(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 515 144**

(51) Int. CI.:

H04W 12/12 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **18.12.2007 E 07856823 (5)**

(97) Fecha y número de publicación de la concesión europea: **06.08.2014 EP 2127453**

(54) Título: **Procedimiento para el reconocimiento de fraude en conexiones en itinerancia en redes de comunicación móviles**

(30) Prioridad:

22.12.2006 DE 102006062210

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.10.2014

(73) Titular/es:

DEUTSCHE TELEKOM AG (100.0%)
FRIEDRICH-EBERT-ALLEE 140
53113 BONN, DE

(72) Inventor/es:

HABERKORN, GÜNTER

(74) Agente/Representante:

ÁLVAREZ LÓPEZ, Sonia

DESCRIPCIÓN

Procedimiento para el reconocimiento de fraude en conexiones en itinerancia en redes de comunicación móviles.

La invención se refiere a un procedimiento para el reconocimiento de fraude (fraude = engaño) en redes de comunicación móviles, y en particular un procedimiento para el reconocimiento de fraude en conexión en itinerancia, también designado como el así denominado fraude de itinerancia.

Por el fraude de itinerancia se les generan a los operadores de redes móviles unas pérdidas por valor de millones por año.

En el fraude de itinerancia se crean módulos de identidad de abonado, así denominadas tarjetas SIM (SIM: Subscriber Identity Module), con indicación de identidad falsa o por medios extorsivos. A continuación con estas tarjetas SIM en el extranjero, es decir en el interior de redes móviles extranjeras (redes en itinerancia: FPLMN) se establecen conexiones permanentes con objetivos internacionales (niveles de tarifas más altos), como por ejemplo con las islas del Mar del Sur. Se trata en general de conexiones permanentes (parcialmente también conexiones múltiples vía multi-party), que se establecen en instantes fuera del tiempo de trabajo regular (p. ej. fin de semana). Precisamente en los fines de semana se producen retardos en la red de adscripción (HPLMN) a reconocer de forma temprana estas actividades e iniciar contramedidas. Los así denominados “High-Usage-Reports” que desvelan un uso masivo de las conexiones en itinerancia, sólo se pueden transmitir parcialmente tras algunos días de la red en itinerancia a la red de adscripción. Por ejemplo, con sólo tres tarjetas SIM y debido a los escenarios de conexión arriba mencionados, en un fin de semana se pueden producir varios miles de euros de pérdidas para el operador de red.

En T-Mobile Deutschland existe un sistema de reconocimiento de abusos (MEGS) que comprende diferentes filtros para el reconocimiento temprano del fraude de itinerancia. En este caso se aplican por ejemplo criterios de filtrado típicos como:

- Tarjeta SIM se usa por primera vez y se inscribe en el extranjero

- Se trata de una tarjeta postpago

- Se usan socios de itinerancia típicos (network scoring)

- El cliente no es un cliente de negocios

- Otros criterios de filtrado

El MEGS está representado esquemáticamente en la figura 1, arriba a la izquierda. Si en el caso de una tarjeta SIM se constatan los criterios arriba mencionados, entonces se emite un tique de alarma. Lamentablemente la cuota de éxito con este método de reconocimiento actualmente sólo se sitúa en un pequeño porcentaje, es decir, de 100 tiques de alarma sólo unos pocos designan casos reales de fraude de itinerancia. Dado que los criterios de filtrado del MEGS la mayoría de las veces son ciertos no sólo en los estafadores sino también en muchos clientes “normales”, se puede llegar a un gran aluvión de alarmas (>100/día) en el caso del MEGS. Para la protección de los clientes “normales” sólo se pueden aplicar medidas de sanción por fraude en los pocos casos con sospecha asegurada. Además, por consiguiente permanecen esencialmente las pérdidas masivas debidas al fraude de itinerancia.

El documento US 2005 0084083 A1 da a conocer un procedimiento para el reconocimiento de fraude en una red de comunicación, en el que las llamadas telefónicas se verifican por un sistema de reconocimiento de abusos mediante reglas fijadas respecto a un posible abuso. Un criterio posible es en este caso la duración de las llamadas telefónicas, que no deberían sobrepasar un valor umbral consabido. Para conexiones en la red fija se puede realizar esto de forma relativamente sencilla. Aquí no se menciona una solución para las conexiones móviles, en particular conexiones en itinerancia.

