(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 822 552**

(51) Int. CI.:

H04W 4/70 (2008.01)
H04L 29/06 (2006.01)
H04W 12/02 (2009.01)
H04W 12/00 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **08.10.2012 PCT/EP2012/004208**

(87) Fecha y número de publicación internacional: **17.04.2014 WO14056511**

(96) Fecha de presentación y número de la solicitud europea: **08.10.2012 E 12773228 (7)**

(97) Fecha y número de publicación de la concesión europea: **15.07.2020 EP 2904820**

(54) Título: **Sistema de comunicación y un método para operar el mismo**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.05.2021

(73) Titular/es:

TELEFÓNICA GERMANY GMBH & CO. OHG (100.0%)
Georg-Brauchle-Ring 50
80992 München, DE

(72) Inventor/es:

HENRICI, DIRK

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Sistema de comunicación y un método para operar el mismo

La presente invención se refiere a un método para operar un sistema de comunicación, en particular una red de comunicación móvil, que incluye una red principal del Subsistema Multimedia de IP (IMS) que funciona en la arquitectura de sistema, en donde uno o más clientes de IMS pueden establecer una sesión de comunicación con otros clientes de IMS a través de la red principal de IMS.

El [Sub-] Sistema Multimedia de Internet (IMS) es una capa de control de sesión normalizada en la parte superior de las redes de IP que usa el Protocolo de Iniciación de Sesión (SIP) para el proceso de señalización. Hoy en día, a menudo se usa IMS para plataformas de voz de red fijas, como el servicio de VoIP sobre DSL, y también para la norma del 3GPP (Proyecto Asociación de 3ª Generación) para servicios de voz de la Evolución a Largo Plazo (LTE) nativos en redes móviles. El Conjunto de Comunicación Enriquecida mejorado (RCSe), alias servicios "Joyn" emplea el IMS también.

El IMS puede interpretarse como un habilitador técnico que proporciona funcionalidad de reutilización de características de IMS especificadas. Los servicios arbitrarios pueden implementarse en la parte superior del IMS y usar los servicios de IMS disponibles. El IMS proporciona servicios de nivel superior a aplicaciones, por ejemplo, manejo de flujos multimedia, manejo de movilidad, gestión de QoS. A partir de una perspectiva del desarrollador, el uso de una red de IMS evita la necesidad de reimplementación se servicios de comunicación básicos en la parte superior de IP para cada aplicación. Pueden tratarse diferentes flujos de comunicación de una manera diferente por la red (por ejemplo, con respecto a QoS requerida).

En la práctica, el IMS se usa en su mayoría para implementar servicios de comunicación de voz más servicios de complementarios interoperables como RCSe. Sin embargo, existen aplicaciones adicionales que pueden beneficiarse de la estructura de IMS.

Un ejemplo son las aplicaciones de M2M que usan uno o más dispositivos (tales como sensores o contadores o cámaras) para capturar un evento, que se retransmite a través de una red (inalámbrica, alámbrica o híbrida) a una aplicación que se ejecuta en un servidor de extremo trasero. En el futuro, cada vez se usarán más las redes móviles para establecer una comunicación entre los dispositivos y los servidores de extremo trasero.

Ya que los dispositivos de M2M normalmente son sistemas embebidos escasos en recursos, son muy vulnerables a ataques como denegación de servicio. Debido a su modo de operación descentralizado y posible naturaleza móvil, son difíciles de gestionar, por ejemplo, para aplicar parches de seguridad a los mismos. Por lo tanto, los dispositivos M2M no deben ser alcanzables desde la Internet pública.

El documento 3GPPTR23.888V 11.0.0 desvela mejoras de sistema para comunicaciones de tipo máquina. En el mismo, se sugiere usar una conexión de VPN para comunicaciones entre un servidor de MTC y un equipo de usuario. El documento 3GPPTR33.868 analiza un requisito de servicio para comunicaciones de tipo máquina.

Los documentos 3GPPTR33.868 V0.10.0, XP050649233; US 2010/095361 A1; y US 2012/180119 A1 representan la técnica anterior relevante adicional.

El sistema anteriormente mencionado debe construirse con respecto a su implementación y costes operativos. Cuanto más atractivo sea el precio para el servicio, más interesante será el producto para el cliente. Los costes internos para el operador/operadora deben mantenerse bajos.

Es el objeto de la presente invención proporcionar un sistema de comunicación y un método mejorado para operar el mismo que ofrece funcionalidad mejorada para una aplicación, en particular una aplicación M2M, una comunicación segura entre al menos dos pares y mantener la implementación y costes operativos tan bajos como sean posibles.

De acuerdo con la presente invención, este objeto se resuelve inicialmente mediante un método con las características de la reivindicación 1 o un sistema correspondiente al mismo con las características de la reivindicación 11. Se proporcionan aspectos ventajosos del método de acuerdo con la presente invención en las reivindicaciones dependientes.

La base para realizar el método es una red principal de IMS que funciona en la infraestructura de sistema del sistema de comunicación operado. Por ejemplo, el sistema de comunicación corresponde a la infraestructura de sistema de un proveedor de red móvil o fija.

