(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 583 727**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **11.02.2010 E 10845478 (6)**

(97) Fecha y número de publicación de la concesión europea: **20.04.2016 EP 2487856**

(54) Título: **Método, equipo y sistema de operación para una clave de transmisión de flujos de medios**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.09.2016

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building, Bantian, Longgang District
Shenzhen, Guangdong 518129, CN

(72) Inventor/es:

YANG, WEIWEI

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método, equipo y sistema de operación para una clave de transmisión de flujos de medios

Campo de la invención

[0001] La presente invención está relacionada con el campo de las tecnologías de las comunicaciones y, en particular, con un método, un equipo y un sistema de operación para una clave de transmisión de flujos de medios.

Antecedentes de la invención

[0002] En una arquitectura en la que la portadora y el control están separados se suele activar habitualmente un protocolo de control de pasarela, por ejemplo, el H.248, como protocolo de control entre una entidad de control de la capa de servicio y una entidad de ejecución del plano de medios. En este mecanismo, la entidad de ejecución del plano de medios incluye una pasarela de medios (Media Gateway, MG), y la entidad de control de la capa de servicio incluye un controlador de pasarela de medios (Media Gateway Controller, MGC).

[0003] Con la creciente utilización de servicios IP adquiere cada vez más importancia el aspecto de la seguridad en la transmisión de datos en una red. Desde la perspectiva del protocolo se puede considerar que la seguridad del servicio IP tiene fundamentalmente dos aspectos: uno es la seguridad en el plano de control y el otro es la seguridad en el plano de medios.

[0004] El protocolo de transporte para aplicaciones de tiempo real (Real-Time Transport Protocol, RTP), formulado por el Grupo de Trabajo de Ingeniería de Internet (Internet Engineering Task Force, IETF), es un protocolo diseñado para la transmisión de flujos de datos multimedia. El RTP es responsable de la transmisión de datos multimedia, en tanto que el protocolo de control de transporte en tiempo real (RTP Control Protocol, RTCP) proporciona funciones tales como la monitorización de la calidad de servicio, el control de congestión y la sincronización de medios. El RTP proporciona un cierto grado de confidencialidad, y puede cifrar la carga útil del RTP. Sin embargo, es fácil descifrar el algoritmo por defecto del RTP. El IETF amplía el protocolo RTP, y propone el Protocolo de Transporte Seguro en Tiempo Real (Secure Real-time Transport Protocol, SRTP). Generalmente, la información de la clave del SRTP que se utiliza en una sesión se negocia a través del Protocolo de Inicio de Sesión (Session Initiation Protocol, SIP), y la información de la clave se transmite mediante una interacción entre la entidad de control de la capa de servicio y la entidad de ejecución del plano de medios. De este modo se implementa la función de seguridad del plano de medios.

[0005] La técnica anterior presenta el siguiente inconveniente: en el escenario de red actual, aunque en las capas de servicio y de portadora se soporta la recepción y utilización de una clave de transmisión de flujos de medios, no es posible realizar una operación sobre el estado del tiempo de vida de la clave de transmisión de los flujos de medios.

[0006] El documento XP017452321, titulado "H.248.SRTP a Proposed initial draft for a new H.248 work item: SRTP Package and Procedures; C338 (H.248.SRTP una Propuesta de borrador inicial para un nuevo elemento operativo H.248: Encapsulado y Procedimientos del SRTP; C338)", ha divulgado que "el evento Master Key About to Expire (mke) (Clave Maestra Próxima a Expirar) permite que el MGC sea notificado cuando una clave maestra esté a punto de caducar (o ya lo haya hecho). Los parámetros del evento RTP Watermark (Marca de agua) (rtpw) y RTCP Watermark (rtcpw) le permiten al MGC controlar cuánto tiempo antes de que caduque la clave se notifica el evento mke. La MG generará el evento cuando la clave maestra haya sido utilizada para (tiempo de vida - rtpw) paquetes RTP o (tiempo de vida - rtcpw) paquetes RTCP (cualquiera que sea lo primero en suceder). Por ejemplo, si el tiempo de vida es 2^{20}, y tanto rtpw como rtcpw son iguales a 2^{16}, el evento será notificado después de que (2^{20} - 2^{16} = 983040) paquetes RTP o RTCP hayan sido protegidos mediante dicha clave".

[0007] El documento XP015009491, titulado "The Secure Real-time Transport Protocol (Protocolo de Transporte Seguro en Tiempo Real" describe "el Protocolo de Transporte Seguro en Tiempo Real (SRTP), un perfil del Protocolo de Transporte de Tiempo Real (RTP) que puede proporcionar confidencialidad, autenticación de mensajes y protección de la repetición para el tráfico RTP y para el tráfico de control para el RTP, el Protocolo de Control de Transporte en Tiempo Real (RTCP)".

Resumen de la invención

[0008] Los modos de realización de la presente invención proporcionan un método, un equipo y un sistema de operación de acuerdo con las reivindicaciones independientes 1, 5 y 7 para una clave de transmisión de flujos de medios, con el fin de resolver un problema consistente en que en la técnica anterior no es posible realizar una operación sobre el estado del tiempo de vida de una clave de transmisión de flujos de medios.

[0009] Un modo de realización de la presente invención proporciona un método de operación para una clave de transmisión de flujos de medios, que incluye:

detectar, por parte de una pasarela de medios, información de estado del tiempo de vida de una clave de transmisión de flujos de medios de acuerdo con un evento de expiración de clave recibido, en donde el evento de

expiración de clave es notificado a la pasarela de medios por un controlador de pasarela de medios; y

cuando la pasarela de medios determina que ha expirado el tiempo de vida de la clave de transmisión de flujos de medios, activar, por parte de la pasarela de medios, un modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con una instrucción del controlador de pasarela de medios.

[0010] Un modo de realización de la presente invención proporciona, además, un módulo de recepción, una pasarela de medios, que incluye un módulo de detección, un módulo de comprobación y un módulo de operación, en donde

el módulo (14) de recepción está configurado para recibir un evento de expiración de clave notificado por un controlador de pasarela de medios;

el módulo de detección está configurado para detectar la información de estado del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con el evento de expiración de clave notificado por el controlador de pasarela de medios y recibido el módulo de recepción;

el módulo de comprobación está configurado para comprobar si el tiempo de vida de la clave de transmisión de flujos de medios ha expirado; y

el módulo de operación está configurado para activar un modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con una instrucción del controlador de pasarela de medios, cuando el módulo de comprobación haya determinado que el tiempo de vida de la clave de transmisión de flujos de medios ha expirado.

[0011] Un modo de realización de la presente invención proporciona, además, un sistema de operación para una clave de transmisión de flujos de medios, que incluye un controlador de pasarela de medios y una pasarela de medios, en donde

el controlador de pasarela de medios está configurado para enviarle un evento de expiración de clave a la pasarela de medios; y

la pasarela de medios está configurada para recibir el evento de expiración de clave notificado por el controlador de pasarela de medios; detectar la información de estado del tiempo de vida de una clave de transmisión de flujos de medios de acuerdo con el evento de expiración de clave recibido notificado por el controlador de pasarela de medios; comprobar si el tiempo de vida de la clave de transmisión de flujos de medios ha expirado; y cuando se haya determinado que el tiempo de vida de la clave de transmisión de flujos de medios ha expirado, activar un modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con una instrucción del controlador de pasarela de medios.

