(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 400 166**

(51) Int. CI.:

H04W 12/08 (2009.01)
H04L 29/06 (2006.01)
H04M 3/533 (2006.01)
H04M 3/38 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **20.10.2008 E 08018300 (7)**

(97) Fecha y número de publicación de la concesión europea: **12.12.2012 EP 2178323**

(54) Título: **Protección de servicios en una red móvil contra la suplantación de CLI**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.04.2013

(73) Titular/es:

KONINKLIJKE KPN N.V. (100.0%)
MAANPLEIN 55
2516 CK THE HAGUE, NL

(72) Inventor/es:

OORTMARSSEN, HANS FREDERIK y
RAMBELJE, ALEXANDER FRANCISCUS

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Protección de servicios en una red móvil contra la suplantación de CLI

Campo de la invención

La invención está relacionada con el control de acceso de un dispositivo de comunicación móvil a un servicio en una red de comunicación a través de una conexión establecida desde el exterior de la red de comunicación. La invención también está relacionada con un equipo de procesamiento de datos y con el software de control para controlar dicho acceso.

Técnica anterior

En una red de telecomunicaciones la función de identificación de la llamada (Caller ID) es un servicio que proporciona al número llamado o al servicio llamado información acerca de una identidad del número que llama. La función Caller ID también recibe el nombre de "Identificación de la línea que llama" (CLI) o "Id de la parte que llama". La CLI permite que el número llamado o el servicio llamado identifiquen y autorice a la parte que llama. El Caller ID es una simple cadena de datos que puede generarse fácilmente mediante un pequeño programa de software. Los agentes de venta telefónica y otros han estado utilizando cierta funcionalidad para interferir con la función de CLI con el fin de alterar u ocultarle su identidad a la parte llamada. Las expresiones suplantación del Caller ID y "suplantación de CLI" se refieren a esta práctica de conseguir que la red de telecomunicaciones le proporcione al número llamado una información de identidad diferente de la información de identidad de la parte que realmente llama. La suplantación de CLI no sólo se utiliza indebidamente para engañar a una parte llamada cuando ésta responde, sino también para acceder al correo de voz de otra persona en un sistema de correo de voz que utiliza la CLI para la identificación.

La suplantación de CLI no representa un riesgo si la llamada se origina dentro de la red del operador, ya que la integridad de la CLI está garantizada. Sí existe un riesgo, sin embargo, si la llamada se genera en otra red diferente de la red doméstica del operador, ya que la CLI puede haber sido manipulada. Por ejemplo, la CLI se puede manipular en redes externas de voz sobre IP (VoIP). Como consecuencia, existe un riesgo de que cualquier llamada que entre en la red doméstica tenga una CLI que haya sido manipulada.

Las redes de telefonía móvil han venido adoptando una infraestructura, denominada "CAMEL", para el control de las llamadas. El acrónimo "CAMEL" significa Lógica Mejorada de Aplicaciones Personalizadas para Redes Móviles, que es un estándar del ETSI/3GPP. CAMEL se refiere a un conjunto de normas diseñadas para operar en una red GSM o UMTS. Las normas le permiten a un operador definir servicios sobre los servicios GSM o UMTS convencionales. La propia arquitectura CAMEL se basa en estándares de Red Inteligente (IN). La arquitectura IN ha sido diseñada para redes de telecomunicaciones fijas, así como para redes de telecomunicaciones móviles. Las normas de IN utilizan el protocolo del Sistema de Señalización #7 (SS7) entre los centros de conmutación de redes de telefonía y otros nodos de red propiedad de los operadores de red. SS7 es un protocolo de comunicaciones de alta velocidad y de alto rendimiento basado en paquetes para el control de las llamadas. En el SS7 la señalización es fuera de banda y se envía a través de un canal de señalización independiente al cual el usuario final no tiene acceso. La ruta de señalización del SS7 es lógicamente independiente y diferente de los canales que transportan la señal de voz. El control de la llamada, proporcionado por los conmutadores de la red, es independiente del control del servicio. El control de los servicios está asignado a unos nodos informáticos de la red. En consecuencia, una red basada en CAMEL proporciona un alto nivel de seguridad, y la suplantación de CLI en una red basada en CAMEL se considera un riesgo muy bajo, o inexistente. Por otra parte, CAMEL permite a los operadores de redes de telefonía móvil ofrecer a sus suscriptores mientras se encuentran en itinerancia en otras redes basadas en CAMEL los mismos servicios de IN que reciben en su red doméstica basada en CAMEL, es decir, la red del operador al que se han abonado.

Un mecanismo de defensa que se aplica comúnmente para neutralizar la suplantación de CLI cuando se utiliza para acceder al correo de voz desde el exterior de la red del operador consiste en solicitar que la parte que accede introduzca una contraseña secreta compartida por el propietario de la cuenta de correo de voz y el sistema de correo de voz. La contraseña es, por ejemplo, una contraseña numérica, como por ejemplo un número de identificación personal (PIN), o una combinación del PIN y el número de teléfono del dispositivo de comunicaciones asociado a la cuenta. De igual modo, la contraseña se puede utilizar para la protección de otros servicios de red que se basan en la CLI, como por ejemplo el servicio al cliente del operador de la red, el servicio de help desk (asistencia al usuario), un portal de voz automático, etc. No obstante, tal como se muestra en "Cell phone voicemail easily hacked" (Acceso fraudulento sencillo al correo de voz de un teléfono móvil), [Online] 28 de febrero de 2005 en MSNBC.com, en http://www.msnbc.msn.com/id/7046776/print/l/displaymode/1098/, de Bob Sullivan, muchos proveedores de teléfonos móviles les ofrecen a los usuarios de correo electrónico la posibilidad de decidir no tener que introducir un código de acceso o un código numérico para acceder a su correo de voz, con el resultado de que muchos usuarios han deshabilitado la funcionalidad asociada al código de acceso para ahorrar tiempo cuando acceden a su propio correo de voz. Esto hace que su correo de voz resulte vulnerable ante accesos fraudulentos por parte de terceros con malas intenciones.