En un aspecto preferible de la invención un servidor de abonado doméstico (HSS) puede actuar como una base de datos de abonados para autenticar los clientes de la red de comunicación como clientes de IMS. Además, puede haber

uno o más servidores de aplicación (AS) que implementa servicios adicionales. Normalmente, hay al menos un AS de telefonía que implementan servicios complementarios. Pueden existir AS adicionales que proporcionan servicios disponibles en el mercado opcionales y/o implementan servicios personalizados.

Los clientes de IMS pueden establecer una sesión de comunicación con al menos otro cliente de IMS a través de la red principal de IMS. El flujo básico para establecer una conexión es como sigue: en primer lugar, ha de negociarse una comunicación mediante un proceso de señalización que tiene lugar mediante la red principal de IMS. El HSS se ve implicado en la autenticación de abonado para asegurar que únicamente pueden conectarse clientes de IMS conocidos y/o válidos y/o permitidos a la red principal de IMS. La ruta de señalización puede dirigirse también mediante uno o más AS (por ejemplo, puede implementarse allí reenvío de llamada). La ruta de señalización se refiere al par de comunicación que tiene que realizar acuse de recibo de la solicitud de entrada para completar el proceso de señalización. Después de un proceso de señalización satisfactorio se establece una conexión de medios entre los pares.

Debido a razones de seguridad, la red principal de IMS debe operarse separada de otras redes, por ejemplo, la Internet pública o cualesquiera redes de cliente. De acuerdo con la invención, la red principal de IMS funciona en separación lógica de otras redes. La arquitectura de sistema comprende medios que proporcionan al menos una Red Privada Virtual (VPN) para un número específico de clientes de IMS.

Una ventaja de la invención es que la solución inventiva proporciona una separación lógica de las conexiones establecidas entre IMS-cliente especificadas y los abonados de red restantes. Con ello, se consigue una protección buena y eficaz contra diversos ataques. Una característica importante adicional de la solución es que todos los clientes de IMS tienen que autenticarse. No existen usuarios anónimos en la VPN. Por lo tanto, cualquier uso malicioso puede mitigarse.

Como el método inventivo está basado en IMS, puede usarse para transportar flujos de datos arbitrarios entre los clientes de IMS. Por lo tanto, puede aumentarse la flexibilidad del sistema. Además, la invención puede implementarse a coste bajo de modo que son posibles márgenes atractivos para el operador de sistema. La implementación hace uso de recursos existentes (IMS principal) que ya están presentes en muchas redes de operadoras.

En un aspecto preferido de la invención, se implementa al menos una VPN usando una VPN de Conmutación de Etiqueta Multiprotocolo (MPLS-VPN). Usando MPLS en la parte superior de una única infraestructura física, pueden establecerse varias infraestructuras lógicamente independientes.
En un escenario de dos partes, el cliente (como la primera parte) tiene una red por sí mismo que puede abarcar la infraestructura de operadora completa (como la segunda parte) que está habilitada para MPLS. El cliente obtiene una "MPLS-VPN". Desde una perspectiva de la operadora, se etiqueta el tráfico de cliente y se transporta lógicamente separado a través de la infraestructura de la operadora cerca del tráfico de los otros clientes, el tráfico de gestión de la operadora o incluso tráfico de Internet.
De acuerdo con otro aspecto de la invención, en un escenario de tres partes, las redes de dos clientes obtienen una VPN de MPLS que separa lógicamente el tráfico a través de la infraestructura de la operadora. En otro aspecto más de la invención, en un escenario de cuatro o más partes, las redes de dos o más clientes obtienen una VPN de MPLS que separa lógicamente el tráfico a través de la infraestructura de dos o más operadoras.

De acuerdo con un aspecto ventajoso de la invención puede definirse al menos una MPLS-VPN para el tráfico de señalización y puede definirse otra MPLS-VPN para el tráfico de medios.

Los clientes de IMS no residen directamente en la red principal de IMS descrita, en particular las MPLS-VPN usadas. Uno o más clientes de IMS están preferentemente ubicados en diversas redes que han de interconectarse a la red principal de IMS para establecer una comunicación basada en IMS. Por lo tanto, una o más pasarelas están integradas actuando como una entrada a la red principal de IMS.

Es preferible proporcionar una interconexión controlada entre las redes separadas y la red principal de IMS. En un aspecto particular de la invención, uno o más denominados Controladores de Frontera de Sesión (SBC) actúan como una pasarela para una o más otras redes separadas. Un SBC puede considerarse como una clase de "cortafuegos de IMS".

De acuerdo con un aspecto adicional de la invención, al menos una red separada es una red de acceso, en particular una red de acceso móvil basada en al menos una de las siguientes normas GSM, GPRS, UMTS o LTE. La red de acceso puede también estar basada en una red de acceso de WLAN o una red de acceso de línea alámbrica tal como DSL, ISDN o POTS.