[0012] En los modos de realización de la presente invención, cuando la pasarela de medios determina que el tiempo de vida de la clave de transmisión de flujos de medios ha expirado, la pasarela de medios activa el modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con la instrucción del controlador de pasarela de medios. Los modos de realización cubren un déficit técnico al realizar una operación sobre el estado del tiempo de vida de una clave de transmisión de flujos de medios en una arquitectura en la que una MG y un MGC se encuentran separados.

Breve descripción de los dibujos

[0013] Con el fin de describir con más claridad las soluciones técnicas de los modos de realización de la presente invención o de la técnica anterior, a continuación se introducen brevemente los dibujos adjuntos necesarios para describir los modos de realización o la técnica anterior. Evidentemente, los dibujos que se adjuntan a la siguiente descripción son sólo algunos modos de realización de la presente invención, y las personas con un conocimiento normal de la técnica también pueden derivar otros dibujos sin esfuerzos creativos a partir de estos dibujos adjuntos.

[0014] La FIG. 1 es un diagrama de flujo de un método de operación para una clave de transmisión de flujos de medios de acuerdo con un modo de realización de la presente invención;

[0015] la FIG. 2 es un diagrama de flujo de un método de operación para una clave de transmisión de flujos de medios de acuerdo con otro modo de realización de la presente invención;

[0016] la FIG. 3 es un diagrama de flujo de un método de operación para una clave de transmisión de flujos de medios de acuerdo con otro modo de realización de la presente invención;

[0017] la FIG. 4 es un diagrama de flujo de un método de operación para una clave de transmisión de flujos de medios de acuerdo con otro modo de realización de la presente invención;

[0018] la FIG. 5 es un diagrama de flujo de señalización de un método de acuerdo con un modo de realización de la presente invención;

[0019] la FIG. 6 es un diagrama esquemático de la estructura de una pasarela de medios de acuerdo con un modo de realización de la presente invención;

[0020] la FIG. 7 es un diagrama esquemático de la estructura de una pasarela de medios de acuerdo con otro modo de realización de la presente invención;

[0021] la FIG. 8 es un diagrama esquemático de la estructura de un controlador de pasarela de medios de acuerdo con un modo de realización de la presente invención; y

[0022] la FIG. 9 es un diagrama esquemático de la estructura de un sistema de operación para una clave de transmisión de flujos de medios de acuerdo con un modo de realización de la presente invención.

Descripción detallada de los modos de realización

[0023] A continuación se describen de forma clara y completa las soluciones técnicas de los modos de realización de la presente invención haciendo referencia a los dibujos que se adjuntan en los modos de realización de la presente invención. Evidentemente, los modos de realización que se van a describir son sólo una parte en lugar de todos los modos de realización de la presente invención. Sobre la base de los modos de realización de la presente invención, cualesquiera otros modos de realización obtenidos por personas con un conocimiento normal de la técnica sin esfuerzos creativos se considerarán dentro del alcance de protección de la presente invención.

[0024] Con el fin de adaptarse a diferentes escenarios de aplicación y mejorar la protección de una red contra diferentes riesgos potenciales de seguridad, a menudo se utilizan y aplican claves diferentes en segmentos de tiempo y campos diferentes. En consecuencia, en la red existe un gran número de claves de transmisión de flujos de medios diferentes. Cada una de las claves de transmisión corresponde a un tiempo de vida diferente, y un tiempo de vida determina el momento de generación de una nueva clave.

[0025] La FIG. 1 es un diagrama de flujo de un método de operación para una clave de transmisión de flujos de medios de acuerdo con un modo de realización de la presente invención. Tal como se muestra en la FIG. 1, el método de este modo de realización incluye:

[0026] Paso 101: Una pasarela de medios detecta información de estado del tiempo de vida de una clave de transmisión de flujos de medios.

[0027] Por ejemplo, una MG puede detectar información de estado del tiempo de vida de una clave de transmisión de flujos de medios de acuerdo con un evento de expiración de clave recibido. El evento de expiración de clave es notificado por un controlador de pasarela de medios a la pasarela de medios, y por supuesto, también se puede haber establecido previamente en la pasarela de medios.

[0028] En un proceso concreto de implementación, en este modo de realización, un evento se puede ampliar en un paquete de características basadas en el protocolo H.248 existente o en un paquete de características ampliado. Por ejemplo, el evento se puede designar como evento "expiración de clave (Key Expiry)", que se abrevia como "ke". Cuando la MG recibe un evento de expiración de clave notificado por un MGC, la MG se puede preparar para recibir información de estado del tiempo de vida de una clave de transmisión de flujos de medios.

[0029] Paso 102: Cuando la pasarela de medios determina que el tiempo de vida de la clave de transmisión de flujos de medios ha expirado, la pasarela de medios activa un modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con una instrucción del controlador de pasarela de medios.

[0030] Por ejemplo, la pasarela de medios detecta una información de estado del tiempo de vida de la clave de transmisión de flujos de medios, y realiza una comprobación sobre la información de estado del tiempo de vida detectada de la clave de transmisión de flujos de medios; cuando la pasarela de medios determina que el tiempo de vida de la clave de transmisión de flujos de medios ha expirado, la pasarela de medios puede activar el modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con la instrucción del controlador de pasarela de medios.

[0031] Por ejemplo, un criterio para determinar si el tiempo de vida de la clave de transmisión de flujos de medios ha expirado puede ser: si el número de paquetes que se han transmitido utilizando la misma clave de transmisión de flujos de medios alcanza el valor máximo establecido para la clave de transmisión de flujos de medios y hasta ese instante todavía no se ha actualizado la clave de transmisión de flujos de medios, se puede determinar que el tiempo de vida de la clave de transmisión de flujos de medios ha expirado.

[0032] Cuando el tiempo de vida de la clave de transmisión de flujos de medios ha expirado, con el fin de que el MGC le ordene a la MG que active el modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios, en este modo de realización se puede ampliar un parámetro del evento "expiración de clave". Por ejemplo, el parámetro se puede designar como "modo de operación de expiración del tiempo de vida de la clave (Key Lifetime Expiry Behaviour)", que se abrevia como "kleb", con el fin de ordenar a la MG que active el modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios correspondiente. Cuando

se recibe un parámetro de un modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios notificado por el MGC, la MG puede activar el modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios correspondiente cuando la clave de transmisión de flujos de medios ha expirado.

