(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 625 481**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/02 (2009.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **10.12.2013 PCT/CN2013/088947**

(87) Fecha y número de publicación internacional: **19.06.2014 WO14090130**

(96) Fecha de presentación y número de la solicitud europea: **10.12.2013 E 13863218 (7)**

(97) Fecha y número de publicación de la concesión europea: **05.04.2017 EP 2919498**

(54) Título: **Método, dispositivo y sistema para procesamiento de paquetes a través de una retransmisión**

(30) Prioridad:

10.12.2012 CN 201210528207

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.07.2017

(73) Titular/es:

HUAWEI DEVICE CO., LTD. (100.0%)
Building B2 Huawei Industrial Base Bantian, Longgang District, Shenzhen
Guangdong 518129, CN

(72) Inventor/es:

DING, ZHIMING y
SHU, GUIMING

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método, dispositivo y sistema para procesamiento de paquetes a través de una retransmisión.

Campo técnico

Las realizaciones de la presente invención se refieren al campo de las tecnologías de la comunicación y, en particular, a un método, aparato y sistema de procesamiento de paquetes.

Antecedentes

En el estándar 802.11ah del Instituto de Ingeniería Eléctrica y Electrónica (IEEE, por sus siglas en inglés), para extender un área de cobertura de un Punto de Acceso (PA), un dispositivo de retransmisión (Retransmisión) se añade, normalmente, entre una Estación (STA, por sus siglas en inglés) y el PA y un paquete encriptado se reenvía entre la STA y el PA mediante el uso de la Retransmisión. Según una implementación estándar, una clave de sesión PTKrd se negocia entre la Retransmisión y la STA, donde la Clave Transitoria por Pares (PTK, por sus siglas en inglés) es una clave transitoria entre nodos, r representa la Retransmisión y d representa un enlace descendente de la Retransmisión. Una clave de sesión PTKra se negocia también entre la Retransmisión y el PA, donde r representa la Retransmisión y a representa un enlace ascendente de la Retransmisión. En general, cuando la Retransmisión reenvía un paquete de enlace ascendente encriptado enviado al PA por la STA, la Retransmisión primero descifra el paquete de enlace ascendente encriptado mediante el uso de la PTKrd y luego encripta el paquete de enlace ascendente encriptado mediante el uso de la PTKra; cuando la Retransmisión reenvía un paquete de enlace descendente encriptado enviado a la STA por el PA, la Retransmisión primero descifra el paquete de enlace descendente encriptado mediante el uso de la PTKra y luego encripta el paquete de enlace descendente encriptado mediante el uso de la PTKrd.

El proceso de procesamiento anterior en el que la Retransmisión necesita llevar a cabo el descifrado y luego llevar a cabo la encriptación cuando reenvía un paquete encriptado entre la STA y el PA necesita ocupar algún tiempo de procesamiento, lo cual reduce la utilización del canal y aumenta el consumo de potencia adicional de la Retransmisión.

El documento US 2011/026505 A1 describe un dispositivo de comunicación inalámbrica, un sistema y un método de reenvío de tramas entre estaciones de un sistema de comunicación inalámbrica. El sistema de comunicación inalámbrica allí descrito incluye una estación de envío, una estación de reenvío y una estación de recepción.

La estación de envío allí descrita puede enviar una trama que incluye un campo de reenvío, un campo de dirección de estación de recepción, un campo de dirección de estación de envío y un campo de dirección de estación de reenvío. La estación de reenvío allí descrita puede recibir dicha trama y reenviar la trama en el estado en el que se encuentre a la estación de recepción.

Compendio

La presente invención provee un método (reivindicaciones 1 y 4), aparato (reivindicaciones 7 y 10) y sistema (reivindicación 13) de procesamiento de paquetes, los cuales se usan para resolver el problema existente de que un proceso de procesamiento en el que un dispositivo de retransmisión necesita llevar a cabo el descifrado y luego llevar a cabo la encriptación cuando reenvía un paquete entre una estación y un punto de acceso resulta en una utilización reducida del canal.

Según un primer aspecto, la presente invención provee un método de procesamiento de paquetes, aplicado a un escenario en el cual un dispositivo de retransmisión reenvía un paquete entre un primer nodo y un segundo nodo, que incluye:

recibir, por el primer nodo, un primer paquete enviado por el dispositivo de retransmisión, donde el primer paquete incluye datos en un segundo paquete enviado por el segundo nodo al dispositivo de retransmisión, los datos en el segundo paquete se encriptan mediante el uso de un segundo dato de autenticación adicional y una clave de sesión entre el primer nodo y el segundo nodo, el segundo dato de autenticación adicional se genera por el segundo nodo según al menos la información de dirección en un encabezado de paquete del segundo paquete mediante el uso de una segunda regla, y la información de dirección en el encabezado de paquete del segundo paquete indica que una parte receptora del segundo paquete es el dispositivo de retransmisión, una parte emisora es el segundo nodo y una siguiente parte receptora es el primer nodo;

generar, por el primer nodo, el primer dato de autenticación adicional según al menos la información de dirección en un encabezado de paquete del primer paquete mediante el uso de una primera regla, donde la información de dirección incluida en el encabezado de paquete del primer paquete indica que una parte receptora del primer paquete es el primer nodo, una parte emisora es el dispositivo de retransmisión y una parte emisora previa es el segundo nodo y el primer dato de autenticación adicional es igual al segundo dato de autenticación adicional; y

descifrar, por el primer nodo, datos en el primer paquete mediante el uso del primer dato de autenticación adicional y la clave de sesión entre el primer nodo y el segundo nodo.

Según el primer aspecto, en una primera manera de implementación, la primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional; o

la primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

Según el primer aspecto o la primera manera de implementación del primer aspecto, en una segunda manera de implementación, la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

Según el primer aspecto, o la primera o segunda manera de implementación del primer aspecto, en una tercera manera de implementación, el segundo paquete incluye además información de autenticación de mensajes de retransmisión, donde la información de autenticación de mensajes de retransmisión se genera por el segundo nodo mediante el uso de una clave de autenticación de mensajes entre el dispositivo de retransmisión y el segundo nodo; después de recibir el segundo paquete, el dispositivo de retransmisión verifica la información de autenticación de mensajes de retransmisión mediante el uso de la clave de autenticación de mensajes y envía el primer paquete al primer nodo si la verificación es exitosa.

Según el primer aspecto, o la primera, segunda o tercera manera de implementación del primer aspecto, en una cuarta manera de implementación, el primer nodo es una estación y el segundo nodo es un punto de acceso; o el primer nodo es un punto de acceso y el segundo nodo es una estación.

Según un segundo aspecto, la presente invención provee un método de procesamiento de paquetes, aplicado a un escenario en el cual un dispositivo de retransmisión reenvía un paquete entre un primer nodo y un segundo nodo, que incluye:

generar, por el segundo nodo, un segundo paquete, donde la información de dirección en un encabezado de paquete del segundo paquete indica que una parte receptora del segundo paquete es el dispositivo de retransmisión, una parte emisora es el segundo nodo y una siguiente parte receptora es el primer nodo;

generar, por el segundo nodo, el segundo dato de autenticación adicional según al menos la información de dirección en el encabezado de paquete del segundo paquete mediante el uso de una segunda regla y encriptar datos en el segundo paquete mediante el uso del segundo dato de autenticación adicional y una clave de sesión entre el primer nodo y el segundo nodo; y

enviar, por el segundo nodo, el segundo paquete encriptado al dispositivo de retransmisión, de modo que después de recibir el segundo paquete, el dispositivo de retransmisión envía un primer paquete al primer nodo, donde el primer paquete incluye los datos en el segundo paquete y la información de dirección incluida en un encabezado de paquete del primer paquete indica que una parte receptora del primer paquete es el primer nodo, una parte emisora es el dispositivo de retransmisión y una parte emisora previa es el segundo nodo; después de recibir el primer paquete, el primer nodo genera el primer dato de autenticación adicional según al menos la información de dirección en el encabezado de paquete del primer paquete mediante el uso de una primera regla y descifra datos en el primer paquete mediante el uso del primer dato de autenticación adicional y la clave de sesión entre el primer nodo y el segundo nodo, donde el primer dato de autenticación adicional es igual al segundo dato de autenticación adicional.

