radiotelefonía móvil se puede registrar en redes exteriores (por ejemplo un operador de servicios móviles extranjero con contrato de itinerancia o para poder realizar llamadas de emergencia aunque el abonado de radiotelefonía móvil no se encuentre en el área de servicio del operador propio). Los componentes relevantes para la facturación se transmiten a través de *Transferred Account Procedure* (TAP) (Procedimiento Contable Transferido).

Los mensajes cortos (SMS, por sus siglas en inglés) también se transmiten en la MAP, además de la itinerancia y el control de las conexiones de voz. Además, en la MAP también se transmiten funciones para determinar el tipo de aparato y la IMEI, con el fin de poder transmitir configuraciones específicas del teléfono móvil desde el operador de telefonía móvil hasta el terminal.

La Parte de Operaciones, Mantenimiento y Administración (OMAP, por sus siglas en inglés) proporciona funciones para operación, mantenimiento y administración, por ejemplo incluyendo mantenimiento de *software*, configuración y establecimiento de bloques de números de llamada para abonados de radiotelefonía móvil.

Concebido originalmente para la señalización en caso de conexiones de red fija, el SS7 se amplió en los años 80 y 90 con muchos suplementos para soportar redes de radiotelefonía móvil, con el fin de posibilitar, por ejemplo, SMS, itinerancia, prepago y tráfico de datos. Al mismo tiempo, entre tanto ya no solo las compañías de telecomunicaciones estatales tienen acceso al SS7, sino también miles de compañías y proveedores más pequeños.

Una parte de protocolo de SS7 que se encarga de la mediación de comunicaciones móviles es la SS7/MAP (Parte de Aplicación de Móviles). La SS7/MAP se utiliza tanto dentro de la estructura de red de un proveedor de radiotelefonía móvil como en la comunicación de los proveedores de radiotelefonía móvil entre sí, por ejemplo para la itinerancia. Aquí, debido al desarrollo histórico del protocolo SS7 y a una implementación insuficiente de mecanismos de protección en elementos de red, existen puntos de ataque por usuarios de SS7 externos. Éstos pueden ser utilizados en los proveedores de radiotelefonía móvil para la realización de fraude, violación de la intimidad de los clientes de radiotelefonía móvil hasta la escucha de conversaciones por radiotelefonía móvil, y también representan un riesgo de seguridad para las redes de señalización SS7 internas de los proveedores de radiotelefonía móvil.

La Parte de Aplicación de Móviles (MAP) es un protocolo SS7 que proporciona una capa de aplicación para los diferentes nodos en redes de núcleo móviles GSM y UMTS y redes de núcleo GPRS para comunicarse entre sí con el fin de poder proporcionar prestaciones de servicios para usuarios de móviles. La Parte de Aplicación de Móviles es la capa de aplicación utilizada para poder acceder al Registro de Posición Propia (HLR, por sus siglas en inglés), al Registro de Posiciones de Visitantes (VLR, por sus siglas en inglés), al Centro de Conmutación Móvil (MSC, por sus siglas en inglés), al Registro de Identidad de Equipo (EIR, por sus siglas en inglés), al Centro de Autentificación (AuC, por sus siglas en inglés), al Centro de Servicio de Mensajes Cortos (SMSC) y al Nodo de Soporte GPRS de Servicio (SGSN, por sus siglas en inglés).

Los servicios esenciales previstos por la MAP son:

Servicios de movilidad: gestión de ubicación (para soportar la itinerancia), autentificación, administración de informaciones de abono de servicios, corrección de errores.

Operación y mantenimiento: seguimiento de abonados de radiotelefonía móvil, la llamada a una IMSI de abonado de radiotelefonía móvil.

Administración de llamadas: enrutamiento, procesamiento de llamadas en la itinerancia, comprobación de la disponibilidad de un abonado de radiotelefonía móvil para recibir llamadas.

Servicios adicionales.

Servicio de mensajes cortos.

Prestaciones de servicios de protocolo de datos por paquetes (PDP) para GPRS: provisión de información de enrutamiento para conexiones GPRS.

Servicios de gestión de servicio de localización: obtención de la ubicación del abonado de radiotelefonía móvil.

Las especificaciones de la Parte de Aplicación de Móviles, que originalmente fueron definidas por la asociación GSM, están controladas ahora por ETSI/3GPP. La MAP se define mediante dos estándares diferentes, en función del tipo de red móvil:

La MAP para GSM (antes de la versión 4) está especificada por 3GPP TS 09.02. La MAP para UMTS ("3G") y GSM (versión 99 o superior) está especificada por 3GPP TS 29.002.

En redes de radiotelefonía móvil basadas en normas ANSI (actualmente CDMA2000, en los últimos AMPS, IS-136 y cdmaOne), la función de la MAP es desempeñada por un protocolo similar, por regla general designado como IS-41 o ANSI-41 (ANSI MAP). Desde el año 2000 es mantenida por 3GPP2 como N.S0005 y desde 2004 se llama 3GPP2 X.S0004.

La MAP es un usuario de la Parte de Aplicación de Capacidades de Transacción (TCAP) y, como tal, puede ser transportada con protocolos SS7 "tradicionales" o a través de IP con Parte de Control de Conexión de Señalización independiente del transporte (SCCP-IT), o con SIGTRAN.

En redes de radiotelefonía móvil como GSM y UMTS se utiliza la MAP de aplicación SS7. Las conexiones de voz son aplicaciones con Conmutación de Circuitos (CS, por sus siglas en inglés) y las conexiones de datos son aplicaciones con Conmutación por Paquetes (PS, por sus siglas en inglés). El termina móvil se designa como ME (por sus siglas en inglés). SCF (por sus siglas en inglés) significa Función de Control de Servicio.

Algunas interfaces con Conmutación de Circuitos GSM/UMTS en el Centro de Conmutación Móvil (MSC), que son transportadas a través de SS7, incluyen las siguientes:

B → VLR (utiliza MAP/B). La mayor parte de los MSC están asignados a un Registro de Posiciones de Visitantes (VLR), de modo que la interfaz B es "interna".

C → HLR (utiliza MAP/C) la interfaz C desarrolla las notificaciones entre MSC y HLR.

D → HLR (utiliza MAP/D) para la conexión con la red CS y para actualizaciones de ubicación.

E → MSC (utiliza MAP/E) para transferencias inter-MSC.

F → EIR (utiliza MAP/F) para comprobaciones de identidad de aparatos.

H → SMSC (utiliza MAP/H) para Servicio de Mensajes Cortos (SMS) a través de CS.

I → ME (utiliza MAP/I) notificaciones entre MSC y ME desarrolladas por la interfaz I.

J → SCF (utiliza MAP/J) la interfaz J desarrolla las notificaciones entre HLR y gsmSCF.

También existen varias interfaces GSM/UMTS PS en el Nodo de Soporte GPRS de Servicio (SGSN), que son transportadas a través de SS7:

Gr → HLR para la conexión de la red PS y la actualización de ubicación.

Gd → SMS-C para SMS a través de PS.

Gs → MSC para señalización combinada CS + PS a través de PS.

Ge → Carga prepagada de tasas para aplicaciones específicas de cliente para lógica mejorada en redes de radiotelefonía móvil (CAMEL/Aplicaciones Personalizadas para Lógica Mejorada de redes Móviles).

Gf → EIR para la comprobación de identidad de aparatos.

Por las publicaciones US 2005/0232 236 A1, US 2001/0046856 A1, US 6,889,328 B1, US 2013/0095793 A1 y US 2010/0105355 A1, US 2011/014939 A1, WO 2014/187969 A1, US 2011/041176 A1, US 5 345 595 A se conocen procedimientos para la protección de redes. Las funciones indicadas no pretenden ser completas, sino que únicamente han de describir la funcionalidad, que se abordará más abajo.

Debido a la multiplicidad de componentes, de operadores de red diferentes y también de fabricantes, se pueden producir ataques a la infraestructura de red de los proveedores de radiotelefonía móvil.

Compendio de la invención

La presente invención describe un sistema de protección que, mediante la combinación de varios procedimientos, protege los accesos a la red SS7 de proveedores de telecomunicaciones contra ataques SS7/MAP detectando y filtrando los mismos. (Figura 1).

Las propiedades de la presente invención se determinan mediante las reivindicaciones adjuntas.

En particular, la invención se refiere a un procedimiento para asegurar una interfaz de sistema de señalización nº 7, interfaz SS7, de un sistema, a través de la cual tiene lugar un acceso a una red de radiotelefonía móvil local, con respecto a un sistema externo, que incluye una o más de las siguientes etapas de análisis:

a) determinar si una SS7/MAP-MSU, Unidad de Señal de Mensaje de Parte de Aplicación de Móviles de sistema de señalización nº 7, utiliza direcciones admisibles dentro de una pluralidad de capas de protocolo en la interconexión entre redes de radiotelefonía móvil y, si no existe ninguna dirección admisible, tiene lugar un rechazo de la SS7/MAP-MSU,

llevando a cabo una determinación de la red de radiotelefonía móvil O del emisor mediante análisis de la Dirección de la Parte de Llamada en la capa SCCP, en donde:

si el plan de numeración está ajustado en "plan de numeración de RDSI/telefonía (UIT-T E.163 y E.164)", el principio de la dirección se busca en una lista de todos los prefijos de operadores de red E.164 y de este modo se determina la red de radiotelefonía móvil O del emisor;

si el plan de numeración está ajustado en "plan de numeración móvil terrestre (UIT-T E.212)", el principio de la dirección se busca en una lista predefinida de todos los códigos de país móviles E.212, MCC (por sus siglas en inglés), y códigos de redes móviles, MNC (por sus siglas en inglés), y de este modo se determina la red de radiotelefonía móvil O del emisor;

llevando a cabo una determinación de la red de radiotelefonía móvil propia H, en donde:

si el abonado de radiotelefonía móvil se direcciona en una capa de aplicación a través de una IMSI, el principio de la IMSI se busca en una tabla predefinida de todos los códigos de país móviles E.212, MCC, y códigos de redes móviles, MNC, y de este modo se determina la red de radiotelefonía móvil propia H;