Por este motivo el objetivo de la invención es especificar un procedimiento para el reconocimiento de fraude en conexiones en itinerancia en redes de comunicación móviles, que presente en comparación al procedimiento aplicado hasta ahora (MEGS) una tasa de reconocimiento positivo esencialmente más elevada.

Este objetivo se consigue según la invención por las características de la reivindicación independiente.

Configuraciones preferidas y otras características ventajosas de la invención están especificadas en las reivindicaciones dependientes.

Se ha reconocido que en el caso de conexiones salientes en el extranjero hasta ahora no tiene lugar una conexión de señalización en la dirección al operador de la red de adscripción. Esto dificulta el reconocimiento en la red de adscripción (HPLMN), de que clientes reconocidos por el MEGS realizan en el extranjero una conexión permanente de varias horas.

Por ello según la invención se valora como criterio adicional unívoco para el filtro ya implementado por el MEGS la "tasa de ocupación" de las tarjetas SIM en cuestión. Es decir, que en el caso de tarjetas SIM llamativas, reconocidas por el MEGS se constata adicionalmente si existe una conexión permanente durante un intervalo de tiempo más largo (p. ej. varias horas). En caso afirmativo se puede introducir una contramedida temprana y unívoca. Por consiguiente, mediante el bloqueo rápido de la tarjeta SIM en cuestión se puede reducir considerablemente el daño global (la mayoría de las veces hasta el 95 %). Otros clientes que se han detectado mediante los métodos de reconocimiento actuales de MEGS, quedan no influenciados por estas medidas.

Mediante la aplicación de una llamada de test (sin indicación de número de llamada), denominada a continuación llamada PING, sobre la tarjeta SIM / alarma prefiltrada por el MEGS, se puede determinar la "tasa de ocupación" de las tarjetas SIM individuales durante un intervalo de tiempo determinado. Después de sobrepasar un valor umbral para la tasa de ocupación se puede derivar de este modo una señal unívoca para otras medidas de sanción, como bloqueo en el HLR (HLR-Barring) o interrupción de la llamada (Cancel Location).

Para la realización de estas llamadas Ping y de los escenarios siguientes adicionales se puede aplicar un simulador de protocolo SS7/ISUP. El SS7, Signalling System #7 (en español sistema de señalización número 7) comprende una serie de protocolos y procedimientos para la señalización en redes de telecomunicaciones, como la red telefónica pública, tanto si es ISDN, red fija o red móvil.

En así denominados User Parts se describen las funciones que están a disposición de un usuario. Estas funciones pueden ser dependientes del servicio usado (ISDN, teléfono analógico, servicio móvil) y por ello se describen por separado. Los User Parts aquí llamados son:

ISUP (ISDN User Part) describe las funciones que están a disposición de usuarios ISDN. Forman parte de ellas como elemento más importante la descripción del servicio o bearer capability. ISDN permite operar distintos terminales, como teléfono, FAX u ordenador en la misma conexión. En una conexión en la red ISDN se envía siempre una descripción del tipo de servicio, para que sólo responda el terminal que también secunda el servicio deseado.

SCCP (Signalling Connection Control Part) es una capa intermedia que pone a disposición otras funciones más allá de MTP Level 3, como por ejemplo comunicación sin conexión u orientada a la conexión entre funciones de red especiales. La aplicación más importante que está construida sobre SCCP es la "red inteligente" o RI. Las funciones de red inteligente se definen en recomendaciones especiales. En aquellos casos también se puede conducir ISUP (ISDN USer Part) a través de SCCP en lugar de a través de MTP3.

MAP (Mobile Application Part) opera las funciones específicas de redes móviles. Naturalmente la itinerancia es especialmente importante. Mediante itinerancia un abonado puede cambiar de una célula de radio a la siguiente, sin pérdida de conexión y se inscribe en redes ajenas.

Al aplicar llamadas PING se debe tener en cuenta lo siguiente:

1) Determinación de la localización VLR actual

Mensaje SS7 relevante: Send_RoutingInfo_for_SM (SRI for Short Message) Resultado: aplicación como Orig-Reference en la parte MAP del protocolo SS7. Consultas con operación: Interrogate_SS conducirían a una Cancel_Location (así como corte de la conferencia) del cliente en cuestión, lo que no se desea en este contexto.