Según el segundo aspecto, en una primera manera de implementación, la primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional; o

la primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es igual a una secuencia de direcciones en

el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

Según el segundo aspecto o la primera manera de implementación del segundo aspecto, en una segunda manera de implementación, la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

Según el segundo aspecto, o la primera o segunda manera de implementación del segundo aspecto, en una tercera manera de implementación, el segundo paquete incluye además información de autenticación de mensajes de retransmisión, donde la información de autenticación de mensajes de retransmisión se genera por el segundo nodo mediante el uso de una clave de autenticación de mensajes entre el dispositivo de retransmisión y el segundo nodo; después de recibir el segundo paquete, el dispositivo de retransmisión verifica la información de autenticación de mensajes de retransmisión mediante el uso de la clave de autenticación de mensajes y envía el primer paquete al primer nodo si la verificación es exitosa.

Según el segundo aspecto, o la primera, segunda o tercera manera de implementación del segundo aspecto, en una cuarta manera de implementación, el primer nodo es una estación y el segundo nodo es un punto de acceso; o el primer nodo es un punto de acceso y el segundo nodo es una estación.

Según un tercer aspecto, la presente invención provee un método de procesamiento de paquetes, aplicado a un escenario en el cual un dispositivo de retransmisión reenvía un paquete entre un primer nodo y un segundo nodo, que incluye:

recibir, por el dispositivo de retransmisión, un segundo paquete enviado por el segundo nodo, donde la información de dirección en un encabezado de paquete del segundo paquete indica que una parte receptora del segundo paquete es el dispositivo de retransmisión, una parte emisora es el segundo nodo y una siguiente parte receptora es el primer nodo; los datos en el segundo paquete se encriptan mediante el uso del segundo dato de autenticación adicional y una clave de sesión entre el primer nodo y el segundo nodo; el segundo dato de autenticación adicional se genera por el segundo nodo según al menos la información de dirección en el encabezado de paquete del segundo paquete mediante el uso de una segunda regla; y

enviar, por el dispositivo de retransmisión, un primer paquete al primer nodo, donde el primer paquete incluye los datos en el segundo paquete y la información de dirección incluida en un encabezado de paquete del primer paquete indica que una parte receptora del primer paquete es el primer nodo, una parte emisora es el dispositivo de retransmisión y una parte emisora previa es el segundo nodo, de modo que el primer nodo genera el primer dato de autenticación adicional según al menos la información de dirección en el encabezado de paquete del primer paquete mediante el uso de una primera regla y descifra datos en el primer paquete mediante el uso del primer dato de autenticación adicional y la clave de sesión entre el primer nodo y el segundo nodo, donde el primer dato de autenticación adicional es igual al segundo dato de autenticación adicional.

Según el tercer aspecto, en una primera manera de implementación, la primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional; o

la primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

Según el tercer aspecto o la primera manera de implementación del tercer aspecto, en una segunda manera de implementación, la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

Según el tercer aspecto, o la primera o segunda manera de implementación del tercer aspecto, en una tercera manera de implementación, el segundo paquete incluye además información de autenticación de mensajes de retransmisión, donde la información de autenticación de mensajes de retransmisión se genera por el segundo nodo mediante el uso de una clave de autenticación de mensajes entre el dispositivo de retransmisión y el segundo nodo; después de recibir el segundo paquete, el dispositivo de retransmisión verifica la información de autenticación de mensajes de retransmisión mediante el uso de la clave de autenticación de mensajes y envía el primer paquete al primer nodo si la verificación es exitosa.

Según el tercer aspecto, o la primera, segunda o tercera manera de implementación del tercer aspecto, en una cuarta manera de implementación, el primer nodo es una estación y el segundo nodo es un punto de acceso; o el primer nodo es un punto de acceso y el segundo nodo es una estación.

Según un cuarto aspecto, la presente invención provee un aparato de procesamiento de paquetes, ubicado en un lado de un primer nodo, aplicado a un escenario en el cual un dispositivo de retransmisión reenvía un paquete entre el primer nodo y un segundo nodo, que incluye:

un módulo de recepción, configurado para recibir un primer paquete enviado por el dispositivo de retransmisión, donde el primer paquete incluye datos en un segundo paquete enviado por el segundo nodo al dispositivo de retransmisión; los datos en el segundo paquete se encriptan mediante el uso de un segundo dato de autenticación adicional y una clave de sesión entre el primer nodo y el segundo nodo; el segundo dato de autenticación adicional se genera por el segundo nodo según al menos la información de dirección en un encabezado de paquete del segundo paquete mediante el uso de una segunda regla y la información de dirección en el encabezado de paquete del segundo paquete indica que una parte receptora del segundo paquete es el dispositivo de retransmisión, una parte emisora es el segundo nodo y una siguiente parte receptora es el primer nodo; y

un módulo de descifrado, configurado para generar un primer dato de autenticación adicional según al menos la información de dirección en un encabezado de paquete del primer paquete mediante el uso de una primera regla, donde la información de dirección incluida en el encabezado de paquete del primer paquete indica que una parte receptora del primer paquete es el primer nodo, una parte emisora es el dispositivo de retransmisión y una parte emisora previa es el segundo nodo y los datos de autenticación adicionales generados mediante el uso de la primera regla son iguales a los datos de autenticación adicionales generados mediante el uso de la segunda regla; y descifrar datos en el primer paquete mediante el uso del primer dato de autenticación adicional y la clave de sesión entre el primer nodo y el segundo nodo, donde el primer dato de autenticación adicional es igual al segundo dato de autenticación adicional.

Según el cuarto aspecto, en una primera manera de implementación, la primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional; o

la primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

Según el cuarto aspecto o la primera manera de implementación del cuarto aspecto, en una segunda manera de implementación, la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

Según el cuarto aspecto, o la primera o segunda manera de implementación del cuarto aspecto, en una tercera manera de implementación, el segundo paquete incluye además información de autenticación de mensajes de retransmisión, donde la información de autenticación de mensajes de retransmisión se genera por el segundo nodo mediante el uso de una clave de autenticación de mensajes entre el dispositivo de retransmisión y el segundo nodo; después de recibir el segundo paquete, el dispositivo de retransmisión verifica la información de autenticación de mensajes de retransmisión mediante el uso de la clave de autenticación de mensajes y envía el primer paquete al primer nodo si la verificación es exitosa.

Según el cuarto aspecto, o la primera, segunda o tercera manera de implementación del cuarto aspecto, en una cuarta manera de implementación, el primer nodo es una estación y el segundo nodo es un punto de acceso; o el primer nodo es un punto de acceso y el segundo nodo es una estación.

Según un quinto aspecto, la presente invención provee un aparato de procesamiento de paquetes, ubicado en un lado de un segundo nodo, aplicado a un escenario en el cual un dispositivo de retransmisión reenvía un paquete entre el segundo nodo y un primer nodo, que incluye:

un módulo de generación de paquetes, configurado para generar un segundo paquete, donde la información de dirección en un encabezado de paquete del segundo paquete indica que una parte receptora del segundo paquete es el dispositivo de retransmisión, una parte emisora es el segundo nodo y una siguiente parte receptora es el primer nodo;

un módulo de encriptación, configurado para generar un segundo dato de autenticación adicional según al menos la información de dirección en el encabezado de paquete del segundo paquete mediante el uso de una segunda regla y encriptar datos en el segundo paquete mediante el uso del segundo dato de autenticación adicional y una clave de sesión entre el primer nodo y el segundo nodo; y

un módulo de envío, configurado para enviar el segundo paquete encriptado al dispositivo de retransmisión, de modo que después de recibir el segundo paquete, el dispositivo de retransmisión envía un primer paquete al primer nodo, donde el primer paquete incluye los datos en el segundo paquete y la información de dirección incluida en un encabezado de paquete del primer paquete indica que una parte receptora del primer paquete es el primer nodo, una parte emisora es el dispositivo de retransmisión y una parte emisora previa es el segundo nodo; después de recibir el primer paquete, el primer nodo genera el primer dato de autenticación adicional según al menos la información de dirección en el encabezado de paquete del primer paquete mediante el uso de una primera regla y descifra datos en el primer paquete mediante el uso del primer dato de autenticación adicional y la clave de sesión entre el primer nodo y el segundo nodo, donde el primer dato de autenticación adicional es igual al segundo dato de autenticación adicional.