Tanto en el documento WO2008082489 como en el US 2008/0159501 se divulga otro enfoque relacionado con métodos de validación del Caller ID y con un sistema de protección contra la suplantación del Caller ID. Cuando se realiza una llamada en una red de comunicación, la señalización de la llamada es recibida por un sistema de validación, y éste procesa la señalización de la llamada con el fin de identificar en dicha señalización de la llamada la información del nodo de origen. La información del nodo de origen es aportada por la red de comunicación cuando ésta gestiona la llamada, y pertenece a un nodo de la red que inicia la llamada en la red. El sistema de validación también procesa la señalización de la llamada para obtener la información del Caller ID. A continuación, el sistema de validación procesa la información del nodo de origen y la información del Caller ID para determinar si la llamada se ha iniciado desde el nodo de origen. Si la llamada se ha iniciado en el nodo de origen, el sistema de validación determina que la información del Caller ID es válida.

Para obtener información de carácter genérico sobre la suplantación, véanse, por ejemplo, los documentos US 20080089501, US 20070081648, US 20020098829, y US 7.342.926.

Para obtener información de carácter genérico sobre las IN, véase, por ejemplo, el documento US 20080155021.

Para obtener información de carácter genérico sobre las redes CAMEL, véanse, por ejemplo, los documentos WO2008/17951, WO2007/126995 y WO2003036994.

Para obtener información de carácter genérico sobre las redes de tránsito, véanse, por ejemplo, los documentos US 20080101568 y WO 2003/036994.

Para obtener información de carácter genérico sobre algunos aspectos de la itinerancia, véanse, por ejemplo, los documentos WO 2006133720, WO2007002524, WO2003055249, EP1106025, EP1933572 y US 6.804.505.

Resumen de la invención

Como se ha mencionado más arriba, la suplantación de CLI no se considera un riesgo para las comunicaciones entre las partes dentro de la red doméstica de un operador de red individual, por ejemplo, una comunicación en la que el usuario final accede a su correo de voz desde dentro de la red, o una comunicación en la que el usuario accede desde dentro de la red doméstica a otros servicios de red que utilizan la CLI. Algunos ejemplos de estos últimos son un servicio al cliente, y un portal de voz automático (un equivalente de voz de un portal Web a través del cual los clientes pueden interactuar con servicios automatizados mediante instrucciones de voz o instrucciones mediante teclado que utilizan una señalización Multifrecuencia de Doble Tono a través de la línea telefónica en la banda de frecuencia de voz). Por otro lado, la suplantación de CLI se considera un riesgo para las llamadas entrantes en la red doméstica, por ejemplo, las llamadas que se originan en redes de VoIP. En general, la red de origen encamina sus llamadas a través de una o más redes de tránsito. Como resultado, en el punto de entrada a la red doméstica ya no es posible identificar la red de origen, y, por consiguiente, cualquier llamada entrante podría haberse originado en una red de VoIP no fiable.

Los inventores son conscientes de que la introducción de contraseñas para acceder al correo de voz u otros servicios basados en la CLI resulta realmente incómoda tal como la percibe el usuario final. El usuario final tiene que recordar su contraseña, y la introducción de la misma requiere un tiempo adicional que, a su vez, incrementa el coste de la conexión de red. En muchos casos, el usuario puede haber olvidado su contraseña, por lo que la llamada no se llegará a completar, dando lugar a una pérdida de ingresos para el operador.

Por otra parte, el sistema conocido divulgado en el documento WO2008082489, mencionado más arriba, requiere que los nodos de red implicados se hayan configurado para construir y comunicar los parámetros relevantes de señalización de la llamada a través de la red.

En consecuencia, los inventores proponen facilitar el acceso a los servicios de red basados en la CLI de la red doméstica desde otra red basada en CAMEL, sin comprometer la seguridad ante la suplantación de CLI. Asimismo, los inventores proponen conseguirlo con las mínimas modificaciones de los componentes de red implicados.

Una propuesta de los inventores está relacionada con un método para controlar el acceso de un dispositivo de comunicaciones móviles a un servicio de una red doméstica a través de una conexión desde el exterior de la red de comunicación. El dispositivo es, por ejemplo, un teléfono móvil. La red doméstica comprende, por ejemplo, una red de móviles. El servicio incluye, por ejemplo, un servicio de correo de voz, un servicio de help desk, un portal de voz automático, etc. El dispositivo está configurado para suministrar un identificador único para identificar el dispositivo ante el servicio. El método comprende los siguientes pasos. Si el identificador se recibe desde el exterior de la red doméstica y a través de un canal de señalización seguro, se almacena en una memoria una primera marca de tiempo. La primera marca de tiempo representa el primer instante en el que se ha recibido el identificador. Cuando se ha establecido una parte de la conexión con un nodo de la red doméstica se genera una segunda marca de tiempo. El nodo comprende, por ejemplo, un conmutador o un servidor que suministra el servicio. A continuación, si la diferencia de tiempo entre la primera y la segunda marcas de tiempo se encuentra dentro de una ventana de tiempo predeterminada, se autoriza el identificador y se le envía al nodo una primera instrucción para establecer un acceso incondicional del dispositivo al servicio. Por ejemplo, en el establecimiento de la llamada desde el nodo al

servicio, se utiliza un indicador para informar al servicio de que el identificador es válido y que, por lo tanto, se puede permitir el acceso incondicional. Si la diferencia de tiempos se encuentra fuera de la ventana de tiempo predeterminada, no se autoriza el identificador y se le envía al nodo una segunda orden para que establezca un acceso condicional del dispositivo al servicio. Por ejemplo, en el establecimiento de la llamada desde el nodo al servicio, se utiliza un indicador para informar al servicio de que el identificador no ha podido ser autorizado y que, por lo tanto, el servicio tiene que actuar en consecuencia, por ejemplo, solicitando una contraseña o el código PIN, o denegando inmediatamente el acceso.

