(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 563 495**

(51) Int. CI.:

H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **29.12.2007 E 07855943 (2)**

(97) Fecha y número de publicación de la concesión europea: **23.12.2015 EP 2151946**

(54) Título: **Procedimiento para la detección de la clave de la red óptica pasiva gigabit**

(30) Prioridad:

10.05.2007 CN 200710104375

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.03.2016

(73) Titular/es:

ZTE CORPORATION (100.0%)
ZTE PLAZA, KEJI ROAD SOUTH, HI-TECH INDUSTRIAL PARK, NANSHAN DISTRICT
SHENZHEN, GUANGDONG 518057, CN

(72) Inventor/es:

ZHANG, WEILIANG y
XIA, SHUNDONG

(74) Agente/Representante:

DURÁN MOYA, Luis Alfonso

DESCRIPCIÓN

Procedimiento para la detección de la clave de la red óptica pasiva gigabit

Sector técnico

La presente invención hace referencia a una técnica de gestión de claves de transmisión segura de datos en una red óptica pasiva gigabit (GPON, Gigabit Passive Optical Network) en el sector de la comunicación y, en particular, a una técnica para la detección de claves de un terminal óptico de línea (OLT, Optical Line Terminal) y a una unidad óptica de red (ONU, Optical Network Unit) en la GPON.

Antecedentes de la invención

La GPON es una tecnología de acceso integrado óptica pasiva de banda ancha de nueva generación basada en el estándar ITU-T G.984x, y el sistema consiste generalmente en un OLT en el lado del extremo de oficina, varias ONU / ONT (Terminaciones de red ópticas, Optical Network Termination) en el lado del usuario, y una OND (Red de distribución óptica, Optical Distribution Network). La ODN, que consiste en dispositivos ópticos pasivos tales como fibra monomodo, divisor óptico, conector óptico, etc., proporciona medios ópticos de transmisión entre la OLT y las ONU. La ODN generalmente tiene una estructura de punto a multipunto, es decir, un OLT se conecta con múltiples ONU. Los datos enviados a las ONU por el OLT se denominan datos de bajada, y los datos enviados al OLT por las ONU se denominan datos de subida.

En un sistema de GPON, los datos de bajada tienen una propiedad de emisión, y los datos enviados por un OLT pueden ser recibidos por todas las ONU conectadas al mismo y, un usuario malintencionado puede reprogramar una ONU controlada y por ello puede escuchar todos los datos de bajada de todos los usuarios. Por lo que respecta a la seguridad, el estándar ITU-T G.984.3 sugiere utilizar una tecnología de encriptación basada en AES (Estándar de encriptación avanzada, Advanced Encryption Standard) para encriptar los datos de bajada, y un OLT y una ONU almacenan cada uno una clave. El desarrollo de gestión de las claves entre el OLT y la ONU puede dividirse en dos etapas: cambio de clave y conversión de clave.

En la etapa de cambio de clave, el OLT envía un mensaje de “Solicitar clave” a la ONU, la ONU genera una nueva clave y un índice de clave y los almacena en el registro de clave oculta (shadow_key).

En la etapa de conversión de clave, el OLT selecciona un número de bloque (que puede denominarse número de bloque de conversión de clave) como el primer bloque en el que se utiliza la nueva clave, y el OLT transfiere el número de multibloques del bloque a la ONU mediante un mensaje de hora de cambio de clave. El mensaje será enviado tres veces, y la ONU solamente necesita recibir una copia correcta para obtener el número de bloque de conversión de clave. La ONU envía un mensaje de acuse de recibo al OLT, indicando que se ha obtenido el número de bloque de conversión de clave. Al inicio del primer bloque en que se debe utilizar la nueva clave, el OLT copia el contenido en el registro de clave oculta en el registro de clave activa, y la ONU copia su registro de clave oculta en el registro de clave activa y, tanto el OLT como la ONU empiezan desde el mismo bloque a utilizar la nueva clave para encriptar y desencriptar los datos de bajada. Las claves en los registros de clave activa del OLT y de la ONU pueden denominarse como claves actuales.

En la etapa de conversión de clave, si el OLT no tiene éxito en la recepción del mensaje de acuse de recibo desde la ONU, no puede determinar si la ONU ha recibido correctamente el número de bloque de conversión de clave. En tales escenarios independientemente de si el OLT ejecuta o no la conversión de clave, posiblemente existirá incoherencia entre las claves del OLT y de la ONU. Suponiendo que el OLT lleva a cabo la conversión de clave, las claves actuales de los dos no serán coherentes si la ONU no recibe la orden de conversión de clave desde el OLT y no hay ninguna conversión de clave en la ONU. Suponiendo que el OLT no realiza la conversión de clave, las claves actuales de los dos no serán coherentes, tanto si la ONU ha obtenido con éxito el número de bloque de conversión de clave como si el mensaje de acuse de recibo enviado por la ONU se ha perdido (se producirá una conversión de clave en la ONU).

La incoherencia entre las claves de un OLT y una ONU ocasionará directamente el resultado de que los datos enviados por el OLT no pueden ser desencriptados correctamente por la ONU, y ocasionarán exclusiones en los servicios relacionados con la ONU. El estándar ITU-T G.984.x no considera la situación en la cual las claves actuales de un OLT y una ONU pueden ser incoherentes, ni proporciona un procedimiento para la detección de si las claves actuales de un OLT y una ONU son coherentes.

El documento U.S.A. 5920627 A1 proporciona un dispositivo de encriptación y un dispositivo de desencriptación para la información transportada por la célula en modo asíncrono de transferencia. Puede utilizarse un dispositivo de encriptación para encriptar unidades de información transportadas por las células que son emitidas desde un nodo de emisión óptico a unidades de red mediante una red óptica pasiva. Cada célula transporta al menos una unidad de información, y cada unidad de información es dirigida a un terminal de abonado respectivo. El dispositivo incluye un

sistema de encriptación que recibe de manera visible al menos una clave de, al menos, un dispositivo de encriptación situado en una unidad de red.

Características de la invención

El objetivo de la presente invención es proporcionar un procedimiento para la detección de claves en una red óptica pasiva gigabit, de manera que el sistema pueda descubrir a tiempo y tratar la situación de que las claves actuales de un OLT y una ONU no sean coherentes, de este modo puede evitarse la exclusión del servicio ocasionada por esta situación.

Con el fin de conseguir el objetivo de la presente invención, la presente invención proporciona un procedimiento para la detección de claves en una red óptica pasiva gigabit, utilizada para detectar la coherencia entre las claves actuales de un terminal óptico de línea y una unidad óptica de red en un sistema de red óptica pasiva gigabit; comprendiendo el procedimiento las etapas siguientes:

(a) el terminal óptico de línea envía un mensaje de solicitud de información sobre la clave actual a la unidad óptica de red, y espera a que la unidad óptica de red devuelva un mensaje de respuesta de información sobre la clave actual;

(b) si la unidad óptica de red recibe el mensaje de solicitud de información sobre la clave actual, lee la información sobre la clave actual almacenada localmente en la unidad óptica de red, y carga el contenido leído en el mensaje de respuesta de información sobre la clave actual, y envía el mensaje de respuesta al terminal óptico de línea;

(c) si el terminal óptico de línea recibe el mensaje de respuesta de información sobre la clave actual en un periodo predeterminado, obtiene la información sobre la clave actual de la unidad óptica de red del mensaje de respuesta, y compara la información sobre la clave actual de la unidad óptica de red del mensaje de respuesta, y compara la información sobre la clave actual de la unidad óptica de red con la información sobre la clave actual almacenada localmente en el terminal óptico de línea y, de acuerdo con el resultado de la comparación, lleva a cabo el correspondiente procesamiento.

Además, el mensaje de solicitud de información sobre la clave actual en la etapa (a) comprende: una identificación de la unidad óptica de la red objetivo y una identificación del mensaje objetivo; en que, la identificación de la unidad óptica de la red objetivo se utiliza para representar una unidad óptica de la red objetivo a la cual es enviado el mensaje de solicitud de información sobre la clave actual; la identificación del mensaje objetivo se utiliza para indicar a la unidad óptica de la red objetivo que el mensaje de solicitud es una petición de información sobre la clave actual; el mensaje de respuesta de información de la clave actual de la etapa (c) comprende: una identificación de la unidad óptica de red origen, una identificación de mensaje origen y datos del cuerpo de información sobre la clave actual; en el que la identificación de la unidad óptica de red origen se utiliza para representar una unidad óptica de la red origen desde la cual es enviado el mensaje de respuesta de información sobre la clave actual; la identificación del mensaje origen se utiliza para indicar al terminal óptico de línea que el mensaje de respuesta es una respuesta al mensaje de solicitud de información sobre la clave actual; los datos del cuerpo de información sobre la clave actual son utilizados por el terminal óptico de línea para obtener un cuerpo de información sobre la clave actual a partir del mensaje de respuesta.