Según el quinto aspecto, en una primera manera de implementación, la primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional; o

la primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

Según el quinto aspecto o la primera manera de implementación del quinto aspecto, en una segunda manera de implementación, la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

Según el quinto aspecto, o la primera o segunda manera de implementación del quinto aspecto, en una tercera manera de implementación, el segundo paquete incluye además información de autenticación de mensajes de retransmisión, donde la información de autenticación de mensajes de retransmisión se genera por el segundo nodo mediante el uso de una clave de autenticación de mensajes entre el dispositivo de retransmisión y el segundo nodo; después de recibir el segundo paquete, el dispositivo de retransmisión verifica la información de autenticación de mensajes de retransmisión mediante el uso de la clave de autenticación de mensajes y envía el primer paquete al primer nodo si la verificación es exitosa.

Según el quinto aspecto, o la primera, segunda o tercera manera de implementación del quinto aspecto, en una cuarta manera de implementación, el segundo nodo es una estación y el primer nodo es un punto de acceso; o el segundo nodo es un punto de acceso y el primer nodo es una estación.

Según un sexto aspecto, la presente invención provee un aparato de procesamiento de paquetes, ubicado en un lado de un dispositivo de retransmisión, aplicado a un escenario en el cual el dispositivo de retransmisión reenvía un paquete entre un primer nodo y un segundo nodo, que incluye:

un módulo de recepción, configurado para recibir un segundo paquete enviado por el segundo nodo, donde la información de dirección en un encabezado de paquete del segundo paquete indica que una parte receptora del segundo paquete es el dispositivo de retransmisión, una parte emisora es el segundo nodo y una siguiente parte receptora es el primer nodo; los datos en el segundo paquete se encriptan mediante el uso de segundos datos de autenticación adicionales y una clave de sesión entre el primer nodo y el segundo nodo; el segundo dato de autenticación adicional se genera por el segundo nodo según al menos la información de dirección en el encabezado de paquete del segundo paquete mediante el uso de una segunda regla; y

un módulo de envío, configurado para enviar un primer paquete al primer nodo, donde el primer paquete incluye los datos en el segundo paquete y la información de dirección incluida en un encabezado de paquete del primer paquete indica que una parte receptora del primer paquete es el primer nodo, una parte emisora es el dispositivo de retransmisión y una parte emisora previa es el segundo nodo, de modo que el primer nodo genera el primer dato de autenticación adicional según al menos la información de dirección en el encabezado de paquete del primer paquete mediante el uso de una primera regla y descifra datos en el primer paquete mediante el uso del primer dato de autenticación adicional y la clave de sesión entre el primer nodo y el segundo nodo, donde el primer dato de autenticación adicional es igual al segundo dato de autenticación adicional.

Según el sexto aspecto, en una primera manera de implementación, la primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional; o

la primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

Según el sexto aspecto o la primera manera de implementación del sexto aspecto, en una segunda manera de implementación, la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

Según el sexto aspecto, o la primera o segunda manera de implementación del sexto aspecto, en una tercera manera de implementación, el segundo paquete incluye además información de autenticación de mensajes de retransmisión, donde la información de autenticación de mensajes de retransmisión se genera por el segundo nodo mediante el uso de una clave de autenticación de mensajes entre el dispositivo de retransmisión y el segundo nodo; después de recibir el segundo paquete, el dispositivo de retransmisión verifica la información de autenticación de mensajes de retransmisión mediante el uso de la clave de autenticación de mensajes y envía el primer paquete al primer nodo si la verificación es exitosa.

Según el sexto aspecto, o la primera, segunda o tercera manera de implementación del sexto aspecto, en una cuarta manera de implementación, el primer nodo es una estación y el segundo nodo es un punto de acceso; o el primer nodo es un punto de acceso y el segundo nodo es una estación.

Según un séptimo aspecto, la presente invención provee un sistema de procesamiento de paquetes, aplicado a un escenario en el cual un dispositivo de retransmisión reenvía un paquete entre un primer nodo y un segundo nodo, que incluye: el primer nodo, el segundo nodo y el dispositivo de retransmisión, donde

el primer nodo incluye el aparato de procesamiento de paquetes según el cuarto aspecto;

el segundo nodo incluye el aparato de procesamiento de paquetes según el quinto aspecto; y

el dispositivo de retransmisión incluye el aparato de procesamiento de paquetes según el sexto aspecto.

En la presente invención, un primer nodo recibe un primer paquete enviado por un dispositivo de retransmisión, donde el primer paquete incluye datos en un segundo paquete enviado por un segundo nodo al dispositivo de retransmisión; los datos en el segundo paquete se encriptan mediante el uso de un segundo dato de autenticación adicional y una clave de sesión entre el primer nodo y el segundo nodo; el segundo dato de autenticación adicional se genera por el segundo nodo según al menos la información de dirección en un encabezado de paquete del segundo paquete mediante el uso de una segunda regla; el primer nodo genera un primer dato de autenticación adicional según al menos la información de dirección en el primer paquete mediante el uso de una primera regla, donde una secuencia de direcciones en el primer dato de autenticación adicional generado por el primer nodo según la primera regla es igual a una secuencia de direcciones en el segundo dato de autenticación adicional generado por el segundo nodo según la segunda regla; el primer nodo descifra además datos en el primer paquete mediante el uso del primer dato de autenticación adicional y la clave de sesión entre el primer nodo y el segundo nodo. De esta manera, cuando recibe el segundo paquete enviado por el segundo nodo, el dispositivo de retransmisión no necesita enviar, después de llevar a cabo, en primer lugar, el descifrado y luego llevar a cabo la encriptación en el segundo paquete, el primer paquete al primer nodo, ahorrando, por consiguiente, tiempo de procesamiento de paquetes del dispositivo de retransmisión, mejorando la utilización del canal y reduciendo el consumo de potencia adicional del dispositivo de retransmisión.

Breve descripción de los dibujos

Con el fin de describir las soluciones técnicas en las realizaciones de la presente invención o en la técnica anterior de forma más clara, a continuación se introducen brevemente los dibujos anexos requeridos para describir las realizaciones o la técnica anterior. De manera aparente, los dibujos anexos en la siguiente descripción muestran algunas realizaciones de la presente invención y las personas con experiencia ordinaria en la técnica pueden derivar otros dibujos a partir de dichos dibujos anexos sin esfuerzos creativos.

La Figura 1 es un diagrama esquemático de un formato de trama, de un paquete encriptado mediante el uso de un CCMP, aplicado a una realización de la presente invención;

la Figura 2 es un diagrama esquemático de un formato de un encabezado MAC aplicado a una realización de la presente invención;

la Figura 3 es un diagrama de flujo esquemático de un método de procesamiento de paquetes según una realización de la presente invención;

la Figura 4 es un diagrama de arquitectura esquemático de un sistema de procesamiento de paquetes aplicado a una realización de la presente invención;

la Figura 5 es un diagrama de flujo esquemático de un método de procesamiento de paquetes según otra realización de la presente invención;

la Figura 6 es un diagrama de flujo esquemático de un método de procesamiento de paquetes según otra realización de la presente invención;

la Figura 7 es un diagrama estructural esquemático de un aparato de procesamiento de paquetes según una realización de la presente invención;

la Figura 8 es un diagrama estructural esquemático de un aparato de procesamiento de paquetes según otra realización de la presente invención;

la Figura 9 es un diagrama estructural esquemático de un aparato de procesamiento de paquetes según otra realización de la presente invención;

la Figura 10 es un diagrama estructural esquemático de un aparato de procesamiento de paquetes según otra realización de la presente invención;

la Figura 11 es un diagrama estructural esquemático de un aparato de procesamiento de paquetes según otra realización de la presente invención;

la Figura 12 es un diagrama estructural esquemático de un aparato de procesamiento de paquetes según otra realización de la presente invención; y

la Figura 13 es un diagrama estructural esquemático de un sistema de procesamiento de paquetes según una realización de la presente invención.