si el abonado de radiotelefonía móvil se direcciona en una capa de aplicación a través de una estación móvil de RDSI, el principio de la estación móvil de RDSI se busca en la lista de los códigos de país de telefonía asignados por la UIT y de este modo se determina la red de radiotelefonía móvil propia H;

si las redes de radiotelefonía móvil O y H no son idénticas, no se trata de una solicitud legítima, y si O y H son idénticas, probablemente se trata de una solicitud legítima;

b) determinar si un abonado de radiotelefonía móvil, en la interconexión entre redes de radiotelefonía móvil, es señalizado por una red de radiotelefonía móvil R como presente en dicha red de radiotelefonía móvil R aunque esté presente en otra red de radiotelefonía móvil, y, si es este el caso, se rechaza una solicitud a la interfaz SS7 en la medida en que, si una red de radiotelefonía móvil ha señalizado al Registro de Posición Propia, HLR, de la red de radiotelefonía móvil propia de un abonado de radiotelefonía móvil, mediante una solicitud "sendAuthenticationInfo" y/o "updateLocation", que dicho abonado de radiotelefonía móvil está presente ahora en la red de radiotelefonía móvil solicitante, mediante una solicitud "provideSubscriberInfo" al VLR V, Registro de Posiciones de Visitantes, en el que estaba presente el abonado de radiotelefonía móvil en último lugar se determina si éste todavía está presente en el mismo y, si es este el caso, la solicitud se rechaza y/o

si un tiempo de viaje determinado teniendo en cuenta una tabla estática, medido desde el último contacto con el VLR V, sería suficiente para un viaje al país en el que se encuentra la red de radiotelefonía móvil R y, si no es este el caso, la solicitud se rechaza;

c) determinar si una SS7/MAP-MSU ha sido enviada de forma masiva a diferentes elementos de red de una red de radiotelefonía móvil en la interconexión entre redes de radiotelefonía móvil para localizar a un abonado de radiotelefonía móvil y, si es este el caso, tiene lugar un rechazo de la SS7/MAP-MSU;

d) determinar si existe una modificación indebida de datos de abonado de radiotelefonía móvil mediante falsificación de una dirección de emisor de SS7/MAP-MSU en la interconexión entre redes de radiotelefonía móvil y, si es este el caso, tiene lugar un rechazo de la SS7/MAP-MSU, en donde un TC-BEGIN entrante de un HLR H se registra con una invocación para insertSubscriberData/deleteSubscriberData y se almacena en memoria tampón como solicitud, el HLR H es informado del éxito de la solicitud insertSubscriberData/deleteSubscriberData con TC-Continue y una otid, *origination transaction id* (identificación de transacción de origen), aleatoria, si el HLR-H no envía ningún TC-END, probablemente no se trata de una solicitud legítima, si se envía un TC-END desde el HLR-H, la solicitud, que ha sido almacenada en memoria tampón, se transmite a un VLR V.

En otra forma de realización posible, en la etapa a) arriba mencionada se examinan las SS7/MAP-MSU que incluyen una solicitud a un VLR (Registro de Posiciones de Visitantes), MSC (Centro de Conmutación Móvil) o SGSN (Nodo de Soporte GPRS de Servicio).

En otra forma de realización posible, en la etapa a) arriba mencionada se lleva a cabo una comprobación del tipo de la dirección, preferiblemente de la Dirección de Llamada SCCP, de un emisor en la capa de transporte, en relación con una o más de las siguientes características:

a. si la dirección no incluye ningún Título Global o ningún Plan de Numeración o ningún Esquema de Codificación o ningún Indicador de la Naturaleza de la Dirección, probablemente no se trata de una solicitud legítima;

b. si el Campo de Esquema de Codificación no está ajustado a BCD, *Binary-coded decimal* (decimal codificado en binario), probablemente no se trata de una solicitud legítima;

c. si el Campo de Naturaleza de la Dirección no está ajustado en "número internacional", probablemente no se trata de una solicitud legítima;

d. si el Campo de Plan de Numeración no es "plan de numeración de RDSI/telefonía (UIT-T E.163 y E.164)" ni "plan de numeración móvil terrestre (UIT-T E.212)", probablemente no se trata de una solicitud legítima.

En otra forma de realización posible, en la etapa a) arriba mencionada de la reivindicación 1 se lleva a cabo una determinación de la red de radiotelefonía móvil emisora por medio de un emisor, preferiblemente de la Dirección de Llamada SCCP, en la capa de transporte, en donde preferiblemente se ejecutan una o más de las siguientes etapas:

e. si el plan de numeración está ajustado en "plan de numeración de RDSI/telefonía (UIT-T E.163 y E.164)":

   i. se busca el principio del Título Global en la lista de los Códigos de País de Telefonía asignados por la UIT para determinar el país de la red de radiotelefonía móvil;

   ii. se debe buscar la parte siguiente del Título Global en una lista de los Códigos de Red de todas las PLMN, *Public Land Mobile Networks* (Redes Móviles Terrestres Públicas), del país correspondiente para determinar una red de radiotelefonía móvil, O;

f. si el plan de numeración es "plan de numeración móvil terrestre (UIT-T E.212)":

   i. se busca el principio del Título Global en la lista de los Códigos de País Móviles, MCC, y los Códigos de Redes Móviles, MNC, de la UIT para determinar una red de radiotelefonía móvil, O;

y una determinación de una red de radiotelefonía móvil propia H de un abonado de radiotelefonía móvil T, preferiblemente mediante la ejecución de una o más de las siguientes etapas:

g. si el abonado de radiotelefonía móvil se direcciona en una capa de aplicación a través de una IMSI: las primeras cifras de la IMSI incluyen igualmente los MCC y los MNC; el principio de la IMSI se busca en la lista de los Códigos de País Móviles, MCC, y los Códigos de Redes Móviles, MNC, de la UIT para determinar una red de radiotelefonía móvil propia H;

h. si el abonado de radiotelefonía móvil se direcciona en la capa de aplicación a través de la estación móvil de RDSI, el principio de la estación móvil de RDSI se busca en la lista de los códigos de país de telefonía asignados por la UIT para determinar el país de la red de radiotelefonía móvil, en donde se puede determinar un grupo de operadores de red H_1 ... H_n preferiblemente a través de una tabla predefinida;

y, si las redes de radiotelefonía móvil O y H no son idénticas, no se trata de una solicitud legítima y, si O y H son idénticas u O está en H_1 ... H_n, probablemente se trata de una solicitud legítima.

En otra forma de realización posible, en la etapa b) arriba mencionada de la reivindicación 1 se reconoce que una red de radiotelefonía móvil ha señalizado al Registro de Posición Propia, HLR, de la red de radiotelefonía móvil propia de un abonado de radiotelefonía móvil, mediante una solicitud "sendAuthenticationInfo" y/o "updateLocation", que dicho abonado de radiotelefonía móvil está presente ahora en la red de radiotelefonía móvil solicitante, aunque todavía esté presente en la red de radiotelefonía móvil anterior. Para ello, mediante una solicitud "provideSubscriberInfo" al VLR, Registro de Posiciones de Visitantes, en el que estaba presente el abonado de radiotelefonía móvil en último lugar, se determina si éste todavía está presente en el mismo y, si es este el caso, la solicitud se rechaza. En este contexto se ejecutan las siguientes etapas para determinar si el abonado de radiotelefonía móvil todavía está presente:

se envía una solicitud "sendAuthenticationInfo" y/o "updateLocation" desde la red de radiotelefonía móvil R correspondiente al abonado de radiotelefonía móvil T, al HLR H de la red de radiotelefonía móvil propia;

- la solicitud se detiene si no procede del VLR V actual (el VLR V designa el VLR en el que está registrado actualmente el abonado de radiotelefonía móvil, a diferencia del VLR general);

- se solicita al HLR H la dirección del último VLR V que se ha encargado del abonado de radiotelefonía móvil T;

- se envía al VLR V una solicitud "provideSubscriberInfo" con la IMSI del abonado de radiotelefonía móvil T, y en este contexto se establece el campo "currentLocation";

- el VLR V activa una Petición de Búsqueda para el terminal de radiotelefonía móvil del abonado de radiotelefonía móvil T, ya que se ha solicitado la "currentLocation";

- si el abonado de radiotelefonía móvil T responde a la Petición de Búsqueda, el VLR V establece en su respuesta el campo "currentLocationRetrieved"; en este caso, la solicitud original de la red de radiotelefonía móvil R es evidentemente incorrecta y se rechaza;

si el abonado de radiotelefonía móvil T no responde a la Petición de Búsqueda, el VLR V no establece en su respuesta el campo "currentLocationRetrieved".

En otra forma de realización posible, en la etapa b) arriba mencionada se ejecutan las siguientes etapas para comprobar adicionalmente la plausibilidad de la solicitud original: la información solicitada por el HLR H se transmite inmediatamente al VLR R remoto, llevándose a cabo lo siguiente mediante evaluación del campo "ageOfLocationInformation":

i. determinar cuánto tiempo hace que el abonado de radiotelefonía móvil T estuvo por última vez en contacto con el VLR V, "ageOfLocationInformation";

j. determinar cuánto duraría en el mejor de los casos un viaje desde el país en el que se encuentra geográficamente VLR V hasta el país en el que se encuentra geográficamente la red de radiotelefonía móvil R, en donde para la determinación serían suficientes valores aproximados que pueden estar almacenados estáticamente en una tabla;

k. si el tiempo transcurrido desde el último contacto del abonado de radiotelefonía móvil T con el VLR V es menor que el tiempo de viaje necesario en el mejor de los casos, la solicitud original de la red de radiotelefonía móvil R es evidentemente incorrecta y se rechaza; en caso contrario, la solicitud original de la red de radiotelefonía móvil R probablemente es legítima y se transmite al HLR H.

En otra forma de realización posible, en la etapa c) arriba mencionada, por medio de SS7/MAP-MSU por unidad de tiempo se decide si una solicitud es admisible o se rechaza, en donde preferiblemente se han de definir grupos de ajuste, grupos de operación y grupos fuente, en donde, al entrar una SS7/MAP-MSU, en primer lugar se determina el grupo de ajuste aplicable, después se asigna la operación SS7/MAP a un grupo de operación, después se determinan uno o más grupos fuente para incrementar luego un contador para la tupla de los grupos fuente, de operación y de ajuste, y después, si el contador se ha incrementado demasiado rápidamente en un período de tiempo determinado, decidir si se rechaza la SS7/MAP-MSU.

