(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 432 668**

(21) Número de solicitud: 201290088

(51) Int. CI.:

H04W 24/06 (2009.01)
H04W 4/24 (2009.01)

(12) SOLICITUD DE PATENTE A2

(22) Fecha de presentación:

05.07.2011

(30) Prioridad:

02.07.2010 US 61/361.136

(43) Fecha de publicación de la solicitud:

04.12.2013

(71) Solicitantes:

ROAMWARE, INC. (100.0%)
20401 Stevens Creek Blvd
95014 Cupertino US

(72) Inventor/es:

JIANG, John, Yue Jun y
GUILLOT, David

(74) Agente/Representante:

TEMIÑO CENICEROS, Ignacio

(54) Título: **PROCEDIMIENTO Y SISTEMA PARA DETECTAR EL FRAUDE POR DERIVACIÓN DE TERMINACIÓN EN UNA RED DE TELECOMUNICACIONES**

(57) Resumen:

Se proporcionan procedimientos y sistemas para detectar e impedir el fraude por derivación en redes de telecomunicaciones, principalmente para detectar e impedir el denominado como fraude SIM box en redes de telecomunicaciones. Los procedimientos incluyen generar una o más llamadas de prueba desde un agente remoto a un agente local donde el agente remoto puede ser un agente de itinerancia o un marcador remoto. El agente local es un número suscriptor. Los procedimientos incluyen adicionalmente facilitar el desvío de las llamadas de prueba del agente local a un número local. Los procedimientos incluyen identificar la presencia de fraude por derivación, analizando la información de identificación del llamante de la llamada de prueba recibida en el número local. Finalmente, los procedimientos incluyen impedir el uso futuro de una puerta de enlace de tipo SIM box detectada.

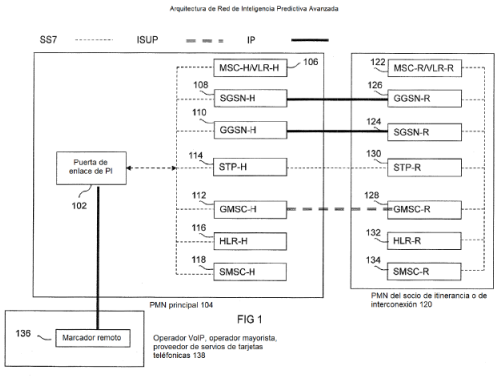

FIG 1

ES 2 432 668 A2

DESCRIPCIÓN

PROCEDIMIENTO Y SISTEMA PARA DETECTAR EL FRAUDE POR DERIVACIÓN DE TERMINACIÓN EN UNA RED DE TELECOMUNICACIONES

CAMPO DE LA INVENCIÓN

La presente invención se refiere a la detección y prevención de fraude en redes de telecomunicaciones. Más específicamente, la presente invención se refiere a procedimientos y sistemas para la detección y prevención en tiempo real de los llamados fraudes por derivación o “by-pass” (en su término en inglés) de terminación, incluyendo la detección y prevención de fraudes basados en puertas de enlace GSM (“global system for mobile”) de tipo “SIM box” en redes de telecomunicaciones.

ANTECEDENTES DE LA INVENCIÓN

Según ha avanzado la tecnología de redes de telecomunicaciones, aunque por un lado resulta enormemente beneficiosa para todos, por otro lado ha dado lugar a diversos tipos de fraudes perpetrados en dichas redes. Un fraude de este tipo se denomina fraude por derivación de terminación, en el que los estafadores cambian el tramo de encaminamiento o enrutamiento (conocido con el término “terminación”) de una llamada telefónica (llamada móvil o llamada de número fijo) para evitar pagar cargos de dicha terminación a una compañía telefónica u operador de terminación para dicha llamada terminada. Estas llamadas pueden ser llamadas nacionales o internacionales que terminan en un operador de terminación.

Por lo general, la derivación de terminación funciona reemplazando la llamada de terminación en la ruta de tránsito de la llamada, por una llamada de origen mediante el uso de otra línea, aprovechando así el coste de arbitraje entre una tasa de terminación de operador de terminación y una cuota de origen de la línea de derivación impuesta por el operador de la línea. Típicamente, esta derivación (o “by-pass”) se realiza usando una línea local, aunque también es posible usar una línea internacional si el estafador de

derivación comete el fraude en la línea internacional. En general, los estafadores de derivación usan una puerta de enlace GSM de tipo SIM box para generar una llamada local de origen GSM, aunque dicha llamada local también puede generarse por un teléfono de línea fija o un teléfono CDMA (del término inglés “code division multiple access”). Además, estos estafadores pueden operar tanto dentro la red (también conocida como “On-net”) como fuera de la red (conocida como “Off-net”). En el caso de la derivación dentro de la red, la línea de derivación usada es la misma que la del operador de terminación de la llamada, mientras que en el caso de la derivación fuera de la red, la línea de derivación usada no es la misma.

Se han diseñado una o más técnicas para hacer frente a tal fraude por derivación. Un procedimiento de este tipo se conoce como sistema de gestión de fraude (en inglés, “fraud management system”, o FMS) en el que éste detecta un SIM box para operadores de telefonía móvil GSM, basándose en el análisis de los registros detallados de llamadas (o, en inglés “call detail record”, conocido por sus siglas CDR). Esto funciona principalmente observando patrones de uso de los SIM box. Por ejemplo, cuando se están haciendo demasiadas llamadas móviles iniciadas sin llamadas móviles terminadas, entonces puede detectarse la presencia de SIM box. Sin embargo, este patrón de análisis no se hace en tiempo real. Además, los estafadores de derivación pueden fingir usos para engañar al FMS. Por lo tanto, el procedimiento FMS puede tener una gran cantidad de falsos positivos si su lógica de implementación no es firme, o puede tener muy pocas detecciones de derivación si es demasiado estricto en su lógica de implementación. Además, el procedimiento FMS puede no detectar a los estafadores de derivación fuera de la red. Adicionalmente, el FMS no realiza una prevención inmediata del estafador. Por otra parte, el FMS no puede impedir que los estafadores de derivación se muevan fuera de la red, lo que lo hace ineficaz para la eliminación del fraude por derivación de terminación, ya que el fraude fuera de la red, aunque menos lucrativo, todavía puede mantener en funcionamiento el negocio del fraude.

Otra técnica para lidiar con los estafadores de derivación es la detección de derivación basada en la generación de llamadas. También se denomina como procedimiento de detección de derivación basado en la generación de llamadas clásicas. Este

procedimiento requiere la implementación de módulos de detección tanto en el país de terminación como en el país de origen y, a continuación, realizar un seguimiento de la llamada internacional que se realiza desde el país de origen al país de terminación para detectar la derivación. Sin embargo, el procedimiento tiene la limitación de hacer necesario el uso de módulos de detección por todo el mundo, en múltiples redes. Al igual que el FMS, no realiza una prevención inmediata de estafadores. Además, no puede impedir que los estafadores de derivación se muevan fuera de la red, lo que lo hace ineficaz para la eliminación del fraude por derivación de terminación, ya que el fraude fuera de la red, aunque menos lucrativo, todavía puede mantener en funcionamiento el negocio del fraude.

En otra solución más, en una de las patentes anteriores de los inventores de la presente solicitud, se ha proporcionado una solución para desarrollar "una solución basada en un solo operador y en el uso de la red para pruebas de itinerancia entrante y saliente, para el descubrimientos de servicios del socio de itinerancia y fraude, sin hacer uso de sondas de itinerancia o el tráfico de itinerancia real". Esta solución se denomina, en lo sucesivo en este documento, como "Inteligencia Predictiva" o "PI", y corresponde a la patente provisional de Estados Unidos Nº 61/361.136 titulada "Advanced Predictive Intelligence".

Hoy en día, la limitación de los procedimientos de detección basados en la generación de llamadas se debe a que implican sólo llamadas de prueba con números de prueba, por lo que los estafadores de derivación inteligentes pueden examinar los patrones de estos números de prueba, y decidir ponerlos en una lista negra para futuros fraudes por derivación. Algunos de los patrones de estos números de prueba son números que llaman demasiadas veces o no contestan muchas veces, etc. Como resultado, los procedimientos de generación de llamadas pierden su eficacia de detección de derivación. Aunque pueden introducirse más números de prueba, surgirá de nuevo el mismo problema de la obtención de los números detectados por el estafador de derivación. Además, el hecho de que los números de prueba sean limitados y que se usen cada vez, implica más trabajo de los operadores de estos números, creando así una solución no escalable.

Mientras que las capacidades de detección de fraude por derivación presentadas en la patente PI anterior sirven para mejorar los resultados del estado de la técnica, tal como se demuestra claramente en dicha patente, todavía existe la necesidad en este campo técnico de aplicar la detección de derivación de manera invisible, para dificultar a los estafadores detectar que están siendo analizados. En particular, los números de prueba utilizados por PI para llamadas pueden detectarse fácilmente por los estafadores de derivación, a menos que se mantengan cambiando de forma continua, lo que debilita el procedimiento. Además, la patente PI anterior únicamente incluye el inicio de llamadas desde redes móviles a través de socios de itinerancia de una red de operador doméstica. Aunque estos inicios de llamada a menudo comparten tránsito y rutas de terminación con llamadas iniciadas no móviles, no obstante aún existen muchas rutas no compartidas. Por lo tanto, todavía puede fallar la detección de líneas de derivación de terminación en esas rutas no compartidas. Además, el procedimiento de PI anterior no termina inmediatamente una línea de derivación una vez detectada. Tan pronto como una línea de derivación se va fuera de la red, la PI anterior será capaz de detectarlo pero incapaz de impedirlo de nuevo.

De acuerdo con lo anterior, existe la necesidad en el citado campo técnico de un sistema, un procedimiento y un producto informático para proporcionar una solución basada en un operador y basada en redes que dé al operador inteligencia para encargarse los problemas que se han mencionado anteriormente.

En este documento, se mezclará el uso de fraude por derivación de terminación y el fraude mediante uso de SIM box para simplificar la descripción, aunque se debe entender que la derivación de terminación es un concepto más genérico que el fraude mediante SIM box, y la solución descrita sobre el fraude de tipo SIM box puede aplicarse igualmente al fraude por derivación de terminación en general.

EXPLICACIÓN DE LA INVENCIÓN

La presente invención se refiere a un procedimiento y a un sistema para detectar e impedir el fraude por derivación en redes de telecomunicaciones. La invención en sus

diversos aspectos se refiere a un procedimiento y un sistema para detectar derivación de terminación en general, y fraude basado en una puerta de enlace GSM de tipo SIM box en particular, en redes de telecomunicaciones introduciendo números de suscriptores reales de un operador base para llamadas de prueba sin afectar a los suscriptores reales.

El procedimiento incluye generar una o más llamadas de prueba desde un agente remoto a un agente local, donde el agente local es un número suscriptor y el agente remoto puede ser un agente de itinerancia o un marcador remoto; considerando que un agente de itinerancia se crea en un socio de itinerancia del operador base (proveedor telefónico) y un marcador remoto es un servicio de marcación conectado a operadores de voz sobre IP (VoIP), operadores mayoristas y servicios de tarjetas telefónicas de todo el mundo. El procedimiento incluye, adicionalmente, facilitar el desvío de las llamadas de prueba del agente local a un número local. El procedimiento incluye adicionalmente responder de forma aleatoria las llamadas de prueba o aplicar identificaciones de llamada diferentes a las llamadas de prueba. El procedimiento incluye identificar la presencia de un fraude por derivación analizando la información de identificación del llamante de una llamada de prueba recibida en el número local. Finalmente, el procedimiento incluye el bloqueo inmediato de la capacidad de llamada de origen de la línea de derivación, agotando su saldo de prepago, suspendiendo o terminando completamente su perfil de suscripción para una línea de derivación de terminación dentro de la red y, para una línea de derivación fuera de la red, el procedimiento usa la base de datos de las líneas de derivación recogidas para interceptar todas las llamadas de las redes fuera de la red, deshabilitando o interrumpiendo las llamadas con un identificador de llamadas de la base de datos de las líneas de derivación fuera de la red.

El sistema de la presente invención, en sus diversas realizaciones, impide el fraude por derivación en redes de telecomunicaciones después de detectar la existencia de derivación usando una puerta de enlace desplegada en un operador base. Para una línea de derivación dentro de la red, la puerta de enlace impide inmediatamente la capacidad de llamadas de origen de la línea, agotando su saldo de prepago, o suspende o termina completamente su perfil de suscripción. Para una línea de derivación fuera de la red, la puerta de enlace las almacena en una base de datos y usa la base de datos para

interceptar todas las llamadas de las redes fuera de la red, deshabilitando o interrumpiendo las llamadas con el identificador de llamadas de la base de datos de las líneas de derivación fuera de la red.