[0033] Por ejemplo, para el parámetro "modo de operación de expiración del tiempo de vida de la clave" se puede definir un tipo de parámetro como un tipo de enumeración (Enumeration), y los posibles valores del parámetro incluyen, al menos uno de los siguientes:

un modo de operación autónomo de la pasarela de medios, esto es, una acción determinada por la pasarela de medios (MG determined action); en este caso, la pasarela de medios no necesita solicitar más indicaciones por parte del controlador de pasarela de medios, y puede determinar un modo de procesamiento de forma independiente. Para el parámetro se puede definir, por ejemplo, el valor 0×0001; o

la pasarela de medios termina un flujo de medios y envía un mensaje de terminación de flujo de medios (por ejemplo, el mensaje BYE del RTCP). Para el parámetro se puede definir, por ejemplo, el valor 0×0002; o

la pasarela de medios le notifica un evento de expiración de clave al controlador de pasarela de medios, y no envía un mensaje de terminación de flujo de medios (por ejemplo, el mensaje BYE del RTCP). Para el parámetro se puede definir, por ejemplo, el valor 0×0003; o

la pasarela de medios le notifica un evento de expiración de clave al controlador de pasarela de medios, termina un flujo de medios y envía un mensaje de terminación de flujo de medios (por ejemplo, el mensaje BYE del RTCP). Para el parámetro se puede definir, por ejemplo, el valor 0×0004.

[0034] En este modo de realización, un objeto al que la pasarela de medios le envía el mensaje de terminación de flujo de medios es otra entidad de red en una capa de portadora, por ejemplo, puede ser un equipo de usuario (User Equipment, UE). La pasarela de medios puede enviarle un mensaje BYE del RTCP a una entidad de red en una capa de portadora en un extremo homólogo, con el fin de terminar un flujo de medios sobre un plano de portadora.

[0035] En este modo de realización, la pasarela de medios le notifica un evento de expiración de clave al controlador de pasarela de medios. Esto es, cuando la MG se lo notifica al MGC a través de un mensaje del protocolo de control de pasarela, el mensaje incluye un evento de expiración de clave. Con el fin de que la MG pueda notificárselo al MGC oportunamente antes de que expire el tiempo de vida de la clave de transmisión de flujos de medios, en un evento de expiración de clave notificado se puede incluir también un parámetro de instrucción de expiración de clave, en donde mediante diferentes valores del parámetro de instrucción se indica si todavía se está utilizando la clave de transmisión de flujos de medios actual. Por ejemplo, el parámetro de instrucción se puede definir como un tipo booleano (Boolean). Un valor "On (Activado)" indica que el número de paquetes de flujos de medios a los que se ha aplicado la clave de transmisión de flujos de medios actual ha alcanzado el valor máximo del tiempo de vida de la clave. Esto es, el tiempo de vida de la clave de transmisión de flujos de medios actual ha expirado. Un valor "Off (Desactivado)" indica que el número de paquetes de flujos de medios a los que se ha aplicado la clave de transmisión de flujos de medios actual no ha alcanzado el valor máximo del tiempo de vida de la clave.

[0036] En este modo de realización, cuando el evento de expiración de clave es notificado por el MGC a la MG, en el evento de expiración de clave se puede incluir el parámetro "modo de operación de expiración del tiempo de vida de la clave" para enviárselo conjuntamente a la MG; y, por supuesto, el parámetro "modo de operación de expiración del tiempo de vida de la clave" también se puede enviar por separado. Cuando el evento de expiración de clave ha sido establecido previamente en la pasarela de medios, el MGC le envía el parámetro "modo de operación de expiración del tiempo de vida de la clave" a la MG por separado.

[0037] En este modo de realización, cuando la pasarela de medios determina que el tiempo de vida de la clave de transmisión de flujos de medios ha expirado, la pasarela de medios puede activar el modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con la instrucción del controlador de pasarela de medios. Este modo de realización cubre un déficit técnico al realizar una operación sobre el estado del tiempo de vida de una clave de transmisión de flujos de medios en una arquitectura en la que la MG y el MGC se encuentran separados. Adicionalmente, mediante la detección del estado del tiempo de vida de la clave de transmisión de flujos de medios se puede implementar la transmisión segura de un flujo de medios.

[0038] Cuando se transmite un flujo de medios, normalmente se utilizan una o más claves de transmisión diferentes, por ejemplo, se pueden incluir una clave maestra (Master Key) y una clave de sesión (Session Key). En este caso se puede mejorar el mecanismo anterior con el fin de implementar operaciones de expiración del tiempo de vida de granularidades diferentes.

[0039] En un método de operación para una clave de transmisión de flujos de medios de acuerdo con otro modo de realización de la presente invención, un evento de expiración de clave "(Key Expiry)" puede ser específico. Por ejemplo, con el fin de implementar la detección de una clave maestra se puede definir un evento específico "expiración de clave maestra (Master Key Expiry)", que se abrevia como "mke". Este modo de realización puede incluir los siguientes pasos.

[0040] 201: Cuando una pasarela de medios recibe un evento de expiración de clave maestra "mke" notificado por un controlador de pasarela de medios, la pasarela de medios se puede disponer para detectar información de estado del tiempo de vida de una clave maestra de transmisión del flujo de medios.

[0041] 202: Cuando la pasarela de medios determina que el tiempo de vida de una clave de transmisión de flujos de medios ha expirado, la pasarela de medios activa un modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con una instrucción del controlador de pasarela de medios.

[0042] En relación con un criterio específico de comprobación, se puede hacer referencia a la descripción del primer modo de realización.

[0043] En relación con un método específico en el que un MGC le ordena a una MG que active el modo de operación de expiración del tiempo de vida de una clave de transmisión de flujos de medios correspondiente, se puede hacer referencia a la descripción del primer modo de realización.

[0044] En un método de operación para una clave de transmisión de flujos de medios de acuerdo con otro modo de realización de la presente invención, las claves de transmisión de flujos de medios se pueden clasificar con el fin de implementar modos de operación de expiración del tiempo de vida para los diferentes tipos de claves de transmisión de flujos de medios. Por ejemplo, en el evento "expiración de clave" se puede definir un parámetro "tipo de clave (Key Type)", y se abrevia como "kt", en donde el valor del parámetro puede incluir una clave maestra y una clave de sesión, con el fin de implementar la detección de los estados del tiempo de vida para los diferentes tipos de claves de transmisión de flujos de medios. Este modo de realización puede incluir los siguientes pasos.

[0045] 301: Cuando una pasarela de medios recibe un evento de expiración de clave que incluye un parámetro de tipo de clave "kt", en donde el evento de expiración de clave ha sido notificado por un controlador de pasarela de medios, la pasarela de medios se puede disponer para detectar información de estado del tiempo de vida de un tipo concreto de clave de transmisión de flujos de medios.

[0046] 302: Cuando la pasarela de medios determina que el tiempo de vida del tipo de clave de transmisión de flujos de medios especificado ha expirado, la pasarela de medios activa un modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con una instrucción del controlador de pasarela de medios.

[0047] En relación con un criterio específico de comprobación, se puede hacer referencia a la descripción del primer modo de realización.