En particular, una red móvil puede establecerse de tal manera que el tráfico para un Nombre de Punto de Acceso (APN) específico alcance exclusivamente el SBC anteriormente mencionado. Un cliente de IMS móvil ubicado en la red móvil usa dicho APN para conectarse virtualmente mediante el SBC directamente con el IMS principal. En

consecuencia, el tráfico de datos de dicho cliente de IMS móvil está completamente separado de cualquier otra red como la Internet.

Preferiblemente, al menos un cliente de IMS puede ser un dispositivo móvil que comprende un transceptor de radio de GSM y/o UMTS y/o LTE.

Adicionalmente o como alternativa, al menos una red separada es una VPN de cliente arbitraria, tal como una intranet de compañía. La VPN de cliente puede también estar basada en una MPLS-VPN. Por ejemplo, unas MPLS-VPN pueden establecerse de tal manera que el SBC puede alcanzarse en la VPN del cliente. De esta manera, un cliente de IMS ubicado en la VPN de cliente puede comunicarse con el IMS principal de una manera controlada. Como una opción adicional, un cortafuegos de cliente puede colocarse en la ruta de tráfico entre el SBC y el nodo de acceso de la VPN de cliente para asegurar la frontera administrativa del cliente.

También es posible interconectar la red principal de IMS mediante un SBC a la red pública (Internet) como una red separada. Esto significa que un cliente de IMS en la Internet puede usar servicios de IMS accediendo a la red de IMS mientras se usa el SBC como una pasarela. Puede ser útil tener cuidado especial en la aseguración de la red de IMS contra ataques de la Internet, por ejemplo, contra ataques de denegación de servicio.

Al menos un cliente de IMS puede ser un servidor de extremo trasero que está ubicado en una red separada, en particular en una VPN de cliente arbitrario, tal como una intranet de la compañía. El al menos un servidor de extremo trasero puede también estar ubicado en la Internet pública. El al menos un servidor de extremo trasero podría conectarse usando una MPLS-VPN o - a un coste inferior, pero de menos seguridad - mediante la Internet. En el último caso, un cortafuegos de cliente debería restringir la comunicación de IMS en la capa de IP para estar permitido únicamente entre el respectivo SBC de la red principal de IMS y el servidor de extremo trasero.

Debido a la separación lógica del tráfico, cualquier comunicación descontrolada entre al menos dos clientes de IMS debe prohibirse, incluso cuando las comunicaciones descontroladas se dirigen mediante al menos un SBC. Es útil permitir únicamente sesiones de comunicación esperadas entre al menos dos clientes de IMS. De acuerdo con otro aspecto ventajoso de la invención, el tráfico de datos entre al menos dos clientes de IMS está únicamente permitido si la conexión se ha negociado antes mediante un proceso de señalización. Por ejemplo, la conexión se negocia mediante el Protocolo de Iniciación de Sesión (SIP) de antemano. El SBC puede escuchar los procesos de señalización y obtener conocimiento acerca de conexiones de datos posteriores. Únicamente deben permitirse estas conexiones.

Por lo tanto, de acuerdo con otro aspecto preferido de la invención, los flujos de medios que se negociaron mediante SIP pueden establecerse directamente entre los clientes de IMS de comunicación cuando pueden alcanzarse entre sí. Si todos los datos relacionados con comunicaciones de IMS, es decir tráfico de señalización y de medios, se dirigen mediante SBC, se asegura que los flujos de tráfico de paso están bajo el control de al menos un SBC, evitando de esta manera la capacidad de alcance directa en la capa de IP entre clientes de IMS

En un aspecto ventajoso de la presente invención, se proporciona al menos una VPN que restringe sesiones de comunicación entre clientes de IMS específicos basándose en una funcionalidad de lista negra y/o lista blanca. Una lista blanca puede contener información acerca de clientes de IMS de destino o de origen que están aprobados explícitamente para conectarse a un cliente de IMS respectivo. La lista puede tener cualquier granularidad según sea necesario. Adicionalmente o como alternativa, puede usarse una lista negra que aprobará todos los clientes de IMS excepto los listados.

Al menos una lista negra y/o una blanca están especializadas a cada cliente de IMS. Cada lista define un número de clientes de IMS de destino que pueden alcanzarse mediante el respectivo cliente y/o un número de clientes de origen que pueden alcanzar el respectivo cliente. Preferentemente, las listas están separadas en al menos una lista de origen por cliente de IMS y al menos una lista de destino por cliente de IMS.

Cuando un cliente de IMS intenta establecer una sesión con otro cliente de IMS, se comprueban las respectivas listas de ambos clientes si el intento de conexión solicitado es permisible o debería rechazarse.

Pueden realizarse agrupaciones de dispositivos/abonados como en las MPLS-VPN mediante las listas blancas y/o negras descritas. Por ejemplo, en una MPLS-VPN de malla completa conocida, todos los clientes en esa VPN pueden comunicarse con todos los demás clientes en esa VPN. De acuerdo con la invención, se realiza lo mismo en la red principal de IMS usando la funcionalidad de generación de listas blancas descrita. Preferentemente, se proporciona una lista blanca que pone en lista blanca a todos los clientes de IMS en una "IMS-VPN" deseada en la lista blanca de destino y en la lista blanca de origen. De esta manera, no es posible establecimiento de sesión a o desde clientes de IMS fuera de la "IMS-VPN".