De acuerdo con ello, a un usuario de un dispositivo válido dado de alta en el servicio se le concede un acceso incondicional cuando inicia la conexión desde otra red que proporciona un canal de datos seguro, por ejemplo, otra red basada en CAMEL. La autorización del usuario no se cuestiona como resultado de haberse recibido el identificador a través del canal de señalización seguro. Los datos que viajan a través del canal seguro no pueden ser manipulados por un impostor. Si el usuario del dispositivo válido se conecta a la red de comunicación desde otra red de comunicación que no ofrezca un canal seguro, nunca se generará una primera marca de tiempo. Como resultado, la diferencia de tiempos se encuentra fuera de la ventana y el acceso concedido es condicional, por ejemplo, dependiente de una contraseña. Si un impostor se conecta a la red de comunicaciones doméstica desde otra red de comunicación que no proporciona el canal de señalización seguro, si el impostor no puede proporcionar la contraseña se le deniega el acceso al servicio.

La invención se pone en práctica de acuerdo con las reivindicaciones independientes 1, 5 y 6.

Breve descripción de los dibujos

La invención se explica de forma más detallada por medio de ejemplos y haciendo referencia a los dibujos adjuntos, en donde:

la Fig. 1 es un diagrama de bloques de un sistema que ilustra la comunicación entre una red de comunicaciones doméstica y una red basada en CAMEL;

la Fig. 2 es un diagrama de flujo que ilustra las etapas de la comunicación en el sistema de la Fig. 1; y

la Fig. 3 es un diagrama de flujo que ilustra el método de la invención.

En todas las figuras, las características similares o correspondientes se designan mediante los mismos números de referencia.

Modos de realización detallados

La Fig. 1 es un diagrama de bloques de un sistema 100 que explica el funcionamiento de una comunicación telefónica móvil entre una red doméstica 102 y una red de itinerancia (106) basada en CAMEL. La red doméstica 102 es una primera red de telecomunicaciones 102 de un primer operador de red, a cuyos servicios se ha abonado un usuario de un dispositivo 104 de telecomunicaciones móviles, por ejemplo, un teléfono móvil. La red 102 tiene una primera cobertura geográfica. La región geográfica cubierta por la red 102 también recibe el nombre de área de servicio de la red 102. El operador de la red 102 ha suscrito acuerdos CAMEL con algunos, pero no necesariamente todos, los operadores de redes de itinerancia. La red de itinerancia 106 basada en CAMEL es una segunda red de telecomunicaciones 106 de un segundo operador. La región geográfica cubierta por la red 106 recibe el nombre de área de servicio de la red 106. El operador de la red 102 ha suscrito un acuerdo CAMEL con el operador de la red 106.

Si el usuario del dispositivo 104 ha abandonado el área de servicio de la red 102 y entra en la red 106, puede seguir utilizando el dispositivo 104 para comunicarse con otras personas que residen en la red 102 (o en otras redes, que no se muestran), por ejemplo, con el usuario de un dispositivo 108 de telecomunicaciones móviles o con un usuario de un teléfono fijo 110, a través de la red de telefonía pública conmutada (PSTN) 112 y de la red de tránsito 113. Esto es debido a los acuerdos de itinerancia entre los operadores de red y a la infraestructura que respalda las redes 102 y 106, como se explicará a continuación.

Supóngase que el usuario del dispositivo 104 enciende el dispositivo 104 por primera vez mientras se encuentra en el área de servicio de la red 106, o está entrando en el área de servicio de la red 106 mientras el dispositivo 104 se encuentra en itinerancia en otra red. La red visitada 106 detecta en ese momento la presencia del dispositivo 104 y, entonces, iniciará un procedimiento de autenticación. Si el dispositivo 104 se encuentra encendido, transmite su número de identificación (en este caso su IMSI (Identificador Internacional de Abonado Móvil)). Este identificador de autenticación es recibido por una estación base 114, y reenviado a través de un controlador de estación base (BSC) 116 a un centro de conmutación de móviles (MSC) 118 de la red 106. Este número IMSI pertenece exclusivamente al dispositivo 104. En un teléfono móvil, se encuentra normalmente almacenado en la tarjeta SIM del teléfono (módulo de identidad del abonado). La red 106 mantiene una base de datos 122 (denominada "registro de localización de visitantes" (VLR)) que contiene los números IMSI de todos los dispositivos de telecomunicaciones móviles que se encuentran actualmente activos dentro del área de servicio de la red 106. El VLR 122 almacena

registros de información acerca de los dispositivos de telecomunicaciones móviles activos, por ejemplo, su número IMSI y su número MSISDN (Abonado Móvil de la Red Digital de Servicios Integrados) y la clase de servicios que cada uno de estos dispositivos está autorizado a utilizar. Como es sabido, el número IMSI y el número MSISDN son dos números importantes para identificar un teléfono móvil. El número IMSI se utiliza normalmente como clave en la base de datos de abonados (véase "HLR 126" que se describe más abajo). El número MSISDN se utiliza habitualmente como identificador para un sistema de correo de voz. El número MSISDN también es generalmente el número que se marca para realizar una llamada a ese teléfono móvil.