[0048] En relación con un método específico en el que un MGC le ordena a una MG que active un modo de operación de expiración del tiempo de vida de una clave de transmisión de flujos de medios correspondiente, se puede hacer referencia a la descripción del primer modo de realización

[0049] En un método de operación para una clave de transmisión de flujos de medios de acuerdo con otro modo de realización de la presente invención, se puede identificar una clave de transmisión de flujos de medios para implementar un modo de operación de expiración de clave para una clave de transmisión de flujos de medios concreta. Por ejemplo, en el evento "expiración de clave" se puede definir un parámetro "identificador de clave (Key Identifier)", y se abrevia como "ki", en donde el valor del parámetro puede ser una clave concreta. Este modo de realización puede incluir los siguientes pasos.

[0050] 401: Cuando una pasarela de medios recibe un evento de expiración de clave que incluye un parámetro identificador de clave "ki", en donde el evento de expiración de clave notificado por un controlador de pasarela de medios, la pasarela de medios se puede disponer para detectar información de estado del tiempo de vida de una clave de transmisión de flujos de medios con un identificador especificado.

[0051] 402: Cuando la pasarela de medios determina que el tiempo de vida de la clave de transmisión de flujos de medios con el identificador especificado ha expirado, la pasarela de medios activa un modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con una instrucción del controlador de pasarela de medios.

[0052] En relación con un criterio específico de comprobación, se puede hacer referencia a la descripción del primer modo de realización.

[0053] En relación con un método específico en el que un MGC le ordena a una MG que active el modo de operación de expiración del tiempo de vida de una clave de transmisión de flujos de medios correspondiente, se puede hacer referencia a la descripción del primer modo de realización.

[0054] En los métodos de operación para una clave de transmisión de flujos de medios de acuerdo con los modos de realización anteriores de la presente invención, se puede especificar el evento de expiración de clave "(Key Expiry)", las claves de transmisión de flujos de medios se pueden clasificar, o a una clave de transmisión de flujos de medios se le puede asignar un identificador. Cuando la pasarela de medios determina que ha expirado el tiempo de vida de

una clave de transmisión de flujos de medios específica, el tiempo de vida de una clave de transmisión de flujos de medios especificada o el tiempo de vida de una clave de transmisión de flujos de medios con un identificador especificado, la pasarela de medios activa un modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con la instrucción del controlador de pasarela de medios. Los modos de realización anteriores de la presente invención cubren un déficit técnico al realizar una operación sobre el estado del tiempo de vida de una clave de transmisión de flujos de medios en una arquitectura en la que una MG y un MGC se encuentran separados. Adicionalmente, mediante la detección del estado del tiempo de vida de la clave de transmisión de flujos de medios se puede implementar la transmisión segura de un flujo de medios.

[0055] La FIG. 5 es un diagrama de flujo de señalización de un método de acuerdo con un modo de realización de la presente invención. Tal como se muestra en la FIG. 5, el método de este modo de realización incluye:

[0056] Paso 501: Un MGC negocia con una MG la información de la clave que se adoptará en la transmisión de flujos de medios. Aquí, la información de la clave puede ser negociada y determinada por la capa de servicio a la que pertenece el MGC, y también puede ser generada por el MGC de acuerdo con una política local y, a continuación, ser indicada a la MG.

[0057] Paso 502: La MG inicia la recepción y el envío de un flujo de medios protegido con clave de acuerdo con una instrucción del MGC, que incluye cifrar un flujo de medios que se va a enviar y descifrar un flujo de medios recibido.

[0058] Paso 503: Tomando un terminal de usuario a modo de ejemplo, la MG y el terminal de usuario inician la transmisión segura de un flujo de medios.

[0059] Paso 504: El MGC le envía a la MG una petición de evento de detección de información de estado del tiempo de vida de la clave de transmisión de flujos de medios, en donde se incluye un evento "expiración de clave (ke)", y el evento "expiración de clave (ke)" contiene un parámetro "modo de operación de expiración del tiempo de vida de la clave (kleb)". En este ejemplo, el valor del parámetro "modo de operación de expiración del tiempo de vida de la clave (kleb)" es "0×0004". Esto es, cuando el tiempo de vida de una clave de transmisión de flujos de medios ha expirado, la pasarela de medios le notifica un evento de expiración de clave al controlador de pasarela de medios, termina el flujo de medios y envía un mensaje de terminación del flujo de medios (por ejemplo, el mensaje BYE del RTCP).

[0060] Paso 505: la MG le envía un mensaje de respuesta al MGC.

[0061] Paso 506: La MG detecta la información de estado del tiempo de vida de una clave de transmisión del flujo de medios correspondiente, y realiza una comprobación sobre la información de estado detectada del tiempo de vida de la clave de transmisión de flujos de medios.

[0062] Paso 507: Cuando se determina que el tiempo de vida de la clave de transmisión de flujos de medios ha expirado, la MG activa un modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con una instrucción del MGC, lo que incluye específicamente que la MG le notifica al MGC un evento de expiración de clave.

[0063] Paso 508: El MGC le envía un mensaje de respuesta a la MG.

[0064] Paso 509: La MG activa el modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con la instrucción del MGC, lo que incluye específicamente que la MG le envía un mensaje BYE del RTCP al terminal de usuario y termina el flujo de medios.

[0065] Este modo de realización cubre un déficit técnico al realizar una operación sobre un estado del tiempo de vida de una clave de transmisión de flujos de medios en una arquitectura en la que una MG y un MGC se encuentran separados. Adicionalmente, mediante la detección del estado del tiempo de vida de la clave de transmisión de flujos de medios se puede implementar la transmisión segura de un flujo de medios.

[0066] Lo anterior toma a modo de ejemplo una clave de transmisión de flujos de medios. Cuando se trata de múltiples claves de transmisión diferentes, un evento de expiración de clave "(Key Expiry)" puede ser específico. Por ejemplo, con el fin de detectar una clave maestra se puede definir un evento "expiración de clave maestra mke". Alternativamente, se pueden clasificar las claves de transmisión de flujos de medios con el fin de implementar modos de operación de expiración del tiempo de vida para diferentes claves de transmisión de flujos de medios. Por ejemplo, en un evento "expiración de clave (ke)" se puede definir un parámetro "tipo de clave kt". Alternativamente, se le puede asignar un identificador a una clave de transmisión de flujos de medios con el fin de implementar un modo de operación de expiración del tiempo de vida de una clave de transmisión de flujos de medios específica. Por ejemplo, en el evento "expiración de clave (ke)" se puede definir un parámetro "identificador de clave ki", en donde el valor de un parámetro puede ser una clave específica. Los diagramas de flujo de señalización específicos de los modos de realización anteriores no se describen de forma detallada en la presente solicitud.

[0067] Un modo de realización de la presente invención proporciona, además, un diagrama esquemático de la estructura de un equipo de operación para una clave de transmisión de flujos de medios, el cual se describe

tomando a modo de ejemplo una pasarela de medios.

[0068] La FIG. 6 es un diagrama esquemático de la estructura de una pasarela de medios de acuerdo con un modo de realización de la presente invención. Tal como se muestra en la FIG. 6, En este modo de realización, la pasarela de medios incluye: un módulo 11 de detección, un módulo 12 de comprobación, y un módulo 13 de operación, en donde el módulo 11 de detección está configurado para detectar información de estado del tiempo de vida de una clave de transmisión de flujos de medios; el módulo 12 de comprobación está configurado para comprobar si la información de estado del tiempo de vida de la clave de transmisión de flujos de medios indica que éste ha expirado; y el módulo 13 de operación está configurado para activar un modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con una instrucción de un controlador de pasarela de medios, cuando el módulo 12 de comprobación determine que el tiempo de vida de una clave de transmisión de flujos de medios ha expirado.