En otra forma de realización posible, en la etapa c) arriba mencionada se determina si se envían de forma masiva solicitudes relativas a un abonado de radiotelefonía móvil a diferentes VLR, Registro de Posiciones de Visitantes, MSC, Centro de Conmutación Móvil, o SGSN, Nodo de Soporte GPRS de Servicio, almacenando en una tabla el momento de cada solicitud y la IMSI del abonado de radiotelefonía móvil, o una identidad inequívoca derivada de ésta, y el Título Global de un receptor durante un intervalo de tiempo definido. En este contexto, si la cantidad de los diferentes Títulos Globales de receptor para una IMSI, o una identidad inequívoca derivada de ésta, sobrepasa un límite definido, se trata de solicitudes masivas para localizar al abonado de radiotelefonía móvil correspondiente en la red de radiotelefonía móvil.

En otra forma de realización posible, en la etapa d) arriba mencionada, un TC-BEGIN entrante de un HLR H se registra con una invocación para insertSubscriberData/deleteSubscriberData y se almacena en memoria tampón. El HLR H es informado del éxito de la llamada con TC-Continue y una otid, identificación de transacción de origen, preferiblemente aleatoria. Si la persona que llama/HLR H no envía ningún TC-END, probablemente no se trata de una solicitud legítima. Si se recibe un TC-END de la persona que llama inicialmente, la solicitud, que ha sido almacenada en memoria tampón, se transmite al propio VLR V.

En otra forma de realización posible, en la etapa e) arriba mencionada, un Título Global de emisor y receptor de cada SS7/MAP-MSU se compara con una lista W, lista blanca, que se mantiene internamente y es configurable. Si el Título Global de emisor o receptor no se encuentra en la lista, no se trata de una solicitud legítima;

y/o

el Título Global de emisor y receptor de cada MSU se compara con una lista B, lista negra, que se mantiene internamente y es configurable. Si el Título Global de emisor o receptor se encuentra en la lista, no se trata de una solicitud legítima;

y/o

el Título Global de emisor y receptor de cada MSU se compara con una lista de todos los Títulos Globales catalogados en todos los documentos GSMA IR.21 de las redes de radiotelefonía móvil de itinerancia de una radiotelefonía móvil. Si el Título Global de emisor o receptor no se encuentra en la lista, probablemente no se trata de una solicitud legítima.

Otra parte de la invención consiste en un procedimiento para extraer de forma transparente MTP/SCCP de paquetes M2PA, M2UA, M3UA y SUA de una conexión SCTP, con un sistema B que está dispuesto entre dos o más STP/pasarelas, en donde una STP/pasarela A establece una conexión IP/SCTP con el sistema B. Como resultado de ello, el sistema B establece una conexión con una STP/pasarela C, en donde la implementación del protocolo tiene lugar entre las STP/pasarelas A y C. Los paquetes de datos entre A y C se analizan mediante el sistema B, se determina la adaptación de usuario respectiva y se extrae la carga útil de MTP/SCCP.

Otra parte de la invención consiste en un sistema caracterizado por una instalación y una configuración que permiten un desarrollo del procedimiento de la invención. En principio se ha de tener en cuenta que este sistema puede consistir en un servidor convencional con componentes correspondientes, como disco duro, memoria principal, procesadores, en el que se ejecuta un sistema operativo conocido, como por ejemplo Unix o variantes de Unix (Linux, FreeBSD) o Windows. Mediante estos sistemas se puede llevar a cabo una programación correspondiente de las interfaces para proporcionar una especie de cortafuegos/*firewall*, que intercepta flujos de datos no autorizados y detecta anomalías. A través de interfaces correspondientes se recibe el flujo de datos y en caso se modifica o rechaza, para después transmitirlo si es admisible. Esto tiene lugar de forma totalmente transparente para la mayor parte de los abonados.

Para simplificar la descripción de la situación, en adelante el concepto "abonado de radiotelefonía móvil" se equipara con la combinación "terminal de radiotelefonía móvil de un abonado de radiotelefonía móvil con su tarjeta SIM": todos los procedimientos descritos identifican al abonado de radiotelefonía móvil a través de la característica de identificación de la tarjeta SIM y no a través de informaciones específicas del terminal de radiotelefonía móvil.

Descripción de las figuras

La figura 1 muestra un procedimiento para un sistema de protección, en el que en una interfaz SS7 externa, la interconexión SS7, tiene lugar la conexión con otros proveedores de telecomunicaciones a través de la red mundial SS7.

La figura 2 muestra un procedimiento que comprueba si una SS7/MAP-MSU (Unidad de Señal de Mensaje) está direccionada de forma admisible en la interconexión entre redes de radiotelefonía móvil según UIT-T Q.703.

Las figuras 3 y 6 muestran un procedimiento en el que se comprueba si un abonado de radiotelefonía móvil T, en la interconexión entre redes de radiotelefonía móvil, es señalizado por una red de radiotelefonía móvil R como presente en dicha red de radiotelefonía móvil R, aunque esté presente en otra red de radiotelefonía móvil V.

La figura 4 muestra un procedimiento en el que se comprueba cuánto tiempo ha pasado desde el último contacto del abonado de radiotelefonía móvil T con el VLR V.

La figura 5 muestra el caso en el que una sendAuthenticationInfo no ha sido enviada por el VLR actual y no se ha producido ningún intento de updateLocation, entonces se ha de notificar un incidente.

Figura 7, este procedimiento protege un VLR V contra modificaciones ilegítimas por un HLR H mediante un sistema S.

Figura 8, procedimiento E: estructura para recibir y procesar MSU (procedimiento "read" - leer).

Figura 9, procedimiento C: determinar si se envía de forma masiva una SS7/MAP-MSU a diferentes elementos de red de una red de radiotelefonía móvil en la interconexión entre redes de radiotelefonía móvil para localizar a un abonado de radiotelefonía móvil (procedimiento "ratelimit" - límite de tasa).

La figura 10 es un modelo de capas.

La figura 11 es una grabación como ejemplo, que incluye la información de dirección de SCCP correspondiente con una solicitud legítima.

Descripción de una forma de realización

La figura 1 muestra un sistema de protección, en el que en una interfaz SS7 externa, la interconexión SS7, tiene lugar la conexión con otros proveedores de telecomunicaciones a través de la red mundial SS7. Los datos SS7/MAP entrantes se analizan de acuerdo con el procedimiento descrito más abajo. Las solicitudes no legítimas se rechazan

a través de un filtro en dirección a la Intranet SS7 y, dependiendo del procedimiento, no se responde al exterior o se responde mediante una respuesta generada. Los resultados del procedimiento de análisis se protocolizan. El sistema puede alarmar a otros sistemas sobre ataques correspondientes, si así se desea. Opcionalmente, el sistema también se puede utilizar de tal modo que no funcione como sistema de filtro con respecto a la Intranet SS7 del proveedor de telecomunicaciones, sino que solo detecte y protocolice/alarme sobre solicitudes no legítimas.

Procedimiento A: Determinar si una SS7/MAP-MSU (Unidad de Señal de Mensaje) está direccionada de forma admisible en la interconexión entre redes de radiotelefonía móvil según UIT-T Q.703, en particular si la dirección del emisor y la dirección del receptor son admisibles. Así, la dirección del emisor en caso de SS7/MAP-MSU entrantes y la dirección del receptor en caso de mensajes salientes han de proceder de la misma red de radiotelefonía móvil a la que también pertenece el abonado de radiotelefonía móvil al que concierne la MSU (a este respecto, véase la figura 2).

Para determinar si una solicitud en relación con un abonado de radiotelefonía móvil, dirigida a un VLR (Registro de Posiciones de Visitantes), MSC (Centro de Conmutación Móvil) o SGSN (Nodo de Soporte GPRS de Servicio), procede de la red propia del abonado de radiotelefonía móvil, se deberían examinar las direcciones en la SS7/MAP-MSU correspondiente. En una SS7/MAP-MSU se pueden incluir informaciones de dirección en diferentes capas de protocolo. Se requiere un ajuste de las informaciones de dirección en las diferentes capas de protocolo.

En el enrutamiento de MSU entre redes de radiotelefonía móvil se utilizan diferentes tipos de direcciones. Por lo tanto, una simple comparación de las direcciones no es suficiente. Para cada tipo de dirección se requiere una función/imagen especial para poder asignar la dirección a la red de radiotelefonía móvil correspondiente:

- En la red de radiotelefonía móvil que ha de ser observada se envía una solicitud concerniente al abonado de radiotelefonía móvil T a un VLR o un MSC o un SGSN V a través de la interconexión.

- Comprobación del tipo de dirección del emisor en la capa de transporte (Dirección de Llamada SCCP) en cuanto a las siguientes características (formato según UIT-T Q.713):

  - Si la dirección no incluye ningún Título Global o ningún Plan de Numeración o ningún Esquema de Codificación o ningún Indicador de la Naturaleza de la Dirección, probablemente no se trata de una solicitud legítima.

  - Si el Campo de Esquema de Codificación no está ajustado a BCD (decimal codificado en binario), probablemente no se trata de una solicitud legítima.

  - Si el Campo de Naturaleza de la Dirección no está ajustado en "número internacional", probablemente no se trata de una solicitud legítima.

  - Si el Campo de Plan de Numeración no está ajustado en "plan de numeración de RDSI/telefonía (UIT-T E.163 y E.164)" ni en "plan de numeración móvil terrestre (UIT-T E.212)", probablemente no se trata de una solicitud legítima.

- Determinación de la red de radiotelefonía móvil emisora por medio del emisor en la capa de transporte (Dirección de Llamada SCCP):

  - Si el plan de numeración está ajustado en "plan de numeración de RDSI/telefonía (UIT-T E.163 y E.164)":

    - Buscar el principio del Título Global en la lista de los Códigos de País de Telefonía asignados por la UIT. De este modo se determina el país de la red de radiotelefonía móvil.

    - Se debe buscar la parte siguiente del Título Global en una lista de los Códigos de Red de todas las PLMN (Redes Móviles Terrestres Públicas) del país correspondiente. De este modo se determina el operador de red de radiotelefonía móvil, O.