El sistema de la presente invención, en sus diversas realizaciones, detecta el fraude por derivación en redes de telecomunicaciones, desplegando una puerta de enlace en una red de un operador base. A continuación, la puerta de enlace genera una o más llamadas de prueba desde un agente remoto a un agente local, donde el agente local es un número suscriptor y el agente remoto puede ser un agente de itinerancia o un marcador remoto; y donde el agente de itinerancia se crea en un socio de itinerancia del operador base, y el marcador remoto es un servicio de marcación conectado a operadores de VoIP, operadores mayoristas y servicios de tarjetas telefónicas por todo el mundo. La puerta de enlace facilita adicionalmente el desvío de las llamadas de prueba del agente local a un número local. Este número local es un número de prueba del operador base. Finalmente, la puerta de enlace identifica la presencia de fraude por derivación, analizando la información de identificación del llamante de la llamada de prueba recibida en el número local.

El sistema de la presente invención, en sus diversos aspectos, detecta el fraude por derivación en redes de telecomunicaciones simulando un comportamiento similar al humano en agentes locales. Esto se consigue respondiendo automáticamente la llamada en el agente local, o dirigiendo la llamada del agente local a un sistema similar a un contestador.

El sistema de la presente invención, en sus diversos aspectos, impide el fraude por derivación en redes de telecomunicaciones después de detectar una derivación, usando una puerta de enlace desplegada en un operador base. Para una línea de derivación dentro de la red, la puerta de enlace impide inmediatamente la capacidad de llamadas de origen de la línea, agotando su saldo de prepago, o suspende o termina completamente su perfil de suscripción. Para una línea de derivación fuera de la red, la puerta de enlace las almacena en una base de datos y usa la base de datos para interceptar todas las llamadas de las redes fuera de la red deshabilitando o interrumpiendo las llamadas con el

identificador de llamadas de la base de datos de las líneas de derivación fuera de la red.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La figura 1 ilustra un esquema del sistema para la detección de fraude por derivación en redes de telecomunicaciones, de acuerdo con un aspecto de la presente invención.

La figura 2 representa un diagrama de flujo de los pasos de un procedimiento para la detección de fraude por derivación en redes de telecomunicaciones, de acuerdo con un aspecto de la presente invención.

La figura 3 representa un diagrama de flujo de los pasos para responder las llamadas de prueba con el fin de detectar el fraude SIM box, de acuerdo con un aspecto del procedimiento según la presente invención.

La figura 4 representa un diagrama de flujo de los pasos para la gestión de las llamadas de prueba para terminaciones de llamada de tipo T-CSI (del inglés, “CAMEL subscription information termination”, donde CAMEL corresponde a las siglas en inglés de “aplicación personalizada para la lógica mejorada de redes móviles”) cuando dicha T-CSI se configura en el perfil del suscriptor con el fin de impedir el fraude SIM box, de acuerdo con un aspecto de la presente invención.

La figura 5 representa un diagrama de flujo para la gestión de las llamadas de prueba mediante desvío de llamadas incondicional (denominado CFU, del inglés “call forward unconditional”), cuando dicho CFU se configura en el perfil del suscriptor para impedir el fraude SIM box, de acuerdo con un aspecto de la presente invención.

La figura 6 representa un diagrama de flujo para desactivar las puertas de enlace de tipo SIM box dentro de la red tras su detección, de acuerdo con un aspecto de la presente invención.

La figura 7 representa un diagrama de flujo de las etapas para bloquear llamadas fuera

de la red en los SIM box fuera de la red detectados, de acuerdo con un aspecto de la presente invención.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

En la siguiente descripción se exponen referencias, materiales y configuraciones con el fin de proporcionar un entendimiento minucioso de la presente invención. Será evidente, no obstante, para un experto en la técnica, que la presente invención puede llevarse a la práctica sin estos detalles específicos. En algunos casos, se pueden omitir o simplificar rasgos bien conocidos, para no oscurecer la presente invención. Adicionalmente, la referencia en la memoria descriptiva a "un aspecto" se refiere a un rasgo, estructura o característica particular descrita junto con el aspecto, incluida en al menos una variación o realización de la presente invención. La aparición de la frase "en un aspecto", en diversos lugares de la memoria descriptiva, no se refiere necesariamente al mismo aspecto.

Con relación a los acrónimos y siglas utilizados en el presente documento, sus referencias y descripciones se incorporan, con fines explicativos, en la sección “Descripción de acrónimos y siglas utilizadas”.

La presente invención proporciona un sistema y un procedimiento para detectar fraude por derivación en redes de telecomunicaciones. La idea general de esta invención es crear una llamada de prueba desde un agente remoto a un agente local de un operador base (es decir, un operador anfitrión) para detectar el fraude por derivación en llamadas de terminación en la red del operador base. El agente remoto puede ser un agente de itinerancia en un socio de itinerancia o de interconexión del operador base, o un marcador remoto conectado a operadores mayoristas, operadores de VoIP o proveedores de servicios de tarjetas telefónicas. Por lo tanto, esto ayuda a impedir pérdidas de ingresos controlando todos los fraudes antes de que tenga lugar cualquier fraude real. La presente invención ayuda, adicionalmente, a que el operador anfitrión aumente sus ingresos, reduzca sus pérdidas, impida el fraude y mejore la experiencia del cliente y la calidad.

El operador de red anfitrión implementa una solución de Inteligencia Predictiva Avanzada, (en lo sucesivo en este documento, de nominada como PI Avanzada o PI) para detectar el fraude por derivación en redes de telecomunicaciones. El operador de red anfitrión instala una puerta de enlace de PI avanzada de la red principal o en una ubicación centralizada que está conectada a la red principal. De este modo, una puerta de enlace de PI es capaz de servir a múltiples operadores en el mismo o en diferentes países para detectar el fraude por derivación.

El procedimiento de PI avanzada incluye crear una llamada de prueba desde un agente remoto en un país de llamada de origen a un agente local del operador base. El número del agente local se selecciona entre un número suscriptor real del operador base. La idea es usar cualquier número suscriptor seleccionado o la totalidad de números del operador base durante un corto tiempo como agentes locales, y después desviar temporalmente la llamada de prueba a un número local (es decir, el número de prueba en un operador anfitrión). Este número local se configura para pasar el control de la llamada a la puerta de enlace de PI desplegada en el país de llamada de terminación (es decir, el operador base/anfitrión). Finalmente, el procedimiento incluye identificar la presencia de un fraude por derivación, analizando el identificador de llamadas de la llamada de prueba recibida en el número local. Después de que se complete la llamada de prueba, el estado de desvío de la llamada inicial del número suscriptor se restaura a su estado anterior. De esta manera, es virtualmente imposible para el estafador de derivación detectar los patrones de uso de los números suscriptores reales. Incluso en el caso de que estos números suscriptores estén en una lista negra para fraude por derivación, no se verán afectados por posible derivación en el futuro ante cualquier llamada a estos, consiguiendo así el objetivo final de reducir el fraude por derivación.

Otro aspecto de la invención se refiere al uso de un agente de itinerancia como agente remoto. Como resultado de la configuración, el flujo de llamadas generales en la realización de este aspecto de la invención es similar: una puerta de enlace de PI crea un agente de itinerancia a través de la creación de un perfil virtual en una red del socio de itinerancia del operador base, donde dicho perfil contiene todos los desvíos de llamadas

condicionales a un agente local. Después, inicia una llamada de prueba al número del agente de itinerancia. La llamada alcanza la red del socio de itinerancia. Ya que el itinerante es virtual, la llamada se desvía al agente local (es decir, el número suscriptor), que básicamente simula una llamada internacional de la red del operador del socio de itinerancia a la red del operador base. Después, la llamada alcanza la red principal en el agente local. Un estafador de derivación podría estar involucrado en esta etapa de la llamada. Como el número suscriptor real se desvía momentáneamente a un número de prueba mediante una puerta de enlace de PI, el control de la llamada termina finalmente en la puerta de enlace de PI. Entonces, la puerta de enlace de PI puede examinar el identificador de llamadas de la llamada de prueba para determinar se ha hecho o no un by-pass.

Otro aspecto de la invención se refiere al uso de un marcador remoto como agente remoto. Como resultado de la configuración, el flujo de llamadas general en esta realización de la invención es similar: una puerta de enlace de PI pasa un número del agente local al marcador remoto para hacer una llamada inmediata. Después, el marcador remoto inicia una llamada de prueba al número del agente local. La llamada alcanza la red del operador base en el agente local. Un estafador de derivación podría estar involucrado en esta etapa de la llamada. Como el número suscriptor real se desvía momentáneamente a un número de prueba mediante una puerta de enlace de PI, el control de la llamada termina finalmente en la puerta de enlace de PI. Entonces, la puerta de enlace de PI puede examinar el identificador de llamadas de la llamada de prueba para determinar se ha hecho o no un by-pass. El marcador remoto informa a la puerta de enlace de PI de la información de la llamada de prueba, tal como el identificador de llamada, número llamado, operador usado, fecha, hora y duración de la llamada. La puerta de enlace de PI pasa el resultado de la llamada de prueba al marcador remoto.

En las diversas realizaciones de la presente invención, la solución de PI avanzada se basa en señalización (por ejemplo, de tipo SS7 o IP) y se implementa para el país de terminación del operador base de una llamada de prueba. Será evidente para un experto en la técnica que la invención también puede usarse para una solución no basada en señalización, aunque entonces requerirá una configuración adicional y será necesario

más control manual.

Para simplificar la descripción del documento, se explicarán los diversos aspectos de la presente invención, de forma intercambiable usando detección mediante puerta de enlace de tipo SIM box GSM, y detección de derivación de terminación, con fines ilustrativos de la invención. Sin embargo, se apreciará por un experto en la técnica que la presente invención puede generalizarse de forma similar a otras líneas de detección de derivación, incluyendo, pero sin limitación, derivación de línea fija, derivación CDMA o derivación GSM en circuitos de llamadas nacionales e internacionales.

La figura 1 ilustra un sistema 100 que implementa la PI avanzada de acuerdo con un aspecto de la presente invención. El sistema 100 incluye un módulo de Inteligencia Predictiva (PI) 102 (es decir, una puerta de enlace de PI o una puerta de enlace convencional) en una red móvil pública principal (PMN) 104 (es decir, la red principal). El módulo de PI 102 tiene la capacidad de detectar el fraude por derivación en redes de telecomunicaciones, y particularmente de detectar, seguir e impedir el fraude de tipo SIM box en telecomunicaciones. El operador de la PMN principal 104 usa el módulo de PI 102 para comunicar con un agente remoto para la generación de llamadas de prueba a un agente local en la PMN principal 104. La PMN principal 104 incluye, adicionalmente, un centro de conmutación móvil (MSG)/registro de ubicación de visitantes (VLR) 106, un nodo de soporte GPRS de servicio (SGSN) 108, un nodo de soporte de puerta de enlace GPRS (GGSN) 110, una puerta de enlace de MSC (GMSC) 112, un punto de transferencia de señalización (STP) 114, un registro de ubicación base (HLR) 116 y un centro servidor de mensajes cortos (SMSC) 118. Ya que los elementos de la red, MSC/VLR 106, SGSN 108, GGSN 110, GMSC 112, STP 114, HLR 116 y SMSC 118, residen en la PMN principal 104, en lo sucesivo en este documento se denominan como MSC-H/VLR-H 106, SGSN-H 108, GGSN-H 110, GMSC-H 112, STP-H 114, HLR-H 116 y SMSC-H 118, respectivamente. Estos elementos de red comunican entre sí por un enlace del sistema de señalización Nº 7 (SS7) (representado por las líneas discontinuas en la figura 1), o a través de un enlace de protocolo de Internet (IP) (representado por líneas continuas en la figura 1).

El sistema 100 incluye adicionalmente una PMN del socio de itinerancia 120 (es decir, la red del socio de interconexión no necesita ser móvil) que está asociada con la PMN principal 104. Será evidente para un experto en la técnica que el sistema 100 puede incluir diversas redes de socios diferentes. Sin embargo, para mayor comodidad, este aspecto considera únicamente una red de socio (es decir, la PMN 120, de itinerancia o interconexión, móvil o no). La PMN del socio 120 incluye un MSC/VLR 122, un SGSN 124, un GGSN 126, una GMSC 128, un STP 130, un HLR 132 y un SMSC 134, y algunos de estos elementos pueden no estar presentes en una red no móvil. Ya que estos elementos de red, MSC/VLR 122, SGSN 124, GGSN 126, GMSC 128, STP 130, HLR 132 y SMSC 134, residen en la PMN del socio de itinerancia 120, en lo sucesivo en este documento se denominan como MSC-R/VLR-R 122, SGSN-R 124, GGSN-R 126, GMSC-R 128, STP-R 130, HLR-R 132 y SMSC-R 134, respectivamente.

Todos estos elementos de red de la PMN del socio 120 comunican entre sí a través del enlace del SS7 o a través del enlace IP. Además, como se muestra en la figura 1, los elementos de red de la PMN del socio 120 también comunican con los elementos de red de la PMN principal 104. Por ejemplo, la GMSC-R 128 comunica con la GMSC-H 112 a través de un enlace de protocolo de parte de usuario ISDN (ISUP), mientras que el SGSN-R 124 y el GGSN-R 126 comunican con el GGSN-H 110 y el SGSN-H 108, respectivamente a través del enlace IP. Otros elementos de red de la PMN del socio 120 (por ejemplo, MSC-R/VLR-R 122) comunican con diversos elementos de red diferentes de la PMN principal 104 (por ejemplo, HLR-H 116) a través del enlace del SS7. También será evidente para un experto en la técnica que la PMN principal 104 también puede incluir diversos componentes de red diferentes (no mostrados en la figura 1), dependiendo de la arquitectura a considerar. En un aspecto de la presente invención, diversos elementos de red de la PMN principal 104 y la PMN del socio 120 se localizan en una base de datos de tipo IR.21 (no se muestra en la figura 1), tal como IR.21 de RAEX. En un aspecto de la presente invención, la base de datos IR.21 se acopla al módulo de PI 102.