[0069] En este modo de realización, la pasarela de medios se corresponde con el método de operación para la clave de transmisión de flujos de medios en el modo de realización que se muestra en la FIG. 1, y en la presente solicitud no se describe en detalle un principio de implementación específico.

[0070] La FIG. 7 es un diagrama esquemático de la estructura de una pasarela de medios de acuerdo con otro modo de realización de la presente invención. Tal como se muestra en la FIG. 7, en este modo de realización la pasarela de medios incluye: un módulo 11 de detección, un módulo 12 de comprobación, y un módulo 13 de operación, e incluye, además: un módulo 14 de recepción, en donde el módulo 14 de recepción está configurado para recibir un evento de expiración de clave notificado por un controlador de pasarela de medios; el módulo 11 de detección está configurado para detectar información de estado del tiempo de vida de una clave de transmisión de flujos de medios de acuerdo con el evento de expiración de clave notificado por el controlador de pasarela de medios y recibido por el módulo 14 de recepción; el módulo 12 de comprobación está configurado para comprobar si la información de estado del tiempo de vida de la clave de transmisión de flujos de medios ha expira do; y el módulo 13 de operación está configurado para activar un modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con una instrucción del controlador de pasarela de medios, cuando el módulo 12 de comprobación determina que el tiempo de vida de la clave de transmisión de flujos de medios ha expirado.

[0071] Opcionalmente, el módulo 14 de recepción está configurado para recibir un evento "expiración de clave maestra mke" notificado por el controlador de pasarela de medios; el módulo 11 de detección está configurado para detectar información de estado del tiempo de vida de una clave maestra de transmisión de flujos de medios de acuerdo con el evento de expiración de clave maestra notificado por el controlador de pasarela de medios y recibido por el módulo 14 de recepción; el módulo 12 de comprobación está configurado para comprobar si la información de estado del tiempo de vida de la clave maestra de transmisión de flujos de medios indica que éste ha expirado; y el módulo 13 de operación está configurado para activar un modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con una instrucción del controlador de pasarela de medios cuando el módulo 12 de comprobación determina que el tiempo de vida de la clave maestra de transmisión de flujos de medios ha expirado.

[0072] En este modo de realización, la pasarela de medios se corresponde con el método de operación para la clave de transmisión de flujos de medios del modo de realización que se muestra en la FIG. 2, y en la presente solicitud no se describe en detalle un principio de implementación específico.

[0073] Opcionalmente, el módulo 14 de recepción está configurado, además, para recibir un parámetro del evento de expiración de clave que incluye un parámetro de tipo de clave "kt", en donde el evento de expiración de clave es notificado por el controlador de pasarela de medios; el módulo 11 de detección está configurado para detectar información de estado del tiempo de vida del tipo especificado de clave de transmisión de flujos de medios de acuerdo con el evento de expiración de clave notificado por el controlador de pasarela de medios y recibido por el módulo 14 de recepción; el módulo 12 de comprobación está configurado para comprobar si la información de estado del tiempo de vida del tipo especificado de clave de transmisión de flujos de medios indica que éste ha expirado; y el módulo 13 de operación está configurado para activar un modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con una instrucción del controlador de pasarela de medios cuando el módulo 12 de comprobación determina que el tiempo de vida del tipo especificado de clave de transmisión de flujos de medios ha expirado.

[0074] En este modo de realización, la pasarela de medios se corresponde con el método de operación para la clave de transmisión de flujos de medios del modo de realización que se muestra en la FIG. 3, y en la presente solicitud no se describe en detalle un principio de implementación específico.

[0075] Opcionalmente, el módulo 14 de recepción está configurado, además, para recibir un evento de expiración de clave que incluye un parámetro identificador de clave "ki", en donde el evento de expiración de clave es notificado por el controlador de pasarela de medios; el módulo 11 de detección está configurado para detectar información de estado del tiempo de vida de una clave de transmisión de flujos de medios con un identificador especificado, de acuerdo con el evento de expiración de clave notificado por el controlador de pasarela de medios y recibido por el módulo 14 de recepción; el módulo 12 de comprobación está configurado para comprobar si la información de

estado del tiempo de vida de la clave de transmisión de flujos de medios con el identificador especificado indica que éste ha expirado; y el módulo 13 de operación está configurado para activar un modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con una instrucción del controlador de pasarela de medios, cuando el módulo 12 de comprobación determina que el tiempo de vida de la clave de transmisión de flujos de medios con el identificador especificado ha expirado.

[0076] En este modo de realización, la pasarela de medios se corresponde con el método de operación para la clave de transmisión de flujos de medios en el modo de realización que se muestra en la FIG. 4, y en la presente solicitud no se describe en detalle un principio de implementación específico.

[0077] Opcionalmente, el módulo 14 de recepción está configurado, además, para recibir un evento de expiración de clave que incluye un parámetro "modo de operación de expiración del tiempo de vida de la clave (Key Lifetime Expiry Behaviour)", en donde el evento de expiración de clave es notificado por el controlador de pasarela de medios; el módulo 13 de operación está configurado para activar un modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con una instrucción del parámetro "modo de operación de expiración del tiempo de vida de la clave (Key Lifetime Expiry Behaviour)" notificado por el controlador de pasarela de medios, cuando el módulo 12 de comprobación determina que el tiempo de vida de la clave de transmisión de flujos de medios ha expirado

[0078] Concretamente, para el parámetro "modo de operación de expiración del tiempo de vida de la clave" se puede definir un tipo de parámetro como un tipo de enumeración (Enumeration), y los posibles valores del parámetro incluyen al menos uno de los siguientes:

un modo de operación autónomo de la pasarela de medios, esto es, una acción determinada por la pasarela de medios (MG determined action); en este caso, la pasarela de medios no necesita solicitar más indicaciones por parte del controlador de pasarela de medios, y puede determinar un modo de procesamiento de forma independiente. Para el parámetro se puede definir, por ejemplo, el valor 0×0001; o

la pasarela de medios termina un flujo de medios y envía un mensaje de terminación de flujo de medios (por ejemplo, el mensaje BYE del RTCP). Para el parámetro se puede definir, por ejemplo, el valor 0×0002; o

la pasarela de medios le notifica un evento de expiración de clave al controlador de pasarela de medios, y no envía un mensaje de terminación de flujo de medios (por ejemplo, el mensaje BYE del RTCP). Para el parámetro se puede definir, por ejemplo, el valor 0×0003; o

la pasarela de medios le notifica un evento de expiración de clave al controlador de pasarela de medios, termina un flujo de medios y envía un mensaje de terminación de flujo de medios (por ejemplo, el mensaje BYE del RTCP). Para el parámetro se puede definir, por ejemplo, el valor 0×0004.