2) Consulta del estado SS Call Wait, Call Forwarding Unconditional y Call Forwarding BUSY:

Mensaje SS7 relevante: Interrogate_SS (código SS)

Resultado: Estado SS del cliente en cuestión.

Para ello en la parte SCCP se debe aplica la dirección del simulador SS7 y en la parte MAP (Orig_Reference) la dirección VLR actual del cliente. Por lo demás se realiza un Cancel_location por el HLR.

3) Realización de la llamada PING

Mensaje ISUP relevante: IAM

Resultado: si el mensaje se transmite en el protocolo ISUP2 (versión 2), independientemente del desvío de llamada o Call Wait se puede evaluar el estado del cliente (libre u ocupado) ya a través del mensaje ACM (Address Complete Message). Sólo en el caso de CFU activo no es posible en este caso un análisis de estado del abonado saliente (véanse opciones). Actualmente aprox. el 90 % de las relaciones de itinerancia dentro de Europa están conectadas con el protocolo ISUP2.

En el caso de una conexión ISUP1 sólo se puede evaluar el estado ALERT o BUSY. No obstante, en este caso se debe tener en cuenta el estado SS de los análisis de punto 2. En el caso de CFbusy o CW activos no se puede valorar el resultado de llamada Ping (véanse opciones).

4) Desactivación temporal de Call Forwarding y Call Wait.

Mensaje ISUP relevante: Desactivate_SS, Activate_SS (con código SS correspondiente)

Resultado: Opcionalmente en el caso de CFU activo o CPbusy/CW activos en conexión con ISUP1" se puede desactivar temporalmente el servicio SS en el HLR. La llamada PING siguiente proporciona por consiguiente un resultado unívoco para el "estado de ocupación" del cliente. El mensaje SS7 "Activate_SS" reestablece el estado SS original después de la realización de la llamada PING (incluso número de llamada) Nota: Duración total entre desactivación y reactivación: es preferentemente menos de 20 segundos.

El resultado de las llamadas PING conduce a un aumento de calidad del reconocimiento de estafadores reales en el caso de las alarmas originales en más del 90 %.

Repeticiones del bucle de examen (Estado CF/CW; llamada PING u opcionalmente: desactivación CF/CW; LLAMADA PING; reactivación CF/CW) conducen a un enriquecimiento de indicios y afinamiento del valor informativo de esta alarma.

Al superar el valor umbral para la "tasa de ocupación" MEGS desencadena un bloqueo en el HLR. No obstante, las conferencias en curso se deben interrumpir adicionalmente por el mensaje SS7 "Cancel Location" (conexión permanente del defraudador). Ésta se puede realizar igualmente por el simulador de protocolo SS7.

Un ejemplo de realización de la invención se describe más en detalle a continuación mediante el dibujo de la figura 1.

Un abonado de itinerancia se encuentra con su terminal móvil 20 usando un módulo de identidad de abonado personal, tarjeta SIM 20a, en la zona de suministro de una red móvil en itinerancia ajena FPLMN. De forma estándar se verifica si existe peligro para un fraude de itinerancia.

Según la invención se usa como siempre el MEGS 24 para el análisis previo de posibles fraudes de itinerancia. El MEGS 24 dispone de varios filtros de fraude de itinerancia, que se aplican en el caso de conexiones en itinerancia sobra las tarjetas SIM. Si en conexión con la tarjeta SIM 20a del terminal móvil 20 se constatan los criterios de filtrado, entonces se emite un tique de alarma 25 por el MEGS 24.

Según la etapa #1 el tique de alarma 25 generado por el MEGS 24 con el número de teléfono móvil (MSISDN) y reconocimiento de abonado móvil (IMSI) de la tarjeta SIM 20a correspondiente se transmite en un simulador de protocolo 26 para la optimización de la alarma. Allí se procesa el tique de alarma en primer lugar mediante una aplicación de control 27 para la determinación del estado SS.