El sistema 100 incluye adicionalmente una o más redes de socios de proveedores de servicios de operadores mayoristas, VoIP o llamadas 138 que están asociados con la

PMN principal 104. Será evidente para un experto en la técnica que el sistema 100 puede incluir diversas redes de socios diferentes. Las redes de socios 138 están conectadas con un marcador remoto, que comunica con la puerta de enlace de PI en la PMN principal 104 a través de señalización IP.

La puerta de enlace de PI 102 conecta con diversos componentes en la PMN principal 104 y la PMN de socios 120 o redes de socios 138 para detectar, seguir e impedir el fraude SIM box que se aplica a sus suscriptores.

La figura 2 representa un diagrama de flujo para la detección de fraude por derivación en redes de telecomunicaciones, de acuerdo con un aspecto de la presente invención. La puerta de enlace de PI 102 comunica con un agente remoto.

Cuando el agente remoto es un marcador remoto, la puerta de enlace de PI 102 comunica con el marcador remoto en una red de socios 138, usando IP con un número del agente local. Ahora, con el fin de comenzar a detectar el fraude SIM box, en la etapa 202, la puerta de enlace de PI 102 ordena al marcador remoto que haga llamadas de prueba al agente local.

Cuando el agente remoto es un agente de itinerancia, la puerta de enlace de PI 102 crea en primer lugar un agente de itinerancia en la PMN del socio de itinerancia 120, usando técnicas de señalización. Esto significa que la puerta de enlace de PI 102 crea un perfil falso de un suscriptor con todos los desvíos de llamadas condicionales a un agente local, en la PMN del socio de itinerancia 120 para formar un agente de itinerancia. Ahora, con el fin de comentar a la detección de un fraude SIM box, en la etapa 202, la puerta de enlace de PI 102 configura llamadas de prueba del agente de itinerancia al agente local. Esto se consigue generando una o más llamadas de prueba a este agente de itinerancia. Con fines de explicación, se considera una llamada de prueba para explicar la función de la invención. Sin embargo, un experto en la técnica apreciará que se harán muchas llamadas de prueba de este tipo por la puerta de enlace de PI 102 para detectar e impedir el fraude SIM. Posteriormente, la puerta de enlace de PI 102 facilita el desvío de la llamada de prueba del agente de itinerancia a un agente local. En un aspecto de la

presente invención, este desvío de llamadas es condicional, ya que el agente de itinerancia no responde a la llamada de prueba, ya que esta no existe, por lo que la llamada de prueba se reenvía a un número de agente local configurado previamente.

Por lo tanto, en la etapa 204, la puerta de enlace de PI 102 facilita el desvío de las llamadas de prueba del agente local a un número local. De acuerdo con un aspecto de la presente invención, el número local es un número de la red PMN principal 104. El número local se selecciona entre una combinación de números predefinidos. En un aspecto de la invención, este desvío de llamadas es el desvío de llamadas incondicional del agente local al número local. Finalmente, en la etapa 206, la puerta de enlace de PI 102 identifica la presencia de un SIM box haciendo un seguimiento de la terminación de las llamadas de prueba al número local.

De acuerdo con un aspecto adicional de la presente invención, la puerta de enlace de PI 102 configura el número local para entregar el control de llamada (a través de la provisión de T-CSI) a la puerta de enlace de PI 102. En base a esto, la puerta de enlace de PI 102 identifica el identificador de llamadas de la llamada de prueba al terminar en el número local. En caso de que este identificador de llamadas sea diferente de del identificación de llamadas establecido en el momento en el que la puerta de enlace de PI inició esta llamada de prueba del agente remoto al agente local, entonces ésta se identifica como un fraude SIM box en el circuito de llamadas después de que el identificador de llamadas pase a través de algunas lógicas de análisis de falso positivo.

Tal y como se ha descrito en el apartado de análisis del estado de la técnica, en sistemas anteriores relacionados con este campo la puerta de enlace no responde a las llamadas de prueba para evitar costes (itinerancia, internacional o nacional) relacionados con estas llamadas de prueba. Esto permite que los estafadores de SIM box determinen que algunas de estas llamadas son realmente llamadas de prueba y, por lo tanto, eviten usar estas llamadas de prueba para el by-pass de SIM box. Por tanto, la premisa clave para una detección de SIM box estable se correlaciona con la no detección de la actividad de seguimiento por parte de los estafadores. Con el fin de superar esta situación, de acuerdo con varios aspectos de la presente invención, la puerta de enlace de PI genera las

llamadas de prueba con parámetros de llamada aleatorios y además responde algunas de las llamadas de prueba para evitar que sean detectadas por los estafadores de SIM box. De este modo, y de acuerdo con un aspecto de la presente invención, los parámetros de llamadas son aleatorios usando uno o más de los siguientes elementos:

1. Parte llamante en la llamada de prueba sin identificación de línea llamante (CLI).
2. Parte llamante en llamadas de prueba con un número suscriptor real.
3. Parte llamante en llamadas de prueba con cualquier número.
4. Llamada de prueba de un número aleatorio de la PMN de itinerancia 120.
5. Llamada de prueba de cualquier número corrupto.
6. Origen de liberación de la llamada de prueba (desde la parte llamante o la llamada).

De acuerdo con un aspecto de la presente invención, la puerta de enlace de PI 102 libera la llamada de prueba inmediatamente después de detectar el fraude SIM box. En otro aspecto de la presente invención, la puerta de enlace de PI 102 libera la llamada de prueba después de un periodo de tiempo configurable. En otro aspecto de la presente invención, el agente local se selecciona entre una agrupación de números en cuarentena. Además, la selección del agente local para una llamada de prueba se controla con el fin de que cualquier agente local no se seleccione dos veces hasta que se use toda la agrupación de agentes locales una vez para la generación de estas llamadas de prueba. En otro aspecto de la presente invención, un agente local puede ser puesto en cuarentena durante más tiempo.

Con el fin de garantizar que los estafadores de SIM box no detecten las llamadas de prueba, de acuerdo con diversos aspectos de la presente invención, la puerta de enlace de PI 102 responde las llamadas de prueba en el número local de terminación. En otro aspecto, las llamadas de prueba se responden durante una duración de tiempo configurable. En otro aspecto más, las llamadas de prueba se responden en base a un coste supervisado de las llamadas de prueba, que ayuda a definir la duración de tiempo configurable de respuesta. En un aspecto de la invención, la puerta de enlace de PI 102 se acopla con un módulo lógico de medición de coste que proporciona el coste de la llamada de prueba. La lógica de medición de coste se lleva a cabo antes de que se

responda la llamada de prueba. En caso de que la lógica de medición de coste detecte que se ha llegado a un tope de presupuesto, la puerta de enlace de PI 102 no lleva a cabo la lógica de respuesta y se libera la llamada de prueba. Ya que el coste de las llamadas de prueba varía con el tipo de llamada, el operador determina diferentes lógicas de respuesta para implementar la PI avanzada en un entorno móvil o subsistemas al por mayor.

En otro aspecto de la presente invención, la PI también se extiende para incluir redes iniciadas no móviles, tales como tarjetas telefónicas, operadores mayoristas y operadores de VoIP. La idea básica es comunicar con un marcador remoto proporcionando un número del agente local para llamar. El marcador remoto puede ser una sonda SIM GSM, una sonda de línea fija, un servicio de tarjeta telefónica o marcador que implica operadores de VoIP y operadores mayoristas. Funciona de forma similar a un agente de itinerancia, con la excepción de que el marcador remoto hará directamente una llamada en lugar de desencadenarse por el desvío de una llamada en un agente de itinerancia iniciado por PI.

La PI también puede proporcionar, opcionalmente, un número llamante al marcador remoto a presentar como el identificador de llamadas de la llamada de prueba. El agente local puede corresponder a números de prueba o suscriptores reales. Después de realizar la llamada de prueba por el marcador remoto, el marcador puede informar al sistema de PI (el número llamado, el número llamante, el tiempo y la zona horaria de la llamada, la ruta o el operador usado). El sistema de PI responderá con el identificador de llamadas recibido actualmente y otra información (tal como la hora de la llamada de prueba recibida). El sistema de PI y el marcador remoto pueden comunicar a través de IP o SS7 o cualquier otro mecanismo de comunicación. La selección del agente local será igual que anteriormente. En particular, cuando se selecciona un suscriptor real para un marcador remoto, la PI realiza el desvío de llamadas incondicional a un número de prueba anticipado. Además, después de que el marcador remoto informe al sistema de PI de la llamada que se acaba de hacer, el sistema de PI restaurará el perfil de desvío de llamadas incondicional del suscriptor real como anteriormente.

En un aspecto de la presente invención, una vez que se identifica un estafador de SIM box o de derivación de terminación a través del uso de un número local, el número local puede ponerse en cuarentena para su uso adicional durante un tiempo en base a alguna lógica.

En las descripciones a continuación, se usa un agente de itinerancia para ilustrar el uso de un agente remoto. Asimismo, resultará evidente para el experto en la técnica que un marcador remoto puede aplicarse de forma similar como agente remoto.

La figura 3 representa un diagrama de flujo para responder las llamadas de prueba con el fin de detectar el fraude SIM box, de acuerdo con un aspecto de la presente invención. Como se ha explicado anteriormente para un agente de itinerancia como agente remoto, la puerta de enlace de PI 102 crea en primer lugar un perfil de un agente de itinerancia en la PMN de itinerancia 120. Posteriormente, inicia una llamada de prueba al agente de itinerancia usando un mensaje de tipo IAM (RA). Ya que el agente de itinerancia, es virtual (inexistente), no responde a la llamada y, por lo tanto, la llamada se desvía a un agente local. El desvío de llamadas condicional se hecho ya por la puerta de enlace de PI 102. Posteriormente, la llamada desviada al agente local alcanza la GMSC de la PMN principal (GMSC-H 112). Después, la GMSC-H 112 envía un mensaje IDP (Agente Local) a la puerta de enlace de PI 102 que solicita la terminación. Ahora, el agente local se preconfigura con el desvío de llamadas incondicional (CFU) a un número local. Si la puerta de enlace de PI 102 decide responder la llamada de prueba, entonces devuelve la consulta IDP del GMSC-H 112 con un mensaje de “continuar” con la dirección de IVR. Esta dirección de IVR es el número de un servidor contestador automatizado usado por el operador de la PMN principal 104. En otro aspecto de la presente invención, la propia puerta de enlace de PI 102 responde la llamada, por lo que devuelve el mensaje de “continuar” con su propia dirección. Por lo tanto, el GMSC-H 112 envía como consecuencia un mensaje IAM a la IVR o la puerta de enlace de PI 102. Posteriormente, después del seguimiento del identificador de llamadas en la terminación, la puerta de enlace de PI 102 determina la presencia de un SIM box y libera la llamada de prueba.

Con las herramientas estadísticas mejoradas para reunir la información de inteligencia

sobre la actividad de la llamada, muchos estafadores de SIM box siguen las llamadas al número del agentes locales y los ponen en una lista negra para líneas de derivación. Con el fin de superar esta limitación, de acuerdo con diversos aspectos de la presente invención, se usan suscriptores reales como agentes locales. Esto permite el aumento del número de agentes locales a potencialmente el número de suscriptores reales con la PMN principal 104. Ahora, ya que el agente local es un suscriptor real, se hace la configuración de su perfil en el HLR-H 116 para permitir que la puerta de enlace de PI 102 obtenga los detalles de la terminación de llamadas. En un aspecto de la presente invención, la puerta de enlace de PI 102 usa un enfoque T-CSI CAMEL en el que el agente local/suscriptor real se suministra con una T-CSI estática en el HLR-H 116. En otro aspecto de la presente invención, la puerta de enlace de PI 102 tiene el desvío de llamadas incondicional (CFU) establecido en el HLR-H 116 para dirigirse a un número local. Estas configuraciones garantizan que no hay ningún impacto para el cliente y que la dependencia de la puerta de enlace de PI no existe. Por ejemplo, cuando la puerta de enlace de PI está operativa, el suscriptor nunca ve que se usó para una llamada de prueba, ya que su experiencia es perfecta. Además, en el caso de que la puerta de enlace de PI no esté operativa, entonces el suscriptor aún recibe sus llamadas regulares, pero no llamadas de prueba.