[0079] En los modos de realización anteriores de la pasarela de medios, cuando el módulo de comprobación determina que el tiempo de vida de la clave de transmisión de flujos de medios ha expirado, el módulo de operación puede activar el modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con la instrucción del controlador de pasarela de medios. Este modo de realización cubre un déficit técnico al realizar una operación sobre el estado del tiempo de vida de una clave de transmisión de flujos de medios en una arquitectura en la que la MG y el MGC se encuentran separados. Adicionalmente, mediante la detección del estado del tiempo de vida de la clave de transmisión de flujos de medios se puede implementar la transmisión segura de un flujo de medios.

[0080] La FIG. 8 es un diagrama esquemático de la estructura de un controlador de pasarela de medios de acuerdo con un modo de realización de la presente invención. Tal como se muestra en la FIG. 8, en este modo de realización el controlador de pasarela de medios incluye: un módulo 21 de envío, en donde el módulo 21 de envío está configurado para notificarle un evento de expiración de clave a una pasarela de medios, con el fin de que la pasarela de medios detecte la información de estado del tiempo de vida de una clave de transmisión de flujos de medios de acuerdo con el evento de expiración de clave.

[0081] Opcionalmente, el módulo 21 de envío está configurado para notificarle a la pasarela de medios un evento "expiración de clave maestra mke".

[0082] Opcionalmente, el módulo 21 de envío está configurado para notificarle a la pasarela de medios un evento de expiración de clave que incluye un parámetro de tipo de clave "kt".

[0083] Opcionalmente, el módulo 21 de envío está configurado para notificarle a la pasarela de medios un evento de expiración de clave que incluye un parámetro identificador de clave "ki".

[0084] Opcionalmente, el módulo 21 de envío está configurado para notificarle a la pasarela de medios un evento de expiración de clave que incluye un parámetro "modo de operación de expiración del tiempo de vida de la clave (Key Lifetime Expiry Behaviour)". Cuando el parámetro "modo de operación de expiración del tiempo de vida de la clave (Key Lifetime Expiry Behaviour)" incluye un evento de expiración de clave notificado por la pasarela de medios al

controlador de pasarela de medios, el controlador de pasarela de medios incluye, además, un módulo 22 de recepción, configurado para recibir el evento de expiración de clave notificado por la pasarela de medios.

[0085] En este modo de realización, el controlador de pasarela de medios se corresponde con los modos de realización del método de operación de la clave de transmisión de flujos de medios, y en la presente solicitud no se describe en detalle un principio de implementación específico.

[0086] La FIG. 9 es un diagrama esquemático de la estructura de un sistema de operación para una clave de transmisión de flujos de medios. Tal como se muestra en la FIG. 9, en este modo de realización el sistema de operación para una clave de transmisión de flujos de medios incluye: un controlador 2 de pasarela de medios y una pasarela 1 de medios, en donde el controlador 2 de pasarela de medios está configurado para notificarle un evento de expiración de clave a la pasarela 1 de medios; y la pasarela 1 de medios está configurada para recibir el evento de expiración de clave notificado por el controlador 2 de pasarela de medios, detectar la información de estado del tiempo de vida de una clave de transmisión de flujos de medios de acuerdo con el evento de expiración de clave recibido notificado por el controlador de pasarela de medios, comprobar si la información de estado del tiempo de vida de la clave de transmisión de flujos de medios indica que éste ha expirado, y activar un modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con una instrucción del controlador de pasarela de medios cuando se determina que el tiempo de vida de la clave de transmisión de flujos de medios ha expirado.

[0087] El modo de realización del sistema anterior se corresponde con los modos de realización del método de operación de la clave de transmisión de flujos de medios, y en la presente solicitud no se describe en detalle un principio de implementación específico.

[0088] El modo de realización del sistema anterior cubre un déficit técnico al realizar una operación sobre el estado del tiempo de vida de una clave de transmisión de flujos de medios en una arquitectura en la que la MG y el MGC se encuentran separados. Adicionalmente, mediante la detección del estado del tiempo de vida de la clave de transmisión de flujos de medios se puede implementar la transmisión segura de un flujo de medios.

[0089] Por último, se debe observar que los modos de realización anteriores se utilizan únicamente para describir las soluciones técnicas de la presente invención, y no pretenden limitar la presente invención. Las personas con un conocimiento normal de la técnica deben entender que, aunque la presente invención se ha descrito en detalle haciendo referencia a algunos ejemplos de modos de realización, es posible realizar modificaciones o sustituciones equivalentes a las soluciones técnicas de la presente invención; sin embargo, dichas modificaciones o sustituciones equivalentes no pueden hacer que las soluciones técnicas modificadas se aparten del alcance de las soluciones técnicas de la presente invención.

REIVINDICACIONES

1. Un método de operación para una clave de transmisión de flujos de medios, que comprende:

detectar (101), por parte de una pasarela de medios, información de estado del tiempo de vida de una clave de transmisión de flujos de medios de acuerdo con un evento de expiración de clave recibido, en donde el evento de expiración de clave es notificado por un controlador de pasarela de medios a la pasarela de medios; y

cuando la pasarela de medios determina que el tiempo de vida de la clave de transmisión de flujos de medios ha expirado, activar (102), por parte de la pasarela de medios, un modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con una instrucción del controlador de pasarela de medios.

2. El método de acuerdo con la reivindicación 1, en el que el evento de expiración de clave comprende un parámetro de tipo de clave, y la pasarela de medios detecta información de estado del tiempo de vida de un tipo especificado de la clave de transmisión de flujos de medios de acuerdo con el evento de expiración de clave que comprende el parámetro de tipo de clave, en donde el evento de expiración de clave es notificado por el controlador de pasarela de medios; cuando la pasarela de medios determina que el tiempo de vida del tipo especificado de clave de transmisión de flujos de medios ha expirado, la pasarela de medios activa un modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con la instrucción del controlador de pasarela de medios; o

el evento de expiración de clave comprende un parámetro identificador de clave, y la pasarela de medios detecta la información de estado del tiempo de vida de una clave de transmisión de flujos de medios con un identificador especificado, de acuerdo con el evento de expiración de clave que comprende el parámetro identificador de clave, en donde el evento de expiración de clave es notificado por el controlador de pasarela de medios; cuando la pasarela de medios determina que el tiempo de vida de la clave de transmisión de flujos de medios con el identificador especificado ha expirado, la pasarela de medios activa un modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con la instrucción del controlador de pasarela de medios.

3. El método de acuerdo con la reivindicación 1, en el que una condición para determinar que el tiempo de vida de la clave de transmisión de flujos de medios ha expirado es que el número de paquetes que se transmiten utilizando la clave de transmisión de flujos de medios alcance al número máximo establecido para la clave de transmisión de flujos de medios.