Descripción de las realizaciones

Con el propósito de esclarecer los objetivos, soluciones técnicas y ventajas de las realizaciones de la presente invención, a continuación se describen, de forma clara y completa, las soluciones técnicas en las realizaciones de la presente invención con referencia a los dibujos anexos en las realizaciones de la presente invención. De manera aparente, las realizaciones descritas son algunas de, pero no todas, las realizaciones de la presente invención. Todas las otras realizaciones que las personas con experiencia ordinaria en la técnica obtengan según las realizaciones de la presente invención sin esfuerzos creativos caerán dentro del alcance de protección de la presente invención.

En el estándar 802.11, una STA se refiere a un dispositivo que admite el protocolo 802.11 e incluye un PA. Se hace referencia a un PA como un PA STA en el estándar y se hace referencia a una STA que no es un PA como una STA que no es un PA en el estándar. Una estación STA descrita en la presente invención se refiere a un terminal de aplicación, es decir, una STA que no es un PA; un punto de acceso PA descrito en la presente invención puede ser un PA STA en el estándar; un dispositivo de retransmisión descrito en la presente invención puede ser una STA de Retransmisión en el estándar.

En el estándar IEEE802.11ah, los datos en un paquete se encriptan, normalmente, mediante el uso de un Modo Conteo con el Protocolo del Código de Autenticación de Mensajes en Cadena para el Bloqueo de Cifrado (CCMP, por sus siglas en inglés). La Figura 1 es un diagrama esquemático de un formato de trama, de un paquete encriptado mediante el uso del CCMP, aplicado a una realización de la presente invención. En general, se hace referencia a un encabezado de paquete como un encabezado de Control de Acceso al Medio (encabezado MAC, por sus siglas en inglés). Como se muestra en la Figura 1, un encabezado MAC y un Encabezado CCMP participan en un cálculo de encriptación, pero no se encriptan ellos mismos; los datos (Datos) y el código de integridad de mensajes (MIC, por sus siglas en inglés) que se encuentran en un paquete a enviarse se encriptan; una secuencia de verificación de trama (FCS, por sus siglas en inglés) se usa para verificar si ocurre un error en una trama en un proceso de transmisión. Un formato de trama, de un paquete encriptado mediante el uso del CCMP, aplicable a la presente realización de la presente invención, no se limita al formato de trama que se muestra en la Figura 1.

En una aplicación real, antes de la encriptación, mediante el uso de un algoritmo CCMP, los Datos y un código de integridad de mensajes MIC que se encuentran en un paquete a enviarse, un PA o una STA necesitan generar datos

de autenticación adicionales (AAD, por sus siglas en inglés) mediante el uso de la información de dirección en un encabezado MAC del paquete a enviarse. La Figura 2 es un diagrama esquemático de un formato de un encabezado MAC aplicado a una realización de la presente invención. Como se muestra en la Figura 2, el encabezado MAC incluye múltiples datos de dirección, donde una secuencia de direcciones incluida en la información de dirección es una dirección D1, una dirección D2, una dirección D3 y una dirección D4, donde D1 es una dirección de recepción, es decir, una dirección de un nodo que recibe, actualmente, un paquete; D2 es una dirección de envío, es decir, una dirección de un nodo que envía, actualmente, un paquete. Cuando una dirección de destino es la dirección de recepción, la dirección de destino no necesita escribirse en el encabezado MAC; o cuando una dirección de destino no es la dirección de recepción, D3 es la dirección de destino; la dirección de destino es, en general, una dirección de un nodo que luego recibe un paquete. Cuando una dirección de origen es la dirección de envío, la dirección de origen no necesita escribirse en el encabezado MAC; o cuando una dirección de origen no es la dirección de envío, la dirección de origen necesita escribirse en D3 o D4; la dirección de origen es, en general, una dirección de un nodo que previamente envía un paquete. El formato, de un encabezado MAC, aplicable a la presente realización de la presente invención, no se limita al formato que se muestra en la Figura 2.

Se puede saber, a partir de la estructura del encabezado MAC que se muestra en la Figura 2, que cada vez que se reenvía un paquete por una Retransmisión, la secuencia de las direcciones en el encabezado MAC seguramente cambia. Dado que la secuencia de las direcciones en el encabezado MAC cambia en un proceso de reenvío de paquetes, los datos de autenticación adicionales AAD generados según la secuencia de las direcciones en el encabezado MAC también cambian; por lo tanto, después de recibir el paquete, la Retransmisión necesita descifrar los datos encriptados en el paquete recibido, reescribir la información de dirección reenviada en el encabezado MAC, luego generar datos de autenticación adicionales según la información de dirección reescrita y encriptar los datos descifrados mediante el uso de los datos de autenticación adicionales regenerados. De esta manera, el tiempo de procesamiento de paquetes de la Retransmisión aumenta, se reduce la utilización del canal y aumenta el consumo de potencia adicional de la Retransmisión.

Considerando el problema existente anterior, las realizaciones de la presente invención proveen un método de procesamiento de paquetes, el cual se aplica a un escenario en el que un dispositivo de retransmisión reenvía un paquete entre un primer nodo y un segundo nodo y puede resolver el problema existente de que un proceso de procesamiento en el que un dispositivo de retransmisión necesita llevar a cabo el descifrado y luego llevar a cabo la encriptación cuando reenvía un paquete entre una estación y un punto de acceso resulta en la utilización reducida del canal.

Se debe notar que en las siguientes realizaciones, si el primer nodo es un punto de acceso PA, el segundo nodo es una estación STA; o si el primer nodo es una estación STA, el segundo nodo es un punto de acceso PA.

La Figura 3 es un diagrama de flujo esquemático de un método de procesamiento de paquetes según una realización de la presente invención, donde el método se aplica a un escenario en el cual un dispositivo de retransmisión reenvía un paquete entre un primer nodo y un segundo nodo. Como se muestra en la Figura 3, el método de procesamiento de paquetes específicamente incluye:

301: un primer nodo recibe un primer paquete enviado por un dispositivo de retransmisión, donde el primer paquete incluye datos en un segundo paquete enviado por un segundo nodo al dispositivo de retransmisión; los datos en el segundo paquete se encriptan mediante el uso de un segundo dato de autenticación adicional y una clave de sesión entre el primer nodo y el segundo nodo, el segundo dato de autenticación adicional se genera por el segundo nodo según al menos la información de dirección en un encabezado de paquete del segundo paquete mediante el uso de una segunda regla y la información de dirección en el encabezado de paquete del segundo paquete indica que una parte receptora del segundo paquete es el dispositivo de retransmisión, una parte emisora es el segundo nodo y una siguiente parte receptora es el primer nodo.

En una implementación específica, la Figura 4 es un diagrama de arquitectura esquemático de un sistema de procesamiento de paquetes aplicado a una realización de la presente invención. Como se muestra en la Figura 4, suponiendo que un punto de acceso PA es un primer nodo y una estación STA es un segundo nodo, la STA genera un segundo paquete, donde una secuencia de direcciones en la información de dirección en un encabezado de paquete (el encabezado MAC que se muestra en la Figura 2) del segundo paquete es que: D1 es una dirección de una Retransmisión, una dirección de envío D2 que también es una dirección de origen es una dirección de la STA y una dirección D3 de una siguiente parte receptora es una dirección del PA. La STA genera un segundo dato de autenticación adicional AAD según al menos la información de dirección en el encabezado de paquete del segundo paquete mediante el uso de una segunda regla y la STA luego encripta datos en el segundo paquete mediante el uso del segundo AAD y una clave de sesión entre la STA y el PA y envía el segundo paquete encriptado a la Retransmisión.

Después de recibir el segundo paquete enviado por la STA, la Retransmisión puede llevar a cabo el reensamblado para obtener un primer paquete, lo cual puede ser, específicamente, que: se completa la información de dirección en un encabezado de paquete (encabezado MAC) del primer paquete, es decir, una dirección de recepción D1 que

también es una dirección de destino es la dirección del PA, una dirección de envío D2 es la dirección de la Retransmisión y una dirección de origen D3 es la dirección de la STA; los datos encriptados en el segundo paquete se completan en una parte de Datos en el primer paquete. El primer paquete se puede obtener también después de actualizar simplemente la información de dirección en el segundo paquete. En la presente realización, la Retransmisión puede directamente completar los datos encriptados en el segundo paquete en la parte de Datos en el primer paquete sin llevar a cabo el procesamiento de descifrado en el segundo paquete enviado por la STA y la Retransmisión luego envía el primer paquete al PA.