Además, el procedimiento comprende asimismo:

la información sobre la clave actual es una clave actual; el mensaje de respuesta de información sobre la clave actual son mensajes de respuesta sobre la clave actual, y los datos del cuerpo de información sobre la clave actual son datos del cuerpo de la clave actual; los datos del cuerpo de la clave actual comprenden además índices de fragmentos de la clave y cuerpos de la clave actual y, en la etapa (c), según los índices de fragmentos de la clave actual, el terminal óptico de línea une múltiples fragmentos de los cuerpos de la clave actuales en múltiples mensajes de respuesta de la clave actual de manera secuencial en una clave actual completa de la unidad óptica de red.

Además, el procedimiento comprende asimismo:

en la etapa (a), el terminal óptico de línea envía un mensaje de solicitud de la clave actual a la unidad óptica de red; en la etapa (b), si la unidad óptica de red recibe el mensaje de respuesta de la clave actual, lee la clave actual almacenada localmente en la unidad óptica de red, divide el contenido leído en fragmentos, carga los fragmentos en múltiples mensajes de respuesta de la clave actual y envía los mensajes de respuesta de manera secuencial a los terminales ópticos de línea; en la etapa (c), si el resultado de la comparación es que la clave actual de la unidad óptica de red es coherente con la clave actual almacenada localmente en el terminal óptico de línea, el terminal óptico de línea lleva a cabo el procesamiento correspondiente a la coherencia de las claves actuales; si el resultado de la comparación es que la clave actual de la unidad óptica de red no es coherente con la clave actual almacenada localmente en el terminal óptico de línea, el terminal óptico de línea lleva a cabo el procesamiento correspondiente a la incoherencia de las claves actuales.

Además, durante un proceso de conversión de clave, si el terminal óptico de línea no recibe un mensaje de acuse de recibo enviado por la unidad óptica de red cuando llega un número de bloque de conversión de clave, se inicia la implementación de la etapa (a) por parte del terminal óptico de línea; en la etapa (c), el procesamiento correspondiente a la coherencia de las claves actuales es: el terminal óptico de línea envía información de éxito en la conversión de la clave con la unidad óptica de red; o el procesamiento correspondiente a la incoherencia de las claves actuales llevado a cabo por el terminal óptico de línea es: el terminal óptico de línea envía información de un fallo en la conversión de la clave con la unidad óptica de red.

Además, para encontrar una razón para un fallo de servicio en la red óptica pasiva gigabit, el personal de mantenimiento del equipo inicia manualmente la implementación de la etapa (a) desde un sistema de gestión del elemento de red; en la etapa (c), el procesamiento correspondiente a la coherencia de las claves actuales es: el terminal óptico de línea informa al sistema de gestión del elemento de red la coherencia entre las claves actuales del terminal óptico de línea y la unidad óptica de red; o el procesamiento correspondiente a la incoherencia de las claves actuales es: el terminal óptico de línea informa al sistema de gestión del elemento de red la incoherencia entre las claves actuales del terminal óptico de línea y la unidad óptica de red.

Además, la implementación de la etapa (a) es iniciada por el terminal óptico de línea en un tiempo definido; en la etapa (c), el procesamiento correspondiente a la coherencia de las claves actuales es: el terminal óptico de línea informa a un sistema de gestión del elemento de red de que las claves actuales del terminal óptico de línea y de la unidad óptica de red son coherentes; o el procesamiento correspondiente a la incoherencia de las claves actuales es: el terminal óptico de línea informa al sistema de gestión del elemento de red de que las claves actuales del terminal óptico de línea y de la unidad de red óptica son incoherentes.

Además, el procedimiento comprende asimismo:

en la etapa (c), si el terminal óptico de línea no recibe los mensajes de respuesta de la clave actual en el periodo predeterminado, envía información de un fallo en la detección de la coherencia entre las claves actuales.

Además, el procedimiento comprende asimismo:

la información sobre la clave actual es un índice de la clave actual; el mensaje de respuesta de información sobre la clave actual es un mensaje de respuesta del índice de la clave actual, y los datos del cuerpo de información sobre la clave actual son datos del cuerpo de índice de la clave actual; en la etapa (a), el terminal óptico de línea envía un mensaje de solicitud de índice de la clave actual a la unidad óptica de red; en la etapa (b), si la unidad óptica de red recibe el mensaje de solicitud de índice de la clave actual, lee el índice de la clave actual almacenado localmente en la unidad óptica de red, carga el contenido leído como datos del cuerpo de índice de la clave actual en el mensaje de respuesta del índice de la clave actual, y envía el mensaje de respuesta al terminal óptico de línea; en la etapa (c), el terminal óptico de línea obtiene los datos del cuerpo de índice de la clave actual como el índice de la clave actual de la unidad óptica de red; si el resultado de la comparación es que el índice de la clave actual de la unidad óptica de red es coherente con el índice de la clave actual almacenado localmente en el terminal óptico de línea, el terminal óptico de línea lleva a cabo el procesamiento correspondiente a la coherencia de las claves actuales; si el resultado de la comparación es que el índice de la clave actual de la unidad óptica de red es incoherente con el índice de la clave actual almacenado localmente en el terminal óptico de línea, el terminal óptico de línea lleva a cabo el procesamiento correspondiente a la incoherencia de las claves actuales.

Además, el procedimiento comprende asimismo:

en la etapa (c), si el terminal óptico de línea no recibe los mensajes de respuesta del índice de clave actual en el periodo predeterminado, envía información de un fallo en la detección de la coherencia entre las claves actuales.

Además, el procedimiento comprende asimismo:

la información sobre la clave actual es un número de bloque de conversión de clave; en la etapa (a), el terminal óptico de línea envía un mensaje de solicitud del número de bloque de conversión a la unidad óptica de red; en la etapa (b), si la unidad óptica de red recibe el mensaje de solicitud del número de bloque de conversión de clave, lee el número de bloque de conversión de clave almacenado localmente en la unidad óptica de red, carga el contenido leído como datos del cuerpo de número de bloque de conversión de clave en un mensaje de respuesta del número de bloque de conversión de clave, y envía el mensaje de respuesta al terminal óptico de línea; en la etapa (c), el terminal óptico de línea obtiene los datos del número de bloque de conversión de clave como el número de bloque de conversión de clave de la unidad óptica de red; si el resultado de la comparación es que el número de bloque de conversión de clave de la unidad óptica de red es coherente con el número de bloque de conversión de clave almacenado localmente en el terminal óptico de línea, el terminal óptico de línea lleva a cabo el procesamiento correspondiente a la coherencia de las claves actuales; si el resultado de la comparación es que el número de bloque de conversión de clave de la unidad óptica de red es incoherente con el número de bloque de conversión de

clave almacenado localmente en el terminal óptico de línea, el terminal óptico de línea lleva a cabo el procesamiento correspondiente a la incoherencia de las claves actuales.

Además, el procedimiento comprende asimismo:

en la etapa (c), si el terminal óptico de línea no recibe los mensajes de respuesta de número de bloque de conversión de clave en el periodo predeterminado, envía información de un fallo en la detección de la coherencia entre las claves actuales.

La presente invención, como suplemento al procedimiento de conversión de clave de la técnica anterior, activa la detección de la coherencia entre las claves actuales de un OLT y una ONU en una GPON de varias maneras; por lo tanto, la incoherencia latente entre las claves actuales del OLT y la ONU puede ser descubierta a tiempo, y se puede realizar el procesamiento correspondiente, de manera que el riesgo de que ocurra la exclusión debido a la incoherencia entre las claves actuales del OLT y la ONU en un servicio de GPON se puede reducir o evitar. Además, la presente invención llena un espacio del estándar ITU-T G.984.x a este respecto y, para el desarrollo de una red óptica pasiva gigabit, la presente invención complementa un método estándar del que carece.

Breve descripción de los dibujos

La figura 1 es un diagrama de desarrollo de un procedimiento para la detección de claves en una red óptica pasiva gigabit de acuerdo con la presente invención;

la figura 2 es un diagrama de desarrollo del ejemplo de aplicación 1 del procedimiento representado en la figura 1;

la figura 3 es un diagrama de desarrollo del ejemplo de aplicación 2 del procedimiento representado en la figura 1;

la figura 4 es un diagrama de desarrollo del ejemplo de aplicación 3 del procedimiento representado en la figura 1.

Realizaciones preferentes de la presente invención

El procedimiento para la detección de claves en una red óptica pasiva gigabit proporcionado en la presente invención es aplicable a la detección de coherencia entre las claves actuales de un OLT y una ONU en un sistema GPON, y el procedimiento adopta el siguiente esquema técnico: el GPON activa la detección de la coherencia entre las claves actuales del OLT y la ONU de varias maneras, y el OLT envía un mensaje de solicitud de la clave actual a la ONU para obtener la clave actual de la ONU; cuando recibe el mensaje de solicitud, la ONU carga su clave actual en los mensajes de respuesta de la clave actual y envía los mensajes al OLT; cuando recibe los mensajes de respuesta, el OLT obtiene la clave actual de la ONU en el mismo y compara la clave actual con una clave actual almacenada localmente y, basándose en el resultado de la comparación, lleva a cabo el procesamiento correspondiente. Si el OLT no recibe los mensajes de respuesta, envía información de aviso de un fallo en la detección de la coherencia entre las claves actuales del OLT y de la ONU.