  - Si el plan de numeración es "plan de numeración móvil terrestre (UIT-T E.212)":

    - Buscar el principio del Título Global en la lista de los Códigos de País Móviles (MCC) y los Códigos de Redes Móviles (MNC) de la UIT. De este modo se determina el operador de red de radiotelefonía móvil, O.

- Determinación del operador de red propia H del abonado de radiotelefonía móvil T:

  - Si el abonado de radiotelefonía móvil T se direcciona en la capa de aplicación a través de la IMSI: las primeras cifras de la IMSI incluyen igualmente los MCC y los MNC. El principio de la IMSI se busca en la lista de los Códigos de País Móviles (MCC) y los Códigos de Redes Móviles (MNC) de la UIT. De este modo se determina el operador de red propia H.

- Si el abonado de radiotelefonía móvil T se direcciona en la capa de aplicación a través de la estación móvil de RDSI: el principio de la estación móvil de RDSI se busca en la lista de los códigos de país de telefonía asignados por la UIT. De este modo se determina el país de la red de radiotelefonía móvil. A través de una tabla predefinida se puede determinar un grupo de operadores de red H_1 ... H_n para poder decidir al menos aproximadamente si el operador de red de radiotelefonía móvil O está en este grupo de operadores de red.

- Si O y H no son idénticas, no se trata de una solicitud legítima.

- Si O y H son idénticas o si O está en H_1 ... H_n, probablemente se trata de una solicitud legítima. Para evitar una falsificación del emisor, en los casos en los que no se requiere ninguna respuesta se puede utilizar el procedimiento D (véase más abajo).

La figura 11 describe una información de dirección de SCCP correspondiente, que contiene los parámetros arriba mencionados de tal modo que la solicitud es legítima.

Procedimiento B: Comprobar si un abonado de radiotelefonía móvil T, en la interconexión entre redes de radiotelefonía móvil, es señalizado por una red de radiotelefonía móvil R como presente en dicha red de radiotelefonía móvil R aunque esté presente en otra red de radiotelefonía móvil V (procedimiento "intercept" - interceptar).

Si una red de radiotelefonía móvil R ha señalizado al HLR (Registro de Posición Propia) de la red de radiotelefonía móvil propia de un abonado de radiotelefonía móvil T, mediante una solicitud "sendAuthenticationInfo" y/o "updateLocation", que dicho abonado de radiotelefonía móvil T está presente ahora en la red de radiotelefonía móvil R solicitante, mediante una solicitud "provideSubscriberInfo" al VLR (Registro de Posiciones de Visitantes) V en el que estaba presente el abonado de radiotelefonía móvil T en último lugar, se puede determinar si éste todavía está presente en el mismo:

- Se envía una solicitud "sendAuthenticationInfo" y/o "updateLocation" desde la red de radiotelefonía móvil R correspondiente al abonado de radiotelefonía móvil T, al HLR H de la red de radiotelefonía móvil propia.

- La solicitud se detiene si no procede del VLR V actual.

- Se solicita al HLR H la dirección del último VLR V que se ha encargado del abonado de radiotelefonía móvil T.

- Se envía al VLR V una solicitud "provideSubscriberInfo" con la IMSI del abonado de radiotelefonía móvil T. En este contexto se establece el campo "currentLocation".

- El VLR V activa una Petición de Búsqueda para el abonado de radiotelefonía móvil T, ya que se ha solicitado la "currentLocation".

- Si el abonado de radiotelefonía móvil T responde a la Petición de Búsqueda, el VLR V establece en su respuesta el campo "currentLocationRetrieved". En este caso, la solicitud original de la red de radiotelefonía móvil R es evidentemente incorrecta y se rechaza.

- Las figuras 3 y 6 representan el procedimiento recién descrito para sendAuthenticationInfo o updateLocation.

- Si el abonado de radiotelefonía móvil T no responde a la Petición de Búsqueda, el VLR V no establece en su respuesta el campo "currentLocationRetrieved". Por regla general, esto dura más de lo que permite un tiempo límite para responder a la solicitud sendAuthentication. Por ello, el sistema transmite inmediatamente al VLR R remoto la información solicitada por el HLR H. Para comprobar adicionalmente la plausibilidad de la solicitud original se puede evaluar el campo "ageOfLocationInformation" de la respuesta del VLR V:

  - ¿Cuánto tiempo hace que el abonado de radiotelefonía móvil T estuvo por última vez en contacto con el VLR V, "ageOfLocationInformation"?

  - ¿Cuánto duraría en el mejor de los casos un viaje desde el país en el que se encuentra geográficamente VLR V hasta el país en el que se encuentra geográficamente la red de radiotelefonía móvil R? Para la determinación son suficientes valores aproximados que pueden estar almacenados estáticamente en una tabla.

  - Si el tiempo transcurrido desde el último contacto del abonado de radiotelefonía móvil T con el VLR V es menor que el tiempo de viaje necesario en el mejor de los casos, la solicitud original de la red de radiotelefonía móvil R es evidentemente incorrecta y se rechaza. En caso contrario, la solicitud original de la red de radiotelefonía móvil R probablemente es legítima y se transmite al HLR H.

- El procedimiento recién descrito se utiliza en la figura 4: una updateLocation del VLR R obtenida en este contexto es retenida por el sistema hasta que mediante el procedimiento arriba mencionado se decide si la solicitud del VLR R es legítima. En caso afirmativo, se transmite al HLR H; en caso negativo, se rechaza y se emite una alarma de ataque. Si sendAuthenticationInfo no ha sido enviada por el VLR actual y no ha producido ningún intento de updateLocation, se ha de notificar un incidente: un nuevo VLR (es decir, un VLR en el que se acaba de registrar el abonado de radiotelefonía móvil) después de una sendAuthenticationInfo siempre ha de enviar una updateLocation. La figura 5 ilustra este caso, representando este gráfico también el caso en el que el VLR R actual envía una respuesta positiva (es decir, el abonado de radiotelefonía móvil T todavía está registrado en el VLR R) o el campo ageOfLocationInformation, después de las evaluaciones arriba presentadas, admite el supuesto de que el abonado de radiotelefonía móvil no puede estar realmente registrado en el VLR remoto.

Procedimiento C: Determinar si se envía de forma masiva una SS7/MAP-MSU a diferentes elementos de red de una red de radiotelefonía móvil en la interconexión entre redes de radiotelefonía móvil para localizar a un abonado de radiotelefonía móvil (procedimiento "ratelimit" - límite de tasa).

En una forma general

- El procedimiento descrito a continuación está representado en la figura 9.
- Es posible definir grupos de ajuste (*match* - correspondencia), grupos de operación y grupos fuente.

  - Un grupo de ajuste puede consistir en la clase de equivalencia de la IMSI u otros criterios de suscriptor.

  - Un grupo de operación consiste en una o más operaciones SS7/MAP.

  - Un grupo fuente puede consistir en un Título Global individual, una gama de Títulos Globales o una lista de Títulos Globales. El grupo fuente se puede combinar con Números de Subsistema (SSN, por sus siglas en inglés).

- Es posible definir reglas con la mejor correspondencia o con correspondencia total.
- Como "Rate-Limit" se definen solicitudes por día, por hora, por minuto, por segundo o criterios similares.

En caso de una SS7/MAP-MSU entrante, en primer lugar se determina el grupo de ajuste aplicable.

- Después se determinan uno o más grupos fuente.
- En primer lugar se incrementa el contador de una tupla de grupos fuente, de operación y de ajuste, y después se aplica el "Rate-Limit".
- Después de aplicar el Rate-Limit se puede rechazar una SS7/MAP-MSU y/o generar un evento de registro.

En una realización especial, para determinar si se envían de forma masiva solicitudes relativas a un abonado de radiotelefonía móvil a diferentes VLR (Registro de Posiciones de Visitantes), MSC (Centro de Conmutación Móvil) o SGSN (Nodo de Soporte GPRS de Servicio), el momento de cada solicitud y la IMSI del abonado de radiotelefonía móvil (o una identidad inequívoca derivada de ésta), y el Título Global de un receptor durante un intervalo de tiempo definido, se almacenan en una tabla. En este contexto, si la cantidad de los diferentes Títulos Globales de receptor para una IMSI sobrepasa un límite definido, se trata de solicitudes masivas para localizar al abonado de radiotelefonía móvil correspondiente en la red de radiotelefonía móvil:

- En la red de radiotelefonía móvil que ha de ser observada se envía una solicitud concerniente al abonado de radiotelefonía móvil T a un VLR o un MSC o un SGSN V a través de la interconexión.
- A partir de la capa de transporte de la solicitud se almacena en memoria la dirección de receptor (Dirección de la Parte de Llamada SCCP).
- A partir de la capa de aplicación de la solicitud se almacena en memoria la IMSI.
- Ambos datos se almacenan junto con el tiempo actual en una base de datos. si la dirección de receptor para esta IMSI (o una identidad inequívoca derivada de ésta) ya está almacenada, la entrada se sobrescribe (por lo tanto, solo se actualiza el sello de tiempo).
- Todas las entradas cuyos sellos de tiempo son más antiguos que el intervalo de tiempo admitido para el almacenamiento de las entradas se borran.

- Si la cantidad de las entradas para esta IMSI sobrepasa un límite previamente definido, se trata de solicitudes masivas para localizar al abonado de radiotelefonía móvil T y la solicitud se puede rechazar y/o se puede generar un evento de registro.

Procedimiento D: Impedir la modificación indebida de datos de abonado de radiotelefonía móvil mediante falsificación de la dirección de emisor de SS7/MAP-MSU en la interconexión entre redes de radiotelefonía móvil (procedimiento "proxy").

Este procedimiento protege un VLR V contra modificaciones ilegítimas por un HLR H mediante un sistema S y está representado en la figura 7, y se describe de la siguiente manera:

Para impedir las operaciones insertSubscriberData/deleteSubscriberData de una Dirección de Llamada SCCP falsa se utiliza un sistema S activo. Un TC-BEGIN entrante de un HLR H se registra con una invocación para insertSubscriberData/deleteSubscriberData y se almacena en memoria tampón. El HLR H es informado del éxito de la llamada con TC-Continue (y otid aleatoria - identificación de transacción de origen). Si la persona que llama no envía ningún TC-END, probablemente no se trata de una solicitud legítima. Si se recibe un TC-END de la persona que llama inicialmente, la solicitud, que ha sido almacenada en memoria tampón, se transmite al propio VLR V.