Cualesquiera otras topologías de VPN como una estrella pueden realizarse con el concepto de lista blanca descrita también. Ya que es posible una definición de nivel de abonado, diferentes "IMS-VPN" pueden solaparse entre sí.

Cada cliente de IMS puede tener cuatro listas blancas y/o negras. Dos de ellas (listas blancas de origen) controlan cuáles otros clientes pueden alcanzar al respectivo cliente de IMS, las otras dos (listas blancas de destino) controlan cuáles otros clientes pueden ser alcanzados por el cliente de IMS. Puede ser útil tener una lista blanca determinada del operador que no puede cambiarse por el mismo cliente y una lista blanca determinada del usuario que puede modificar el cliente. Son concebibles diversas maneras para realizar esa modificación.

Las listas blancas determinadas del operador pueden usarse para que el operador de red de IMS imponga restricciones dependiendo de la tarifa que haya elegido el usuario para una suscripción. Por ejemplo, podría haber una lista blanca que únicamente permita que pueda alcanzarse un cierto cliente o una que permita que pueda alcanzarse únicamente un cierto grupo de clientes (por ejemplo, clientes que pertenecen a la misma cuenta de cliente). De manera similar en la otra dirección, podría haber una lista blanca en la que el operador define que el respectivo cliente únicamente puede alcanzarse por un cierto otro cliente o un cierto grupo de otros clientes (por ejemplo, clientes que pertenecen a la misma cuenta de cliente).

Además, el cliente puede tener listas blancas definidas por el usuario similares para la respectiva suscripción de IMS. Estas pueden adaptarse por el cliente. La generación de listas blancas de un cliente tiene que hacerse tanto en listas blancas determinadas por el operador como determinadas por el usuario para comprobar intentos de comunicación con respecto a su admisión. Si un abonado está únicamente en lista blanca en una de las dos listas blancas, se rechazan los intentos de comunicación.

Al menos una lista blanca y/o lista negra determinadas por el usuario puede modificarse por el operador del sistema de comunicación, probablemente bajo demanda del cliente.

De acuerdo con un aspecto ventajoso de la invención, la lista determinada por el usuario puede configurarse por un auto-servicio del cliente. El usuario puede controlar las listas blancas determinadas por el usuario y también incluir una lista de clientes determinados por el usuario especificados en las listas blancas determinadas por el usuario. Un auto-servicio de cliente puede proporcionarse preferentemente mediante una API, tal como el entorno SOAP y RESTful, y/o mediante un extremo frontal de web y/o mediante correos electrónicos especialmente formateados.

La modificación de las listas blandas puede ser gratuita o facturarse por el operador.

La gestión del sistema de comunicación y/o la administración de la al menos una lista blanca y/o negra pueden simplificarse usando referencias en al menos una lista blanca. Puede ser útil administrar una lista blanca y/o negra central que se referencian por al menos una lista blanca y/o negra especializadas a un cliente de IMS. Son concebibles referencias únicas o múltiples.

Como en el escenario de ejemplo de una VPN de malla completa todos los clientes de IMS tienen la misma lista blanca, tiene sentido tener listas de clientes que pueden incluirse en otras listas blancas. Cada cliente comprende una lista blanca que hace referencia/incluye una lista de clientes común. Cuando se modifica la lista de clientes comunes, esto afectaría a la VPN total de modo que se proporciona la posibilidad de una gestión central. El operador de la red de IMS puede proporcionar también listas de clientes determinadas por el operador (por ejemplo, con todos los clientes de una cuenta de cliente) que pueden estar incluidos en listas blancas determinadas por el usuario por el cliente.

De acuerdo con la invención, el objeto anteriormente mencionado se resuelve también mediante un sistema de comunicación que comprende medios para realizar el método inventivo como se ha especificado anteriormente. De manera evidente, el sistema ofrece las mismas características y beneficios que el método anteriormente mencionado.

La invención también se refiere a una aplicación inventiva del sistema inventivo anteriormente mencionado. De acuerdo con la invención, el sistema de comunicación inventivo sirve para una aplicación de Máquina a Máquina (M2M). Al menos dos dispositivos de cliente pueden comunicarse a través del sistema de comunicación para implementar una aplicación de M2M.

Se explicarán detalles y ventajas adicionales de la invención en detalle con referencia a una realización ilustrada en un dibujo. La misma figura muestra una vista general de la arquitectura de sistema de acuerdo con la invención.

El sistema de comunicación mostrado se subdivide en la red principal de IMS 10, la red móvil 20 y la Internet pública 30. Debería observarse que la presente invención hace referencia principalmente a la red principal de IMS que está funcionando en la arquitectura de sistema de unos proveedores de red. La red principal de IMS proporciona medios para conectar de manera segura dispositivos de M2M 60 ubicados en la red móvil 20 a un servidor de extremo trasero 700 ubicado en la Internet pública.