De manera opcional, el segundo paquete enviado por la STA a la Retransmisión puede incluir además información de autenticación de mensajes de retransmisión, donde la información de autenticación de mensajes de retransmisión se puede generar por la STA mediante el uso de una clave de autenticación de mensajes entre la STA y la Retransmisión; después de recibir el segundo paquete, la Retransmisión verifica la información de autenticación de mensajes de retransmisión, mediante el uso de la clave de autenticación de mensajes y envía el primer paquete al PA si la verificación es exitosa.

302: el primer nodo genera el primer dato de autenticación adicional según al menos la información de dirección en un encabezado de paquete del primer paquete mediante el uso de una primera regla, donde la información de dirección incluida en el encabezado de paquete del primer paquete indica que una parte receptora del primer paquete es el primer nodo, una parte emisora es el dispositivo de retransmisión y una parte emisora previa es el segundo nodo y el primer dato de autenticación adicional es igual al segundo dato de autenticación adicional.

Se debe notar que la presente realización de la presente invención se aplica a un escenario en el que un dispositivo de retransmisión reenvía un paquete entre un primer nodo y un segundo nodo; por lo tanto, después de recibir el primer paquete, el PA necesita determinar, según la información de dirección en el encabezado de paquete del primer paquete, si el primer paquete se reenvía por la Retransmisión. Suponiendo que la dirección de envío D2 es la dirección de la Retransmisión, se puede determinar que el primer paquete se reenvía por la Retransmisión; o después de que el PA recibe el primer paquete, se supone que el encabezado de paquete del primer paquete lleva un bit indicador enviado por la Retransmisión, por ejemplo, cuando el bit indicador es 1, indica que el primer paquete se envía por la Retransmisión y cuando el bit indicador es 0, indica que el primer paquete no se envía por la Retransmisión. En una implementación específica, el bit indicador enviado por la Retransmisión se puede identificar mediante el uso de un bit reservado en el control de trama (FC) del encabezado MAC.

Dado que seguramente que cada vez que un paquete se reenvía por la Retransmisión, una secuencia de direcciones en un encabezado de paquete cambie, la secuencia de las direcciones en el primer paquete recibido por el PA y enviado por la Retransmisión es diferente de la secuencia de las direcciones en el segundo paquete enviado por la STA a la Retransmisión. Con el fin de implementar ello, la Retransmisión no necesita llevar a cabo el procesamiento de descifrado en los datos encriptados en el segundo paquete enviado por la STA y el PA puede descifrar los datos encriptados que se incluyen en el primer paquete enviado por la Retransmisión y se encuentra en el segundo paquete desde la STA, el primer dato de autenticación adicional generado por el PA según la información de dirección en el encabezado de paquete del primer paquete mediante el uso de la primera regla necesita ser igual al segundo dato de autenticación adicional generado por la STA según la información de dirección en el encabezado de paquete del segundo paquete mediante el uso de la segunda regla. En una implementación específica:

si la primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es igual a la secuencia de las direcciones en el encabezado de paquete del primer paquete, la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es diferente de la secuencia de las direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional generado según la segunda regla es igual a la secuencia de las direcciones en el primer dato de autenticación adicional generado según la primera regla; o

si la primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es diferente de la secuencia de las direcciones en el encabezado de paquete del primer paquete, la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional generado según la segunda regla es igual a la secuencia de las direcciones en el primer dato de autenticación adicional generado según la primera regla.

Como se muestra en la Figura 4, suponiendo que el segundo nodo, a saber, la STA, genera el segundo dato de autenticación adicional según la información de dirección en el encabezado de paquete del segundo paquete mediante el uso de la segunda regla, donde la segunda regla es que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el encabezado de paquete del segundo paquete, el primer nodo, a saber, el PA, genera el primer dato de autenticación adicional según la información de dirección en el encabezado de paquete del primer paquete mediante el uso de la primera regla, donde la primera regla es que la secuencia de las direcciones en el primer dato de autenticación adicional es diferente de la secuencia de las direcciones en el encabezado de paquete del primer paquete, de modo que la secuencia de las direcciones

en el segundo dato de autenticación adicional generado por el segundo nodo, a saber, la STA, según la información de dirección en el encabezado de paquete del segundo paquete mediante el uso de la segunda regla es igual a la secuencia de las direcciones en el primer dato de autenticación adicional generado por el primer nodo, a saber, el PA, según la información de dirección en el encabezado de paquete del primer paquete mediante el uso de la primera regla.

En una implementación específica, por ejemplo, una tabla de mapeo de direcciones se puede preestablecer en el primer nodo, a saber, el PA, donde una relación de mapeo, de cada dirección en el encabezado de paquete del primer paquete enviado por la Retransmisión, en un lugar de cada campo de dirección en el AAD generado por el PA se establece en la tabla de mapeo de direcciones.

La Tabla 1 es una tabla de mapeo de direcciones preestablecida en la presente realización de la presente invención. Como se muestra en la Figura 1, el enlace descendente representa que el PA envía un paquete a la STA mediante el uso de la Retransmisión y el enlace ascendente representa que la STA envía un paquete al PA mediante el uso de la Retransmisión. Con el fin de implementar ello, el PA descifra, de manera correcta, el dato encriptado que se incluye en el primer paquete enviado por la Retransmisión y se encuentra en el segundo paquete desde la STA, la secuencia de las direcciones en el AAD generado por el PA necesita ser coherente con la secuencia de las direcciones en el AAD generado por la STA.

Tabla 1

Dirección	Primer campo de dirección en AAD del PA	Segundo campo de dirección en AAD del PA	Tercer campo de dirección en AAD del PA	Cuarto campo de dirección en AAD del PA
Enlace descendente	D3 en paquete enviado por el PA a la Retransmisión	D1 en paquete enviado por el PA a la Retransmisión	D2 en paquete enviado por el PA a la Retransmisión	
Enlace ascendente	D2 en paquete enviado por la Retransmisión al PA	D3 en paquete enviado por la Retransmisión al PA	D1 en paquete enviado por la Retransmisión al PA	

Se debe notar que, de manera opcional, el AAD del PA puede tener un cuarto campo de dirección y el contenido que existe cuando el cuarto campo de dirección existe no se muestra específicamente en la Tabla 1.

Según el hecho anterior de que el primer nodo, a saber, el PA, ha determinado que el primer paquete se envía por la Retransmisión, el PA adquiere la información de dirección en el encabezado de paquete del primer paquete, donde la información de dirección es, específicamente, que: la dirección de recepción D1 que también es la dirección de destino es la dirección del PA, la dirección de envío D2 es la dirección de la Retransmisión y la dirección de origen D3 es la dirección de la STA; y consulta la tabla de mapeo de direcciones que se muestra en la Tabla 1 para obtener una secuencia de direcciones mapeadas que corresponde a la secuencia adquirida de las direcciones en el encabezado de paquete del primer paquete, es decir, la dirección de recepción D1 (la dirección del PA) en el encabezado de paquete del primer paquete corresponde a D3 en las direcciones mapeadas, la dirección de envío D2 (la dirección de la Retransmisión) en el encabezado de paquete del primer paquete corresponde a D1 en las direcciones mapeadas y la dirección de origen D3 (la dirección de la STA) en el encabezado de paquete del primer paquete corresponde a D2 en las direcciones mapeadas.