Otro procedimiento posible es el

procedimiento E: Comprobación de elementos de red legítimos de un socio de itinerancia.

- El Título Global de emisor y receptor de cada SS7/MAP-MSU se compara con una lista W, que se mantiene internamente en el sistema y es configurable. Si el Título Global de emisor o receptor no se encuentra en la lista, no se trata de una solicitud legítima ("lista blanca").
- El Título Global de emisor y receptor de cada MSU se compara con una lista B, que se mantiene internamente en el sistema y es configurable. Si el Título Global de emisor o receptor se encuentra en la lista, no se trata de una solicitud legítima ("lista negra").
- El Título Global de emisor y receptor de cada MSU se compara con una lista de todos los Títulos Globales catalogados en todos los documentos GSMA IR.21 de los socios de itinerancia de un operador de red. Si el Título Global de emisor o receptor no se encuentra en la lista, muy probablemente no se trata de una solicitud legítima.

Procedimiento F: Estructura para recibir y procesar MSU (procedimiento "read").

Se describe un procedimiento para extraer de forma transparente MTP/SCCP de paquetes M2PA, M2UA, M3UA y SUA de una conexión SCTP, sin implementar las máquinas de estados respectivas. La figura 8 representa este procedimiento en un diagrama de secuencia. Para ello, el sistema (designado aquí como sistema B) está dispuesto entre dos o más STP/pasarelas. Una STP/pasarela A establece una conexión IP/SCTP con el sistema B. Como resultado de ello, el sistema B establece una conexión con una STP/pasarela C. La implementación del protocolo tiene lugar exclusivamente entre las STP/pasarelas A y C. Los paquetes de datos entre A y C se analizan, se determina la adaptación de usuario respectiva y se extrae la carga útil de MTP/SCCP. Ésta puede ser procesada, analizada y evaluada por el sistema B. En la conexión entre A y C se pueden introducir paquetes, modificar paquetes entrantes o rechazar los mismos.

REIVINDICACIONES

1. Un procedimiento para asegurar una interfaz de sistema de señalización nº 7, interfaz SS7, de un sistema, a través de la cual tiene lugar un acceso a una red de radiotelefonía móvil local, con respecto a un sistema externo, que incluye una o más de las siguientes etapas de análisis:

a) determinar si una SS7/MAP-MSU, Unidad de Señal de Mensaje de Parte de Aplicación de Móviles de sistema de señalización nº 7, utiliza direcciones admisibles dentro de una pluralidad de capas de protocolo en la interconexión entre redes de radiotelefonía móvil y, si no existe ninguna dirección admisible, tiene lugar un rechazo de la SS7/MAP-MSU,

llevando a cabo una determinación de la red de radiotelefonía móvil O del emisor mediante análisis de la Dirección de la Parte de Llamada en la capa SCCP, en donde:

si el plan de numeración está ajustado en "plan de numeración de RDSI/telefonía (UIT-T E.163 y E.164)", el principio de la dirección se busca en una lista de todos los prefijos de operadores de red E.164 y de este modo se determina la red de radiotelefonía móvil O del emisor;

si el plan de numeración está ajustado en "plan de numeración móvil terrestre (UIT-T E.212)", el principio de la dirección se busca en una lista predefinida de todos los códigos de país móviles E.212, MCC, y códigos de redes móviles, MNC, y de este modo se determina la red de radiotelefonía móvil O del emisor;

llevando a cabo una determinación de la red de radiotelefonía móvil propia H, en donde:

si el abonado de radiotelefonía móvil se direcciona en una capa de aplicación a través de una IMSI, el principio de la IMSI se busca en una tabla predefinida de todos los códigos de país móviles E.212, MCC, y códigos de redes móviles, MNC, y de este modo se determina la red de radiotelefonía móvil propia H;

si el abonado de radiotelefonía móvil se direcciona en una capa de aplicación a través de una estación móvil de RDSI, el principio de la estación móvil de RDSI se busca en la lista de los códigos de país de telefonía asignados por la UIT y de este modo se determina la red de radiotelefonía móvil propia H;

si las redes de radiotelefonía móvil O y H no son idénticas, no se trata de una solicitud legítima, y si O y H son idénticas, probablemente se trata de una solicitud legítima;

b) determinar si un abonado de radiotelefonía móvil, en la interconexión entre redes de radiotelefonía móvil, es señalizado por una red de radiotelefonía móvil R como presente en dicha red de radiotelefonía móvil R aunque esté presente en otra red de radiotelefonía móvil, y, si es este el caso, se rechaza una solicitud a la interfaz SS7 en la medida en que, si una red de radiotelefonía móvil ha señalizado al Registro de Posición Propia, HLR, de la red de radiotelefonía móvil propia de un abonado de radiotelefonía móvil, mediante una solicitud "sendAuthenticationInfo" y/o "updateLocation", que dicho abonado de radiotelefonía móvil está presente ahora en la red de radiotelefonía móvil solicitante, mediante una solicitud "provideSubscriberInfo" al VLR V, Registro de Posiciones de Visitantes, en el que estaba presente el abonado de radiotelefonía móvil en último lugar se determina si éste todavía está presente en el mismo y, si es este el caso, la solicitud se rechaza y/o

si un tiempo de viaje determinado teniendo en cuenta una tabla estática, medido desde el último contacto con el VLR V, sería suficiente para un viaje al país en el que se encuentra la red de radiotelefonía móvil R y, si no es este el caso, la solicitud se rechaza;

c) determinar si una SS7/MAP-MSU ha sido enviada de forma masiva a diferentes elementos de red de una red de radiotelefonía móvil en la interconexión entre redes de radiotelefonía móvil para localizar a un abonado de radiotelefonía móvil y, si es este el caso, tiene lugar un rechazo de la SS7/MAP-MSU;

d) determinar si existe una modificación indebida de datos de abonado de radiotelefonía móvil mediante falsificación de una dirección de emisor de SS7/MAP-MSU en la interconexión entre redes de radiotelefonía móvil y, si es este el caso, tiene lugar un rechazo de la SS7/MAP-MSU, en donde un TC-BEGIN entrante de un HLR H se registra con una invocación para insertSubscriberData/deleteSubscriberData y se almacena en memoria tampón como solicitud, el HLR H es informado del éxito de la solicitud insertSubscriberData/deleteSubscriberData con TC-Continue y una otid, *origination transaction id* (identificación de transacción de origen), aleatoria, si el HLR-H no envía ningún TC-END, probablemente no se trata de una solicitud legítima, si se envía un TC-END desde el HLR-H, la solicitud, que ha sido almacenada en memoria tampón, se transmite a un VLR V.

2. El procedimiento según la reivindicación precedente, en donde en la etapa a) de la reivindicación 1, siempre que las SS7/MAP-MSU incluyen una solicitud a un VLR (Registro de Posiciones de Visitantes), MSC (Centro de Conmutación Móvil) o SGSN (Nodo de Soporte GPRS de Servicio), se comprueba si la dirección en la SS7/MAP-MSU respectiva procede de una red propia del abonado de radiotelefonía móvil.

3. El procedimiento según una o más de las reivindicaciones precedentes, en donde en la etapa a)

tiene lugar una comprobación del tipo de dirección, o de la Dirección de Llamada SCCP, de un emisor en la capa de transporte en relación con una o más de las siguientes características:

a. si la dirección no incluye ningún Título Global o ningún Plan de Numeración o ningún Esquema de Codificación o ningún Indicador de la Naturaleza de la Dirección, probablemente no se trata de una solicitud legítima;

b. si el Campo de Esquema de Codificación no está ajustado a BCD, *Binary-coded decimal* (decimal codificado en binario), probablemente no se trata de una solicitud legítima;

c. si el Campo de Naturaleza de la Dirección no está ajustado en "número internacional", probablemente no se trata de una solicitud legítima;

d. si el Campo de Plan de Numeración no es "plan de numeración de RDSI/telefonía (UIT-T E.163 y E.164)" ni "plan de numeración móvil terrestre (UIT-T E.212)", probablemente no se trata de una solicitud legítima.

4. El procedimiento según una o más de las reivindicaciones precedentes, en donde en la etapa a) de la reivindicación 1 tiene lugar una determinación de la red de radiotelefonía móvil emisora por medio de un emisor, o de la Dirección de Llamada SCCP, en la capa de transporte, en donde preferiblemente se ejecutan una o más de las siguientes etapas:

a. si el plan de numeración está ajustado en "plan de numeración de RDSI/telefonía (UIT-T E.163 y E.164)":

i. se busca el principio del Título Global en la lista de los Códigos de País de Telefonía asignados por la UIT para determinar el país de la red de radiotelefonía móvil;

ii. se debe buscar la parte siguiente del Título Global en una lista de los Códigos de Red de todas las PLMN, *Public Land Mobile Networks* (Redes Móviles Terrestres Públicas), del país correspondiente para determinar una red de radiotelefonía móvil, O;

b. si el plan de numeración es "plan de numeración móvil terrestre (UIT-T E.212)":

i. se busca el principio del Título Global en la lista de los Códigos de País Móviles, MCC, y los Códigos de Redes Móviles, MNC, de la UIT para determinar una red de radiotelefonía móvil, O;

y una determinación de una red de radiotelefonía móvil propia H de un abonado de radiotelefonía móvil mediante la ejecución de una o más de las siguientes etapas:

c. si el abonado de radiotelefonía móvil se direcciona en una capa de aplicación a través de una IMSI: las primeras cifras de la IMSI incluyen igualmente los MCC y los MNC; el principio de la IMSI se busca en la lista de los Códigos de País Móviles, MCC, y los Códigos de Redes Móviles, MNC, de la UIT para determinar una red de radiotelefonía móvil propia H;

d. si el abonado de radiotelefonía móvil se direcciona en la capa de aplicación a través de la estación móvil de RDSI, el principio de la estación móvil de RDSI se busca en la lista de los códigos de país de telefonía asignados por la UIT para determinar el país de la red de radiotelefonía móvil, en donde se puede determinar un grupo de operadores de red H_1 ... H_n a través de una tabla predefinida;

y, si las redes de radiotelefonía móvil O y H no son idénticas, no se trata de una solicitud legítima y, si O y H son idénticas u O está en H_1 ... H_n, probablemente se trata de una solicitud legítima.