A fin de obtener esta información, el VLR 122 identifica la red doméstica correspondiente de un dispositivo detectado a partir del número IMSI recibido por la red 106. La red doméstica del dispositivo 104 es la red 102. El VLR 122 utiliza el número IMSI recibido del dispositivo 104 para acceder a una base de datos 126 (denominada Registro de Localización Base, o HLR) de la red doméstica 102, y solicita información sobre los privilegios del dispositivo 104. El HLR 126 mantiene unos registros que especifican esta clase de información para cada abonado individual de los servicios de la red doméstica 102. Con el fin de autorizar al dispositivo 104 a partir del número IMSI, el HLR 126 y el módulo de identidad del abonado (SIM) (no se muestra) del dispositivo 104 inician un procedimiento denominado "procedimiento de autenticación GSM". En este procedimiento, se intercambia información criptográfica entre el SIM del dispositivo 104 y el HLR 126. Como la red 102 y la red 106 han suscrito Acuerdo de Itinerancia CAMEL, el HLR 126 le devuelve al VLR 122 tras la finalización del procedimiento de autenticación la información necesaria para que el VLR 122 determine si el dispositivo 104 está o no autorizado para transitar por la red 106 y la clase de servicios que está autorizado a utilizar, así como para qué servicios hay que contactar con la red doméstica antes de la ejecución de los servicios. Por ejemplo, el HLR 126 le devuelve al VLR 122 información sobre cómo proceder en caso de que el dispositivo 102 intente establecer una llamada. El HLR 126 le proporciona al VLR 122 datos de activación para indicarle al MSC 118 que contacte con la Red Inteligente (IN) 124 de la red doméstica 102 en caso de que el dispositivo 104 intente establecer una llamada, y para indicarle al MSC 118 que espere nuevas instrucciones de la IN 124. La comunicación entre el MSC 118 de la red 106 y la IN 124 de la red 102 utiliza un canal de señalización seguro, como ocurre con la comunicación entre el VLR 122 de la red 106 y el HLR de la red 102. Por ejemplo, la comunicación entre el MSC 118 y la IN 124, y la comunicación entre el VLR 122 y el HLR 126 utiliza una red de señalización 125 cerrada.

Considérese el escenario en el que el usuario del dispositivo 104, mientras se encuentra en itinerancia en la red 106 (la red visitada), quiere hacer una llamada al usuario del dispositivo 108 de la red 102 (la red de origen) o al usuario del teléfono fijo 110.

Cuando el dispositivo 104 marca un número de teléfono para realizar una llamada telefónica desde su ubicación actual, es decir, dentro de la red 106, el MSC 118 utiliza los datos de activación recibidos del VLR 122 y consulta la IN 124 en la red 102 antes de establecer la llamada al destino marcado. La IN 124 analiza la información recibida del MSC 118 y en este caso podría determinar que no se requiere ninguna acción especial. A continuación, la IN 124 le indicará al MSC 118 que establezca la llamada al destino deseado de acuerdo con el número marcado originalmente por el usuario del dispositivo 104.

Si el destino deseado es el teléfono fijo 110, el MSC 118 establece la llamada al teléfono 110 a través de una red de tránsito 113 y a través de la PSTN 112. Si el destino deseado es el dispositivo 108, el MSC 118 establece la llamada al dispositivo 108 a través de la red de tránsito 113 y a través de un MSC 128 de la red 102. A continuación la llamada se encamina desde el MSC 128 a un BSC 130 de la red 102 y a una estación base 132 de la red 102.

Considérese ahora un escenario en el que el dispositivo 104, registrado en la red 102, se utiliza para acceder desde la red 106 a un servicio de la red 102 basado en la CLI, por ejemplo, el correo de voz dirigido al dispositivo 104. Los mensajes de voz se almacenan en un servidor de correo de voz 134 de la red 102. El usuario del dispositivo 104 introduce la dirección de red de su correo de voz, bien un número de teléfono completo o únicamente el código abreviado. Por ejemplo, el código abreviado para acceder al propio correo de la voz en la red de KPN en los Países Bajos es "1233", en tanto que el número de teléfono completo que se debería marcar es "+31 (0)6 1200 1233".

Como el dispositivo 104 se encuentra dentro del área de servicio de la red 106, la llamada se establece a través del MSC 118. Tal como se ha especificado más arriba, al recibir la solicitud para establecer una llamada desde el dispositivo 104, el MSC 118 le solicita a la IN 124 que le indique cómo procesar la llamada. La IN 124 le indica al MSC 118 que establezca la llamada al sistema de correo de voz 134 utilizando la dirección de red apropiada del servidor 134. La dirección de red apropiada en este ejemplo es "+31-6-1200-1233". Si en lugar de ésta el usuario ha marcado el número abreviado, por ejemplo, "1233" en el ejemplo anterior, la IN 124 le indica al MSC 118 que conecte la llamada al número "+31-6-1200-1233". La llamada se establecerá desde el MSC 118, a través de la red de tránsito 113 y el MSC 128 hasta el servidor 134.

La Fig. 2 es un diagrama de flujo 200 que resume los pasos en el escenario expuesto más arriba haciendo referencia a la Fig. 1. Se supone que se ha detectado la presencia del dispositivo 104 y que el VLR 122 ha recibido desde el HLR 126 los datos de activación para poder indicarle al MSC 118 que se ponga en contacto con la IN 124 de la red doméstica 102 cuando el dispositivo 104 inicie una llamada. En el paso 202, el MSC 118 detecta que el dispositivo 104 está iniciando una llamada a un destino específico. En el paso 204, el MSC 118 contacta con la IN

124 para pedirle instrucciones acerca de cómo procesar la llamada. La IN 124 comprueba los registros y devuelve, en el paso 206, instrucciones específicas sobre cómo procesar la llamada, si las hubiere. En el paso 208, el MSC 118 establece la llamada a través de la red de tránsito 113 y el MSC 128. En el paso 210, el MSC 128 encamina la llamada hacia el dispositivo 108.