La figura 4 representa un diagrama de flujo para la gestión de las llamadas de prueba cuando la T-CSI se configura en el perfil del suscriptor con el fin de impedir el fraude SIM box, de acuerdo con un aspecto de la presente invención. El operador de la PMN principal 104 define un equivalente de tipo T-CSI o INAP, que se dirige a la puerta de enlace de PI 102 en el perfil del suscriptor. Esta configuración sucede a través de un proceso HLR regular en el operador de la PMN principal 104. Como resultado, cualquier llamada a un suscriptor desencadena una interacción CAMEL/IDP entre el GMSC-H 112 y la puerta de enlace de PI 102. Ya que las llamadas de prueba se controlan por la puerta de enlace de PI 102, sólo estas llamadas de prueba se liberan por la puerta de enlace de PI 102. Se permite cualquier llamada fuera de las llamadas de prueba para continuar como habitualmente. La puerta de enlace de PI 102 configura la T-CSI CAMEL con una Gestión de llamadas por error para continuar, con el fin de garantizar que llamadas MT para el suscriptor están realizándose sin problemas incluso cuando la puerta de enlace

de PI 102 no está disponible. Como se muestra en la figura 4, la puerta de enlace de PI 102 envía un IAM para el suscriptor como Agente local, al VLR-R 122. El VLR-R 122 devuelve el IAM al GMSC-R 128, que, a su vez, desvía el IAM (suscriptor) al GMSC-H 112. Después, el GMSC-H 112 envía una SRI al HLR-H 116, y cuando el GMSC-H 112 recibe la T-CSI en ACK SRI entonces desencadena el MT-IDP CAMEL para la puerta de enlace de PI 102. Ahora, la puerta de enlace de PI 102 puede liberar o continuar dependiendo de si la llamada de prueba está en curso. En caso de que el suscriptor real no se esté usando para llamadas de prueba, cualquier llamada al suscriptor se responde por la puerta de enlace de PI 102 con un mensaje de “continuar”.

Como la T-CSI requiere una configuración estática, en un aspecto alternativo de la presente invención, la puerta de enlace de PI 102 controla dinámicamente la configuración de activación o desactivación del desvío de llamadas incondicional (CFU) para un suscriptor seleccionado que se dirige a un agente local existente. El CFU se configura después de que se haga la prueba, actualizando el perfil HLR del suscriptor. De acuerdo con diversos aspectos de la presente invención, únicamente se selecciona un suscriptor a la vez como un agente local. Tan pronto como la llamada de prueba se completa, el CFU se elimina del perfil del suscriptor. La figura 5 representa un diagrama de flujo para la gestión de las llamadas de prueba cuando el CFU se configura en el perfil del suscriptor para impedir el fraude SIM box, de acuerdo con un aspecto de la presente invención. Una vez que la puerta de enlace de PI 102 crea el agente de itinerancia, éste envía un mensaje de Interrogar SS al HLR-H 116 y establece un CFU en el perfil del suscriptor. Posteriormente, cuando la puerta de enlace de PI 102 inicia la llamada de prueba al agente de itinerancia, éste obtiene la devolución de la llamada ya que el agente de itinerancia tiene un CF condicional (sin respuesta) al suscriptor. Posteriormente, la puerta de enlace de PI 102 envía un mensaje SRI al HLR-H 116. El HLR-H 116 devuelve el CFU a la puerta de enlace de PI 102, posteriormente, el GMSC-H 112 envía el IDP (suscriptor) a la puerta de enlace de PI 102. La puerta de enlace de PI 102 libera la llamada de prueba y después borra la configuración del CFU de la puerta de enlace de PI a la dirección CFU antigua.

De acuerdo con diversos aspectos de la presente invención, únicamente se usa a la vez

un suscriptor real como agente local. Aunque el operador de la PMN principal 104 puede asignar potencialmente millones de suscriptores como agentes locales, evitando así la detección de los estafadores de SIM box, el procedimiento se aplica sólo a un suscriptor a la vez y se suspende tan pronto como termine la prueba. Adicionalmente, antes de realizar esta llamada de prueba, la puerta de enlace de PI 102 almacena siempre la dirección CFU original del suscriptor que se recupera una vez se completa la prueba. Todas las acciones tomadas por la puerta de enlace de PI se mantienen en un medio no volátil que garantiza una desactivación del CFU a través de procesos de vigilancia externa.

En otro aspecto de la presente invención, el patrón de las llamadas de prueba a suscriptores como agentes locales se configura en línea con el patrón de tráfico actual y el comportamiento de destino final. Esto ayuda a mantener el modo silencioso de detección SIM box. Esto se logra al azar respondiendo a una llamada de prueba con duración aleatoria, también desviando de forma aleatoria una llamada de prueba a un dispositivo similar a un contestador o cambiando de manera aleatoria el identificador de llamadas (desconocido, número internacional, cualquier número de suscriptor real, identificador de llamadas en falso o mal formateado, etc.).

Además del coste de respuesta de las llamadas contestadas intencionalmente, también hay costes del fraude de respuesta temprana en las llamadas de prueba. Estos se generan para algunos operadores de tránsito para contestar una llamada antes de que la parte llamada responda realmente a la llamada. Para controlar estos costes, las llamadas contestadas se miden en base a una configuración. La medición puede hacerse por una red remota que puede ser una red del socio de itinerancia, una red del operador mayorista, un operador de VoIP o un proveedor de servicios de tarjetas telefónicas.

Una vez que se identifica el estafador de SIM box o de derivación de terminación, es importante que se impida un uso futuro de la línea de derivación. Para un SIM box dentro de la red, la puerta de enlace impide inmediatamente la capacidad de llamadas de origen del SIM box, agotando su saldo de prepago o suspendiendo o terminando completamente su perfil de suscripción. Para una línea de derivación fuera de la red, la puerta de enlace

las almacena en una base de datos y usa la base de datos para interceptar todas las llamadas de las redes fuera de la red deshabilitando o interrumpiendo las llamadas con el identificador de llamadas de la base de datos de las líneas de derivación fuera de la red.

En un aspecto de la presente invención, la puerta de enlace de PI 102 desactiva el SIM box dentro de la red bloqueando todas las llamadas internacionales al VLR en el que se está bloqueando el SIM box. Existe una diferencia de tiempo configurable establecida entre el que el SIM box se detecta y se desactiva. Se asegura que esta diferencia de tiempo no forme un patrón que pueda afectar al modo silencioso de detección de SIM box.

La figura 6 representa un diagrama de flujo para la desactivación de puertas de enlace SIM box tras su detección, de acuerdo con un aspecto de la presente invención. Tras la detección de la ISDN de la MS del SIM box, la puerta de enlace de PI envía una SRI-SM al HLR-H 116 con un MSISDN como el número del SIM box para obtener su ubicación. El HLR-H 116 en respuesta a puerta de enlace de PI 102, con SRI-SM ACK envía la dirección MSC en la que se bloquea el SIM box. A partir de entonces, la puerta de enlace de PI 102 encuentra el VLR correspondiente del mapeo de la dirección del MSC-VLR. Posteriormente, la puerta de enlace de PI envía SAISD (con BOAC o ODB, o ambos) a este VLR identificado para bloquear todas las llamadas internacionales para este MSISDN SIM box. El VLR puede enviar “continuar” en respuesta a la puerta de enlace de PI 102. Finalmente, la puerta de enlace de PI 102 envía “fin” para cerrar la transacción. Esto significa que el número del SIM box se bloquea satisfactoriamente en este VLR para cualquier llamada. En el caso de que el VLR no responda con ”continuar” o se recibe un error, la puerta de enlace de PI 102 envía de nuevo el SAISD al VLR dependiendo de la configuración en la tabla pi_error_retry_details. Esta tabla contiene información sobre el código de error en el que debe hacerse un reintento de enviar de nuevo SAISD al VLR y cuántas veces debe hacerse este reintento.

En otro aspecto de la presente invención, la desactivación del SIM box dentro de la red sólo puede suspenderse o deshabilitarse del perfil de la línea del suscriptor a través de la red del operador de base API.

En otro aspecto de la presente invención, el SIM box dentro de la red no se desactiva, pero se sigue para su uso posterior en análisis de la ubicación del operador SIM box. Esto se consigue creando un perfil de suscripción de tipo O-CSI para el SIM box. Para cada llamada iniciada por el SIM box, el control de la llamada llegará a la puerta de enlace de PI, que puede entonces registrar el uso, información de ubicación, etc.

En otro aspecto de la presente invención, la desactivación del SIM box dentro de la red también depende del saldo restante en la cuenta de prepago. En otras palabras, la puerta de enlace de PI 102 envía una consulta de USSD al sistema de prepago (PPS) para solicitar el nivel de crédito en la cuenta de prepago. En un aspecto, cuando el nivel del crédito está por debajo de un umbral configurable (por ejemplo 3 Euros), la desactivación se completa por la puerta de enlace de PI 102. En otro aspecto de la invención, cuando el crédito es superior, la puerta de enlace de PI 102 sondea el nivel de crédito a intervalos predeterminados o al final de las siguientes llamadas de prueba (si está habilitado el seguimiento de la actividad). Como alternativa, la puerta de enlace de PI 102 envía un correo electrónico SNMP a los estafadores para vaciar la cuenta de prepago.

En otro aspecto de la presente invención, para una línea de derivación fuera de la red, la puerta de enlace las almacena en una base de datos e intercepta todas las llamadas de las redes fuera de la red deshabilitando o interrumpiendo las llamadas con el identificador de llamadas de la base de datos de las líneas de derivación fuera de la red. Los desencadenantes de la llamada desde redes fuera de la red pueden ser un control de llamada basado en sistemas de tipo SS7, tal como ISUP, IN, CAMEL, o un control de llamada basado en IP, tal como SIP, etc. La figura 6 representa un diagrama de flujo para bloquear las llamadas fuera de la red, que implica SIM boxes fuera de la red de la base de datos. Una llamada fuera de la red con el identificador de llamadas A a un número B de la PMN principal 104 alcanza el GMSC-H 112, que pasa un control de llamadas a la puerta de enlace de PI. Si A se encuentra en la base de datos del SIM box fuera de la red, la PI libera la llamada; de lo contrario, la PI continua la llamada.

Será evidente para un experto en la técnica que la presente invención también puede

aplicarse al acceso múltiple por división de código (CDMA)/Instituto Nacional Americano de Normalización Nº 41D (ANSI-41D), y a diversas tecnologías diferentes tales como, pero sin limitación, VoIP, WiFi, 3GSM e itinerancia inter-estándar. Por ejemplo, un abonado itinerante emisor CDMA viaja con un microteléfono CDMA de HPMN. En otro ejemplo, el abonado itinerante emisor CDMA viaja con un SIM de GSM de HPMN y un microteléfono GSM. En otro ejemplo más, un abonado itinerante emisor GSM viaja con un RUIM de CDMA de HPMN y un microteléfono CDMA. Para soportar estas variaciones, el sistema 100 tendrá un SS7 separado e interfaces de red, que corresponden tanto a redes HPMN como VPMN. Será evidente también para un experto en la técnica, que estas dos interfaces en diferentes direcciones pueden no tener las mismas tecnologías. Además, podrían ser múltiples tipos de interfaces en ambas direcciones.

En la tabla que se muestra a continuación se describe, a modo de referencia, una lista de ejemplo de mapeo entre la MAP de GSM y ANSI-41.

MAP de GSM	**ANSI-41D**
Actualización de la localización/ISD	NOREG
Cancelar localización	PERMITIR REG
Registrar SS	SOLICITUD DE CARACTERÍSTICA
Preguntar SS	SOLICITUD DE CARACTERÍSTICA
SRI-SM	SOLICITUD DE SMS
SRI	SOLICITUD DE LOCALIZACIÓN
ReenviarSMS	DPP de SMS
ListoParaSMS	NOTIFICACIÓN DE SMS
Centro de servicio de alertas	NOTIFICACIÓN DE SMS
Informar de la difusión de SMS	DPP de SMS
Proporcionar número itinerante	SOLICITUD DE ENRUTAMIENTO

La presente invención puede adoptar la forma de un aspecto de hardware en su totalidad, un aspecto de software en su totalidad, o un aspecto que contenga ambos elementos de hardware y software. De acuerdo con un aspecto de la presente invención, el software, que incluye, pero sin limitación, un firmware, un software residente y un microcódigo,

implementa la invención.

Además, la invención puede adoptar la forma de un producto de programa informático, accesible desde un medio utilizable o legible por ordenador que proporciona un código de programación para su uso por, o junto con, un ordenador o cualquier sistema de ejecución de instrucciones. Para los fines de esta descripción, un medio utilizable o legible por ordenador puede ser cualquier aparato que pueda contener, almacenar, comunicar, propagar o transportar el programa para su uso por, o junto con, el sistema, aparato o dispositivo de ejecución de instrucciones.

El medio puede ser un sistema (o aparato o dispositivo) electrónico, magnético, óptico, electromagnético, infrarrojo o semiconductor, o un medio de propagación. Los ejemplos de un medio legible por ordenador incluyen una memoria semiconductora o en estado sólido, una cinta magnética, un disquete informático extraíble, una memoria de acceso aleatorio (RAM), una memoria sólo de lectura (ROM), un disco magnético rígido, y un disco óptico. Los ejemplos habituales de discos ópticos incluyen un disco compacto de memoria sólo de lectura (CDROM), un disco compacto de lectura/escritura (CD-R/W), y un disco versátil digital (DVD).