5. El procedimiento según una o más de las reivindicaciones precedentes, en donde en la etapa b) de la reivindicación 1 se reconoce que una red de radiotelefonía móvil ha señalizado al Registro de Posición Propia, HLR, de la red de radiotelefonía móvil propia de un abonado de radiotelefonía móvil, mediante una solicitud "sendAuthenticationInfo" y/o "updateLocation", que dicho abonado de radiotelefonía móvil está presente ahora en la red de radiotelefonía móvil solicitante, mediante una solicitud "provideSubscriberInfo" al VLR, Registro de Posiciones de Visitantes, en el que estaba presente el abonado de radiotelefonía móvil en último lugar, se determina si éste todavía está presente en el mismo y, si es este el caso, la solicitud "sendAuthenticationInfo" y/o "updateLocation" se rechaza.

6. El procedimiento según la reivindicación 1, en donde en la etapa b) se ejecutan las siguientes etapas para determinar si el abonado de radiotelefonía móvil todavía está presente:

se envía una solicitud "sendAuthenticationInfo" y/o "updateLocation" desde una red de radiotelefonía móvil R correspondiente a un abonado de radiotelefonía móvil T, al HLR H de la red de radiotelefonía móvil propia;

- la solicitud "sendAuthenticationInfo" y/o "updateLocation" se detiene si no procede del VLR V actual;

- se solicita al HLR H la dirección del último VLR V que se ha encargado del abonado de radiotelefonía móvil;

- se envía al VLR V una solicitud "provideSubscriberInfo" con la IMSI del abonado de radiotelefonía móvil, y en este contexto se establece el campo "currentLocation";

- el VLR V activa una Petición de Búsqueda para el abonado de radiotelefonía móvil T, ya que se ha solicitado la "currentLocation";

- si el abonado de radiotelefonía móvil responde a la Petición de Búsqueda, el VLR V establece en su respuesta el campo "currentLocationRetrieved"; en este caso, la solicitud "sendAuthenticationInfo" y/o "updateLocation" de la red de radiotelefonía móvil R es evidentemente incorrecta y se rechaza;

si el abonado de radiotelefonía móvil T no responde a la Petición de Búsqueda, el VLR V no establece en su respuesta el campo "currentLocationRetrieved".

7. El procedimiento según la reivindicación precedente, en donde se ejecutan las siguientes etapas para comprobar adicionalmente la plausibilidad de la solicitud "sendAuthenticationInfo" y/o "updateLocation": la información solicitada por el HLR H se transmite inmediatamente al VLR V, llevándose a cabo lo siguiente mediante evaluación del campo "ageOfLocationInformation":

a. determinar cuánto tiempo hace que el abonado de radiotelefonía móvil estuvo por última vez en contacto con el VLR V, "ageOfLocationInformation";

b. determinar cuánto duraría en el mejor de los casos un viaje desde el país en el que se encuentra geográficamente VLR V hasta el país en el que se encuentra geográficamente la red de radiotelefonía móvil R, en donde para la determinación serían suficientes valores aproximados que pueden estar almacenados estáticamente en una tabla;

c. si el tiempo transcurrido desde el último contacto del abonado de radiotelefonía móvil con el VLR V es menor que el tiempo de viaje necesario en el mejor de los casos, la solicitud "sendAuthenticationInfo" y/o "updateLocation" de la red de radiotelefonía móvil R es evidentemente incorrecta y se rechaza; en caso contrario, la solicitud "sendAuthenticationInfo" y/o "updateLocation" de la red de radiotelefonía móvil R probablemente es legítima y se transmite al HLR H.

8. El procedimiento según una o más de las reivindicaciones precedentes, en donde en la etapa c) de la reivindicación 1, por medio de SS7/MAP-MSU por unidad de tiempo se decide si una solicitud SS7/MAP-MSU es admisible o se rechaza, en donde se han de definir grupos de ajuste, grupos de operación y grupos fuente, en donde, al entrar una SS7/MAP-MSU, en primer lugar se determina un grupo de ajuste aplicable, después se asigna la operación SS7/MAP a un grupo de operación, después se determinan uno o más grupos fuente para incrementar luego un contador para la tupla de los grupos fuente, de operación y de ajuste, y después, si el contador se ha incrementado demasiado rápidamente en un período de tiempo determinado, decidir si se rechaza la SS7/MAP-MSU.

9. El procedimiento según una o más de las reivindicaciones precedentes, en donde en la etapa c) de la reivindicación 1 se determina si se envían de forma masiva solicitudes relativas a un abonado de radiotelefonía móvil a diferentes VLR, Registro de Posiciones de Visitantes, MSC, Centro de Conmutación Móvil, o SGSN, Nodo de Soporte GPRS de Servicio, almacenando en una tabla el momento de cada solicitud y la IMSI del abonado de radiotelefonía móvil, o una identidad inequívoca derivada de ésta, y el Título Global de un receptor durante un intervalo de tiempo definido, si en este contexto la cantidad de los diferentes Títulos Globales de receptor para una IMSI, o una identidad inequívoca derivada de ésta, sobrepasa un límite definido, se trata de solicitudes masivas para localizar al abonado de radiotelefonía móvil correspondiente en la red de radiotelefonía móvil.

10. El procedimiento según una o más de las reivindicaciones precedentes, en donde tiene lugar una determinación de la legitimidad de un sistema externo mediante comprobación del Título Global de emisor y receptor de la SS7/MAP-MSU;

un Título Global de emisor y receptor de cada SS7/MAP-MSU se compara con una lista W, lista blanca, que se mantiene internamente y es configurable, y, si el Título Global de emisor o receptor no se encuentra en la lista, no se trata de una solicitud legítima;

y/o

el Título Global de emisor y receptor de cada MSU se compara con una lista B, lista negra, que se mantiene internamente y es configurable, y, si el Título Global de emisor o receptor se encuentra en la lista, no se trata de una solicitud legítima;

y/o

el Título Global de emisor y receptor de cada MSU se compara con una lista de todos los Títulos Globales catalogados en todos los documentos GSMA IR.21 de las redes de radiotelefonía móvil de itinerancia de un operador de red y, si el Título Global de emisor o receptor no se encuentra en la lista, probablemente no se trata de una solicitud legítima.

11. El procedimiento según una o más de las reivindicaciones precedentes, para extraer de forma transparente MTP/SCCP de paquetes M2PA, M2UA, M3UA y SUA de una conexión SCTP, con un sistema B que está dispuesto entre dos o más STP/pasarelas, en donde una STP/pasarela A establece una conexión IP/SCTP con el sistema B y, como resultado de ello, el sistema B establece una conexión con una STP/pasarela C, en donde la implementación del protocolo tiene lugar entre las STP/pasarelas A y C; los paquetes de datos entre A y C se analizan mediante el sistema B, se determina la adaptación de usuario respectiva y se extrae la carga útil de MTP/SCCP.

12. Sistema caracterizado por un dispositivo y una configuración que llevan a cabo un desarrollo de un procedimiento según una o más de las reivindicaciones precedentes.

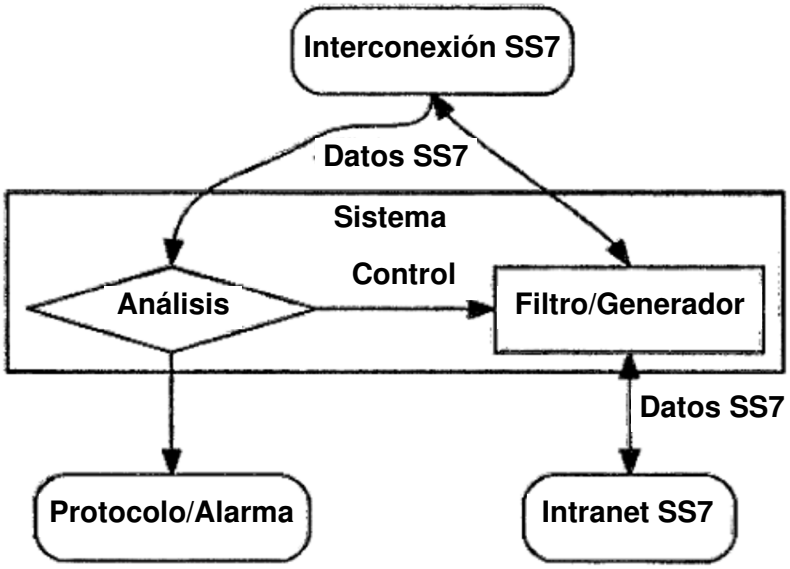
Interconexión SS7
Datos SS7
Sistema
Control
Análisis
Filtro/Generador
Datos SS7
Protocolo/Alarma
Intranet SS7

Fig. 1

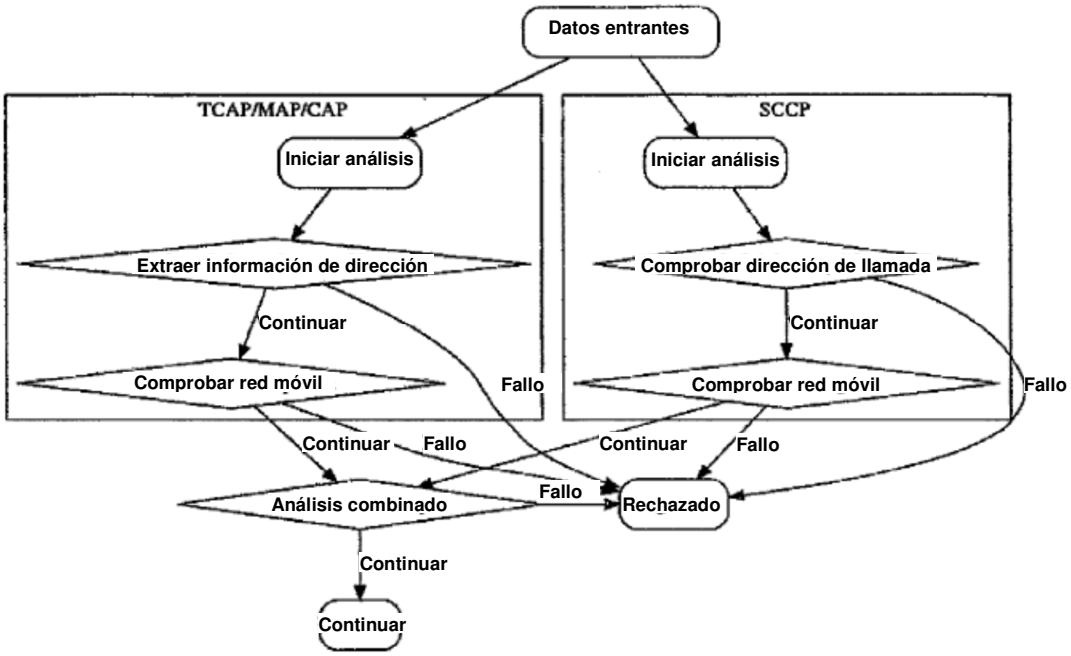
Datos entrantes
TCAP/MAP/CAP
SCCP
Iniciar análisis
Iniciar análisis
Extraer información de dirección
Comprobar dirección de llamada
Continuar
Continuar
Comprobar red móvil
Comprobar red móvil
Fallo
Fallo
Continuar
Fallo
Continuar
Fallo
Análisis combinado
Fallo
Rechazado
Continuar
Continuar