4. El método de acuerdo con una cualquiera de las reivindicaciones 1 a 3, en el que la instrucción del controlador de pasarela de medios comprende al menos una de las siguientes acciones:

ordenarle a la pasarela de medios que determine un modo de procesamiento de forma independiente; o

ordenarle a la pasarela de medios que termine un flujo de medios y envíe un mensaje de terminación del flujo de medios; o

ordenarle a la pasarela de medios que notifique un evento de expiración de clave sin enviar un mensaje de terminación del flujo de medios; o

ordenarle a la pasarela de medios que notifique un evento de expiración de clave, termine un flujo de medios y envíe un mensaje de terminación del flujo de medios.

5. Una pasarela de medios, caracterizada por que la pasarela de medios comprende un módulo de recepción, un módulo de detección, un módulo de comprobación y un módulo de operación, en donde

el módulo (14) de recepción está configurado para recibir un evento de expiración de clave notificado por un controlador de pasarela de medios;

el módulo (11) de detección está configurado para detectar información de estado del tiempo de vida de una clave de transmisión de flujos de medios de acuerdo con el evento de expiración de clave notificado por el controlador de pasarela de medios y recibido por el módulo (14) de recepción;

el módulo (12) de comprobación está configurado para comprobar si el tiempo de vida de la clave de transmisión de flujos de medios ha expirado; y

el módulo (13) de operación está configurado para activar un modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con una instrucción de un controlador de pasarela de medios, cuando el módulo (12) de comprobación determina que el tiempo de vida de la clave de transmisión de flujos de medios ha expirado.

6. La pasarela de medios de acuerdo con la reivindicación 5, en la que el módulo de recepción está configurado,

además, para recibir un evento de expiración de clave que comprende un parámetro de tipo de clave o un parámetro identificador de clave;

el módulo de detección está configurado para detectar información de estado del tiempo de vida de un tipo especificado de clave de transmisión de flujos de medios o información de estado del tiempo de vida de una clave de transmisión de flujos de medios con un identificador especificado de acuerdo con el evento de expiración de clave notificado por el controlador de pasarela de medios y recibido por el módulo de recepción;

el módulo de comprobación está configurado para comprobar si la información de estado del tiempo de vida del tipo especificado de clave de transmisión de flujos de medios o la información de estado del tiempo de vida de la clave de transmisión de flujos de medios con el identificador especificado ha expirado; y

el módulo de operación está configurado para activar un modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con la instrucción del controlador de pasarela de medios, cuando el módulo de comprobación determina que el tiempo de vida del tipo especificado de clave de transmisión de flujos de medios o el tiempo de vida de la clave de transmisión de flujos de medios con el identificador especificado ha expirado.

7. Un sistema de operación para una clave de transmisión de flujos de medios, caracterizado por que el sistema de operación comprende un controlador de pasarela de medios y una pasarela de medios, en donde

el controlador (2) de pasarela de medios está configurado para enviarle un evento de expiración de clave a la pasarela de medios; y

la pasarela (1) de medios está configurada para recibir el evento de expiración de clave enviado por el controlador de pasarela de medios; detectar, de acuerdo con el evento de expiración de clave recibido notificado por el controlador de pasarela de medios, la información de estado del tiempo de vida de una clave de transmisión de flujos de medios; comprobar si el tiempo de vida de la clave de transmisión de flujos de medios ha expirado; y, cuando se determine que el tiempo de vida de la clave de transmisión de flujos de medios ha expirado, activar un modo de operación de expiración del tiempo de vida de la clave de transmisión de flujos de medios de acuerdo con una instrucción del controlador de pasarela de medios.

8. El sistema de acuerdo con la reivindicación 7, en el que la pasarela de medios comprende la pasarela de medios de acuerdo con una cualquiera de las reivindicaciones 5 a 6.