El esquema técnico anterior de la presente invención se expondrá en detalle con realizaciones específicas y con los dibujos que se acompañan.

La incoherencia entre las claves actuales de un OLT y una ONT aparecidas en un sistema de GPON puede ser detectada de tres maneras: la primera es comprobar directamente las claves actuales del OLT y de la ONU; la segunda es comprobar los índices de clave relativos a las claves del OLT y de la ONU; dado que cada vez la ONU genera una nueva clave, generará también un índice de clave correspondiente, y enviará la nueva clave y el índice de clave al OLT simultáneamente; por lo tanto, comprobando los índices de la clave actuales del OLT y de la ONT, la comprobación de si las claves actuales del OLT y de la ONU son coherentes puede ser implementada indirectamente; la tercera es comprobar los números de bloque de conversión de clave en el OLT y la ONU; dado que el OLT seleccionará un número de bloque de conversión de clave así como el tiempo de conversión de clave e informará a la ONU, por lo tanto, la comprobación de los números de bloque de conversión de clave del OLT y de la ONU puede ser implementada indirectamente para comprobar si las claves actuales del OLT y de la ONU son coherentes.

Tal como se muestra en la figura 1, el procedimiento para la detección de claves en una red óptica pasiva gigabit de acuerdo con la presente invención comprende las siguientes etapas:

101: Activar una detección de la coherencia entre las claves actuales de un OLT y una ONU en una cierta situación;

En esta memoria, las situaciones que activan la detección pueden ser las siguientes, pero no están limitadas a las mismas:

(1) Durante la conversión de clave, el OLT no recibe un mensaje de acuse de recibo desde la ONU cuando llega el número de bloque de conversión de clave, a continuación el OLT determina si existe una conversión de clave en la ONU iniciando una detección de coherencia de la clave actual;
(2) cuando el personal de mantenimiento del equipo está tratando de encontrar una razón para un fallo de servicio, puede iniciar una detección de la coherencia entre las claves actuales del OLT y la ONU a partir del sistema de gestión del elemento de red;

(3) el OLT inicia de manera rutinaria una detección de la coherencia entre las claves actuales del mismo y la ONU en un tiempo definido.

Los primeros dos tipos de activación anteriores son la activación pasiva, es decir, la detección se inicia de manera pasiva por aparición de una exclusión; mientras que el último tipo de activación es la activación activa, es decir, el OLT puede iniciar activamente la detección de la coherencia entre las claves del mismo y el OLT en cualquier momento. En otras palabras, el OLT puede activar la detección de la coherencia entre las claves del mismo y la ONU de varias maneras pasivas o activas.

102: el OLT envía un mensaje de solicitud de información sobre la clave actual a la ONU y espera a que la ONU devuelva un mensaje de respuesta de información sobre la clave actual.

En esta memoria, la información sobre la clave actual comprende cualquier información, o una combinación de una clave actual, un índice de la clave actual o un número de bloque de conversión de la clave (es decir, un número de bloque de conversión de la clave actual).

103. Si la ONU recibe el mensaje de solicitud de información sobre la clave actual desde el OLT, lee la información sobre la clave en el registro de clave activa local, carga el contenido leído en un mensaje de respuesta de la clave actual y envía el mensaje al OLT.

104: el OLT pregunta si el mensaje de respuesta de información sobre la clave actual devuelto por la ONU ha sido recibido en un periodo predeterminado y, si no ha sido así, avanza a la etapa 105, mientras que si se ha recibido, avanza a la etapa 106;

105: el OLT envía información de un fallo en la detección de coherencia de la clave actual, y el desarrollo finaliza.

De acuerdo con la situación de activación correspondiente a la detección de coherencia de la clave actual, el procesamiento realizado puede ser un procesamiento de exclusión de conversión de la clave llevado a cabo por el OLT pero no está al mismo; o el OLT informa del resultado del fallo en la detección de coherencia de la clave actual al sistema de gestión del elemento de red.

106: El OLT obtiene la información sobre la clave actual de la ONU en el mensaje y la compara con la información sobre la clave actual almacenada en el registro de clave activa local;

107: de acuerdo con el resultado de la comparación, el OLT lleva a cabo el procesamiento correspondiente, y el desarrollo finaliza.

Primera realización

Para implementar la detección anterior de la coherencia entre las claves actuales del OLT y la ONU, en esta realización, los dos mensajes mencionados anteriormente, el mensaje de solicitud de información sobre la clave actual y el mensaje de respuesta de información sobre la clave actual se definen como sigue según el formato de mensaje de Operaciones de capa física, administración y mantenimiento (PLOAM, Physical Layer Operations, Administración and Maintenance) en el Protocolo de subcapa de convergencia de transmisión GPON G.984.3. Por supuesto, el contenido de estos dos mensajes puede ser ligeramente diferente en diferentes realizaciones.

(1) El mensaje de solicitud de la clave actual, Solicitar clave actual, es un mensaje de bajada enviado por un OLT a una ONU para obtener la clave actual de la ONU, y el contenido y la interpretación semántica de cada parte del formato de mensaje se muestran en la Tabla 1.

Tabla 1

Mensaje de solicitud de la clave actual, Solicitar clave actual		
Byte	Contenido	Interpretación semántica
1	ONU-ID	Identificación de ONU, utilizada para identificar la ONU objetivo a la cual se envía el mensaje
2	00010101	Identificación del mensaje, utilizada para indicar que es un mensaje de Solicitar clave actual
3 – 12	Reservado	

Dado que el mensaje de Solicitar clave actual es un mensaje de bajada, tiene características de emisión, y después que múltiples ONU reciban el mensaje, cada una de ellas determina si el mensaje es enviado a sí mismo de acuerdo con la identificación de la ONU (ONU-ID) en el mismo y, de acuerdo con la identificación de mensaje (00010101), identifica el tipo del mensaje como una solicitud de que la clave actual local sea enviada por el OLT a la ONU.

(2) El mensaje de respuesta de la clave actual, Clave de encriptación actual, es un mensaje de subida enviado por una ONU a un OLT para devolver la clave actual local de la ONU, y el contenido y la interpretación semántica de cada parte del mensaje formal se muestran en la Tabla 2.

Tabla 2

Mensaje de respuesta de la clave actual, Clave de encriptación actual		
Byte	Contenido	Interpretación semántica
1	ONU-ID	Identificación de ONU, utilizada para identificar la ONU origen a la cual se envía el mensaje
2	00001010	Identificación del mensaje, utilizada para indicar que es un mensaje de Clave de encriptación actual
3	Índice de fragmento	Índice de fragmento de clave, utilizado para indicar el número de secuencia del fragmento de clave contenido en el mensaje
4	KeyBYTE0	Byte de clave 0, es decir, el 1er byte del fragmento con el número de secuencia del Índice de fragmento de la clave actual
5	KeyBYTE1	Byte de clave 1, es decir, el 2º byte del fragmento con el número de secuencia del Índice de fragmento de la clave actual
6	KeyBYTE 2	Byte de clave 2, es decir, el 3er byte del fragmento con el número de secuencia del Índice de fragmento de la clave actual
7	KeyBYTE 3	Byte de clave 3, es decir, el 4º byte del fragmento con el número de secuencia del Índice de fragmento de la clave actual
8	KeyBYTE 4	Byte de clave 4, es decir, el 5º byte del fragmento con el número de secuencia del Índice de fragmento de la clave actual
9	KeyBYTE 5	Byte de clave 5, es decir, el 6º byte del fragmento con el número de secuencia del Índice de fragmento de la clave actual
10	KeyBYTE 6	Byte de clave 6, es decir, el 7º byte del fragmento con el número de secuencia del Índice de fragmento de la clave actual
11	KeyBYTE 7	Byte de clave 7, es decir, el 8º byte del fragmento con el número de secuencia del Índice de fragmento de la clave actual
12	Reservado	

En la tabla 2, los bytes 3 – 11 se denominan en conjunto como datos del cuerpo de la clave actual, utilizados por el OLT para obtener una clave actual completa de la ONU a través de los datos del cuerpo de clave. Tras recibir el mensaje de Clave de encriptación actual, de acuerdo con la identificación de mensaje (00001010), el OLT identifica el tipo del mensaje como respuesta de la ONU a una solicitud de la clave actual y, de acuerdo con la identificación de la ONU (ONU-ID), encuentra la unidad de registro de clave activa correspondiente que almacena localmente el cuerpo de la clave actual de la ONU y, a continuación a partir de la unidad de registro extrae el cuerpo de la clave actual almacenado localmente para su comparación.

Generalmente, la longitud de una clave es una serie de bytes; así, se puede requerir estipular que una clave se divida en múltiples fragmentos que estén contenidos respectivamente en múltiples cuerpos de mensaje de Encriptación de la clave actual para ser enviados, y el Índice de fragmento en el cuerpo de mensaje indica a qué fragmento de la clave de la serie de bytes contenidos en el cuerpo del mensaje de encriptación de la clave actual, pertenece.