Fig. 2

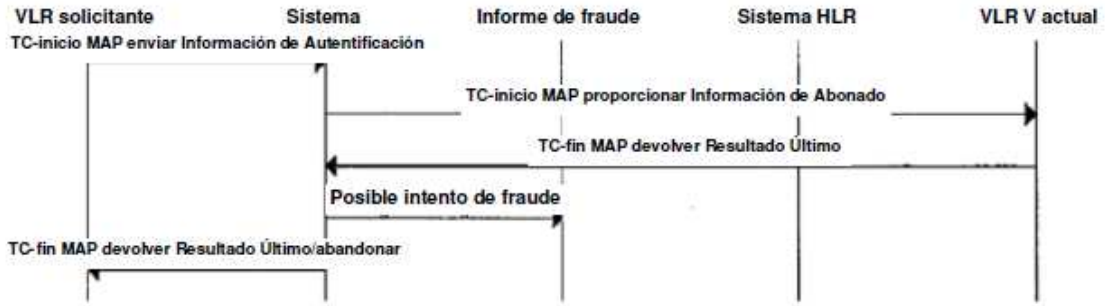
VLR solicitante
Sistema
Informe de fraude
Sistema HLR
VLR V actual
TC-inicio MAP enviar Información de Autentificación
TC-inicio MAP proporcionar Información de Abonado
TC-fin MAP devolver Resultado Último
Posible intento de fraude
TC-fin MAP devolver Resultado Último/abandonar

Fig. 3

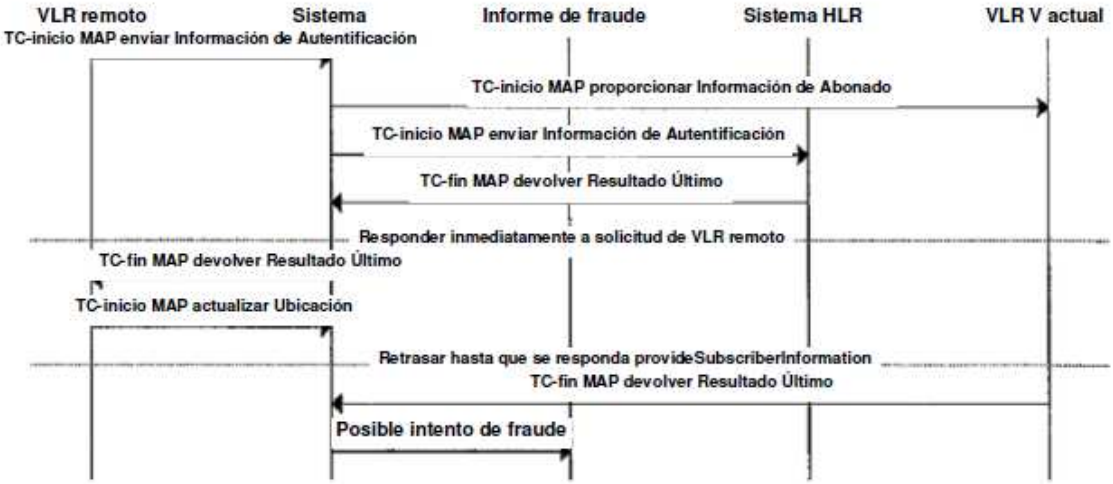
VLR remoto
Sistema
Informe de fraude
Sistema HLR
VLR V actual
TC-inicio MAP enviar Información de Autentificación
TC-inicio MAP proporcionar Información de Abonado
TC-inicio MAP enviar Información de Autentificación
TC-fin MAP devolver Resultado Último
Responder inmediatamente a solicitud de VLR remoto
TC-fin MAP devolver Resultado Último
TC-inicio MAP actualizar Ubicación
Retrasar hasta que se responda provideSubscriberInformation
TC-fin MAP devolver Resultado Último
Posible intento de fraude

Fig. 4

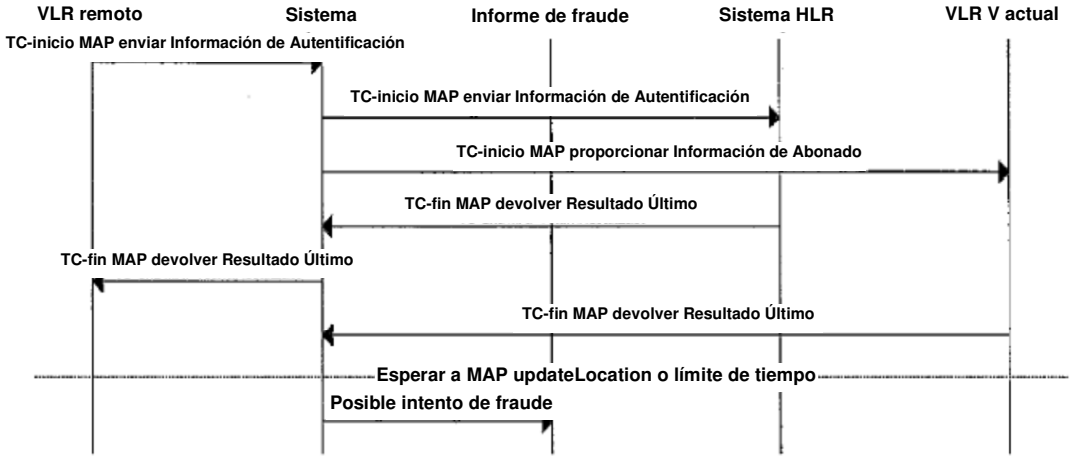
VLR remoto
Sistema
Informe de fraude
Sistema HLR
VLR V actual
TC-inicio MAP enviar Información de Autentificación
TC-inicio MAP enviar Información de Autentificación
TC-inicio MAP proporcionar Información de Abonado
TC-fin MAP devolver Resultado Último
TC-fin MAP devolver Resultado Último
TC-fin MAP devolver Resultado Último
Esperar a MAP updateLocation o límite de tiempo
Posible intento de fraude

Fig. 5

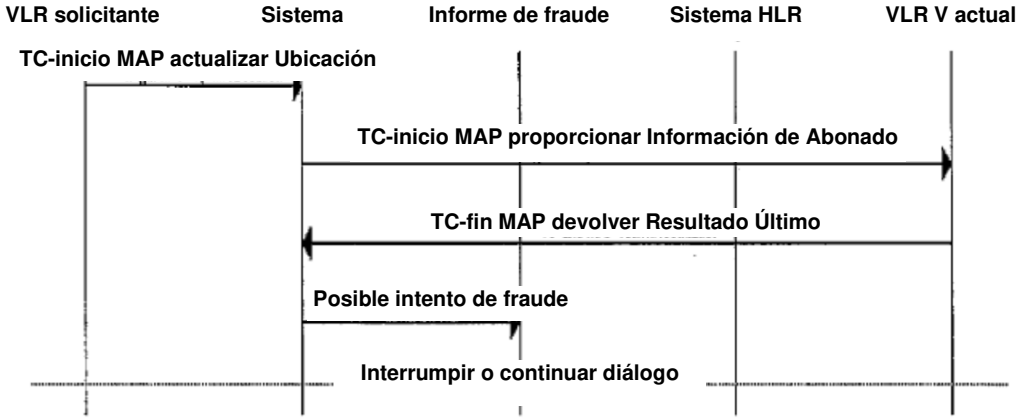
VLR solicitante
Sistema
Informe de fraude
Sistema HLR
VLR V actual
TC-inicio MAP actualizar Ubicación
TC-inicio MAP proporcionar Información de Abonado
TC-fin MAP devolver Resultado Último
Posible intento de fraude
Interrumpir o continuar diálogo

Fig. 6

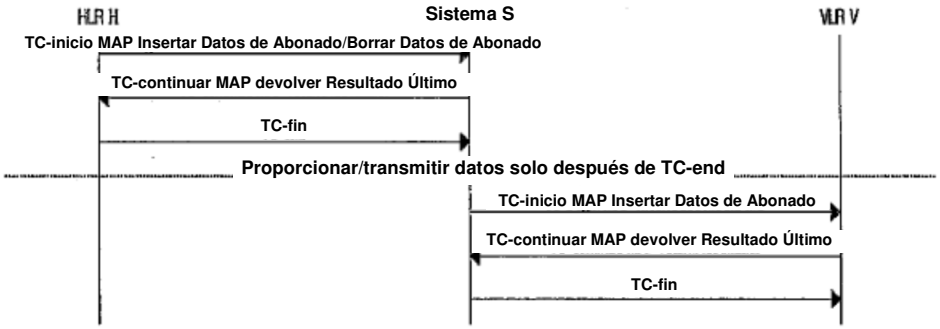
HLR H
Sistema S
VLR V
TC-inicio MAP Insertar Datos de Abonado/Borrar Datos de Abonado
TC-continuar MAP devolver Resultado Último
TC-fin
Proporcionar/transmitir datos solo después de TC-end
TC-inicio MAP Insertar Datos de Abonado
TC-continuar MAP devolver Resultado Último
TC-fin