En una etapa #2, mediante un módulo de localización 28 del simulador de protocolo 26 se realiza una consulta de localización actual (dirección VLR), es decir, la determinación del registro de localización de visitantes VLR 22 (Visitor Location Register) responsable para la tarjeta SIM 20a, mediante la orden MAP Send Routing Info for Short Message (SRIfSM).

En una etapa #3 por un módulo de análisis SS 29 se realiza un examen del estado de las características de servicio (Supplementary Services) técnicas en la comunicación y ajustadas para la tarjeta SIM 20a, en el registro de adscripción HLR 23 responsable. El examen del estado SS puede tener los resultados siguientes: mantener la conexión (Call Wait), desvío de llamada en caso de ocupado (Call Forwarding Busy: CFBusy) y desvío de llamada condicionado (Call Forwarding Unconditional: CFU).

Según una etapa #4 se realiza una transmisión de los resultados de examen de SS a distintos módulos del simulador de protocolo 26. Si, por ejemplo, CFU no está activo, entonces se transmite el tratamiento posterior al módulo 30 para la realización de una llamada Ping.

En una etapa #5 se realiza ahora una LLAMADA-PING. Al usar el protocolo ISUP1 (versión 1) se realiza una evaluación de “alarma” (Alert) u “ocupado” (Busy) teniendo en cuenta el estado SS determinado anteriormente. En general se activa básicamente un desvío de llamada activo al contestador del abonado. En este caso se realiza una transmisión del resultado al módulo de “desactivación temporal opcional de SS” 31.

Al usar el protocolo ISUP2 (versión 2) se realiza una evaluación a través del mensaje Address Complete Message ACM (estado ocupado). El disparo de la conexión se realiza directamente tras la recepción del mensaje de contestación relevante para evitar el tono de llamada o conexiones sujetas a tasas.

En una etapa #6 se realiza una transmisión del resultado al módulo de “resultado” 32. Se sigue con la etapa #7 o bajo condiciones determinadas con las etapas 4a o 6a.

Etapas intermedias opcionales o alternativas (etapas #4a a #6d)

Las llamadas PING con ISUP1 y Call Forwarding$_{[s1]}$ Busy (CFbusy) o Call Wait (CW) activados y consultas SS, que producen un Call Forwarding Unconditional (CFU) activo, conducen a una transmisión al módulo de “desactivación temporal opcional del SS” 31. El MEGS ejecuta la activación / desactivación de este módulo.

En una etapa #4a o #6a se realiza un tratamiento posterior en el módulo de “desactivación temporal opcional de SS” 31:

La acción aquí realizada comprende la desactivación de todo CF/CW activo constatado (resultados del módulo d “análisis SS”). Mensaje SS7: deactivate_SS (código SS).

En la parte SCCP se debe usar la dirección del simulador SS7 y en la parte MAP (Orig_Reference) la dirección VLR actual del abonado. Por lo demás se realiza un Cancel_location por el HLR 23 que conduce al corte de la conferencia.

Una actualización del VLR 22 se realiza a través del mensaje “insert subscriber data”. Este mensaje se envía automáticamente al VLR 22 por el HLR 23.

En la etapa #4b o #6b se realiza la llamada PING 33. La evaluación de los resultados de la llamada PING se realiza según se describe en la etapa #5.

En las etapas #4c o #6c se realiza una reactivación 34 del servicio SS desactivado anteriormente con mensaje SS: activate_SS (código SS). Un desvío activo anteriormente obtiene con ello automáticamente el mismo número de llamada (p. ej. contestador) según se ha establecido anteriormente.

En este caso en la parte SCCP se debe usar la dirección del simulador SS7 y en la parte MAP (Orig_Reference) la dirección VLR actual del cliente. Por lo demás se realiza un Cancel_location por parte del HLR 23 que conduce al corte de conferencia.

Una actualización del VLR 22 se realiza a través del mensaje “insert subscriber data”. Este mensaje se envía automáticamente al VLR 22 por el HLR 23.

En las etapas #4d o #6d se realiza una transmisión del resultado al módulo de “resultado” 32. El resultado contiene el estado de ocupación del terminal móvil 20 operado con la tarjeta SIM 20a durante un intervalo de tiempo observado, por ejemplo, “ocupado durante al menos 60 minutos”.