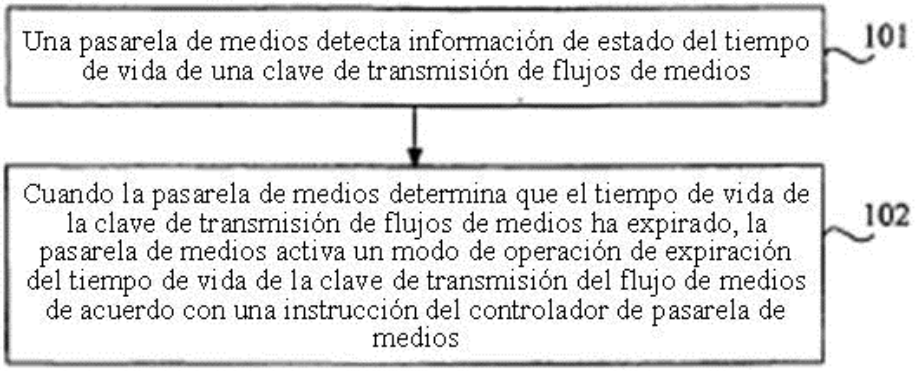

FIG. 1

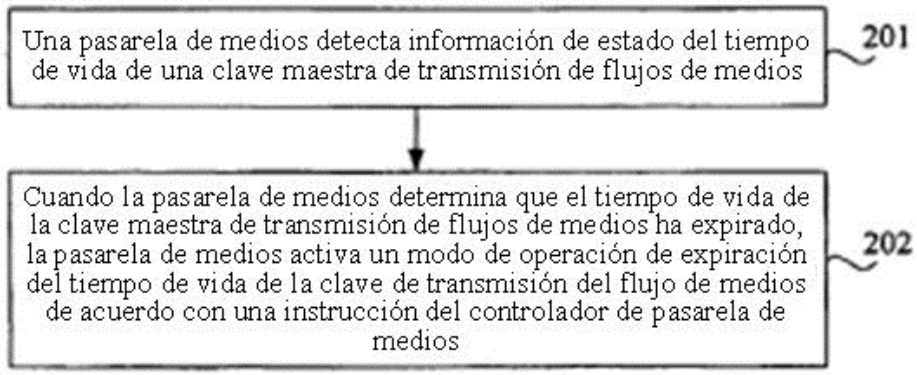

FIG. 2

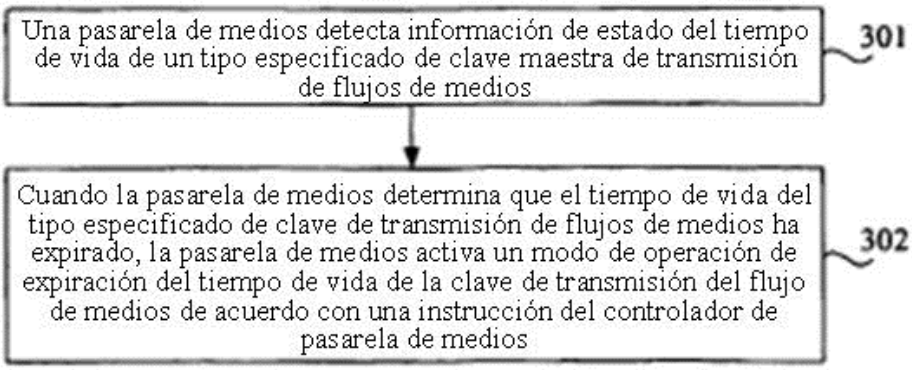

FIG. 3

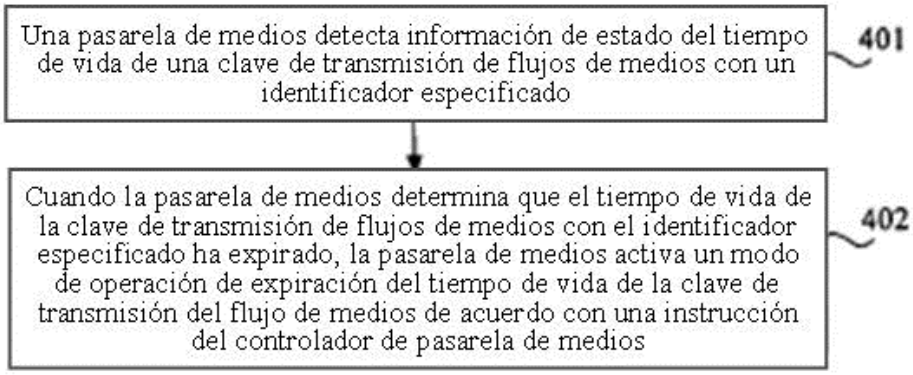
Una pasarela de medios detecta información de estado del tiempo de vida de una clave de transmisión de flujos de medios con un identificador especificado
401
Cuando la pasarela de medios determina que el tiempo de vida de la clave de transmisión de flujos de medios con el identificador especificado ha expirado, la pasarela de medios activa un modo de operación de expiración del tiempo de vida de la clave de transmisión del flujo de medios de acuerdo con una instrucción del controlador de pasarela de medios
402

FIG. 4

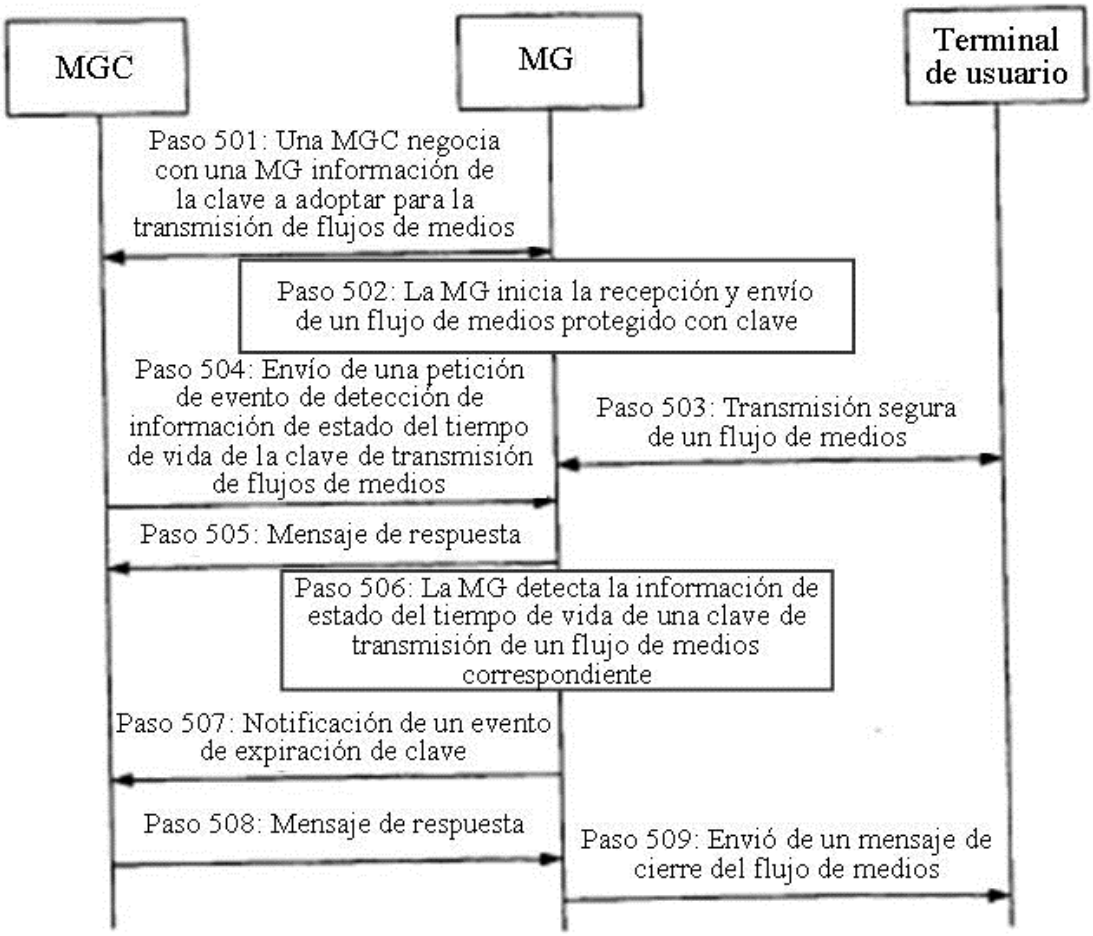
MGC
MG
Terminal de usuario
Paso 501: Una MGC negocia con una MG información de la clave a adoptar para la transmisión de flujos de medios
Paso 502: La MG inicia la recepción y envío de un flujo de medios protegido con clave
Paso 504: Envío de una petición de evento de detección de información de estado del tiempo de vida de la clave de transmisión de flujos de medios
Paso 503: Transmisión segura de un flujo de medios
Paso 505: Mensaje de respuesta
Paso 506: La MG detecta la información de estado del tiempo de vida de una clave de transmisión de un flujo de medios correspondiente
Paso 507: Notificación de un evento de expiración de clave
Paso 508: Mensaje de respuesta
Paso 509: Envió de un mensaje de cierre del flujo de medios

FIG. 5

FIG. 6

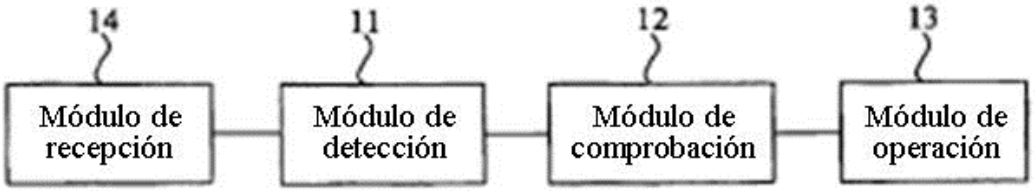

FIG. 7

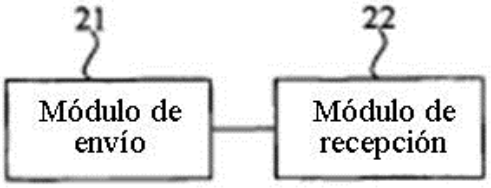

FIG. 8

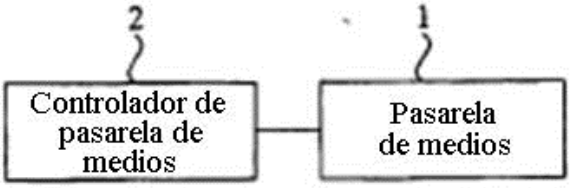

FIG. 9