Los componentes del presente sistema descrito anteriormente incluyen cualquier combinación de dispositivos y componentes informáticos que funcionan a la vez. Los componentes del presente sistema también pueden ser componentes o subsistemas que están dentro de una gran red o sistema informático. Los componentes del presente sistema también se pueden acoplar con cualquier número de diferentes componentes (no mostrados), tales como otros puertos o buses, controladores, dispositivos de memoria, y servicios de entrada/salida de datos, en numerosas combinaciones. Además, cualquier número o combinación de otros componentes basados en procesadores pueden realizar las funciones del presente sistema.

Se ha de tener en cuenta que los diversos componentes descritos en este documento pueden realizarse usando herramientas de diseño asistidas por ordenador y/o expresados (o representados) como datos y/o instrucciones, interpretados en diversos

medios legibles por ordenador, en cuanto a su comportamiento, transferencia de registro, componente lógico, transistor, geometrías de formato, y/o otras características. Los medios legibles por ordenador, en los que se pueden interpretar dichos datos y/o instrucciones formateadas incluyen, pero sin limitación, medios de almacenamiento no volátiles en diversas formas (por ejemplo, medios de almacenamiento ópticos, magnéticos o semiconductores), y ondas portadoras que se pueden usar para transferir dichos datos y/o instrucciones formateados a través de medios de señalización inalámbricos, ópticos o por cable, o cualquier combinación de los mismos.

A menos que el contexto indique claramente otra cosa, a lo largo de toda la descripción y de las reivindicaciones, las palabras "comprende", "que comprende", y similares, deben interpretarse en un sentido inclusivo en comparación con un sentido exclusivo o exhaustivo; es decir, en el sentido de "incluyendo, pero sin limitación". Las palabras que usan el número singular o plural también incluyen el número plural o singular, respectivamente. Adicionalmente, las palabras "en este documento", "a continuación en este documento", "anteriormente", "a continuación", y palabras de significado similar, se refieren a esta solicitud en su totalidad y no a cualquier parte particular de esta solicitud. Cuando se usa la palabra "o" con referencia a una lista de dos o más artículos, ésta incluye cada una de las siguientes interpretaciones: cualquiera de los artículos de la lista, todos los artículos de la lista, y cualquier combinación de los artículos de la lista.

La descripción anterior de los aspectos ilustrados del presente sistema no pretende ser exhaustiva o limitar el presente sistema a la forma precisa desvelada. Aunque en este documento se describen con fines ilustrativos realizaciones específicas de, y ejemplos para, el presente sistema, son posibles diversas modificaciones equivalentes dentro del alcance del presente sistema, como reconocerán los expertos en la técnica. Las enseñanzas del presente sistema proporcionado en este documento pueden aplicarse a otros sistemas y procedimientos de procesamiento. Pueden no limitarse a los sistemas y procedimientos que se han descrito anteriormente.

Los elementos y actuaciones de los diversos aspectos que se han descrito anteriormente se pueden combinar para proporcionar realizaciones adicionales. Estos y otros cambios

pueden hacerse a la luz de la descripción detallada anterior.

OTRAS VARIANTES DE LA INVENCIÓN

Los apartados anteriores han de ser entendidos para su interpretación por parte de los expertos en la técnica, y no como una limitación del alcance de la invención, donde se detallan ilustraciones de un esquema para pruebas de itinerancia proactivas, descubrimientos de servicios del socio de itinerancia y descubrimientos de fraude en itinerancia usando un tráfico de itinerancia simulado. Por supuesto, a los expertos habituales en la técnica se les ocurrirán numerosas variaciones y modificaciones dentro del espíritu de la presente invención, en vista de los aspectos aquí divulgados. Por ejemplo, la presente invención se implementa principalmente desde el punto de vista de redes móviles GSM como se describe en los aspectos. No obstante, la presente invención también puede implementarse eficazmente en GPRS, 3G, CDMA, WCDMA, WiMax, etc., o en cualquier otra red de telecomunicaciones provista por un operador común en la que normalmente se configuran usuarios finales que operen dentro de una red "doméstica" a la que generalmente están suscritos, pero además tienen la capacidad de operar en otras redes vecinas, que pueden incluso traspasar los límites internacionales.

Los ejemplos del sistema de la presente invención detallados en los ejemplos ilustrativos contenidos en este documento se describen usando términos y construcciones tomados en gran parte a partir de la infraestructura de telefonía móvil GSM. Sin embargo, el uso de estos ejemplos no debe interpretarse como limitante de la invención a aquellos medios. El sistema y el procedimiento pueden utilizarse y proporcionarse a través de cualquier tipo de medio de telecomunicaciones, incluyendo, pero sin limitación: (i) cualquier red de telefonía móvil que incluye, sin limitación, GSM, 3GSM, 3G, CDMA, WCDMA o GPRS, teléfonos vía satélite u otros sistemas o redes de telefonía móvil; (ii) cualquier aparato conocido como WiFi usado normalmente en una red doméstica o suscrita, pero que también está configurado para usarse en una red visitada o no doméstica o inusual, incluyendo los aparatos que no están dedicados a las telecomunicaciones, tales como ordenadores personales y los dispositivos del tipo Palm o

Windows Mobile; (iii) una plataforma de consola de entretenimiento, tal como Sony Playstation, PSP u otros aparatos capaces de enviar y recibir servicios de telecomunicaciones por redes domésticas o no domésticas, o incluso (iv) dispositivos de línea fija diseñados para recibir servicios de comunicaciones, pero que pueden desplegarse en numerosas localizaciones mientras que mantienen constante la ID del abonado, tal como los dispositivos eye2eye de Dlink, o el equipo de telecomunicaciones pensado para voz por el sistema de comunicaciones IP, tales como los proporcionados por Vonage o Packet8.

En la descripción de ciertos aspectos del sistema según la presente invención, el presente documento detalla la trayectoria de una llamada por un servicio de telecomunicaciones, desde una parte llamante a una parte llamada. Para evitar cualquier duda, una llamada de este tipo puede ser una llamada de voz normal, en la que el equipo de telecomunicaciones del abonado también puede mostrar imágenes visuales, audiovisuales o en movimiento. Como alternativa, aquellos dispositivos o llamadas pueden ser de texto, vídeo, imágenes u otros datos comunicados.

En la presente memoria descriptiva se han descrito aspectos específicos de la presente invención. Sin embargo, un experto habitual en la técnica apreciará que pueden hacerse diversas modificaciones y cambios sin apartarse del alcance de la presente invención como se establece en las reivindicaciones que se indican a continuación. Por consiguiente, la memoria descriptiva y las figuras se han de interpretar más bien en un sentido ilustrativo en lugar de restrictivo, y todas estas modificaciones pretenden incluirse dentro del alcance de la presente invención. Los beneficios, ventajas, soluciones a problemas, y cualquier elemento o elementos que puedan beneficiar, aportar ventajas o soluciones, o hacerse más acentuados, no deben ser interpretarse como un elemento o particularidad crítica, requerida o esencial de cualquiera o todas las reivindicaciones.

DESCRIPCIÓN DE ACRÓNIMOS Y SIGLAS UTILIZADAS

Acrónimo	**Descripción**
3G	Tercera generación de móviles.

ACM	Mensaje de dirección completa de ISUP.
ANM	Mensaje de respuesta de ISUP.
ANSI-41	Instituto Nacional Americano de Normalización Nº 41.
ATI	Interrogación en cualquier momento.
BCSM	Modelo de estado de llamada básica.
BSC	Controlador de estación base.
BOIC	Bloqueo de llamadas internacionales salientes.
BOIC-EX-Home	Bloqueo de llamadas internacionales salientes excepto al país de origen.
CAMEL	Aplicación personalizada para la lógica mejorada de redes móviles.
CAP	Parte de aplicación CAMEL.
CB	Bloqueo de llamadas.
CC	Código de país.
CDMA	Acceso múltiple por división de código.
CdPA	Dirección de la parte llamada.
CDR	Registro detallado de llamadas.
CF	Desvío de llamadas.
CgPA	Dirección de la parte llamante.
CIC	Código de identificación del circuito.
CLI	Identificación de línea llamante.
CSD	Datos por conmutación de circuitos.
CSI	Información de suscripción CAMEL.
DPC	Código del punto de destino.
DSD	Datos de suscriptores borrados.
DTMF	Multifrecuencia de doble tono.
ERB	Modelo básico de notificación de eventos del estado de llamada por CAP.
EU	Unión europea.
FPMN	Red móvil pública amigable.
FTN	Desvío a un número.
GLR	Registro de la ubicación de la puerta de enlace.
GGSN	Nodo de soporte de puerta de enlace GPRS.

GMSC	Puerta de enlace de MSC.
GMSC-F	GMSC en FPMN.
GMSC-H	GMSC en HPMN.
GPRS	Sistema general de radio por paquetes.
GSM	Sistema global de comunicación móvil.
GSMA	Asociación GSM.
GSM SSF	Función de conmutación de servicio GSM.
GsmSCF	Función de control de servicio GSM.
GT	Título global.
GTP	Protocolo de túnel de GPRS.
HLR	Registro de ubicación base.
HPMN	Red móvil pública doméstica.
IN	Red inteligente.
IOT	Tarifa inter-operador.
GTT	Traducción de títulos globales.
IAM	Mensaje de dirección inicial.
IDP	Mensaje de DP inicial IN/CAP.
IDD	Marcado directo internacional.
IMSI	Identidad internacional del abonado a un móvil.
IMSI-H	IMSI de HPMN.
IN	Red inteligente.
INAP	Parte de aplicación de red inteligente.
INE	Entidad de red interrogante.
IP	Protocolo de Internet.
IREG	Grupo experto en itinerancia internacional.
IRS	Servicio de impuestos interno.
ISC	Servicio portador internacional.
ISD	Inserción de datos del abonado basado en MAP.
ISG	Puerta de enlace de señal internacional.
IST	Terminación inmediata del servicio.
ISTP	STP internacional.
ISTP-F	ISTP conectado a STP de FPMN.

ISTP-H	ISTP conectado a STP de HPMN.
ISUP	Parte de usuario ISDN.
ITPT	Iniciación del perfil de prueba del abonado receptor.
ITR	Redirección del tráfico del abonado receptor.
IVR	Respuesta de voz interactiva.
LU	Actualización de ubicación.
LUP	Actualización de ubicación MAP.
MAP	Parte de aplicación móvil.
MCC	Código del país de móvil.
MD	Datos perdidos.
ME	Equipo móvil.
MGT	Título global móvil.
MMS	Servicio de mensajes multimedia.
MMSC	Centro de servicio de mensajes multimedia.
MMSC-F	MMSC de FPMN.
MMSC-H	MMSC de HPMN.
MNC	Código de red de móvil.
MNP	Portabilidad numérica móvil.
MO	Iniciado en el terminal móvil.
MOS	Puntuación de opinión media.
MS	Estación móvil.
MSC	Centro de conmutación móvil.
MSISDN	Número internacional de abonado de la estación móvil.
MSISDN-F	MSISDN de FPMN.
MSISDN-H	MSISDN de HPMN.
MSRN	Número de itinerancia de la estación móvil.
MSRN-F	MSRN de FPMN.
MSRN-H	MSRN de HPMN.
MT	Terminado en el móvil.
MTP	Parte de transferencia de mensajes.
NDC	Código nacional de marcación.
NP	Plan de numeración.

NPI	Indicador de plan de numeración.
NRTRDE	Intercambio de datos de itinerancia instantánea.
O-CSI	Información de suscripción CAMEL de origen.
OCN	Número llamado original.
ODB	Bloqueo para un operador determinado.
OPC	Código del punto de origen.
OR	Enrutamiento óptimo.
ORLCF	Enrutamiento óptimo para desvío de llamadas tardías.
OTA	Por el aire.
OTPI	Iniciación del perfil de prueba del abonado emisor.
PDP	Protocolo de paquete de datos.
PDN	Red de paquete de datos.
PDU	Unidad de paquete de datos.
PRN	Suministro de número itinerante por MAP.
PSI	Suministro de la información del abonado por MAP.
QoS	Calidad de servicio.
RAEX	Intercambio de acuerdo itinerancia.
RI	Indicador de itinerancia.
RIS	Sistema de inteligencia de itinerancia.
RDN	Número de redirección.
RNA	Itinerancia no permitida.
RR	Itinerancia restringida debido a una función no soportada.
RRB	Modelo básico del estado de llamada de notificación de solicitudes CAP.
RSD	Datos de recuperación.
RTP	Protocolo de transporte en tiempo real.
SAI	Información de autenticación enviada.
SC	Código corto.
SCA	Asistente inteligente de llamadas.
SCCP	Parte de control de conexión de señal.
SCP	Punto de control de señalización.
SF	Fallo del sistema.