Fig. 7

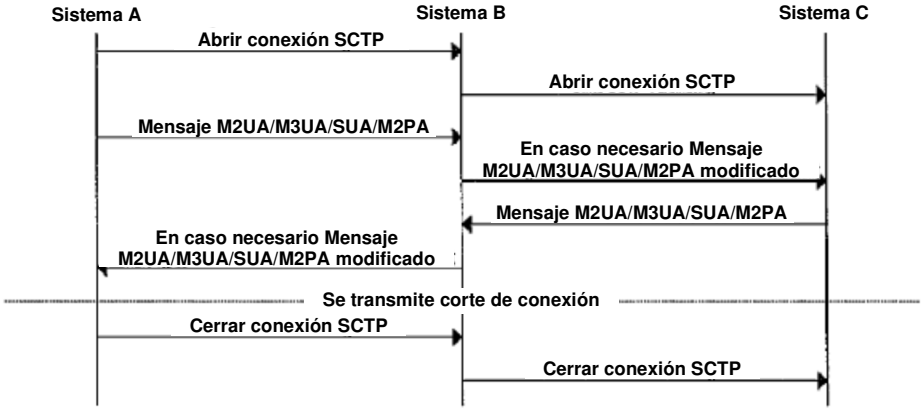
Sistema A
Sistema B
Sistema C
Abrir conexión SCTP
Abrir conexión SCTP
Mensaje M2UA/M3UA/SUA/M2PA
En caso necesario Mensaje M2UA/M3UA/SUA/M2PA modificado
Mensaje M2UA/M3UA/SUA/M2PA
En caso necesario Mensaje M2UA/M3UA/SUA/M2PA modificado
Se transmite corte de conexión
Cerrar conexión SCTP
Cerrar conexión SCTP

Fig. 8

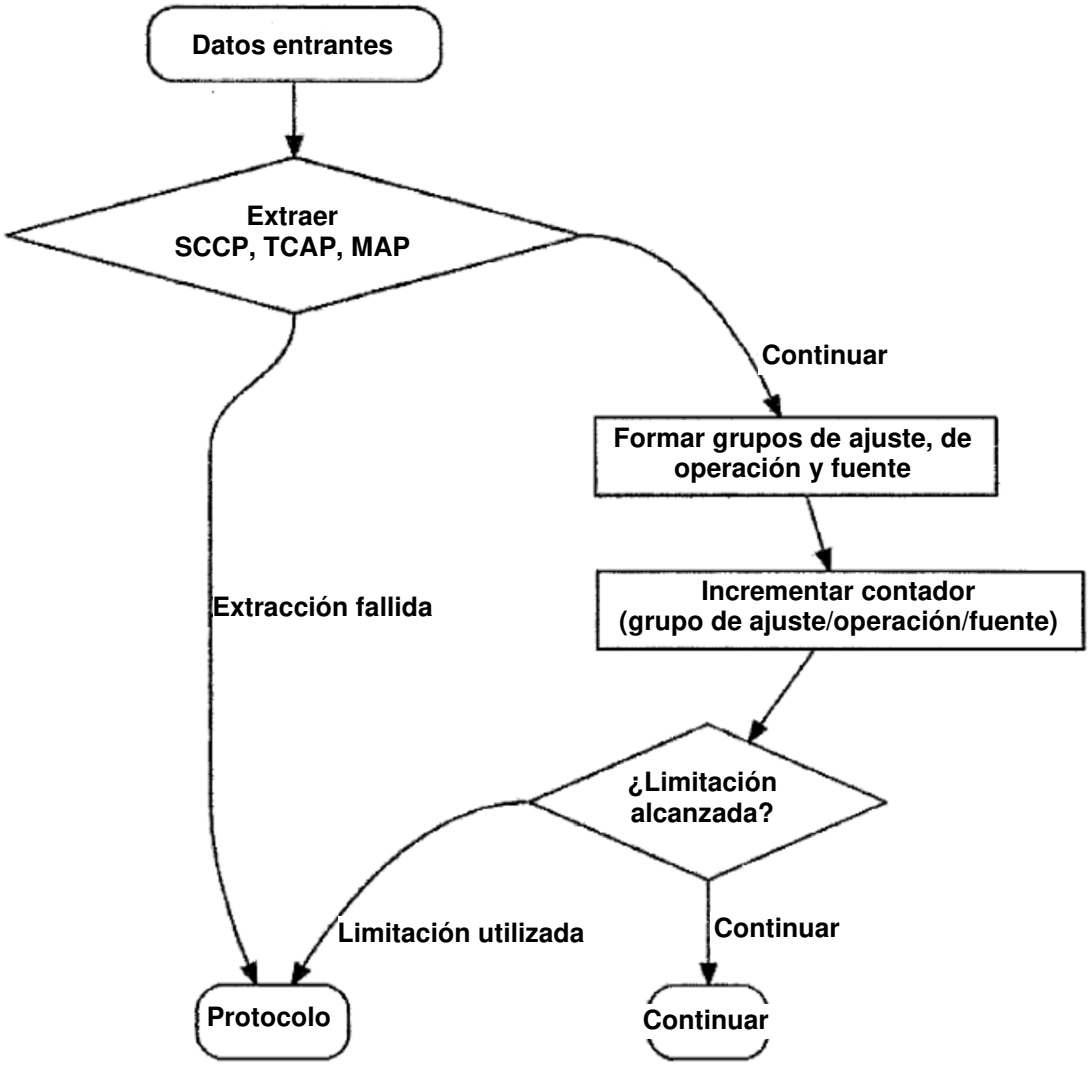
Datos entrantes
Extraer
SCCP, TCAP, MAP
Continuar
Formar grupos de ajuste, de operación y fuente
Incrementar contador
(grupo de ajuste/operación/fuente)
Extracción fallida
¿Limitación alcanzada?
Limitación utilizada
Continuar
Protocolo
Continuar

Fig. 9

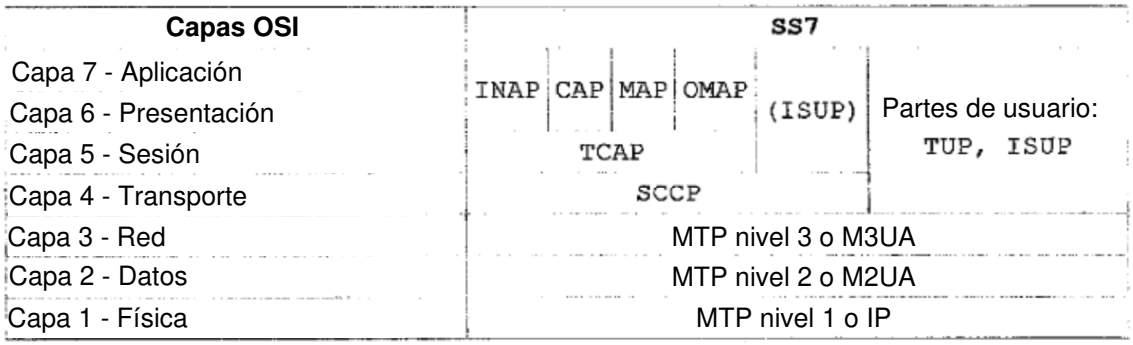
Capas OSI
SS7
Capa 7 - Aplicación
Capa 6 - Presentación
Capa 5 - Sesión
Capa 4 - Transporte
Capa 3 - Red
Capa 2 - Datos
Capa 1 - Física
INAP
CAP
MAP
OMAP
(ISUP)
TCAP
SCCP
Partes de usuario:
TUP, ISUP
MTP nivel 3 o M3UA
MTP nivel 2 o M2UA
MTP nivel 1 o IP

Fig. 10

```
Signalling Connection Control Part
    Message Type: Unitdata (0x09)
    .... 0001 = Class: 0x01
    1000 .... = Message handling: Return message on error (0x08)
    Pointer to first Mandatory Variable parameter: 3
    Pointer to second Mandatory Variable parameter: 14
    Pointer to third Mandatory Variable parameter: 24
    Called Party address (11 bytes)
        Address Indicator
            0... .... = Reserved for national use: 0x00
            .0.. .... = Routing Indicator: Route on GT (0x00)
            ..01 00.. = Global Title Indicator: Translation Type,
Numbering Plan, Encoding Scheme, and Nature of Address Indicator
included (0x04)
            .... ..1. = SubSystem Number Indicator: SSN present
(0x01)
            .... ...0 = Point Code Indicator: Point Code not
present (0x00)
        SubSystem Number: MSC (Mobile Switching Center) (8)
        [Linked to TCAP, TCAP SSN linked to GSM_MAP]
        Global Title 0x4 (9 bytes)
            Translation Type: 0x00
            0001 .... = Numbering Plan: ISDN/telephony (0x01)
            .... 0001 = Encoding Scheme: BCD, odd number of
digits (0x01)
            .000 0100 = Nature of Address Indicator:
International number (0x04)
            Called Party Digits: 62811006827
                Called or Calling GT Digits: 62811006827
                Number of Called Party Digits: 11
                Country Code: 62 Indonesia (Republic of) (length
2)
    Calling Party address (10 bytes)
        Address Indicator
            0... .... = Reserved for national use: 0x00
            .0.. .... = Routing Indicator: Route on GT (0x00)
            ..01 00.. = Global Title Indicator: Translation Type,
Numbering Plan, Encoding Scheme, and Nature of Address Indicator
included (0x04)
            .... ..1. = SubSystem Number Indicator: SSN present
(0x01)
            .... ...0 = Point Code Indicator: Point Code not
present (0x00)
        SubSystem Number: HLR (Home Location Register) (6)
        [Linked to TCAP, TCAP SSN linked to GSM_MAP]
        Global Title 0x4 (8 bytes)
            Translation Type: 0x00
            0001 .... = Numbering Plan: ISDN/telephony (0x01)
            .... 0010 = Encoding Scheme: BCD, even number of
digits (0x02)
            .000 0100 = Nature of Address Indicator:
International number (0x04)
```

```
            Calling Party Digits: 6281105190
                Called or Calling GT Digits: 6281105190
                Number of Calling Party Digits: 10
                Country Code: 62 Indonesia (Republic of) (length
2)
```

Fig. 11