Los dispositivos móviles del cliente 60 son de un diseño de sistema embebido que incluye un transceptor de radio de GSM/UMTS/LTE y una tarjeta de SIM. Se usa una biblioteca de software adicional para proporcionar funcionalidad de cliente de IMS dentro del software operativo de los dispositivos 60. Puede proporcionarse también funcionalidad de

nivel superior (por ejemplo, envío de flujo continuo de medios para cámaras web) etc., si fuera necesario, posibilitando por lo tanto el desarrollo rápido de aplicaciones complejas. Los dispositivos 60 pueden comunicarse con otros dispositivos 60 así como los servidores de extremo trasero 700 usando la red principal de IMS.

Dentro de la red móvil 20 el tráfico de datos puede separarse usando Nombres de Punto de Acceso (APN) 100 separados definidos como puntos de extremo lógicos en el Nodo de Soporte de GPRS de pasarela (GGSN) o pasarela de PDN (P-GW). Cada APN 100 puede tratarse de manera diferente, por ejemplo, con respecto a QoS (calidad de servicio) o al punto de extremo asociado para entregar datos. Por ejemplo, un primer APN puede estar configurado para tráfico de Internet habitual en donde un segundo APN específico sirve para otros fines especificados.

Los dispositivos móviles 60 se conectan al APN especificado 101 que encamina el tráfico de los dispositivos móviles 60 al SBC 40. De esta manera, los dispositivos móviles que usan este APN 101 virtualmente se conectan mediante el SBC 40 directamente con el IMS principal 10. El tráfico se separa completamente de otras redes como la Internet 30.

Se muestra otro cliente de IMS mediante el servidor de extremo trasero 700 que está interconectado a través de la Internet pública 30 a la red principal de IMS 10. Una interconexión controlada entre el IMS 10 y la Internet pública se consigue mediante un segundo SBC 500 que actúa como una pasarela. Un cortafuegos de cliente 80 y/o lista de accesos están dispuestos entre el SBC 500 y el servidor de extremo trasero 700. El cortafuegos 80 está configurado para limitar las comunicaciones al servidor 700 a conexiones de datos de IMS que se establecen entre el servidor 700 y el SBC de la operadora 500.

Los clientes 60, 700 pueden únicamente conectarse a la red principal de IMS 10 si se autentican a sí mismos como clientes de IMS. Por lo tanto, se incluye un HSS 90 (servidor de abonado doméstico) en la red principal de IMS 10 que actúa como una entidad de autenticación. Además, puede haber servidores de aplicación (AS) que implementan servicios adicionales.

Para establecer una conexión entre al menos uno de los dispositivos 60 y el servidor de extremo trasero 700 ha de iniciarse un proceso de señalización. La ruta de señalización 300 tiene lugar mediante el IMS principal que implica el HSS para autenticación de los clientes de IMS 60, 700. La señalización puede dirigirse mediante uno o más AS 90 (por ejemplo, puede implementarse allí reenvío de llamada). Al final, la señalización alcanza el cliente de comunicación de destino 700 que realiza acuse de recibo de la solicitud de entrada. A continuación, se establece la conexión de medios 200 que se negoció usando la ruta de señalización 300 entre los pares 60, 700.

En la configuración de un operador descrito se requiere que ambos clientes de IMS pertenezcan a la misma VPN definida en la red principal de IMS 20. Por lo tanto, el HSS o el AS 90 almacena y administra un total de cuatro listas blancas para cada cliente de IMS 60, 700. Dos listas blancas por cliente de IMS 60, 700, una lista de origen determinada por el usuario y una determinada por el operador, controlan cuáles otros clientes de IMS 60, 700 pueden alcanzar el cliente de IMS especificado. Por ejemplo, puede definirse que el dispositivo 60 puede ser alcanzado exclusivamente por el servidor de extremo trasero 700. Las otras dos listas, también una lista de destino determinada por el usuario y una determinada por el operador, controlan cuáles otros clientes pueden alcanzar el respectivo cliente. Por ejemplo, puede definirse que el dispositivo 60 puede alcanzar exclusivamente el servidor de extremo trasero 700.

Cuando el cliente de IMS 60 intenta establecer una sesión con el cliente 700 han de compararse las dos listas blancas de origen del cliente 60 que iniciaron la sesión y las dos listas blancas de terminación del cliente de destino 700. En detalle, todas las listas han de comprobarse si es admisible la conexión planeada. La comparación también se inicia durante el proceso de señalización.

Las listas blancas determinadas del operador pueden usarse para que el operador de red de IMS imponga restricciones dependiendo de la tarifa que haya elegido el usuario para una suscripción. Por ejemplo, podría haber una lista blanca que únicamente permita que pueda alcanzarse un cierto cliente o una que permita que pueda alcanzarse únicamente un cierto grupo de clientes (por ejemplo, clientes que pertenecen a la misma cuenta de cliente). De manera similar en la otra dirección, podría haber una lista blanca en la que el operador define que el respectivo cliente únicamente puede alcanzarse por un cierto otro cliente o un cierto grupo de otros clientes (por ejemplo, clientes que pertenecen a la misma cuenta de cliente).