Por ejemplo, en esta realización, la longitud de una clave es 16 bytes y está estipulado que una clave está dividida en dos fragmentos, cada uno de los cuales tiene ocho bytes, y los dos fragmentos están contenidos respectivamente en dos cuerpos de mensaje de Clave de Encriptación actual para ser enviados, y el Índice de fragmento en un cuerpo de mensaje indica si los 8 bytes contenidos en el cuerpo de mensaje de clave de encriptación actual

pertenecen al primer fragmento de la clave o al segundo fragmento de la clave. Esta estipulación en la realización se utiliza solamente para ilustrar pero no para limitar la presente invención. Cualquier estipulación realizada de acuerdo con la idea de la presente invención entrará dentro del alcance reivindicado por la presente invención.

Con el fin de ilustrar cómo se utilizan los dos mensajes anteriores para detectar la coherencia entre claves actuales de un OLT y una ONU en un proceso de conversión de clave, se muestran a continuación ejemplos de aplicación para ilustrar esto con mayor detalle.

Tal como se muestra en la figura 2, por ejemplo, durante un proceso de conversión de clave, el OLT no recibe un mensaje de acuse de recibo desde una ONU cuando llega el número de bloque de conversión de clave; entonces el OLT inicia el desarrollo de detección de la coherencia de la clave actual, que comprende las siguientes etapas:

201: Después de que el OLT inicia la conversión de clave, no ha recibido el mensaje de acuse de recibo de la ONU cuando se inicia el bloque de conversión de clave;

202: El OLT envía un mensaje de Solicitud de la clave actual a la ONU tres veces y espera a que la ONU devuelva mensajes de Clave de encriptación actual.

203: Si la ONU recibe el mensaje de Solicitud de la clave actual desde el OLT, extrae la clave del registro de clave activa y divide la clave en dos fragmentos iguales, y rellena los mensajes de Clave de encriptación actual con la identificación de la ONU, la identificación del mensaje y la información del cuerpo de clave (incluyendo un índice de fragmento de clave y un cuerpo de clave) según el formato del mensaje de Clave de encriptación actual, y envía los mensajes al OLT;

204: el OLT pregunta si se reciben los mensajes de Clave de encriptación actual desde la ONU y, si se reciben, avanza a la etapa 205, mientras que si no se reciben, avanza a la etapa 206;

205: El OLT obtiene la clave actual de la ONU de los mensajes de Clave de encriptación actual y la compara con la clave actual almacenada localmente y, a continuación, avanza a la etapa 207.

El OLT obtiene la clave actual de la ONU de acuerdo con la información del cuerpo de clave de los mensajes de Clave de encriptación actual; y encuentra el correspondiente registro de clave activa local correspondiente según el ONU-ID en el mensaje de Clave de encriptación actual, y lee la clave actual almacenada en el mismo y compara las dos claves.

206: El OLT considera fallida la conversión de clave con la ONU y, después de que el OLT envía la información correspondiente, el desarrollo finaliza;

207: Comprobar el resultado de la comparación para determinar si las dos claves son coherentes y, si son coherentes, avanza a la etapa 208, mientras que si son incoherentes, vuelven a la etapa 206.

208: El OLT considera correcta la conversión con la ONU y, después de que el OLT envíe la información correspondiente, el desarrollo finaliza.

Tal como se muestra en la figura 3, cuando al personal de mantenimiento del equipo se le informa de que se ha producido un fallo en un servicio de GPON para un usuario, necesita preguntar si el fallo se ha producido por incoherencia entre las claves del OLT y la ONU y, a continuación, el personal de funcionamiento y de mantenimiento inicia el desarrollo de detección de la coherencia entre las claves actuales del OLT y la ONU desde el sistema de gestión del elemento de red, y el desarrollo comprende las siguientes etapas:

301: el personal de funcionamiento y de mantenimiento inicia manualmente la detección de la coherencia entre las claves actuales del OLT y la ONU del sistema de gestión del elemento de red;

302: el OLT envía un mensaje de Solicitar clave actual a la ONU tres veces y espera los mensajes de Clave de encriptación actual devueltos por la ONU;

303: Si la ONU recibe el mensaje de solicitud de la clave actual desde el OLT, divide en dos fragmentos la clave del registro de la clave actual, y envía mensajes que contienen los fragmentos al OLT, de acuerdo con el formato del mensaje de Clave de encriptación actual;

304: el OLT pregunta si los mensajes de Clave de encriptación actual desde la ONU son recibidos en el periodo predeterminado y, si no son recibidos, avanza a la etapa 305, mientras que si son recibidos, avanza a la etapa 306;

305: El OLT informa al sistema de gestión del elemento de red de un fallo en la detección de coherencia de la clave actual; y el desarrollo finaliza;

306: El OLT obtiene la clave actual de la ONU de los mensajes de Clave de encriptación actual y la compara con la clave actual almacenada localmente;

307: Compara las dos claves y determina si son coherentes y, si lo son, avanza a la etapa 308, mientras que si son incoherentes, avanza a la etapa 309;

308: el OLT informa al sistema de gestión del elemento de red que su clave actual es coherente con la de la ONU; y el desarrollo finaliza;

309: El OLT informa al sistema de gestión del elemento de red que su clave actual es incoherente con la de la ONU; y el desarrollo finaliza.

La figura 4 muestra el desarrollo de detección de la coherencia entre las claves actuales de un OLT y una ONU iniciada por el OLT periódicamente, y el desarrollo comprende las siguientes etapas:

401: Un temporizador finaliza, el cual activa periódicamente la detección de la coherencia entre las claves actuales del OLT y de la ONU;

402: Reiniciar el temporizador para preparar la temporización de la siguiente detección;

403: El OLT envía un mensaje de Solicitar clave actual a la ONU tres veces y espera los mensajes de clave de encriptación actual devueltos por la ONU;

404: Si la ONU recibe el mensaje de Solicitar clave actual desde el OLT, divide en dos fragmentos la clave del registro de clave activa, y envía mensajes al OLT de acuerdo con el formato del mensaje de Clave de encriptación actual;

405: El OLT pregunta si los mensajes de Clave de encriptación actual desde la ONU se han recibido en un periodo predeterminado y, si se han recibido, avanza a le etapa 406, mientras que si no se han recibido, avanza a la etapa 410;

406: El OLT obtiene la clave actual de la ONU de los mensajes de Clave de encriptación actual, y los compara con la clave actual almacenada localmente;

407: Compara las dos claves y determina si son coherentes y, si lo son, avanza a la etapa 408, mientras que si son incoherentes, avanza a la etapa 409;

408: El OLT informa al sistema de gestión del elemento de red que su clave actual es coherente con la de la ONU; y el desarrollo finaliza;

409: El OLT informa al sistema de gestión del elemento de red que su clave actual es incoherente con la de la ONU; y el desarrollo finaliza.

410; El OLT informa al sistema de gestión de elementos de red de un fallo en la detección de coherencia de la clave actual; y el desarrollo finaliza.

Segunda realización

El esquema técnico de esta realización es substancialmente idéntico al desarrollo de la primera realización; la única diferencia es que el objeto de comparación en la detección de coherencia de clave es diferente y, en esta realización, el objeto de comparación en la detección de la coherencia de la clave es el índice de la clave actual.

Esto se debe a que cada vez que una ONU genera una nueva clave, generará también el índice de clave correspondiente, y enviará la nueva clave y el índice de clave simultáneamente a un OLT. La longitud de un índice de clave es un byte, y la regla para que una ONU genere un índice de clave es que al índice de clave se le suma 1 cada vez que se genera una nueva clave, y vuelve a 0 si supera 255, y durante 256 conversiones de clave consecutivas, el índice de clave corresponde únicamente a la clave actual, y la posibilidad de una aparición consecutiva de 256 exclusiones de conversión de clave en un sistema GPON es reducida. Por lo tanto, la detección de la coherencia entre las claves de los dos se puede conseguir detectando y comparando los índices de clave de los dos y determinando si son coherentes.

De acuerdo con ello, el formato de un mensaje de solicitud del índice de la clave actual enviado por un OLT a una ONU se muestra en la Tabla 3.

Tabla 3

Mensaje de solicitud de la clave actual, Solicitar clave actual		
Byte	Contenido	Interpretación semántica
1	ONU-ID	Identificación de ONU, utilizada para identificar la ONU objetivo a la cual se envía el mensaje
2	00010110	Identificación del mensaje, utilizada para indicar que es un mensaje de Solicitar índice de la clave actual
3 - 12	Reservado	

La identificación del mensaje en la Tabla 3 se utiliza para indicar a la ONU que el objeto solicitado del mensaje es el índice de la clave actual. El formato del mensaje de respuesta del índice de la clave actual devuelto por la ONU al OLT se muestra en la Tabla 4.