SG	Puerta de enlace de señalización.
SGSN	Nodo de soporte GPRS de servicio.
SGSN-F	SGSN de FPMN.
SIM	Módulo de identidad de suscriptor.
SIGTRAN	Protocolo de transporte de señalización.
SME	Entidad de mensajes cortos.
SM-RP-UI	Información de usuario del protocolo de transmisión de mensajes cortos.
SMS	Servicio de mensajes cortos.
SMSC	Centro servidor de mensajes cortos.
SMSC-F	SMSC de FPMN.
SMSC-H	SMSC de HPMN.
SoR	Direccionamiento de la itinerancia.
SPC	Código de punto de señal.
SRI	Información de enrutamiento de envío por MAP.
SRI-SM	Información de enrutamiento de envío por MAP para mensajes cortos.
SS	Servicios suplementarios.
SS7	Sistema de señalización por canal común Nº 7.
SSN	Número de subsistemas.
SSP	Punto de conmutación de servicio.
STK	Aplicación del kit de herramientas SIM.
STP	Punto de transferencia de señalización.
STP-F	STP de FPMN.
STP-H	STP de HPMN.
TADIG	Grupo de intercambio de datos de cuentas transferidas.
TAP	Procedimiento de cuentas transferidas.
TCAP	Parte de aplicación de transacción de capacidades.
VT-CSI	Información de servicio CAMEL de terminación visitado.
TP	Protocolo de transporte para SMS.
TR	Redirección del tráfico.
TS	Direccionamiento del tráfico.
TT	Tipo de traducción.

UD	Datos de usuario.
UDH	Cabecera de datos de usuario.
UDHI	Indicador de cabecera de datos de usuario.
USSD	Datos de servicio suplementario no estructurados.
VAS	Servicio de valor añadido.
VIP	Persona muy importante.
VLR	Registro de localización visitado.
VLR-F	VLR de FPMN.
VLR-H	VLR de HPMN.
VLR-V	VLR de VPMN.
VMSC	Centro de conmutación móvil visitado.
VoIP	Voz sobre IP.
VPMN	Red pública móvil visitada.
ATI	Información de transporte de acceso.
UDV	Valor de datos inesperados.
USI	Información de servicios de usuario.
WAP	Protocolo de acceso inalámbrico.

REFERENCIAS TÉCNICAS DEL DOCUMENTO

John Jiang and David Gillot [PI 2007], “A single operator and network side solution for inbound and outbound roaming tests and discoveries of roaming partner services and fraud without involving remote probes or real roamer traffic - Phase 1”

John Jiang and David Gillot [PI 2008], “A single operator and network side solution for inbound and outbound roaming tests and discoveries of roaming partner services and fraud without involving remote probes or real roamer traffic”.

GSM 378 - Camel Fase 2.

Camel 978 - Protocolo de aplicación Camel.

GSM 379 sobre soporte CAMEL de enrutamiento óptimo (SOR).

GSM 318 sobre Manejo básico de llamadas CAMEL.

IREG 32.

IREG 24.

Recomendación Q.1214 de la ITU-T (1995), Plan funcional distribuido para red inteligente CS-1.

Recomendación Q.1218 de la ITU-T (1995), Recomendación de interfaz para red inteligente CS-1.

Recomendación Q.762 de la ITU-T (1999), Sistema de señalización Nº 7 - Funciones generales de parte de usuarios ISDN de mensajes y señales.

Recomendación Q.763 de la ITU-T (1999), Sistema de señalización Nº 7 - Formatos y códigos de parte de usuario de red ISDN.

Recomendación Q.764 de la ITU-T (1999), Sistema de señalización Nº 7 - Procedimientos de señalización de parte de usuario de red ISDN.

Recomendación Q.766 de la ITU-T (1993), Objetivos de rendimiento en la aplicación de red digital de servicios integrados.

Recomendación Q.765 de la ITU-T (1998), Sistema de señalización Nº 7 - Mecanismo de transporte de aplicaciones.

Recomendación Q.769.1 de la ITU-T (1999), Sistema de señalización Nº 7 - Mejoras en la parte de usuario ISDN para el soporte de la portabilidad del número.

BA 19 RAEX de GSMA sobre AA 14 e IR 21.

FF 17 Fraude al servicio de impuestos interno.

REIVINDICACIONES

1. Procedimiento para detectar el fraude por derivación en una red de telecomunicaciones, comprendiendo dicho procedimiento las siguientes etapas:

- generar una o más llamadas de prueba desde un agente remoto a un agente local, en el que el agente local es un número suscriptor de un suscriptor;
- realizar el desvío de las llamadas de prueba del agente local a un número local; e
- identificar la presencia de fraude por derivación analizando la información de identificación del llamante de la llamada de prueba recibida en el número local.

2. Procedimiento según la reivindicación 1, en el que las llamadas de prueba del agente remoto se realizan por medio de una puerta de enlace de inteligencia predictiva (PI).

3. Procedimiento según la reivindicación 1, en el que el número suscriptor se selecciona como un agente local entre una combinación de números suscriptores.

4. Procedimiento según la reivindicación 1, en el que el desvío de llamadas del agente local al número local se realiza estableciendo un desvío de llamadas incondicional en un perfil del suscriptor al número local.

5. Procedimiento según la reivindicación 1, en el que el agente remoto es un agente de itinerancia creado en una red del socio de itinerancia de la red a la que pertenecen los números suscriptores, en el que el agente de itinerancia tiene un perfil de desvío de llamadas condicional establecido para el agente local.

6. Procedimiento según la reivindicación 1, en el que se almacena un perfil de desvío de llamadas incondicional actual del suscriptor antes de facilitar el desvío de llamadas del agente local al número local.

7. Procedimiento según la reivindicación 1, que comprende adicionalmente restaurar el perfil de desvío de llamadas incondicional almacenado del suscriptor después de que se complete la llamada de prueba.

8. Procedimiento según la reivindicación 1, en el que la derivación detectada es una puerta de enlace de tipo SIM box GSM dentro de la red o fuera de la red.

9. Procedimiento según la reivindicación 1, en el que la derivación detectada es una derivación de terminación.

10. Procedimiento según la reivindicación 1, en el que la derivación detectada es una derivación de terminación de línea fija.

11. Procedimiento según la reivindicación 1, en el que la derivación detectada es una derivación de terminación CDMA.

12. Procedimiento según la reivindicación 2, en el que el número suscriptor se proporciona con terminación de tipo T-CSI en su registro de ubicación base, para pasar el control de la llamada de terminación a la puerta de enlace de inteligencia predictiva.

13. Procedimiento según la reivindicación 1, en el que el número suscriptor posee desvío de llamadas incondicional establecido para el número local en su registro de ubicación base.

14. Procedimiento según la reivindicación 1, en el que el número local se selecciona entre una combinación de números predefinidos.

15. Procedimiento según la reivindicación 1, en el que se hacen una o más llamadas de prueba usando parámetros de llamada aleatorios.

16. Procedimiento según la reivindicación 15, en el que los parámetros de llamadas son aleatorios usando uno o más de los siguientes elementos:

una parte llamante en llamadas de prueba sin identificación de línea llamante;
una parte llamante en llamadas de prueba con un número suscriptor real;
una parte llamante en llamadas de prueba con cualquier número;
llamadas de prueba de un número aleatorio de un rango de un país socio de itinerancia;
llamadas de prueba de números corruptos; y
un origen de liberación de la llamada de prueba.

17. Procedimiento según la reivindicación 8, en el que la presencia de la puerta de enlace de tipo SIM box GSM se detecta mediante el seguimiento del identificador de llamadas al terminar las llamadas de prueba al número local.

18. Procedimiento según la reivindicación 17, en el que la presencia de la puerta de enlace de tipo SIM box GSM se determina cuando un identificador de llamadas de origen en las llamadas de prueba generadas al agente de itinerancia es diferente del identificador de llamadas en las llamadas de prueba de terminación del número local.

19. Procedimiento según la reivindicación 17, en el que se sigue el identificador de llamadas de la llamada de prueba proporcionando la terminación de tipo T-CSI en el perfil del número local.

20. Procedimiento según la reivindicación 8, que comprende adicionalmente,
la liberación de las llamadas de prueba tras la detección de la puerta de enlace de tipo SIM box GSM.

21. Procedimiento según la reivindicación 20, en el que las llamadas de prueba se liberan inmediatamente después de la detección de la puerta de enlace de tipo SIM box GSM.

22. Procedimiento según la reivindicación 20, en el que las llamadas de prueba se liberan después de un periodo de tiempo configurable.

23. Procedimiento según la reivindicación 8 que comprende, adicionalmente, responder las llamadas de prueba para identificar la puerta de enlace de tipo SIM box GSM.

24. Procedimiento según la reivindicación 23, en el que las llamadas de prueba se responden durante un periodo de tiempo predefinido.

25. Procedimiento según la reivindicación 23, en el que el coste de las llamadas de prueba se controla para determinar el periodo de tiempo predefinido para responder las llamadas de prueba.

26. Procedimiento según la reivindicación 8, en el que la puerta de enlace de tipo SIM box GSM es una puerta de enlace dentro de la red, comprendiendo adicionalmente el procedimiento la desactivación de la puerta de enlace SIM box GSM dentro de la red, bloqueando todas las llamadas al VLR en el que se está bloqueando el SIM box GSM.

27. Procedimiento según la reivindicación 8, en el que la puerta de enlace SIM box GSM es una puerta de enlace dentro de la red, comprendiendo adicionalmente el procedimiento la deshabilitación de la puerta de enlace SIM box dentro de la red, en base al saldo disponible en la cuenta de prepago.

28. Procedimiento según la reivindicación 8, en el que la puerta de enlace SIM box GSM es una puerta de enlace dentro de la red, y en el que un perfil de la puerta de enlace SIM box GSM dentro de la red se suspende o se deshabilita.

29. Procedimiento según la reivindicación 8, en el que la puerta de enlace de tipo SIM box GSM es una puerta de enlace dentro de la red, comprendiendo adicionalmente el procedimiento el control de un uso, una ubicación y un movimiento de la puerta de enlace SIM box GSM dentro de la red.

30. Procedimiento según la reivindicación 8, en el que la puerta de enlace de tipo SIM box GSM es una puerta de enlace fuera de la red, comprendiendo adicionalmente el

procedimiento almacenar la puerta de enlace fuera de la red en una base de datos y usar la base de datos para liberar cualquier llamada fuera de la red de las redes secundarias, con el identificador de llamadas de la base de datos de la puerta de enlace fuera de la red.

31. Procedimiento según la reivindicación 8, en el que la puerta de enlace de tipo SIM box GSM es una puerta de enlace fuera de la red, en el que se garantiza el número de prueba durante un tiempo cada vez que la llamada de prueba que implica el número de prueba descubra una puerta de enlace de tipo SIM box GSM.

32. Procedimiento según la reivindicación 1, en el que el agente remoto es un marcador que usa uno de entre los siguientes: operadores de voz sobre IP, operadores mayoristas y tarjetas telefónicas.

33. Procedimiento según la reivindicación 1, en el que el coste de la llamada de prueba se mide para controlar el coste del fraude de respuesta temprana.

34. Sistema para impedir el fraude por derivación de terminación en comunicaciones móviles, comprendiendo el sistema una puerta de enlace configurada para provocar una o más llamadas de prueba desde un agente remoto a un agente local;
en el que la puerta de enlace comprende medios para facilitar el desvío de las llamadas de prueba del agente local a un número local; y
en el que la puerta de enlace comprende medios para identificar la presencia del fraude por derivación de terminación analizando la terminación de las llamadas de prueba al número local.

35. Sistema según la reivindicación 34, en el que la puerta de enlace es un módulo de detección de derivación de terminación.

36. Sistema según la reivindicación 34, en el que el agente local es un suscriptor.

37. Sistema según la reivindicación 34, en el que la puerta de enlace posee

medios de señalización para generar la llamada de prueba del agente remoto al agente local.

38. Sistema según la reivindicación 34, en el que la puerta de enlace comprende medios para liberar las llamadas de prueba tras la detección de la derivación de terminación.

39. Sistema según la reivindicación 38, en el que la puerta de enlace comprende medios para liberar las llamadas de prueba inmediatamente después de la detección de la derivación de terminación.

40. Sistema según la reivindicación 38, en el que la puerta de enlace comprende medios para liberar las llamadas de prueba después de un periodo de tiempo configurable.

41. Sistema según la reivindicación 38, en el que la puerta de enlace comprende medios de respuesta a las llamadas de prueba para identificar una puerta de enlace de tipo SIM box.