En la etapa #7 se transmiten los resultados de análisis con los indicios del “estado de ocupación”, MSISDN, IMSI, VLR, ID, Versión ISUP, estado CF y estado CW por el módulo de resultado 32 en forma de un tique de alarma 35 optimizado al MEGS 24.

En la etapa #8 MEGS 24 valora el resultado de cada tarjeta SIM en un contador de valor umbral 36 sobre la “tasa de ocupación”. Para ello se puede fijar a partir de qué número de repeticiones o a qué “tasa de ocupación” se puede iniciar un bloqueo de la tarjeta SIM 20a en cuestión.

En la etapa #9 se inicia de nuevo otra LLAMADA PING, según el mismo escenario que se ha descrito en las etapas #2 - #6, si el número necesario de repeticiones todavía no se ha alcanzado. Un control de repeticiones 37 examina en este caso el retardo necesario entre las LLAMADAS PING y asume otros controles de la función de repetición (véase fig. 1).

En la etapa #10 se desencadena otra LLAMADA PING a través de la interfaz de entrada (aplicación de control 27) entre el MEGS 24 y el simulador de protocolo 26.

Las etapas #11 y #12 designan la repetición de las etapas #1 - #7 (función de repetición) según se ha descrito arriba.

Según la etapa #13 no se inicia otra LLAMADA PING si se ha alcanzado el número necesario de repeticiones. El módulo de examen del contador de valor umbral 36 examina si la “tasa de ocupación” de la tarjeta SIM en cuestión ha sobrepasado el valor umbral definido (p. ej. 60 minutos).

Según la etapa #14 se envía una señal para el inicio del bloqueo al módulo de “bloqueo” 38 al sobrepasar el valor umbral para la tarjeta SIM 20a en cuestión.

Según la etapa #15 el módulo de “bloqueo” 38 induce el bloqueo de la tarjeta SIM en el HLR 23 (Barring) y una señal al simulador de protocolo 26 para el envío de mensaje “Cancel Location”. Para ello se aplica el VLR-Global Title que se ha constatado por el módulo de examen de “localización” 28 (SRIfSM).

Según la etapa #16 el simulador de protocolo 26 envía el mensaje “Cancel Location” a través del módulo de Cancel Location 39 al VLR 22 actual. De este modo se rompe una conferencia existente y la tarjeta SIM 20a en cuestión se debe inscribir nuevamente en el VLR 22. En caso de otras actividades de la tarjeta SIM actúa el bloqueo de SIM activado nuevamente en el HLR 23 por el MEGS 24. Los parámetros correspondientes para el bloqueo de la SIM se transmiten automáticamente por el HLR 23 al VLR 22 mediante el mensaje “insert subscriber data”.

Mediante la optimización del reconocimiento del fraude según el concepto propuesto existe la posibilidad de reducir esencialmente las pérdidas originadas por el así denominado fraude de itinerancia.

Lista de referencias

#1 a #16. Etapas del procedimiento

20. Terminal móvil

20a. Tarjeta SIM

21. Red móvil de itinerancia (FPLMN)

22. Registro de localización de visitantes VLR (del FPLMN)

23. Registro de adscripción HLR (del HPLMN)

24. MEGS (sistema de reconocimiento de abusos)

25. Tique de alarma

26. Simulador de protocolo

27. Aplicación de control (estado SS)

28. Módulo de “localización”

29. Módulo de “análisis SS”

30. Módulo de “llamada PING”

31. Módulo de “desactivación CF/CW”

32. Módulo de “resultado”

33. Módulo de “llamada PING”

34. Módulo de “reactivación CF/CW”

35. Tique de alarma optimizado

36. Módulo de “contador de valor umbral”

37. Módulo de “control de repetición”

38. Módulo de “bloqueo”

39. Módulo de “Cancel Location”

REIVINDICACIONES

1. Procedimiento para el reconocimiento de fraude en redes de comunicación móviles, en particular para el reconocimiento de fraude en conexiones en itinerancia, en el que para el análisis previo de posibles fraudes de itinerancia se usa un sistema de reconocimiento de abusos, MEGS, (24) existente y en el caso de un módulo de identificación de abonado, tarjeta SIM, (20a) llamativo, reconocido por el MEGS (24) se verifica una conexión en itinerancia asociada al módulo de identificación de abonado mediante al menos un criterio adicional respecto a un posible abuso,