Tabla 4

Mensaje de solicitud de la clave actual, Solicitar clave actual		
Byte	Contenido	Interpretación semántica
1	ONU-ID	Identificación de ONU, utilizada para identificar la ONU origen desde la cual se envía el mensaje
2	00001011	Identificación del mensaje, utilizada para indicar que es un mensaje del índice de la clave de codificación actual
3	BYTE de índice	Byte de Índice de clave, es decir, el byte del índice de la clave actual
4 - 12	Reservado	

La identificación del mensaje en la Tabla 4 se utiliza para indicar al OLT que el objeto de la respuesta del mensaje es el índice de la clave actual. El contenido del byte 3 (Índice BYTE) se denomina de acuerdo con esto como datos del cuerpo de la clave actual, es decir, el índice de la clave actual.

El OLT obtiene el índice de la clave actual de la ONU a partir del mensaje de respuesta y lo compara con el índice de la clave actual almacenado localmente en el OLT y, si el resultado de la comparación es que el índice de la clave actual de la ONU es incoherente con el índice de la clave actual almacenado localmente en el OLT, el OLT inicia el procesamiento correspondiente a la incoherencia con la clave actual de la ONU.

El diagrama de desarrollo del procedimiento de acuerdo con la presente invención mostrado en la figura 1 comprende la situación de esta realización, y las situaciones que activan la ejecución del desarrollo de esta realización son las mismas que las de la primera realización, así que no se repiten en esta memoria.

Tercera realización

El esquema técnico de esta realización difiere de los desarrollos de las realizaciones primera y segunda también en el objeto de la comparación en la detección de la coherencia, y el objeto de la comparación en la detección de coherencia de la clave en esta realización es el número del bloque de conversión de clave.

Dado que no existe ninguna estipulación con respecto a la selección del número de bloque de conversión de clave en el estándar G.984.x, esta realización realiza algunas restricciones para seleccionar el número de bloque de conversión de clave: el número de bloque tiene una longitud de 4 bytes, el OLT almacena N números de bloque consecutivos de conversión de la clave histórica, y el número de bloque de conversión de clave determinado por el OLT debe ser diferente de los N números de bloque históricos de conversión de clave, y el rango de valores de N es 0 ~ 0xffffffff. De acuerdo con la regla para seleccionar el número de bloque de conversión de clave, si N es 256, se puede conseguir un resultado similar al del índice de clave, y en un sistema GPON, la posibilidad de una aparición consecutiva de N = 256 exclusiones de conversión de la clave es reducida, y la expansión del rango de valores de N puede disminuir también la posibilidad de N exclusiones de conversión de la clave consecutivas. Por lo tanto, la detección de la coherencia entre las claves de los dos se puede conseguir detectando y comparando los números de bloque de conversión de clave de los dos y determinando si son coherentes.

De acuerdo con ello, el formato de un mensaje de solicitud de número de bloque de conversión de la clave enviado por un OLT a una ONU y el formato del mensaje de respuesta del número de bloque de conversión de clave devuelto por la ONU al OLT se muestran respectivamente en la Tabla 5 y la Tabla 6.

Tabla 5

Mensaje de solicitud del número del bloque de conversión de la clave, Solicitar el número actual del re-bloque		
Byte	Contenido	Interpretación semántica
1	ONU-ID	Identificación de ONU, utilizada para identificar la ONU objetivo a la cual se envía el mensaje
2	00010111	Identificación de mensaje, utilizada para indicar que es un mensaje de Solicitar número de re-bloque actual
3 - 12	Reservado	

La identificación del mensaje en la Tabla 5 se utiliza para indicar a la ONU que el objeto de la solicitud del mensaje es el número de bloque de conversión de la clave.

Tabla 6

Mensaje de repuesta de número de bloque de conversión de la clave. Número actual de encriptación del re-bloque		
Byte	Contenido	Interpretación semántica
1	ONU-ID	Identificación de la ONU, utilizada para identificar la ONU origen desde la cual se envía el mensaje
2	00001100	Identificación de mensaje, utilizada para indicar que es un mensaje de Número actual de encriptación del re-bloque
3	NumBYTE 0	Byte 0 del número de bloque de conversión de la clave, es decir, el primer byte del número de bloque de conversión de la clave
4	NumBYTE 1	Byte 1 del número de bloque de conversión de la clave, es decir, el segundo byte del número de bloque de conversión de la clave
5	NumBYTE 2	Byte 2 del número de bloque de conversión de la clave, es decir, el tercer byte del número de bloque de conversión de la clave
6	NumBYTE 3	Byte 3 del número de bloque de conversión de la clave, es decir, el cuarto byte del número de bloque de conversión de la clave
7 ~ 12	Reservado	

La identificación del mensaje en la Tabla 6 se utiliza para indicar al OLT que el objeto de la respuesta del mensaje es el número de bloque de conversión de la clave. El contenido de los Bytes 3 – 6 es, de acuerdo con los datos del cuerpo de número de bloque de conversión de la clave, es decir, el número de bloque de conversión de clave.

El OLT obtiene el número de bloque de conversión de la clave de la ONU a partir del mensaje de respuesta de la ONU, y lo compara con el número de bloque de conversión de la clave almacenado localmente en el OLT y, si el resultado de la comparación es que el número de bloque de conversión de la clave de la ONU es incoherente con el número de bloque de conversión de la clave almacenado localmente en el OLT, el OLT inicia el procesamiento correspondiente a la incoherencia con la clave actual de la ONU.

El diagrama de desarrollo del procedimiento de acuerdo con la presente invención mostrado en la figura 1 comprende la situación de esta realización, y las situaciones que activan la ejecución del desarrollo de esta realización son las mismas que las de la primera realización, así que no se repiten en esta memoria.

De la descripción de las realizaciones y ejemplos anteriores se puede apreciar que la presente invención activa la detección de la coherencia entre las claves del OLT y de una ONU de varias maneras y con varios procedimientos, de tal manera que la incoherencia latente entre las claves actuales del OLT y la ONU en un GPON puede ser descubierta a tiempo, e informa al sistema de gestión del elemento de red que debe realizarse el correspondiente procesamiento para garantizar que los datos enviados por el OLT pueden ser desencriptados fiable y correctamente por la ONU, y con ello el riesgo de que ocurra una exclusión debido a la incoherencia entre las claves actuales del OLT y la ONU en un servicio de GPON puede reducirse o evitarse.

La descripción anterior son solo realizaciones preferentes de la presente invención y no se utiliza para limitar la presente invención.

Aplicabilidad industrial

La presente invención puede llenar un hueco en el estándar G.984.x en lo que se refiere a la detección de la coherencia entre las claves actuales de un OLT y una ONU en la etapa de la conversión de la clave en un GPON, y propone un procedimiento estándar para un desarrollo rápido de una red óptica en una red óptica pasiva gigabit.

REIVINDICACIONES

1. Procedimiento para la detección de claves en una red óptica pasiva gigabit, utilizado para la detección de la coherencia entre las claves actuales de un terminal óptico de línea y una unidad óptica de red en un sistema de red óptica pasiva gigabit; en el que dicho procedimiento comprende las etapas siguientes de:

(a) dicho terminal óptico de línea envía un mensaje de solicitud de información sobre la clave actual a dicha unidad óptica de red, y espera a que la unidad óptica de red devuelva un mensaje de respuesta de información sobre la clave actual (102);
(b) si dicha unidad óptica de red recibe dicho mensaje de respuesta de información de la clave actual, lee la información sobre la clave actual almacenada localmente en dicha unidad óptica de red, y carga el contenido leído en dicho mensaje de respuesta de información sobre la clave actual y envía el mensaje de respuesta a dicho terminal óptico de línea (103);
(c) si dicho terminal óptico de línea recibe dicho mensaje de respuesta de información sobre la clave actual en un periodo predeterminado, obtiene la información sobre la clave actual de dicha unidad óptica de red de dicho mensaje de respuesta, y compara la información sobre la clave actual de dicha unidad óptica de red con la información sobre la clave actual almacenada localmente en dicho terminal óptico de línea (106), y según el resultado de la comparación, efectúa el correspondiente procesamiento (107).

2. Procedimiento, según la reivindicación 1, en el que,
dicho mensaje de solicitud de información sobre la clave actual en la etapa (a) comprende: una identificación de la unidad óptica de la red objetivo y una identificación del mensaje objetivo; en el que, dicha identificación de unidad óptica de red se utiliza para representar una unidad óptica de la red objetivo a la cual se envía dicho mensaje de solicitud de información sobre la clave actual; dicha identificación de mensaje objetivo se utiliza para indicar a dicha unidad óptica de la red objetivo que dicho mensaje de solicitud
es una solicitud de dicha información sobre la clave actual;
dicho mensaje de solicitud de información sobre la clave actual en la etapa (c) comprende: la identificación de la unidad óptica de la red origen, la identificación del mensaje origen y datos del cuerpo de información sobre la clave actual; en el que dicha identificación de la unidad óptica de la red origen se utiliza para representar una unidad óptica de red origen desde la cual es enviado dicho mensaje de respuesta de información sobre la clave actual; dicha identificación del mensaje origen se utiliza para indicar a dicho terminal óptico de línea que dicho mensaje de respuesta es una respuesta a dicho mensaje de solicitud de información sobre la clave actual; dichos datos del cuerpo de la información sobre la clave actual son utilizados por dicho terminal óptico de línea para obtener un cuerpo de información sobre la clave actual de dicha unidad óptica de red de dicho mensaje de respuesta.