Luego, la generación, mediante el PA, de los datos de autenticación adicionales correspondientes según la información de dirección en el encabezado de paquete del primer paquete mediante el uso de la primera regla puede ser, específicamente: completar, por el PA según la secuencia de las direcciones mapeadas que corresponde a la secuencia de las direcciones en el encabezado de paquete del primer paquete, las direcciones mapeadas de forma separada en los lugares correspondientes de D1, D2 y D3 en un encabezado MAC de los datos de autenticación adicionales generados, es decir, completar la dirección de la Retransmisión en el lugar de D1, completar la dirección de la STA en el lugar de D2 y completar la dirección del PA en el lugar de D3, para generar el primer dato de autenticación adicional, donde la secuencia de las direcciones en el primer dato de autenticación adicional es la dirección de la Retransmisión, la dirección de la STA y la dirección del PA. En el presente caso, el primer nodo, a saber, el PA, genera el primer dato de autenticación adicional correspondiente según la información de dirección en el encabezado del primer paquete mediante el uso de la primera regla, donde la primera regla es que la secuencia de las direcciones en el primer dato de autenticación adicional es diferente de la secuencia de las direcciones en el encabezado del primer paquete y luego la segunda regla es que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el encabezado del segundo paquete. Dado que la secuencia de las direcciones en la información de dirección en el encabezado del segundo paquete es que:

D1 es la dirección de la Retransmisión, la dirección de envío D2 que también es la dirección de origen es la dirección de la STA y la dirección D3 del siguiente nodo de recepción es la dirección del PA, la secuencia de las direcciones en el segundo dato de autenticación adicional correspondiente generado por el segundo nodo, a saber, la STA, según la información de dirección en el encabezado del segundo paquete mediante el uso de la segunda regla es la dirección de la Retransmisión, la dirección de la STA y la dirección del PA. De esta manera, la secuencia de las direcciones en el primer AAD generado por el PA es igual a la secuencia de las direcciones en el segundo AAD generado por la STA; por lo tanto, el PA puede descifrar, de forma correcta, los datos encriptados que se incluyen en el primer paquete enviado por la Retransmisión y se encuentran en el segundo paquete desde la STA.

Se debe notar que, como se muestra en la Figura 4, suponiendo que el segundo nodo, a saber, la STA, genera el segundo dato de autenticación adicional según la información de dirección en el encabezado de paquete del segundo paquete mediante el uso de la segunda regla, donde la segunda regla es que la secuencia de las direcciones en el segundo dato de autenticación adicional es diferente de la secuencia de las direcciones en el encabezado de paquete del segundo paquete, el primer nodo, a saber, el PA, genera el primer dato de autenticación adicional según la información de dirección en el encabezado de paquete del primer paquete mediante el uso de la primera regla, donde la primera regla es que la secuencia de las direcciones en el primer dato de autenticación adicional es igual a la secuencia de las direcciones en el encabezado de paquete del primer paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional generado por el segundo nodo, a saber, la STA, según la información de dirección en el encabezado de paquete del segundo paquete mediante el uso de la segunda regla es igual a la secuencia de las direcciones en el primer dato de autenticación adicional generado por el primer nodo, a saber, el PA, según la información de dirección en el encabezado de paquete del primer paquete mediante el uso de la primera regla. En una implementación específica, por ejemplo, una tabla de mapeo de direcciones se puede preestablecer en el segundo nodo, a saber, la STA, donde una relación de mapeo, de cada dirección en el encabezado de paquete del primer paquete enviado por la Retransmisión, en un lugar de cada campo de dirección en el AAD generado por el segundo nodo, a saber, la STA, se puede establecer en la tabla de mapeo de direcciones y un principio de mapeo no se describe nuevamente.

303: el primer nodo descifra datos en el primer paquete mediante el uso del primer dato de autenticación adicional generado según la primera regla y la clave de sesión entre el primer nodo y el segundo nodo.

En una implementación específica, el primer nodo puede llevar a cabo una serie de funciones según un algoritmo CCMP mediante el uso del primer dato de autenticación adicional, la información de número de secuencia de paquete en un encabezado CCMP en el primer paquete, la clave de sesión entre el primer nodo y el segundo nodo y similares para generar un primer valor de clave de una cadena de claves, luego llevar a cabo un cálculo en el primer valor de clave con una fórmula fija para generar un segundo valor de clave y luego llevar a cabo un cálculo en el segundo valor de clave con la fórmula fija para generar un tercer valor de clave y el resto se puede deducir por analogía, donde la serie de valores de claves se llaman cadena de claves. Cada valor de clave en la cadena de claves puede tener 128 bits y una función OR exclusiva se lleva a cabo, de forma secuencial, en cada valor de clave y 128 bits en los datos a descifrarse para obtener los datos de texto sin formato correspondientes. Las personas con experiencia en la técnica pueden comprender que el algoritmo CCMP puede ser una tecnología existente, la cual no se encuentra limitada en la presente invención.

Se debe notar además que los datos de autenticación adicionales pueden incluir solamente información de dirección y pueden usar también otra información, excepto la información de dirección en un encabezado de paquete, por ejemplo, un campo de control de trama (FC), un campo de calidad de control de servicio (control QoS) y un campo de control de secuencia (SC). Dichos campos incluyen muchos bits de información de indicación; algunos de dichos bits de información mantienen, en los datos de autenticación adicionales, los mismos valores que en el encabezado de paquete y algunos se establecen en valores fijos en los datos de autenticación adicionales. Para asegurar que el primer nodo y el segundo nodo generen los mismos datos de autenticación adicionales para los mismos datos transmitidos entre el primer nodo y el segundo nodo, los bits de información que cambian después de que la Retransmisión lleva a cabo el reenvío se pueden establecer en valores fijos en los datos de autenticación adicionales generados. Por ejemplo, el campo FC tiene dos bits de información que son toDS y fromDS, los cuales representan, respectivamente, si el paquete se envía a un lado de red o proviene de un lado de red; cuando la Retransmisión recibe un paquete enviado por la STA, los valores de los dos bits de información pueden ser "10" y cuando la Retransmisión envía el paquete al PA, los valores de los dos bits de información pueden ser "11"; por lo tanto, cuando se generan datos de autenticación adicionales, la STA o el PA establecen los dos bits de información en los datos de autenticación adicionales en un valor fijo, por ejemplo, "11". El establecimiento de los bits de información en los datos de autenticación adicionales en el valor fijo no representa un significado específico y solo pretende permitir a la STA y al PA obtener los mismos datos de autenticación adicionales.

Asimismo, se debe notar además que un *nonce* se puede generar también en el algoritmo CCMP según una dirección D2 en un encabezado de paquete y el *nonce* participa en un proceso de cálculo de encriptación; por lo tanto, antes de llevar a cabo el descifrado de forma correcta, el primer nodo necesita generar un mismo *nonce* después de recibir el primer paquete. Como se muestra en la Figura 4, D2 en el primer paquete enviado por la Retransmisión al PA es diferente de D2 en el segundo paquete recibido por la Retransmisión desde la STA. Para

permitir que el PA y la STA usen un mismo *nonce*, por ejemplo, en un caso de enlace ascendente, el PA necesita determinar, según la relación de mapeo de dirección que se muestra en la Tabla 1, que la dirección D3 en el encabezado de paquete del primer paquete enviado por la Retransmisión al PA es igual a D2 en el segundo paquete enviado por la STA a la Retransmisión; por lo tanto, el PA puede generar un *nonce* según la dirección D3 en el encabezado del primer paquete. De esta manera, el *nonce* generado por el PA es igual a un *nonce* generado por la STA.

En la presente realización de la presente invención, un primer nodo recibe un primer paquete enviado por un dispositivo de retransmisión, donde el primer paquete incluye datos en un segundo paquete enviado por un segundo nodo al dispositivo de retransmisión; los datos en el segundo paquete se encriptan usando un segundo dato de autenticación adicional y una clave de sesión entre el primer nodo y el segundo nodo; el segundo dato de autenticación adicional se genera por el segundo nodo según al menos la información de dirección en un encabezado de paquete del segundo paquete usando una segunda regla; el primer nodo genera el primer dato de autenticación adicional según al menos la información de dirección en el primer paquete usando una primera regla, donde una secuencia de direcciones en el primer dato de autenticación adicional generado por el primer nodo según la primera regla es igual a una secuencia de direcciones en el segundo dato de autenticación adicional generado por el segundo nodo según la segunda regla; el primer nodo además descifra los datos en el primer paquete usando el primer dato de autenticación adicional y la clave de sesión entre el primer nodo y el segundo nodo. De esta manera, cuando recibe el segundo paquete enviado por el segundo nodo, el dispositivo de retransmisión no necesita enviar, después de llevar a cabo, en primer lugar, el descifrado y luego llevar a cabo la encriptación en el segundo paquete, el primer paquete al primer nodo, ahorrando, por consiguiente, tiempo de procesamiento de paquetes del dispositivo de retransmisión, mejorando la utilización del canal y reduciendo el consumo de potencia adicional del dispositivo de retransmisión.