Supóngase ahora un dispositivo de comunicación 136 que se hace pasar por el dispositivo 104 mediante suplantación de CLI para acceder a los mensajes de voz dirigidos al usuario del dispositivo 104. El dispositivo 136 ha sido manipulado para iniciar una llamada en la que la cadena de datos es idéntica a la CLI asociada al dispositivo 104 con el fin de confundir a la red 102. El dispositivo 136 es, por ejemplo, un ordenador personal (PC) que utiliza el protocolo de voz sobre IP (VoIP). Sin otras medidas adicionales, al dispositivo 136 que se hace pasar por el dispositivo 104 se le permitirá acceder al correo de voz en el servidor 134, sobre la base de la CLI adoptada por el dispositivo 136. El operador de la red 102 podría disponer una barrera adicional, permitiendo un acceso condicional al correo de voz al recibir la contraseña correcta (por ejemplo, el PIN) tal como se encuentre registrada para el usuario del dispositivo 104. Como se ha mencionado más arriba, ésta es una solución que presenta una desventaja, ya que incomodaría al usuario legítimo cada vez que éste accede a su correo de voz. El servicio sería percibido entonces como no demasiado sencillo de utilizar y, como resultado, el tráfico de red, generado a partir de los accesos al correo de voz desde otra red, se reduciría significativamente, al igual que los ingresos para el operador de la red derivados de los accesos desde la red exterior 102.

El inventor propone, entre otras cosas, para evitar que el usuario del dispositivo 104 tenga que introducir una contraseña cuando llama desde otra red basada en CAMEL a un servicio basado en la CLI en su red doméstica que también está basada en CAMEL, y proporcionar al mismo tiempo seguridad contra la suplantación de CLI. Esto se explica haciendo referencia a las Fig. 1 y 3.

La Fig. 3 es un diagrama de flujo 300 que ilustra los pasos en un proceso de establecimiento de una llamada a un servicio, en este caso el servicio de correo de voz 134, de acuerdo con la invención y que implica redes 102 y 106 basadas en CAMEL. Los pasos que el diagrama 300 tiene en común con el diagrama 200 se indican mediante los mismos números de referencia. En el paso 202, el MSC 118 detecta que el dispositivo 104 está iniciando una llamada. En el paso 204, el MSC 118 contacta con la IN 124 para pedirle instrucciones acerca de cómo procesar la llamada. En un paso 302 la IN 124 reconoce que se ha marcado un número de servicio basado en la CLI y almacena el identificador (en este caso el número MSISDN) del dispositivo 104 y el número del servicio en una memoria local (no se muestra), junto con una primera marca de tiempo que representa el instante T_1 de recepción del identificador a través del canal seguro entre la red 102 y la red 106. En el paso 206, la IN 124 le indica al MSC 118 que establezca la llamada al número de servicio internacional, y en el paso 208, el MSC 118 establece la llamada al MSC 128. En el paso 304, el MSC 128 contacta con la IN 124 con el identificador (el MSISDN) del dispositivo 104 que ha recibido. El MSC 128 ha sido programado previamente con reglas que se activan mediante el número del servicio que se ha marcado. En el paso 306, la IN 124 recibe del MSC 128 el identificador del dispositivo para el que se ha establecido la llamada hasta el MSC 128, junto con el número del servicio utilizado. La IN 124 genera una segunda marca de tiempo para un instante T_2 en el que se ha establecido la llamada hasta el MSC 128. En el paso 308, la IN 124 comprueba si el identificador fue almacenado previamente en la etapa 302. Si no es así, en el paso 310 la IN 124 le indica al MSC 128 que establezca la conexión con el servidor de correo de voz 134 en un modo condicional. Esto es, para acceder al correo de voz en el servidor 134 durante esta conexión, el usuario del dispositivo conectado sólo dispone de un acceso condicional al servidor de correo de voz 134 cuando cumpla con una condición predeterminada, por ejemplo la introducción de una contraseña. De este modo, el MSC 128 le indica al servidor de correo de voz 134 que asuma el modo condicional. El servidor 134 asume el modo condicional de acuerdo con la información codificada por el MSC 128 en el número del servicio utilizado para dirigirse al servidor 134, por ejemplo, cuando el MSC 128 se dirige al servidor 134 con un prefijo P_1 delante del número del servicio, o cuando el MSC 128 se dirige al servidor 134 a través del código largo de acceso. Por otra parte, si en el paso 302 se almacenó el identificador, la IN 124 comprueba si la diferencia entre T_2 y T_1 es menor que un umbral predeterminado T. El valor de T se fija normalmente en un valor representativo del periodo de tiempo necesario para que el MSC 118 y el MSC 128 completen el establecimiento de la llamada. Un valor típico de T se encuentra en el orden de unos pocos segundos. Si la diferencia no es menor que el umbral T, el proceso continúa en el paso 310 proporcionando un acceso condicional al servicio 134, tal como se ha mencionado más arriba. Si la diferencia es menor que el umbral T, el proceso continúa en un paso 314, en el que la IN 124 le indica al MSC 128 que se conecte al servidor 134 en modo incondicional, esto es, un modo en donde la persona que llama tiene acceso directo al servicio. El servidor 134 asume el modo incondicional sobre la base de la información codificada por el MSC 128 en el número de servicio utilizado para dirigirse al servidor 134, por ejemplo, cuando el MSC 128 se dirige al servidor 134 con un prefijo P_2 (diferente de P_1) delante del número del servicio, o cuando el MSC 128 se dirige al servidor 134 a través del código de acceso abreviado.