3. Procedimiento, según la reivindicación 2, que comprende además:

dicha información sobre la clave actual es una clave actual; dicho mensaje de respuesta de información sobre la clave actual son mensajes de respuesta de la clave actual, y dichos datos del cuerpo de información sobre la clave actual son datos del cuerpo de la clave actual; dichos datos del cuerpo de la clave actual comprenden además índices de fragmentos de la clave actual y los cuerpos de la clave actual y en la etapa (c), según dichos índices de fragmentos de la clave actual, dicho terminal óptico de línea une múltiples fragmentos de dichos cuerpos de la clave actual en múltiples mensajes de respuesta de la clave actual de manera secuencial en una clave actual completa de dicha unidad óptica de red.

4. Procedimiento, según reivindicación 3, que comprende además:

en la etapa (a), dicho terminal óptico de línea envía un mensaje de solicitud sobre la clave actual a dicha unidad óptica de red; en la etapa (b), si dicha unidad óptica de red recibe dicho mensaje de solicitud sobre la clave actual, lee la clave actual almacenada localmente en dicha unidad óptica de red, divide el contenido leído en fragmentos, carga los fragmentos en múltiples mensajes de respuesta sobre la clave actual y envía los mensajes de respuesta de manera secuencial a dicho terminal óptico de línea; en la etapa (c), si dicho resultado de la comparación es que la clave actual de dicha unidad óptica de red es coherente con la clave actual almacenada localmente en dicho terminal óptico de línea, dicho terminal óptico de línea efectúa un procesamiento correspondiente a la coherencia de dichas claves actuales; si dicho resultado de la comparación es que la clave actual de dicha unidad óptica de red es incoherente con la clave actual almacenada localmente en dicho terminal óptico de línea, dicho terminal óptico de línea efectúa el procesamiento correspondiente a la incoherencia de dichas claves actuales.

5. Procedimiento, según la reivindicación 4, en el que, durante un proceso de conversión de clave, si dicho terminal óptico de línea no recibe un mensaje de acuse de recibo enviado por dicha unidad óptica de red cuando llega un número de bloque de conversión de clave (201), la implementación de dicha etapa (a) es iniciada por dicho terminal óptico de línea; en la etapa (c), el procesamiento correspondiente a la coherencia de dichas claves actuales es: dicho terminal óptico de línea envía información del éxito en la conversión de la clave con dicha unidad óptica de red (208); o el procesamiento correspondiente a la incoherencia de dichas claves actuales ejecutado por dicho terminal óptico de línea es: dicho terminal óptico de línea envía información de un fallo en la conversión de la clave con dicha unidad óptica de red (206).

6. Procedimiento, según la reivindicación 4, en el que, para encontrar el motivo de un fallo de servicio en dicha red óptica pasiva gigabit, el personal de mantenimiento del equipo inicia la implementación de dicha etapa (a) desde un sistema de gestión del elemento de red (301); en la etapa (c), el procesamiento correspondiente a la coherencia de de dichas claves actuales es: dicho terminal óptico de línea informa al sistema de gestión del elemento de red de la coherencia entre las claves actuales de dicho terminal óptico de línea y dicha unidad óptica de red (308); o el procesamiento correspondiente a la incoherencia de dichas claves actuales es: dicho terminal óptico de línea informa al sistema de gestión del elemento de red la incoherencia entre las claves actuales de dicho terminal óptico de línea y dicha unidad óptica de red (309).

7. Procedimiento, según la reivindicación 4, en el que la implementación de dicha etapa (a) es iniciada por dicho terminal óptico de línea en un tiempo definido; en la etapa (c), el procesamiento correspondiente a la coherencia de dichas claves actuales es: dicho terminal óptico de línea informa al sistema de gestión del elemento de red que las claves actuales de dicho terminal óptico de línea y dicha unidad óptica de red son coherentes (408); o el procesamiento correspondiente a la incoherencia de dichas claves actuales es: dicho terminal óptico de línea informa al sistema de gestión del elemento de red que las claves actuales de dicho terminal óptico de línea y dicha unidad óptica de red son incoherentes (409).

8. Procedimiento, según la reivindicación 4, que comprende además:

en la etapa (c), si dicho terminal óptico de línea no recibe dichos mensajes de respuesta de la clave actual en el periodo predeterminado, envía información de un fallo en la detección de la coherencia entre las claves actuales.

9. Procedimiento, según la reivindicación 2, que comprende además:

dicha información sobre la clave actual es un índice de la clave actual; dicho mensaje de respuesta de información sobre la clave actual es un mensaje de respuesta del índice de la clave actual, y dichos datos del cuerpo de información sobre la clave actual son datos del cuerpo de índice de la clave actual; en la etapa (a), dicho terminal óptico de línea envía un mensaje de solicitud del índice de la clave actual a dicha unidad óptica de red; en la etapa (b), si dicha unidad óptica de red recibe dicho mensaje de solicitud del índice de la clave actual, lee el índice de la clave actual almacenado localmente en dicha unidad óptica de red, carga el contenido leído como dichos datos del cuerpo de índice de la clave actual en dicho mensaje de respuesta del índice de la clave actual y envía el mensaje de respuesta a dicho terminal óptico de línea; en la etapa (c). dicho terminal óptico de línea obtiene dichos datos del cuerpo del índice de la clave actual como el índice de la clave actual de dicha unidad óptica de red; si dicho resultado de la comparación es que el índice de la clave actual de dicha unidad óptica de red es coherente con el índice de la clave actual almacenado localmente en dicho terminal óptico de línea, dicho terminal óptico de línea efectúa un procesamiento correspondiente a la coherencia de dichas claves actuales; si dicho resultado de la comparación es que el índice de la clave actual de dicha unidad óptica de red es incoherente con el índice de la clave actual almacenado localmente en dicho terminal óptico de línea, dicho terminal óptico de línea efectúa el procesamiento correspondiente a la incoherencia de dichas claves actuales.

10. Procedimiento, según la reivindicación 9, que comprende además:

en la etapa (c), si dicho terminal óptico de línea no recibe dichos mensajes de respuesta del índice de la clave actual en el periodo predeterminado, envía información de un fallo en la detección de la coherencia entre las claves actuales.

11. Procedimiento, según la reivindicación 2, que comprende además:

dicha información sobre la clave actual es un número del bloque de conversión de la clave; en la etapa (a), dicho terminal óptico de línea envía un mensaje de solicitud del número del bloque de conversión de la clave actual a dicha unidad óptica de red; en la etapa (b), si dicha unidad óptica de red recibe dicho mensaje de solicitud del número del bloque de conversión de la clave, lee el número del bloque de conversión de la clave almacenado localmente en dicha unidad óptica de red, carga el contenido leído como datos del cuerpo del número del bloque de conversión de la clave en un mensaje del respuesta del número de bloque de conversión de la clave y envía el mensaje de respuesta a dicho terminal óptico de línea; en la etapa (c), dicho terminal óptico de línea obtiene dichos datos del cuerpo del número de bloque de conversión de la clave como el número de bloque de conversión de la clave de dicha unidad óptica de red; si dicho resultado de la comparación es que el número del bloque de conversión de la clave de dicha unidad óptica de red es coherente con el número del bloque de conversión de la clave almacenado localmente en dicho terminal óptico de línea, dicho terminal óptico de línea efectúa el procesamiento correspondiente a la coherencia de dichas claves actuales; si dicho resultado de la comparación es que el número del bloque de conversión de dicha unidad óptica de red es incoherente con el número del bloque de conversión de la clave almacenado localmente en dicho terminal óptico de línea, dicho terminal óptico de línea efectúa el procesamiento correspondiente a la incoherencia de dichas claves actuales.

12. Procedimiento, según la reivindicación 11, que comprende además:

en la etapa (c), si dicho terminal óptico de línea no recibe dichos mensajes de respuesta del número del bloque de conversión de la clave en el periodo predeterminado, envía información de un fallo en la detección de la coherencia entre las claves actuales.