La Figura 5 es un diagrama de flujo esquemático de un método de procesamiento de paquetes según otra realización de la presente invención, donde el método se aplica a un escenario en el cual un dispositivo de retransmisión reenvía un paquete entre un primer nodo y un segundo nodo. Como se muestra en la Figura 5, el método de procesamiento de paquetes específicamente incluye:

501: un segundo nodo genera un segundo paquete, donde la información de dirección en un encabezado de paquete del segundo paquete indica que una parte receptora del segundo paquete es un dispositivo de retransmisión, una parte emisora es el segundo nodo y una siguiente parte receptora es un primer nodo.

En una implementación específica, como se muestra en la Figura 4, suponiendo que el segundo nodo es un PA y el primer nodo es una STA, cuando el PA necesita enviar un dato encriptado a la STA, el PA puede generar un segundo paquete y completar la información de dirección en un encabezado de paquete del segundo paquete, donde una dirección de recepción D1 es una dirección de una Retransmisión, una dirección de envío D2 que también es una dirección de origen es una dirección del PA y una dirección de destino D3 es una dirección de la STA; y completar los datos a enviarse en una parte de Datos del segundo paquete.

502: el segundo nodo genera el segundo dato de autenticación adicional según al menos la información de dirección en el encabezado de paquete del segundo paquete mediante el uso de una segunda regla y encripta datos en el segundo paquete mediante el uso del segundo dato de autenticación adicional y una clave de sesión entre el primer nodo y el segundo nodo.

En una implementación específica, antes de que el PA envíe el segundo paquete, el PA necesita generar el segundo dato de autenticación adicional; en la presente realización, el PA genera el segundo dato de autenticación adicional según al menos la información de dirección en el segundo paquete mediante el uso de la segunda regla, donde la segunda regla puede ser que una secuencia de direcciones en el segundo dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del segundo paquete, o la segunda regla puede ser también que una secuencia de direcciones en el segundo dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del segundo paquete.

Luego, el PA encripta los datos en el segundo paquete mediante el uso del segundo dato de autenticación adicional y la clave de sesión entre el primer nodo y el segundo nodo. En una implementación específica, el PA puede llevar a cabo una serie de funciones según un algoritmo CCMP mediante el uso del segundo dato de autenticación adicional, la información de número de secuencia de paquete en un encabezado CCMP en el segundo paquete, la clave de sesión entre el PA y la STA y similares para generar un primer valor de clave de una cadena de claves, luego llevar a cabo un cálculo en el primer valor de clave con una fórmula fija para generar un segundo valor de clave y luego llevar a cabo un cálculo en el segundo valor de clave con la fórmula fija para generar un tercer valor de clave y el resto se puede deducir por analogía, donde la serie de valores de clave se llama cadena de claves. Cada valor de clave en la cadena de claves puede tener 128 bits y los datos de texto cifrado correspondientes se pueden obtener llevando a cabo, de forma secuencial, una función OR exclusiva en cada valor de clave y 128 bits en los datos a encriptarse.

503: el segundo nodo envía el segundo paquete encriptado al dispositivo de retransmisión, de modo que después de recibir el segundo paquete, el dispositivo de retransmisión envía un primer paquete al primer nodo, donde el primer paquete incluye los datos en el segundo paquete y la información de dirección incluida en un encabezado de paquete del primer paquete indica que una parte receptora del primer paquete es el primer nodo, una parte emisora es el dispositivo de retransmisión y una parte emisora previa es el segundo nodo; después de recibir el primer paquete, el primer nodo genera el primer dato de autenticación adicional según al menos la información de dirección en el encabezado de paquete del primer paquete mediante el uso de una primera regla, y descifra datos en el primer paquete mediante el uso del primer dato de autenticación adicional y la clave de sesión entre el primer nodo y el segundo nodo, donde el primer dato de autenticación adicional es igual al segundo dato de autenticación adicional.

En la presente realización, como se muestra en la Figura 4, después de recibir el segundo paquete enviado por el PA, la Retransmisión no necesita descifrar los datos encriptados en el segundo paquete y la Retransmisión puede llevar a cabo el reensamblado para obtener el primer paquete, el cual puede ser específicamente que: los datos encriptados en el segundo paquete se completan en una parte de Datos en el primer paquete y la información de dirección en el encabezado de paquete del primer paquete se completa como se describe a continuación: una dirección de recepción D1 que es también una dirección de destino es la dirección de la STA, una dirección de envío D2 es la dirección de la Retransmisión y una dirección de origen D3 es la dirección del PA. El primer paquete se puede obtener también después de actualizar simplemente la información de dirección en el segundo paquete. Luego, la Retransmisión envía el primer paquete a la STA.

Para permitir que la STA descifre, en forma correcta, los datos encriptados que se incluyen en el primer paquete y se encuentran en el segundo paquete desde el PA, el primer dato de autenticación adicional generado por la STA según la información de dirección en el primer paquete usando la primera regla necesita ser igual al segundo dato de autenticación adicional generado por el PA según la información de dirección en el encabezado de paquete del segundo paquete usando la segunda regla, lo cual puede incluir que una secuencia de direcciones en el primer dato de autenticación adicional generado por la STA usando la primera regla necesite ser igual a la secuencia de las direcciones en el segundo dato de autenticación adicional generado por el PA usando la segunda regla, lo cual puede ser como se describe a continuación en una implementación específica:

si la segunda regla usada por el PA es que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el encabezado de paquete del segundo paquete, la primera regla usada por la STA es que la secuencia de las direcciones en el primer dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del primer paquete, de modo que la secuencia de las direcciones en el primer dato de autenticación adicional generado por la STA usando la primera regla es igual a la secuencia de las direcciones en el segundo dato de autenticación adicional generado por el PA mediante el uso de la segunda regla, o

si la segunda regla usada por el PA es que la secuencia de las direcciones en el segundo dato de autenticación adicional es diferente de la secuencia de las direcciones en el encabezado de paquete del segundo paquete, la primera regla usada por la STA es que la secuencia de las direcciones en el primer dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del primer paquete, de modo que la secuencia de las direcciones en el primer dato de autenticación adicional generado por la STA usando la primera regla es igual a la secuencia de las direcciones en el segundo dato de autenticación adicional generado por el PA usando la segunda regla.

Asimismo, en una manera de implementación opcional de la presente invención, el segundo paquete generado por el PA puede incluir además información de autenticación de mensajes de retransmisión, donde la información de autenticación de mensajes de retransmisión se genera por el PA mediante el uso de una clave de autenticación de mensajes entre la Retransmisión y el PA, de modo que después de recibir el segundo paquete enviado por el PA, la Retransmisión verifica la información de autenticación de mensajes de retransmisión mediante el uso de la clave de autenticación de mensajes y envía el primer paquete a la STA si la verificación es exitosa. La información de autenticación de mensajes de retransmisión se puede obtener por el PA llevando a cabo una función de encriptación o una función de troceo en un campo FCS del segundo paquete usando la clave de autenticación de mensajes, lo cual puede ser como se describe a continuación en una implementación específica:

por ejemplo, como se muestra en la Figura 4, antes de enviar el segundo paquete a la Retransmisión, el PA puede negociar una clave de autenticación de mensajes de retransmisión con la Retransmisión, donde la clave de autenticación de mensajes de retransmisión se usa para llevar a cabo la autenticación simple de mensajes en el segundo paquete enviado por el PA a la Retransmisión. Normalmente, el PA puede llevar a cabo una función de encriptación o una función de troceo en el campo FCS en el segundo paquete a enviarse usando la clave de autenticación de mensajes de retransmisión negociada entre el PA y la Retransmisión y usar un campo FCS obtenido después de la función de encriptación o troceo como información de autenticación de mensajes de retransmisión para reemplazar el campo FCS original. En la presente realización, para una mejor descripción, se puede hacer referencia al FCS obtenido después del troceo como un campo de autenticación de retransmisión R-Auth. Después de recibir el segundo paquete enviado por el PA, la Retransmisión verifica la información de

autenticación de mensajes de retransmisión usando la clave de autenticación de mensajes de retransmisión, es decir, se verifica el campo de autenticación de retransmisión R-Auth llevado en el segundo paquete. Un método de verificación específico puede ser que: R-Auth' se genera usando un proceso que es igual al proceso en el cual el PA genera R-Auth; entonces R-Auth' y R-Auth en el paquete se comparan y si R-Auth' y R-Auth son iguales, la verificación es exitosa; de lo contrario, la verificación falla. Basada en el hecho de que la verificación en R-Auth es exitosa, la Retransmisión ensambla los datos encriptados en el segundo paquete en el primer paquete y envía el primer paquete a la STA. De manera opcional, si la verificación llevada a cabo por la Retransmisión en R-Auth falla, la Retransmisión puede directamente descartar el segundo paquete.