Nótese que en el paso 302 no se genera nunca una primera marca de tiempo o no hay ninguna marca de tiempo reciente disponible si el usuario del dispositivo válido 104 se conecta a la red 102 desde una red de comunicación que no disponga de un canal seguro, por ejemplo, una red no basada en CAMEL. Como resultado, el proceso pasará del paso 308 al paso 310. El acceso al servicio 134 se concede en modo condicional, por ejemplo, en función de una contraseña. Si un impostor suplantador 136 se conecta a la red 102 desde una red no basada en CAMEL, el acceso al servicio es condicional. En este caso, el acceso se deniega si el impostor 136 no conoce la contraseña.

Para completar el proceso anterior, la IN 124 se amplía con un componente 138 contra suplantación de CLI que lleva a cabo las actividades que se han especificado más arriba en los pasos 302-314. El componente 138 puede ser un elemento independiente de hardware de procesamiento de datos o un elemento dedicado de software que se debe instalar en el sistema de procesamiento de datos que actúa como IN 124, o una combinación de hardware y software. Por lo general, si un operador ya dispone de un sistema de IN, la incorporación de una aplicación de IN, como por ejemplo contra la suplantación de CLI, es tan solo cuestión de instalar un componente de software.

Nótese que la decisión de conceder un acceso condicional o un acceso incondicional al servidor 134 la toma la IN 124 en el momento en que se ha establecido la conexión al MSC 128. En un modo de realización alternativo, la decisión la toma la IN 124 en el momento en que se ha establecido la conexión con el servicio. En ese caso, la IN 124 le indica al propio servidor 134 que conceda un acceso condicional o un acceso incondicional. Esto puede requerir que cada servidor individual al que se accede desde el MSC 128 disponga de su propia interfaz con la IN 124 para procesar las instrucciones pertinentes. Esta última opción introduce alguna complejidad adicional en el sistema. En el modo de realización de la invención descrito mediante referencia a las Fig. 1-3, la implementación es mucho menos engorrosa y mucho menos costosa, ya que en el número llamado únicamente se codifica la información a partir de la cual se asume uno de los modos, condicional o incondicional.

REIVINDICACIONES

1. Un método para controlar el acceso de un dispositivo (104) de comunicación móvil a un servicio (134) basado en la CLI en una red (102) de comunicación a través de una conexión desde el exterior de la red de comunicación, en donde

el método comprende:

emitir, por parte del dispositivo, un identificador único para la identificación del dispositivo por parte del servicio;

si el identificador se recibe desde el exterior de la red de comunicación y a través de un canal (125) de señalización seguro, almacenar (302) en una memoria una primera marca de tiempo que representa el primer instante de recepción del identificador;

establecer (208) la conexión y generar (306) una segunda marca de tiempo que representa un segundo instante en el que se establece la conexión con un nodo (128) en la red de comunicación;

emitir (314) una primera instrucción al nodo para establecer un acceso incondicional del dispositivo al servicio si una diferencia entre el segundo y el primer instantes de tiempo se encuentra dentro de una ventana de tiempo predeterminada; y

emitir (310) una segunda instrucción al nodo para conceder un acceso condicional del dispositivo al servicio, si la diferencia de tiempo se encuentra fuera de la ventana de tiempo predeterminada.

2. El método de la reivindicación 1, en donde el servicio comprende al menos uno entre los siguientes: un servicio de correo de voz, un servicio de help desk, y un portal de voz automático.

3. El método de la reivindicación 1 ó 2, en donde el nodo comprende un conmutador de red.

4. El método de la reivindicación 1 ó 2, en donde el nodo comprende un servidor que proporciona el servicio.

5. Un sistema de procesamiento de datos con funcionalidad de Punto de Control de Servicio y configurado para controlar el acceso de un dispositivo (104) de comunicación móvil a un servicio (134) basado en la CLI en una red (102) de comunicación a través de una conexión desde el exterior de la red de comunicación, en donde:

el dispositivo está configurado para emitir un identificador único para la identificación del dispositivo por parte del servicio; y

el sistema comprende una memoria y está configurado para ejecutar los siguientes los pasos:

si el identificador se recibe desde el exterior de la red de comunicación y a través de un canal (125) de señalización seguro, almacenar (302) en la memoria una primera marca de tiempo que representa el primer instante de recepción del identificador;

establecer (208) la conexión y generar (306) una segunda marca de tiempo que representa un segundo instante en el que se establece la conexión con un nodo (128) en la red de comunicación;

emitir (314) una primera instrucción al nodo para establecer un acceso incondicional del dispositivo al servicio si una diferencia entre el segundo y el primer instantes de tiempo se encuentra dentro de una ventana de tiempo predeterminada; y

emitir (310) una segunda instrucción al nodo para conceder un acceso condicional del dispositivo al servicio, si la diferencia de tiempo se encuentra fuera de la ventana de tiempo predeterminada.

6. Software de control en un soporte de datos para ser instalado en un Punto de Control de Servicio en una red de comunicación para controlar el acceso de un dispositivo (104) de comunicación móvil a un servicio (134) basado en la CLI en una red (102) de comunicación a través de una conexión desde el exterior de la red de comunicaciones, en donde:

el software comprende:

un primer código de control legible por ordenador para almacenar (302) en una memoria una primera marca de tiempo que representa un primer instante de recepción de un identificador recibido desde el dispositivo, en donde el identificador identifica al dispositivo, y si el identificador se ha recibido desde el exterior de la red de comunicaciones y sobre un canal (125) seguro de señalización;

un segundo código de control legible por ordenador para establecer (208) la conexión y generar (306) una segunda marca de tiempo que representa un segundo instante en el que se establece la conexión con un nodo (128) en la red de comunicación;

un tercer código de control legible por ordenador para la emisión (314) de una primera instrucción para el nodo para establecer un acceso incondicional del dispositivo al servicio, si una diferencia entre el segundo y el primer instantes de tiempo se encuentra dentro de una ventana de tiempo predeterminada; y

un cuarto código de control legible por ordenador para la emisión (310) de una segunda instrucción para el nodo para conceder un acceso condicional del dispositivo al servicio, si la diferencia de tiempo se encuentra fuera de la ventana de tiempo predeterminada.