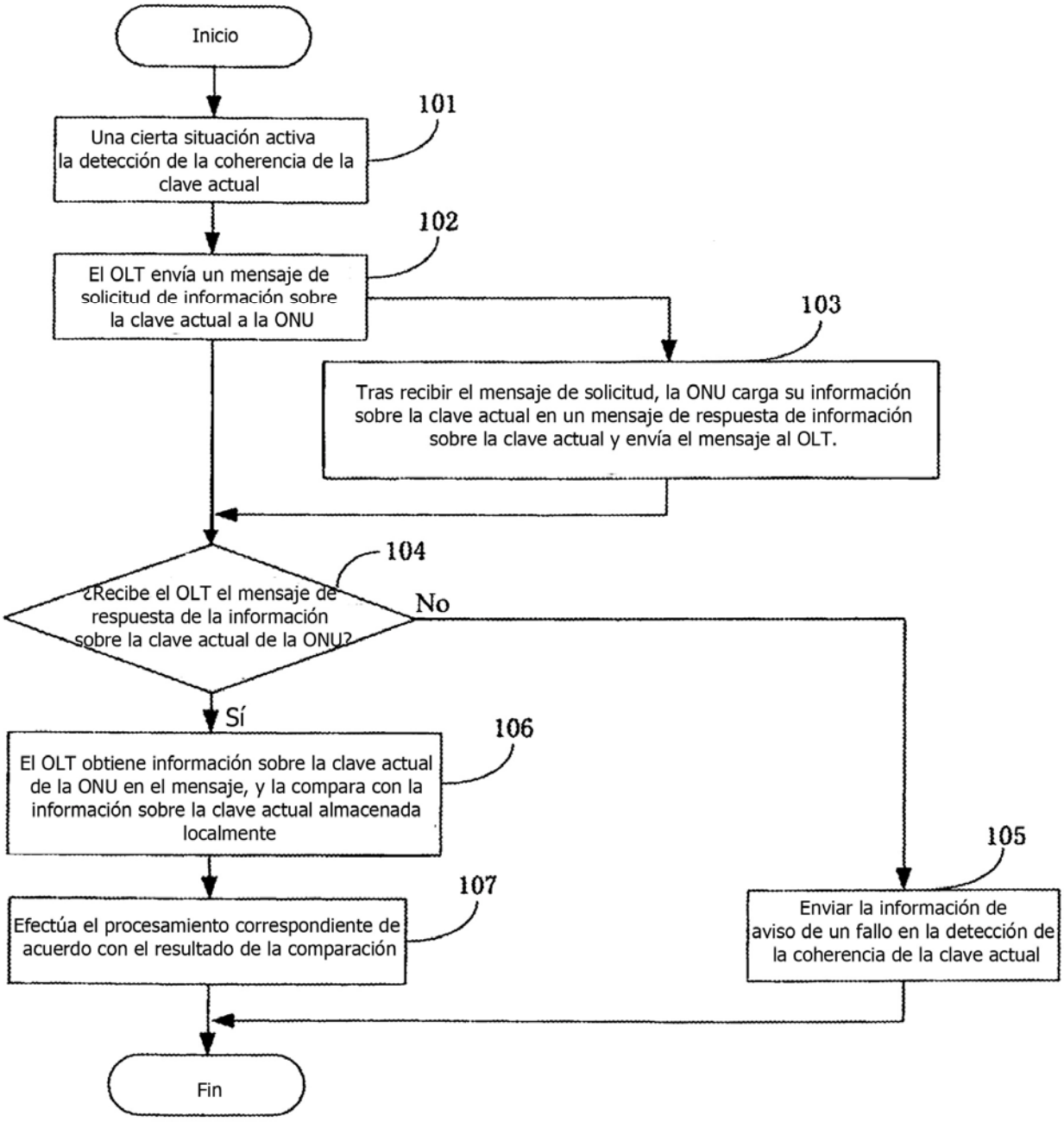
Inicio
101
Una cierta situación activa la detección de la coherencia de la clave actual
102
El OLT envía un mensaje de solicitud de información sobre la clave actual a la ONU
103
Tras recibir el mensaje de solicitud, la ONU carga su información sobre la clave actual en un mensaje de respuesta de información sobre la clave actual y envía el mensaje al OLT.
104
¿Recibe el OLT el mensaje de respuesta de la información sobre la clave actual de la ONU?
No
Sí
106
El OLT obtiene información sobre la clave actual de la ONU en el mensaje, y la compara con la información sobre la clave actual almacenada localmente
105
107
Efectúa el procesamiento correspondiente de acuerdo con el resultado de la comparación
Enviar la información de aviso de un fallo en la detección de la coherencia de la clave actual
Fin

FIG. 1

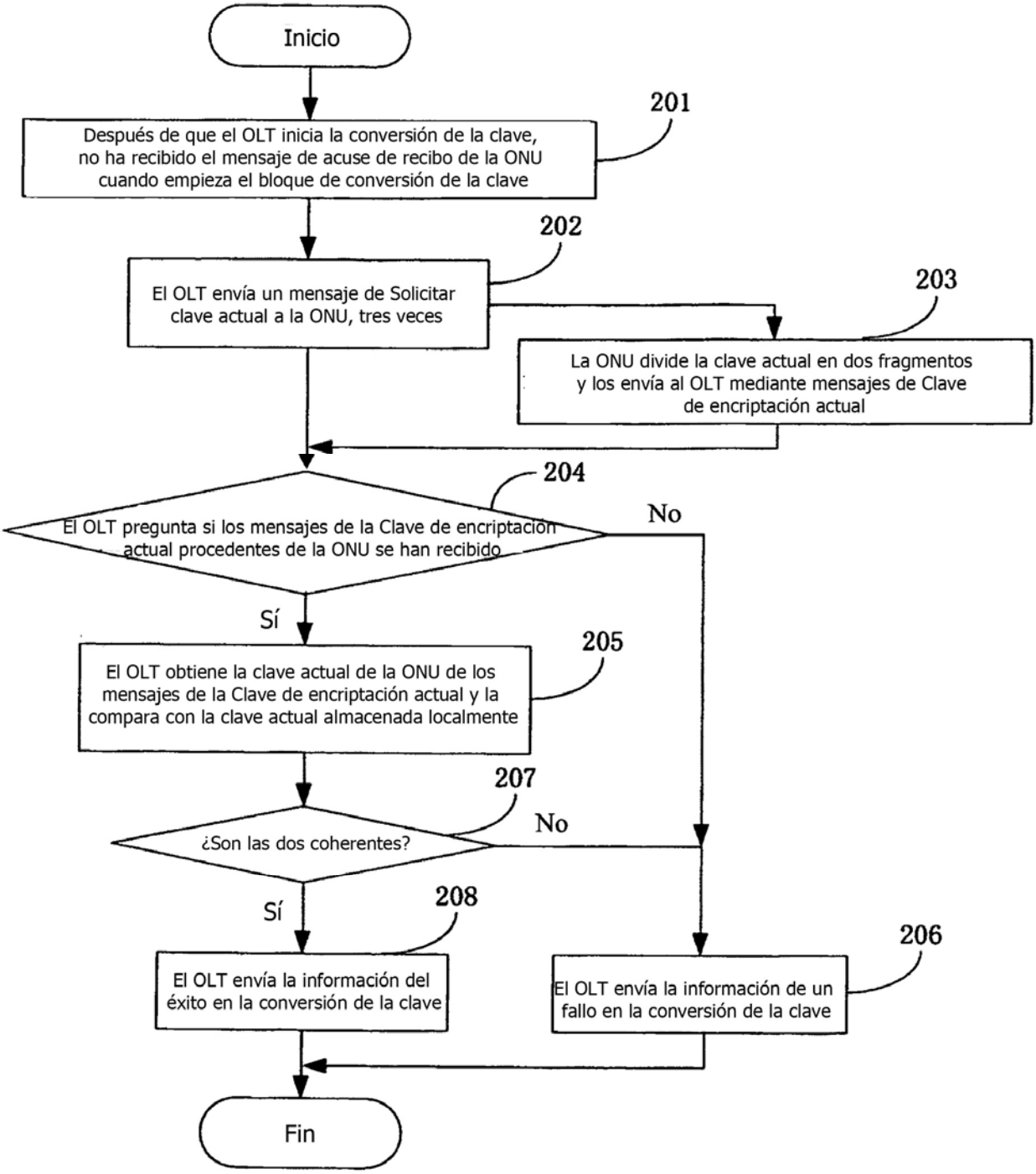
Inicio
201
Después de que el OLT inicia la conversión de la clave, no ha recibido el mensaje de acuse de recibo de la ONU cuando empieza el bloque de conversión de la clave
202
El OLT envía un mensaje de Solicitar clave actual a la ONU, tres veces
203
La ONU divide la clave actual en dos fragmentos y los envía al OLT mediante mensajes de Clave de encriptación actual
204
El OLT pregunta si los mensajes de la Clave de encriptación actual procedentes de la ONU se han recibido
No
Sí
205
El OLT obtiene la clave actual de la ONU de los mensajes de la Clave de encriptación actual y la compara con la clave actual almacenada localmente
207
¿Son las dos coherentes?
No
Sí
208
El OLT envía la información del éxito en la conversión de la clave
206
El OLT envía la información de un fallo en la conversión de la clave
Fin