Una comunicación de ejemplo típica que también hace uso del sistema de comunicación de IMS mostrado podría ser una aplicación de cámara de vigilancia como un dispositivo móvil 60. Las cámaras de vigilancia deberán comunicarse con un servidor de extremo trasero 700 como un servicio de análisis central para las imágenes. Los dispositivos embebidos 60 con las cámaras pueden conectarse a continuación de manera segura a los servidores de extremo trasero 700 usando el enfoque propuesto. La comunicación está limitada a las rutas entre los dispositivos de cámara 60 y los servidores de extremo trasero 700 restringiendo comunicaciones de IP para permitir únicamente conexiones a los SBC 40, 500 y proporcionando listas blancas apropiadas en la capa de IMS. Los dispositivos embebidos 60 no pueden alcanzarse por pares no autorizados, ni en la capa de IMS ni en la capa de IP. El dispositivo por lo tanto se asegura contra ataques del exterior.

El sistema de comunicación puede servir también para establecer canales de comunicación seguros para respectivas aplicaciones. Hay multitud de aplicaciones que necesitan canales de comunicación seguros, por ejemplo, banca en línea, comunicación con el elemento seguro en NFC, y muchas más aplicaciones. En ese caso, podrían usarse sesiones de IMS para transferencia de datos. Esto proporciona una separación lógica de otras redes, especialmente la Internet abierta 30. El enfoque de lista blanca propuesto limita la comunicación a clientes en lista blanca. En este escenario, los dispositivos de comunicación 60 pertenecen en varios dominios administrativos, por ejemplo, dispositivos móviles del usuario 60 (portátil, tableta, teléfono inteligente) y, por otra parte, un servidor de extremo trasero 700, por ejemplo, uno para banca en línea. Para la cuenta de IMS del servidor de extremo trasero 700, el banco limitaría la comunicación de IMS para que esté permitida por dispositivos de usuario registrados 60 únicamente (es decir, la suscripción de IMS del servidor de extremo trasero tendría una lista blanca de "destino determinado por el usuario" que contiene todos los dispositivos de cliente registrados únicamente).

El sistema de comunicación también se posibilita que proporcione un túnel de datos en una red de cliente (por ejemplo, dispositivo móvil como portátil o PC de tableta a la intranet de cliente). En este escenario, la generación de listas blancas restringiría la comunicación a que estuviera permitida entre los dispositivos registrados del usuario 60 y el punto de extremo del túnel 700 en la red de la compañía. Una sesión de IMS se usaría para establecer un túnel seguro entre el dispositivo del usuario 60 y el punto de extremo del túnel de la compañía 700 a través de la cual pueden intercambiarse datos arbitrarios. En los puntos de extremo, pueden crearse dispositivos de red virtuales (por ejemplo, interfaces tun/tap en Linux). De esta manera, la solución actúa como una VPN (capa 2 o capa 3) como creadas por otras soluciones de VPN. El túnel puede encriptarse opcionalmente, por ejemplo, usando SSL/TLS (por ejemplo, usando stunnel).

Una ventaja principal de una solución basada en IMS de este tipo para la creación de una VPN que puede transportar tráfico de IP arbitrario es que puede hacerse uso de las características de movilidad del IMS. Puede haber muchas soluciones que proporcionan la posibilidad de un traspaso sin interrupciones si cambia la red de acceso. De esta manera, las sesiones de IMS (y en este caso la conexión de VPN) pueden persistir mientras el usuario es móvil y/o está conectado mediante diferentes redes (fijas, cable, WiFi, GSM/UMTS/LTE).

Similar a la creación de un túnel para fines de VPN como se ha indicado anteriormente, puede usarse un túnel para ayudar en proyectos de introducción de IPv6. Mediante un túnel que se realiza a través de una sesión de IMS, un dispositivo 60 que únicamente tiene conectividad de IPv4 por sí mismo puede conectarse a una red de IPv6.

La invención puede usarse también para proporcionar la capacidad para comunicaciones de P2P que está restringida a un grupo de usuarios particular por las listas blancas. El IMS proporciona una capa de indirección, de modo que la comunicación se vuelve independiente de las redes de acceso subyacentes (dirección de IP, sin limitaciones por conectividad de extremo a extremo restringida).

El sistema de comunicación inventivo puede implementarse a bajo coste de modo que son posibles márgenes atractivos. La razón es que hace uso de recursos existentes (IMS principal) que ya están presentes en muchas redes de operadora. El aprovisionamiento es mucho más sencillo que para otras soluciones como MPLS-Enlace puesto que todo del aprovisionamiento puede hacerse al nivel de abonado de IMS y no requiere configuración por abonado en nivel de IP.

Los dispositivos no necesitan hacer uso intensivo de protocolos criptográficos intensivos en recursos. Únicamente puede alcanzarse a los abonados de IMS en lista blanca en nivel de IP mediante los SBC de modo que los dispositivos no necesiten hacer frente a solicitudes indeseadas.