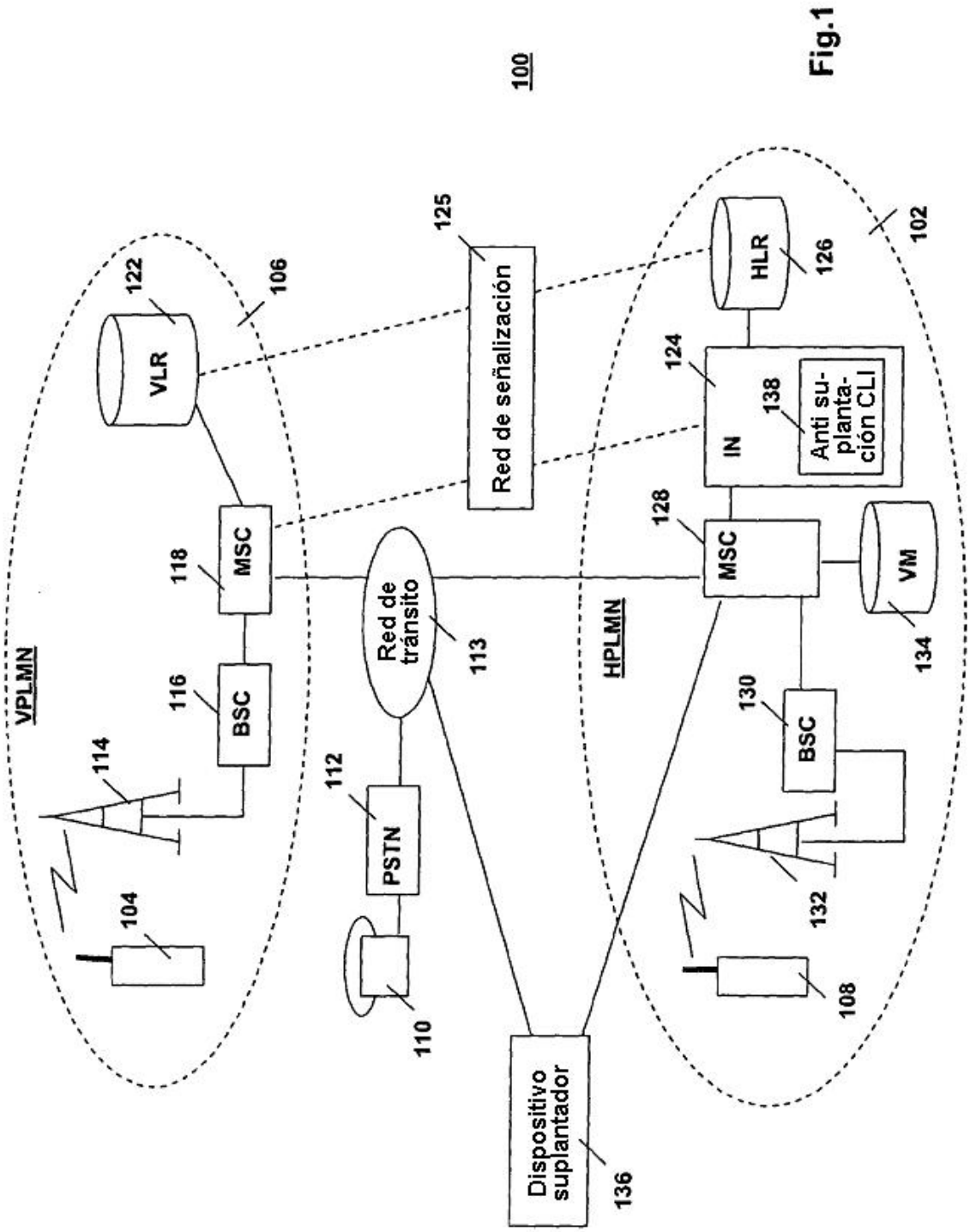
100
VPLMN
HPLMN
VLR
122
106
MSC
118
BSC
116
114
104
Red de señalización
125
Red de tránsito
113
PSTN
112
110
Dispositivo suplantador
136
HLR
126
102
IN
124
Anti suplantación CLI
138
MSC
128
VM
134
BSC
130
132
108

Fig.1

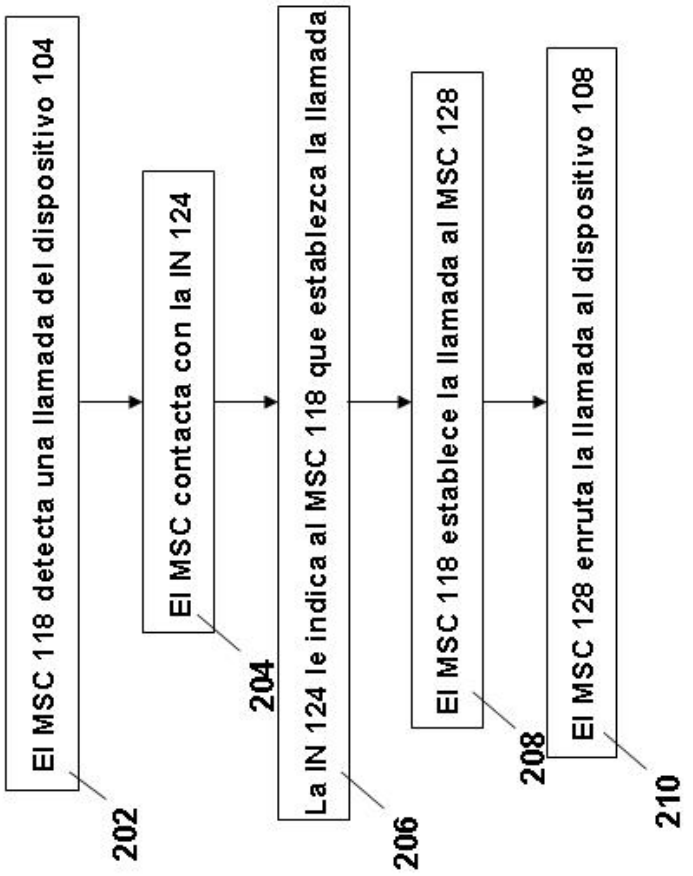
El MSC 118 detecta una llamada del dispositivo 104
202
El MSC contacta con la IN 124
204
La IN 124 le indica al MSC 118 que establezca la llamada
206
El MSC 118 establece la llamada al MSC 128
208
El MSC 128 enruta la llamada al dispositivo 108
210
200