FIG. 2

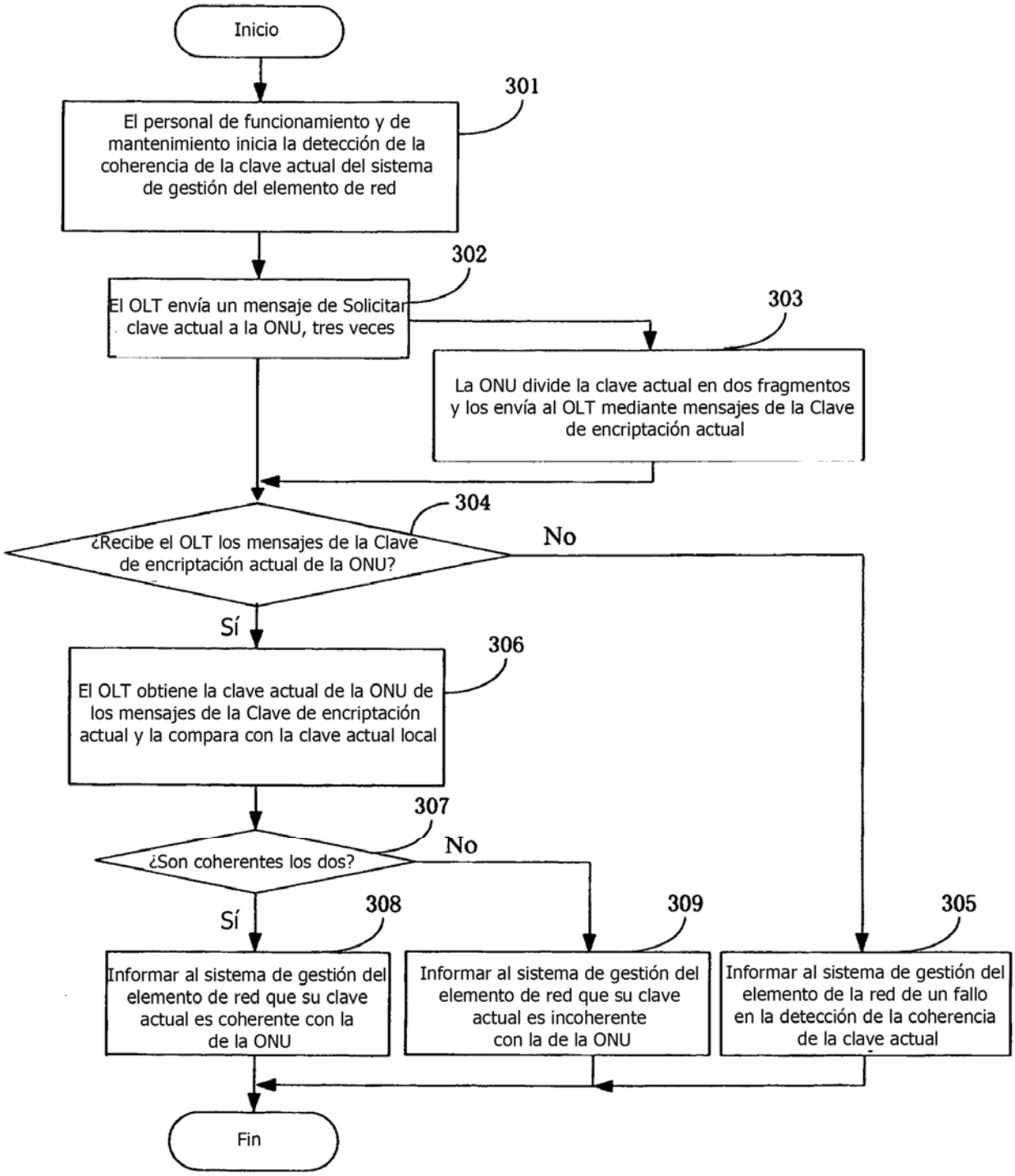
Inicio
301
El personal de funcionamiento y de mantenimiento inicia la detección de la coherencia de la clave actual del sistema de gestión del elemento de red
302
El OLT envía un mensaje de Solicitar clave actual a la ONU, tres veces
303
La ONU divide la clave actual en dos fragmentos y los envía al OLT mediante mensajes de la Clave de encriptación actual
304
¿Recibe el OLT los mensajes de la Clave de encriptación actual de la ONU?
No
Sí
306
El OLT obtiene la clave actual de la ONU de los mensajes de la Clave de encriptación actual y la compara con la clave actual local
307
¿Son coherentes los dos?
No
Sí
308
Informar al sistema de gestión del elemento de red que su clave actual es coherente con la de la ONU
309
Informar al sistema de gestión del elemento de red que su clave actual es incoherente con la de la ONU
305
Informar al sistema de gestión del elemento de la red de un fallo en la detección de la coherencia de la clave actual
Fin

FIG. 3

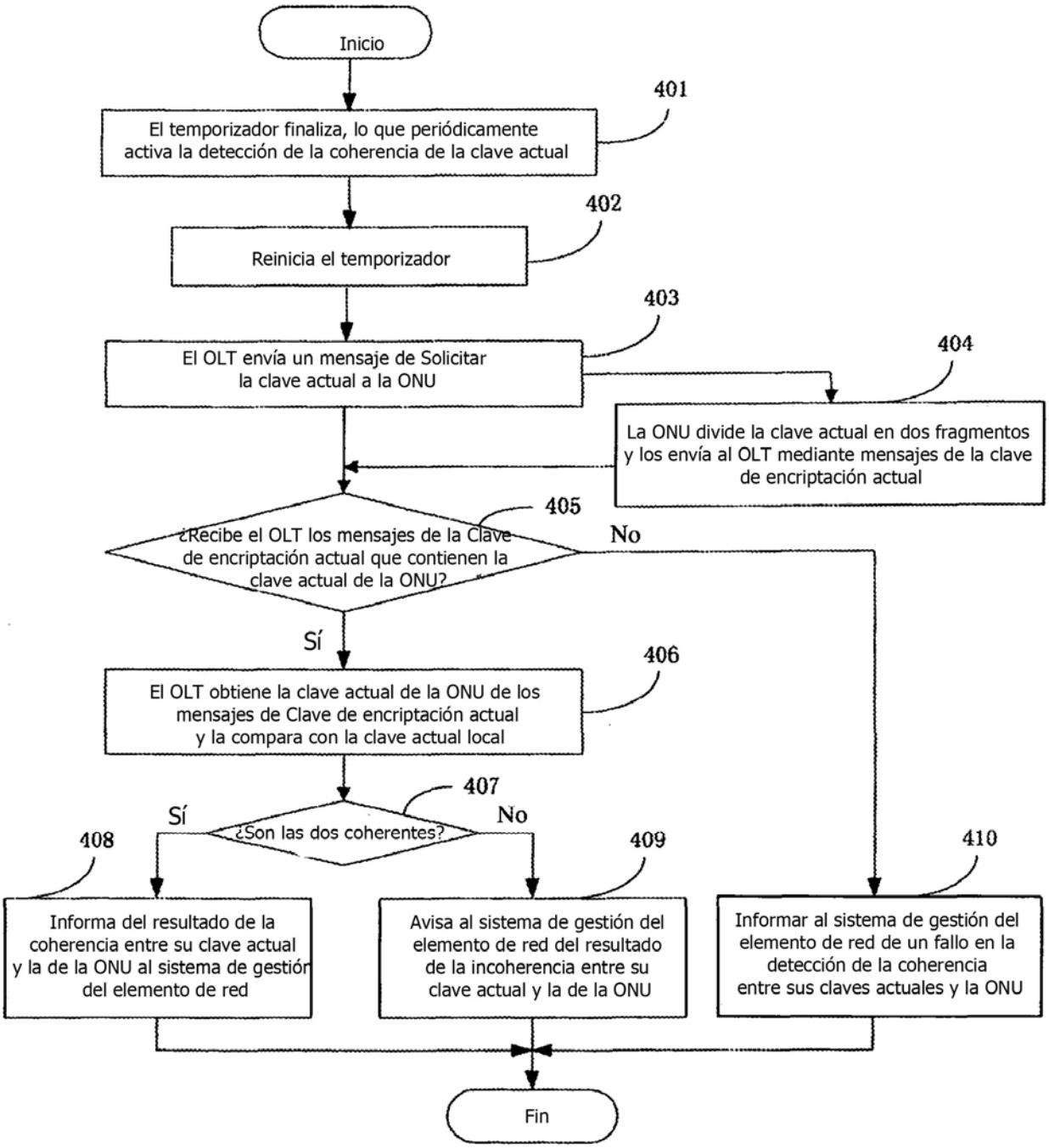
Inicio
401
El temporizador finaliza, lo que periódicamente activa la detección de la coherencia de la clave actual
402
Reinicia el temporizador
403
El OLT envía un mensaje de Solicitar la clave actual a la ONU
404
La ONU divide la clave actual en dos fragmentos y los envía al OLT mediante mensajes de la clave de encriptación actual
405
¿Recibe el OLT los mensajes de la Clave de encriptación actual que contienen la clave actual de la ONU?
No
Sí
406
El OLT obtiene la clave actual de la ONU de los mensajes de Clave de encriptación actual y la compara con la clave actual local
407
Sí
¿Son las dos coherentes?
No
408
Informa del resultado de la coherencia entre su clave actual y la de la ONU al sistema de gestión del elemento de red
409
Avisa al sistema de gestión del elemento de red del resultado de la incoherencia entre su clave actual y la de la ONU
410
Informar al sistema de gestión del elemento de red de un fallo en la detección de la coherencia entre sus claves actuales y la ONU
Fin

FIG. 4