Arquitectura de Red de Inteligencia Predictiva Avanzada

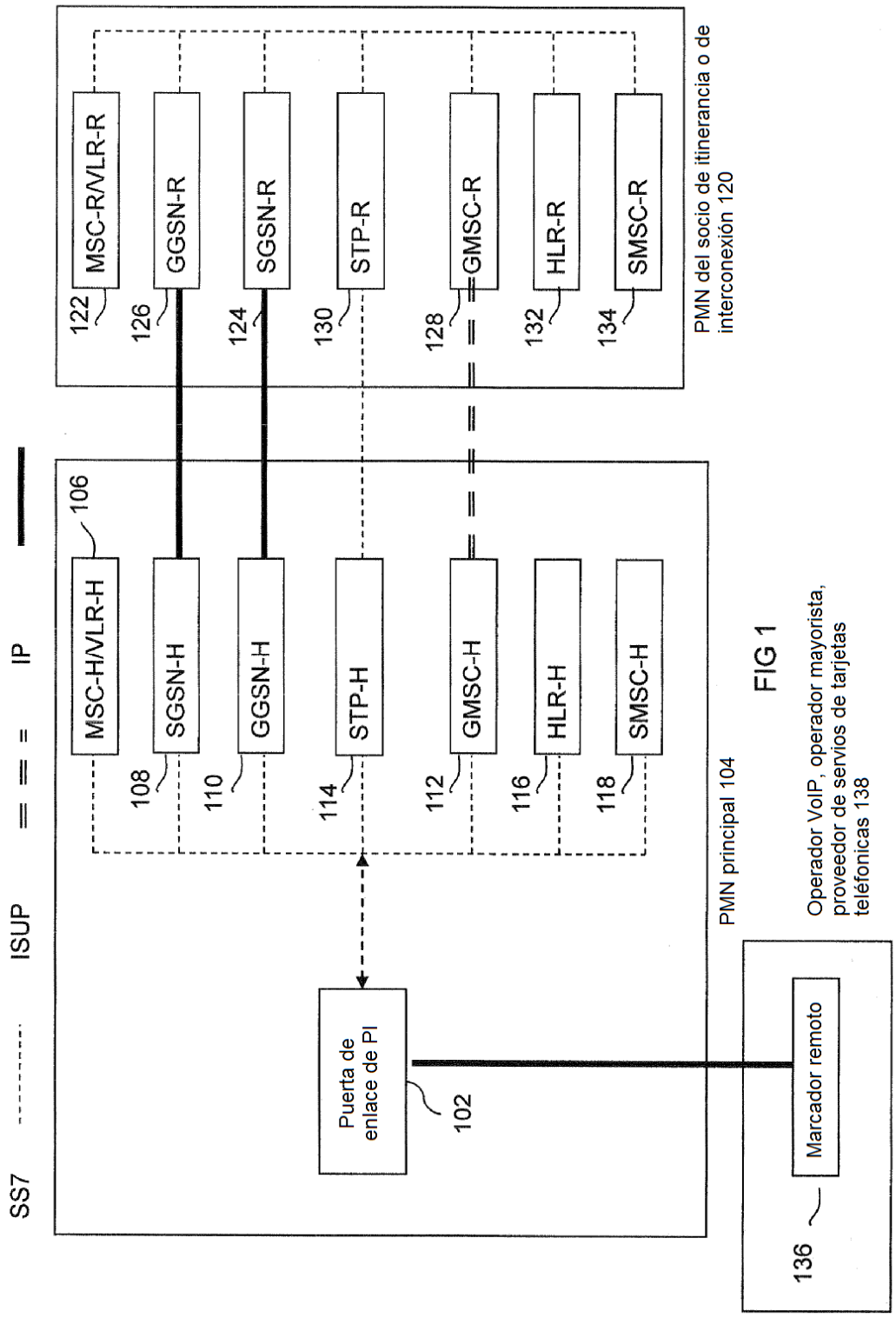

FIG 1

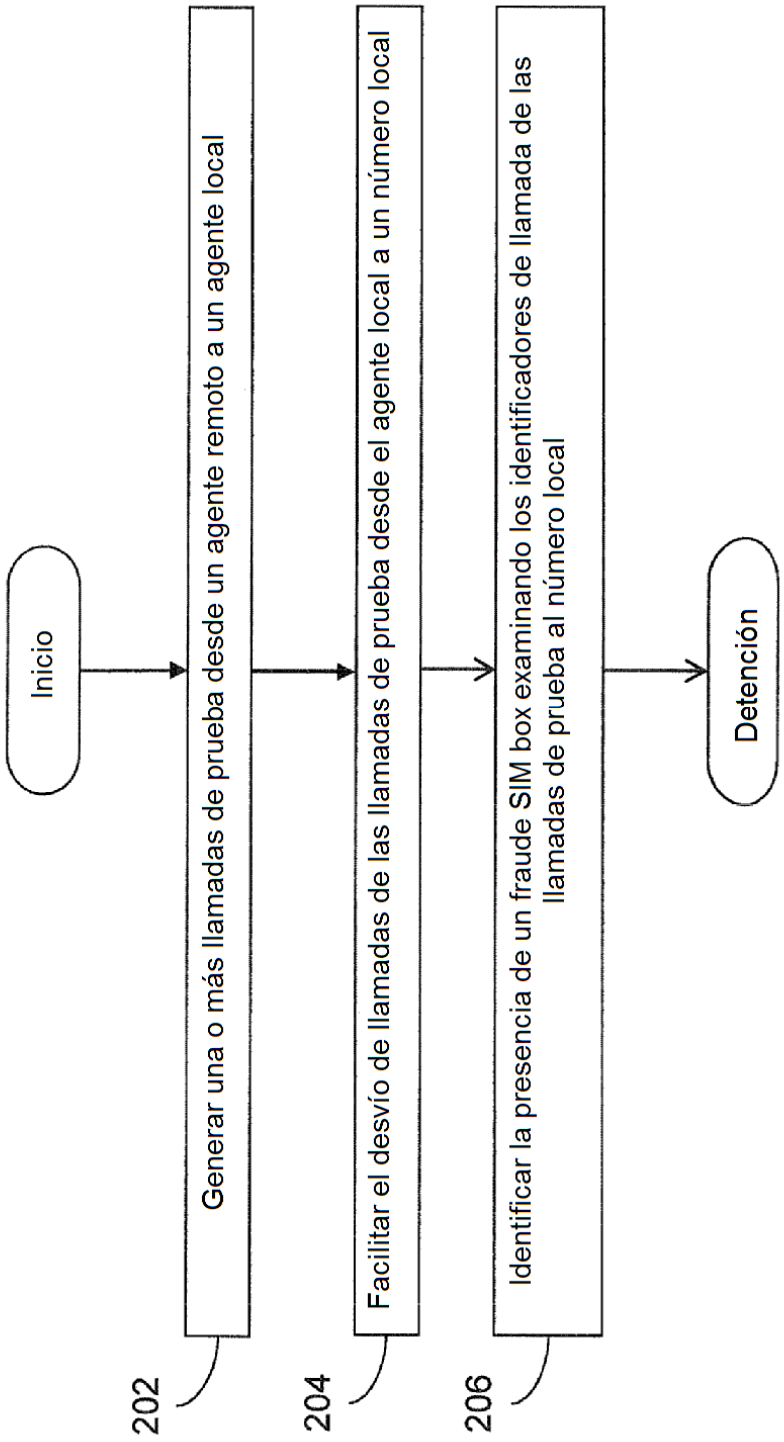
Inicio
Generar una o más llamadas de prueba desde un agente remoto a un agente local
Facilitar el desvío de llamadas de las llamadas de prueba desde el agente local a un número local
Identificar la presencia de un fraude SIM box examinando los identificadores de llamada de las llamadas de prueba al número local
Detención
202
204
206

FIG. 2

Mecanismo de contestación de llamadas de prueba usando un Servidor contestador o una puerta de enlace de PI para el agente de itinerancia