Fig. 2

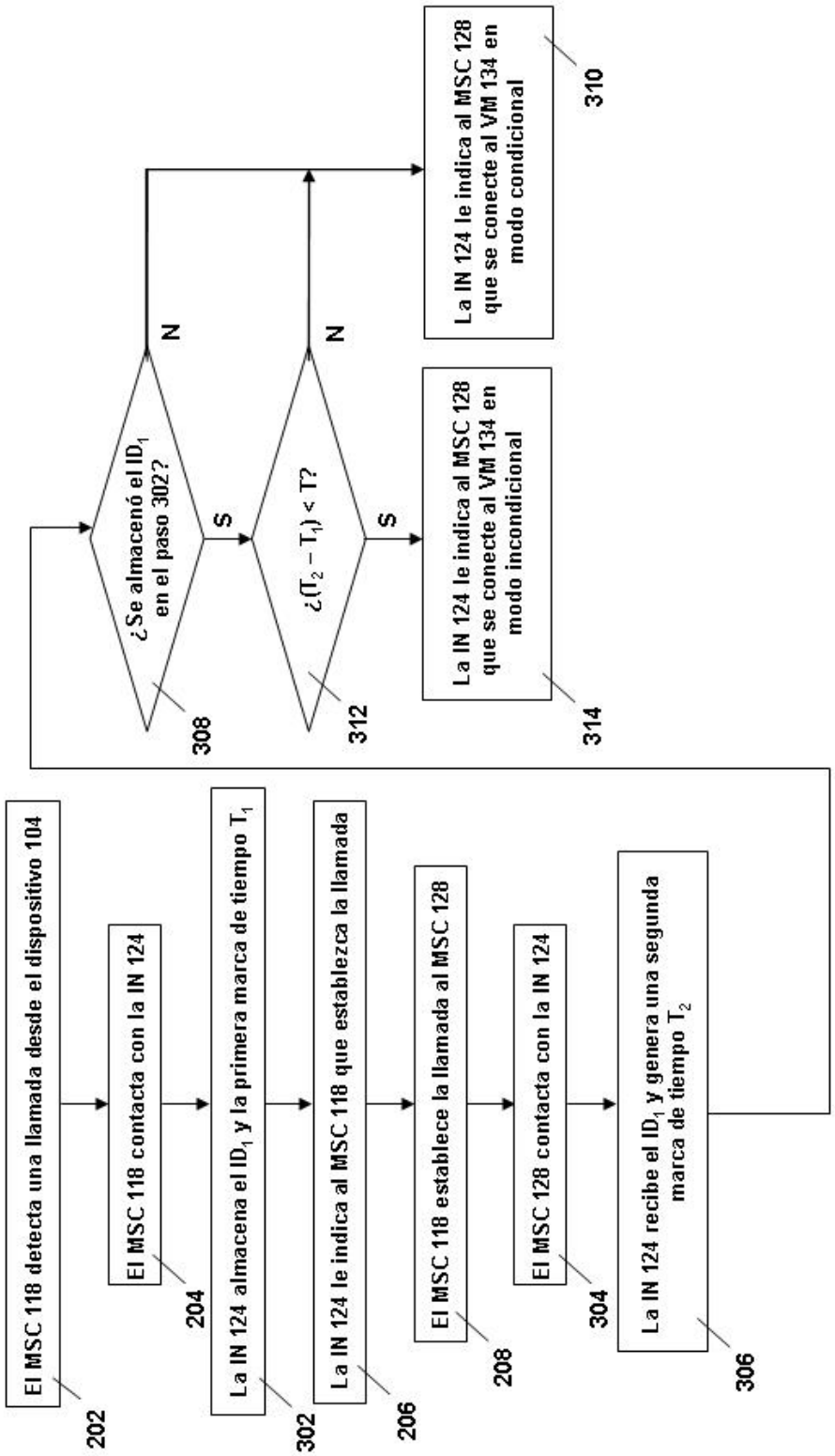
El MSC 118 detecta una llamada desde el dispositivo 104
202
El MSC 118 contacta con la IN 124
204
La IN 124 almacena el ID1 y la primera marca de tiempo T1
302
La IN 124 le indica al MSC 118 que establezca la llamada
206
El MSC 118 establece la llamada al MSC 128
208
El MSC 128 contacta con la IN 124
304
La IN 124 recibe el ID1 y genera una segunda marca de tiempo T2
306
¿Se almacenó el ID1 en el paso 302?
308
S
N
¿(T2 – T1) < T?
312
S
N
La IN 124 le indica al MSC 128 que se conecte al VM 134 en modo incondicional
314
La IN 124 le indica al MSC 128 que se conecte al VM 134 en modo condicional
310
300

Fig. 3