caracterizado porque

como criterio se examina la “tasa de ocupación” del módulo de identidad de abonado (20a) en cuestión durante un intervalo de tiempo determinado, averiguándose la tasa de ocupación del módulo de identidad de abonado (20a) mediante al menos una llamada de test, llamada PING, al módulo de identidad de abonado, usándose para la realización de la llamada PING un simulador de protocolo SS7/ISUP (26),

porque antes de la realización de la llamada PING se determina la ubicación actual del módulo de identidad de abonado (20a) mediante una consulta de la dirección VLR actual (#2),

porque usando la dirección VLR y antes de la realización de la llamada PING se averigua el estado SS actual del módulo de identidad de abonado, que comprende Call Wait, CV, Call Forwarding Unconditional, CFU, y Call Forwarding BUSY, CFBusy, en el registro de adscripción, HLR, (23) (#3), y

porque en el caso de CFU activo o CFBusy/CW activo en conexión con ISUP1 se desactiva temporalmente el servicio SS en el HLR (31), a continuación se realiza la llamada PING (33), y después de la realización de la llamada PING se reestablece el estado SS original (34).

2. Procedimiento según la reivindicación 1, **caracterizado porque** en el caso de que la tasa de ocupación sobrepase un valor umbral temporal determinado se inician medidas para impedir un abuso frente al módulo de identidad de abonado (20a).

3. Procedimiento según una de las reivindicaciones anteriores, **caracterizado porque** las medidas para impedir un abuso comprenden un bloqueo en el HLR (23), HLR-Barring, o una interrupción de la llamada, Cancel Location.

4. Procedimiento según una de las reivindicaciones anteriores, **caracterizado porque** mediante la llamada Ping, en el caso de una conexión ISUP2, independientemente del desvío de llamada o Call Wait ya se puede evaluar el estado del módulo de identidad de abonado a través del mensaje ACM, Address Complete Message, no siendo posible un análisis de estado del abonado itinerante saliente en caso de CFU activo.

5. Procedimiento según una de las reivindicaciones anteriores, **caracterizado porque** mediante la llamada Ping, en el caso de una conexión ISUP1, se puede evaluar el estado ALERT o BUSY, no pudiéndose valorar el resultado de la llamada Ping en el caso de CFbusy o CW activos.

6. Dispositivo para la realización del procedimiento según una de las reivindicaciones 1 a 5, que comprende un sistema de reconocimiento de abusos MEGS (24) y un simulador de protocolo (26).

7. Programa de procesamiento de datos con un código de programa que realiza un procedimiento según una de las reivindicaciones 1 a 5 ejecutado sobre uno o varios dispositivos de procesamiento de datos.

8. Producto de programa de procesamiento de datos, que comprende código de programa ejecutable sobre uno o varios dispositivos de procesamiento de datos para la realización del procedimiento según una de las reivindicaciones 1 a 5.