La invención proporciona separación de red lógica y con ello buena protección contra diversos ataques. Para proporcionar confidencialidad, puede implementarse una capa adicional de encriptación en la parte superior si fuera necesaria, por ejemplo, usando SSL/TLS. Una característica importante de la solución es que todos los clientes se autentican. No hay usuarios anónimos; cualquier uso malicioso puede mitigarse por lo tanto fácilmente.

Ya que la solución está basada en IMS, puede usarse para transportar flujos de datos arbitrarios entre los clientes. Por lo tanto, es muy flexible. Si la implementación de IMS proporciona traspaso sin interrupciones, los flujos pueden incluso sobrevivir a cambios en redes de acceso, por ejemplo, debido a movilidad del usuario. No hay restricciones de capa de red en la capacidad de alcance de extremo a extremo, por ejemplo, como introducidos por NAT. Por lo tanto, no hay restricción no deseada que el par establezca una sesión.

Los servicios de IMS no están limitados a una única operadora. Las interconexiones basadas en IMS están planificadas, por ejemplo, para realizar RCS. Esto permite que se use el concepto mediante múltiples portadoras / operadores de red de IMS. Esto proporciona más posibilidades que MPLS-VPN ya que estas normalmente están limitadas a una única operadora.

REIVINDICACIONES

1. Un método para operar un sistema de comunicación que comprende una red de comunicación móvil, que incluye una red principal de subsistema multimedia de IP IMS (10) que funciona en la arquitectura de sistema, en donde uno o más clientes de IMS (60, 700) pueden establecer una sesión de comunicación con otros clientes de IMS (60, 700) a través de la red principal de IMS (10), en donde al menos un cliente de IMS (60) es un dispositivo de M2M y reside en una red de acceso móvil (10, 30) que está interconectada con la red de IMS (10) mediante al menos un controlador de frontera de sesión (SBC) (40, 500), en donde se proporciona al menos una red privada virtual VPN para un número específico de clientes de IMS (60, 700) que se comunican a través de la red principal de IMS (10) para asegurar una separación de red lógica de la red principal de IMS (10), en donde la red de acceso móvil está configurada de manera que el tráfico para un nombre de punto de acceso APN específico exclusivamente alcanza dicho controlador de frontera de sesión SBC y dicho al menos un dispositivo de M2M de IMS (60) ubicado en la red de acceso móvil está configurado para usar dicho nombre de punto de acceso específico para conectar directamente mediante dicho controlador de frontera de sesión a la red principal de IMS, y en donde se proporciona la al menos una VPN en el IMS (10) que restringe al menos una sesión de comunicación entre clientes de IMS específicos (60, 700) mediante una lista negra y/o una lista blanca especializada a cada cliente de IMS y que definen clientes de IMS de destino (60, 700) aprobados para ser alcanzados mediante el cliente de IMS especializado (60, 700) y/o que definen clientes de IMS de origen (60, 700) aprobados para alcanzar el cliente de IMS especializado (60, 700).

2. El método de acuerdo con la reivindicación 1, **caracterizado por que** al menos una VPN se implementa mediante una MPLS-VPN.

3. El método de acuerdo con cualquiera de las reivindicaciones anteriores **caracterizado por que** se proporciona al menos una VPN, en particular MPLS-VPN, para tráfico de señalización y/o tráfico de medios en la red principal de IMS (10).

4. El método de acuerdo con cualquiera de las reivindicaciones anteriores **caracterizado por que** el tráfico de medios de una conexión entre al menos dos clientes de IMS (60, 700) puede restringirse o prohibirse si dicha conexión no se ha señalizado de antemano, por ejemplo, negociado mediante SIP.

5. El método de acuerdo con cualquiera de las reivindicaciones 1 a 4 **caracterizado por que** la red principal de IMS (10) está configurada de manera que todo el tráfico de datos de IMS, es decir tráfico de señalización y de medios, pasa a al menos un SBC (40, 500).

6. El método de acuerdo con cualquiera de las reivindicaciones anteriores **caracterizado por que** al menos un cliente de IMS (700) reside en una red separada que es una VPN de cliente, en particular una red de MPLS-VPN de cliente, y/o una Internet de red pública (30).

7. El método de acuerdo con cualquiera de las reivindicaciones anteriores **caracterizado por que** al menos un cliente de IMS (60, 700) es un dispositivo móvil y/o un servidor de extremo trasero en donde el al menos un dispositivo móvil (60) comprende un transceptor de radio de GSM y/o UMTS y/o LTE.