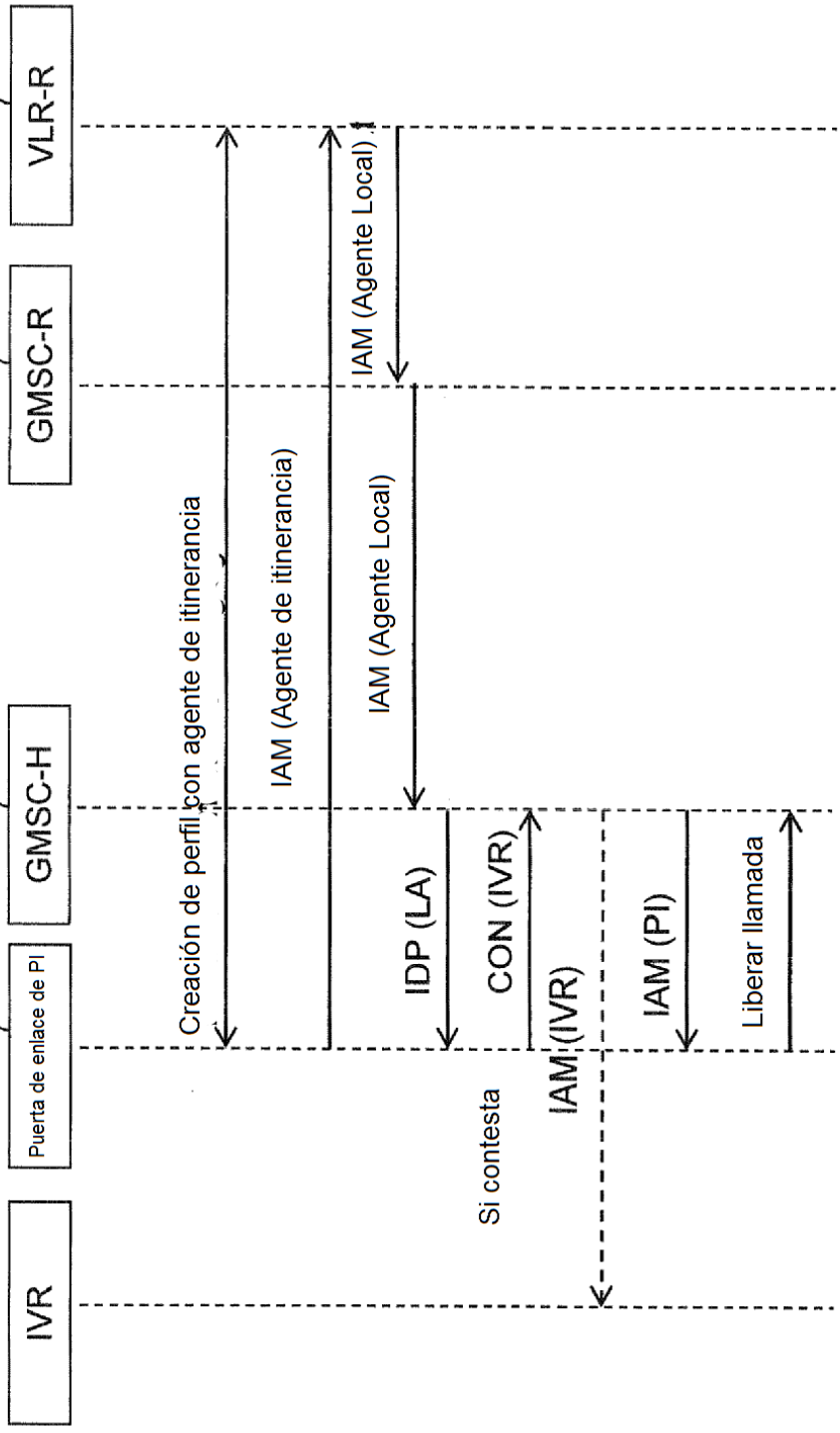

FIG. 3

Enfoque de T-CSI para la terminación de llamadas para un agente de itinerancia

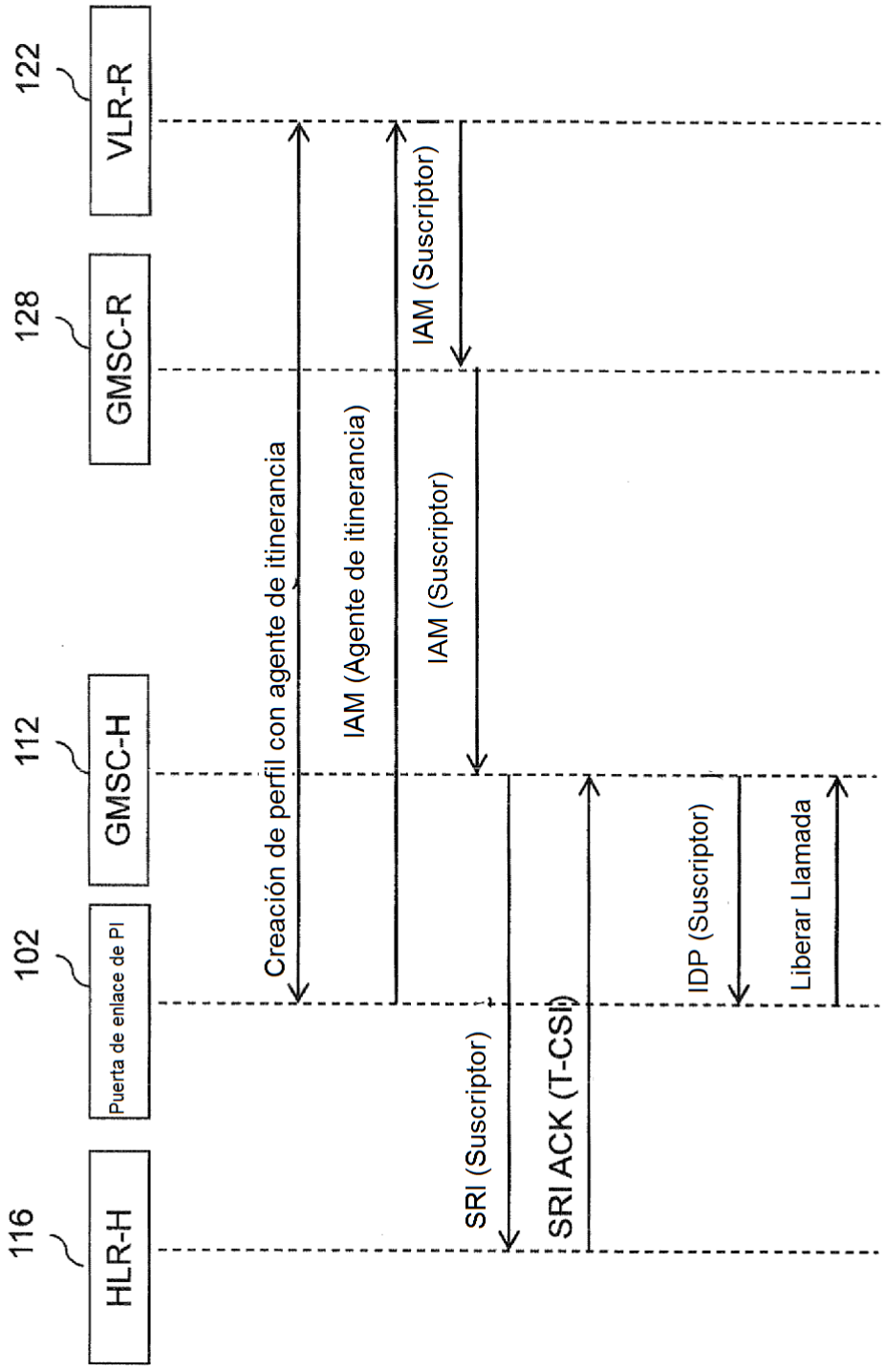

FIG. 4

Enfoque de CFU para la terminación de llamadas para el agente de itinerancia

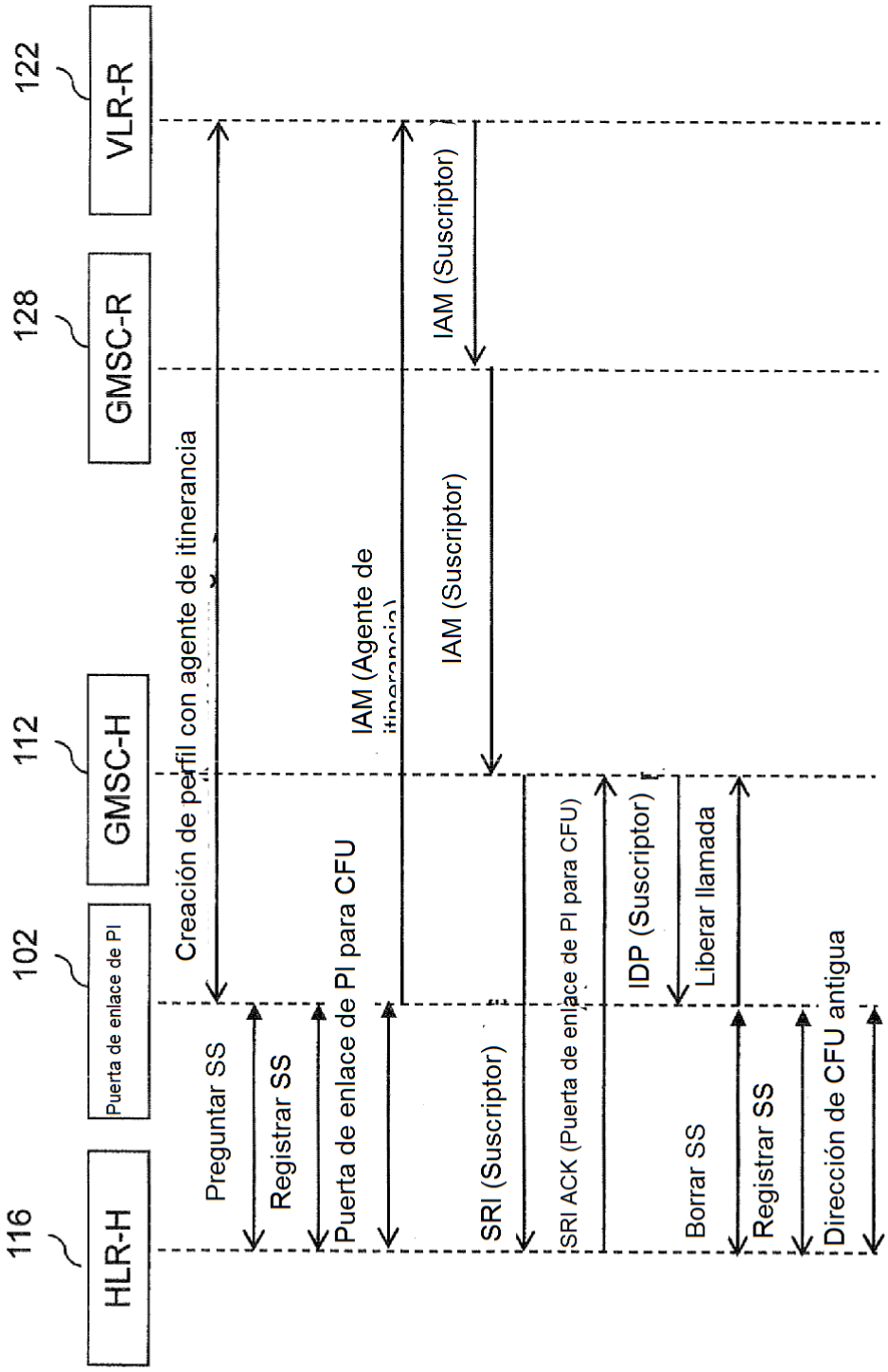

FIG. 5

Procedimiento de desactivación de SIM box para simbox on-net

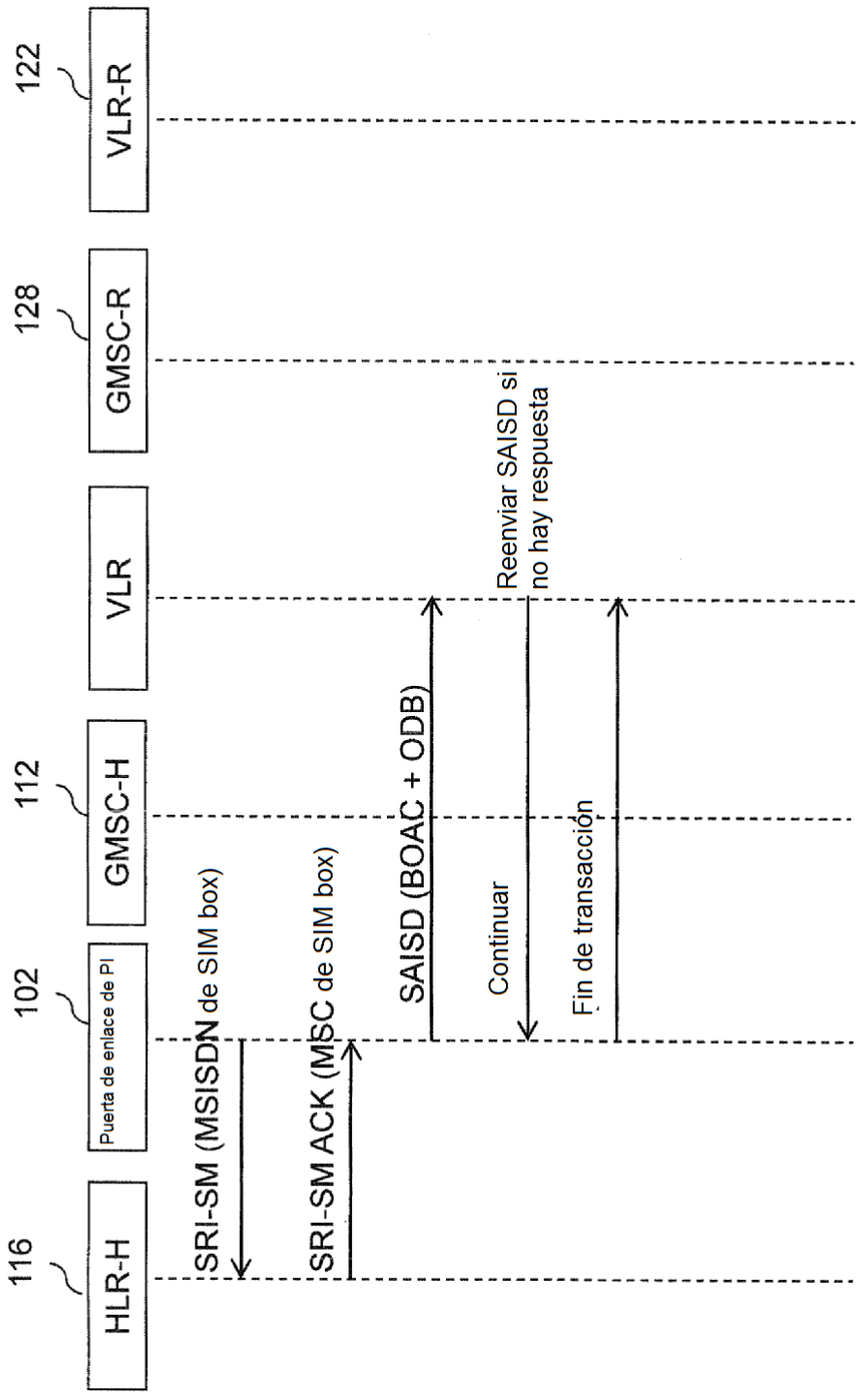

FIG. 6

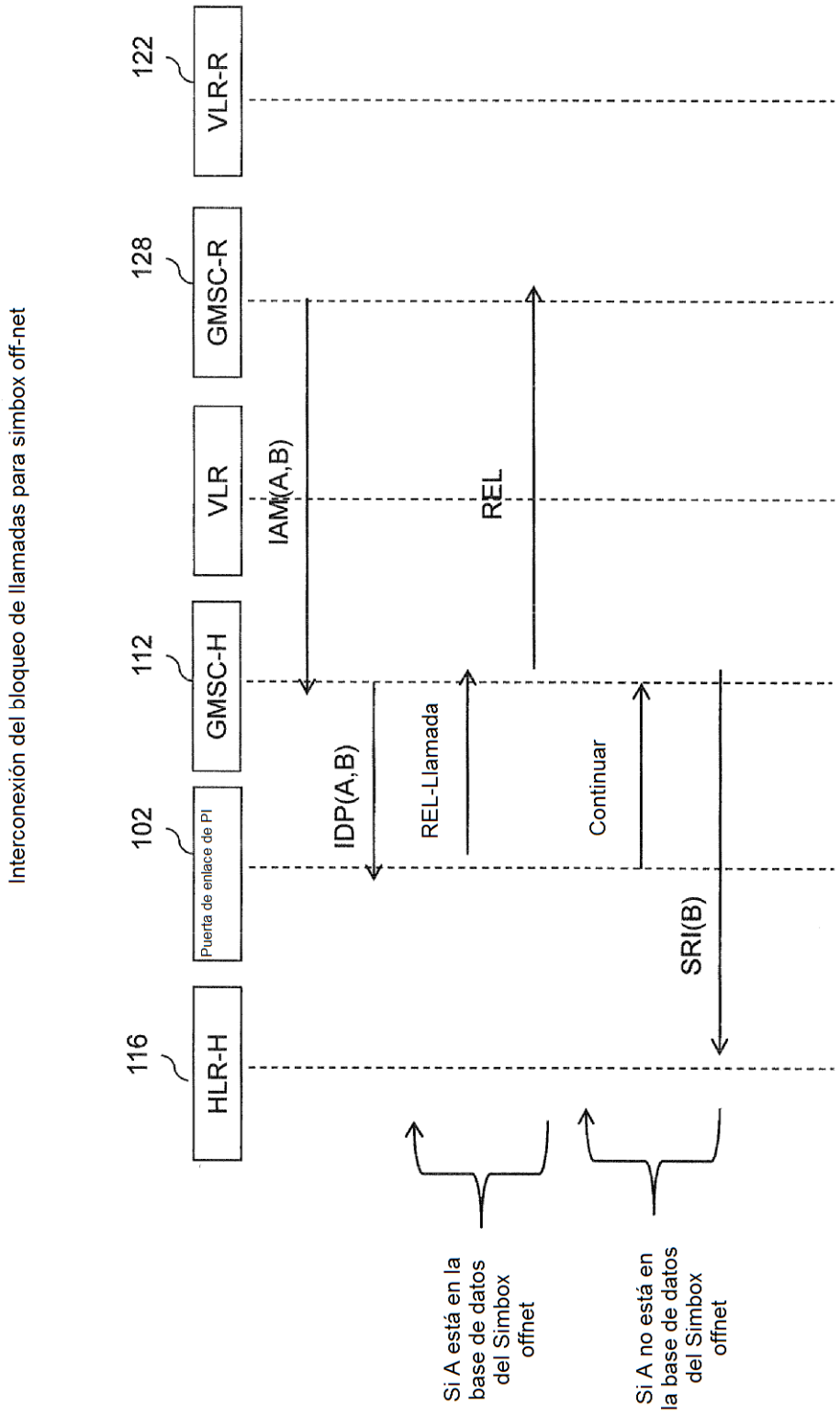
Interconexión del bloqueo de llamadas para simbox off-net
116
HLR-H
102
Puerta de enlace de PI
112
GMSC-H
VLR
128
GMSC-R
122
VLR-R
IAM(A,B)
REL
IDP(A,B)
REL-Llamada
Continuar
SRI(B)
Si A está en la base de datos del Simbox offnet
Si A no está en la base de datos del Simbox offnet

FIG. 7