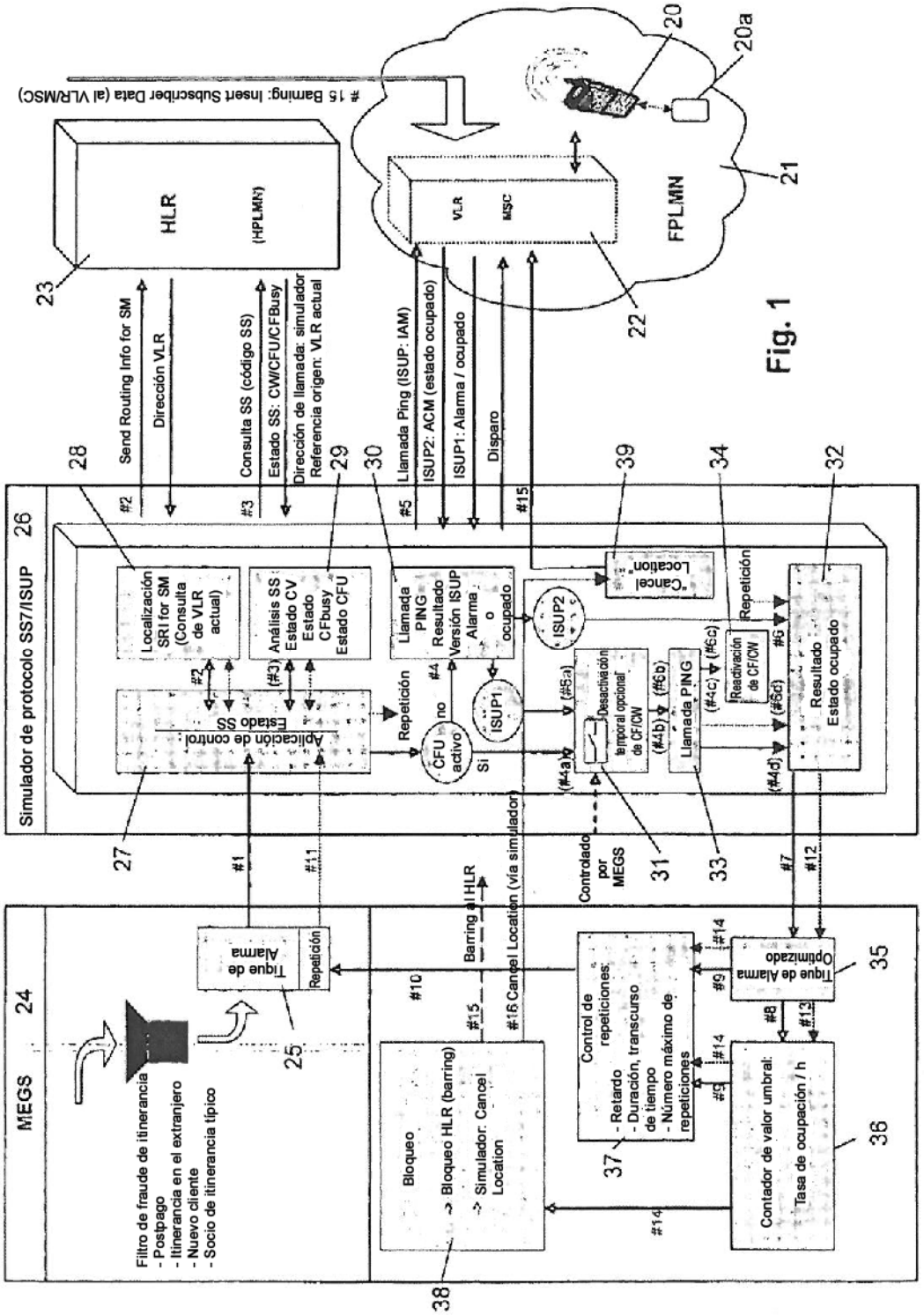
20
20a
21
22
23
HLR
(HPLMN)
FPLMN
VLR
MSC
15 Barring: Insert Subscriber Data (al VLR/MSC)
Send Routing Info for SM
Dirección VLR
Consulta SS (código SS)
Estado SS: CW/CFU/CFBusy
Dirección de llamada: simulador
Referencia origen: VLR actual
Llamada Ping (ISUP: IAM)
ISUP2: ACM (estado ocupado)
ISUP1: Alarma / ocupado
Disparo
Simulador de protocolo SS7/ISUP
26
28
29
30
39
34
32
Localización SRI for SM (Consulta de VLR actual)
Análisis SS: Estado CV Estado CFbusy Estado CFU
Llamada PING Resultado Versión ISUP Alarma: o ocupado
"Cancel Location"
Repetición
Aplicación de control Estado SS
CFU activo
no
Si
ISUP1
ISUP2
Desactivación temporal opcional de CF/CW
Llamada PING
Reactivación de CF/CW
Resultado Estado ocupado
27
31
33
Controlado por MEGS
MEGS
24
Filtro de fraude de itinerancia
- Postpago
- Itinerancia en el extranjero
- Nuevo cliente
- Socio de itinerancia típico
Tique de Alarma
Repetición
25
Barring al HLR
Cancel Location (vía simulador)
Bloqueo
-> Bloqueo HLR (barring)
-> Simulador: Cancel Location
38
Control de repeticiones:
- Retardo
- Duración, transcurso de tiempo
- Número máximo de repeticiones
37
Tique de Alarma Optimizado
35
Contador de valor umbral:
Tasa de ocupación / h
36

Fig. 1