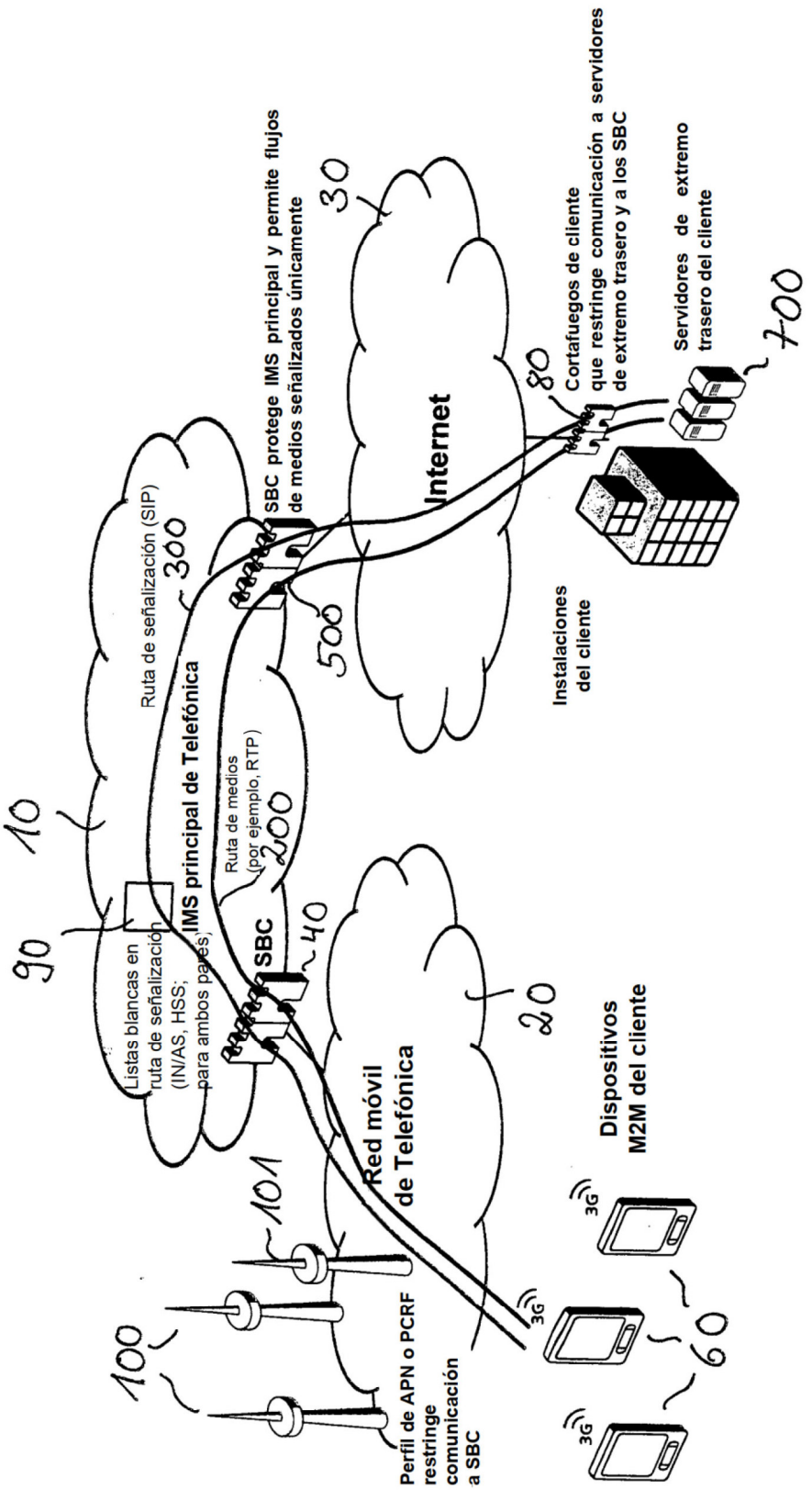
8. El método de acuerdo con cualquiera de las reivindicaciones anteriores **caracterizado por que** el sistema proporciona al menos una lista blanca y/o negra determinada por el operador configurable por el operador de red y/o al menos una lista blanca y/o negra determinada por el usuario configurable por el cliente de IMS especializado (60, 700).

9. El método de acuerdo con la reivindicación 8 **caracterizado por que** la lista blanca y/o negra determinada por el usuario es configurable por un auto-servicio de cliente, por ejemplo mediante API, en particular SOAP y/o RESTful, y/o mediante extremo frontal de web y/o mediante correos electrónicos especialmente formateados.

10. El método de acuerdo con cualquiera de las reivindicaciones anteriores **caracterizado por que** al menos una lista blanca y/o negra contiene una referencia a al menos otra lista, en particular una lista blanca y/o negra gestionada central.

11. Un sistema de comunicación que comprende medios para realizar el método de acuerdo con cualquiera de las reivindicaciones anteriores.

12. El sistema de comunicación de acuerdo con la reivindicación 11 usado para una aplicación de máquina a máquina M2M.


10
90
Listas blancas en ruta de señalización (IN/AS, HSS; para ambos países)
Ruta de señalización (SIP)
300
IMS principal de Telefónica
Ruta de medios (por ejemplo, RTP)
200
SBC
40
SBC protege IMS principal y permite flujos de medios señalizados únicamente
500
30
Internet
80
Cortafuegos de cliente que restringe comunicación a servidores de extremo trasero y a los SBC
Servidores de extremo trasero del cliente
700
Instalaciones del cliente
20
Red móvil de Telefónica
101
100
Perfil de APN o PCRF restringe comunicación a SBC
3G
3G
3G
Dispositivos M2M del cliente
60