En la presente realización de la presente invención, un segundo nodo genera un segundo dato de autenticación adicional según la información de dirección en un segundo paquete usando una segunda regla, encripta datos en el segundo paquete usando el segundo dato de autenticación adicional y una clave de sesión entre un primer nodo y el segundo nodo y luego envía el segundo paquete a un dispositivo de retransmisión, de modo que el dispositivo de retransmisión añade directamente los datos encriptados en el segundo paquete a un primer paquete sin descifrar los datos encriptados en el segundo paquete y envía el primer paquete al primer nodo; por lo tanto, el primer nodo genera el primer dato de autenticación adicional según la información de dirección en el primer paquete usando una primera regla, donde el primer dato de autenticación adicional generado mediante el uso de la primera regla es igual al segundo dato de autenticación adicional generado mediante el uso de la segunda regla; el primer nodo descifra los datos encriptados en el primer paquete usando el primer dato de autenticación adicional y la clave de sesión entre el primer nodo y el segundo nodo. De esta manera, el dispositivo de retransmisión puede omitir un proceso de llevar a cabo el descifrado en primer lugar y llevar a cabo la encriptación luego en un proceso de reenvío del paquete encriptado y así ahorrar tiempo de procesamiento de paquetes, mejorar la utilización del canal y reducir el consumo de potencia adicional del dispositivo de retransmisión.

La Figura 6 es un diagrama de flujo esquemático de un método de procesamiento de paquetes según otra realización de la presente invención, donde el método se aplica a un escenario en el cual un dispositivo de retransmisión reenvía un paquete entre un primer nodo y un segundo nodo. Como se muestra en la Figura 6, el método de procesamiento de paquetes específicamente incluye:

601: un dispositivo de retransmisión recibe un segundo paquete enviado por un segundo nodo, donde la información de dirección en un encabezado de paquete del segundo paquete indica que una parte receptora del segundo paquete es el dispositivo de retransmisión, una parte emisora es el segundo nodo y una siguiente parte receptora es un primer nodo; los datos en el segundo paquete se encriptan mediante el uso del segundo dato de autenticación adicional y una clave de sesión entre el primer nodo y el segundo nodo; el segundo dato de autenticación adicional se genera por el segundo nodo según al menos la información de dirección en el encabezado de paquete del segundo paquete mediante el uso de una segunda regla.

602: el dispositivo de retransmisión envía un primer paquete al primer nodo, donde el primer paquete incluye los datos en el segundo paquete y la información de dirección incluida en un encabezado de paquete del primer paquete indica que una parte receptora del primer paquete es el primer nodo, una parte emisora es el dispositivo de retransmisión y una parte emisora previa es el segundo nodo, de modo que el primer nodo genera el primer dato de autenticación adicional según al menos la información de dirección en el encabezado de paquete del primer paquete mediante el uso de una primera regla y descifra datos en el primer paquete mediante el uso del primer dato de autenticación adicional y la clave de sesión entre el primer nodo y el segundo nodo, donde el primer dato de autenticación adicional es igual al segundo dato de autenticación adicional.

En la presente realización, después de recibir el segundo paquete enviado por el segundo nodo, el dispositivo de retransmisión puede completar directamente los datos encriptados en una parte de Datos en el primer paquete sin descifrar los datos encriptados en el segundo paquete y completar la información de dirección en el encabezado de paquete del primer paquete como se describe a continuación: una dirección de recepción D1 que es también una dirección de destino es una dirección del primer nodo, una dirección de envío D2 es una dirección del dispositivo de retransmisión y una dirección de origen D3 es una dirección del segundo nodo. Luego, el dispositivo de retransmisión envía el primer paquete al primer nodo.

La primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional; o

la primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

Además, la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

El primer nodo es una estación y el segundo nodo es un punto de acceso; o el primer nodo es un punto de acceso y el segundo nodo es una estación.

Además, en una manera de implementación de la presente invención, el segundo paquete que se recibe por el dispositivo de retransmisión y se envía por el segundo nodo puede además incluir información de autenticación de mensajes de retransmisión, donde la información de autenticación de mensajes de retransmisión se genera por el segundo nodo mediante el uso de una clave de autenticación de mensajes entre el dispositivo de retransmisión y el segundo nodo, de modo que después de recibir el segundo paquete, el dispositivo de retransmisión verifica la información de autenticación de mensajes de retransmisión mediante el uso de la clave de autenticación de mensajes y envía el primer paquete al primer nodo si la verificación es exitosa. La información de autenticación de mensajes de retransmisión se genera por el segundo nodo usando una clave de autenticación de mensajes entre el dispositivo de retransmisión y el segundo nodo. En una implementación específica, la información de autenticación de mensajes de retransmisión se puede obtener por el segundo nodo llevando a cabo una función de encriptación o una función de troceo en un campo FCS del segundo paquete usando la clave de autenticación de mensajes. Para más detalles, se puede hacer referencia a la descripción de la parte anterior relacionada, la cual no se describe nuevamente en la presente memoria.

Cuando el dispositivo de retransmisión en la presente realización de la presente invención recibe un segundo paquete enviado por un segundo nodo, el dispositivo de retransmisión puede reensamblar directamente los datos encriptados en el segundo paquete en un primer paquete sin un proceso de llevar a cabo el descifrado primero y luego llevar a cabo la encriptación en los datos encriptados y así ahorrar tiempo de procesamiento de paquetes del dispositivo de retransmisión, mejorar la utilización del canal y reducir el consumo de potencia adicional del dispositivo de retransmisión.

La Figura 7 es un diagrama estructural esquemático de un aparato de procesamiento de paquetes según una realización de la presente invención, donde el aparato de procesamiento de paquetes se ubica en un lado de un primer nodo y se aplica a un escenario en el cual un dispositivo de retransmisión reenvía un paquete entre el primer nodo y un segundo nodo. Como se muestra en la Figura 7, el aparato de procesamiento de paquetes incluye:

un módulo de recepción 71, configurado para recibir un primer paquete enviado por el dispositivo de retransmisión, donde el primer paquete incluye datos en un segundo paquete enviado por el segundo nodo al dispositivo de retransmisión, los datos en el segundo paquete se encriptan mediante el uso de un segundo dato de autenticación adicional y una clave de sesión entre el primer nodo y el segundo nodo, el segundo dato de autenticación adicional se genera por el segundo nodo según al menos la información de dirección en un encabezado de paquete del segundo paquete mediante el uso de una segunda regla y la información de dirección en el encabezado de paquete del segundo paquete indica que una parte receptora del segundo paquete es el dispositivo de retransmisión, una parte emisora es el segundo nodo y una siguiente parte receptora es el primer nodo; y

un módulo de descifrado 72, configurado para generar un primer dato de autenticación adicional según al menos la información de dirección en un encabezado de paquete del primer paquete mediante el uso de una primera regla, donde la información de dirección incluida en el encabezado de paquete del primer paquete indica que una parte receptora del primer paquete es el primer nodo, una parte emisora es el dispositivo de retransmisión y una parte emisora previa es el segundo nodo, y los datos de autenticación adicionales generados mediante el uso de la primera regla son iguales a los datos de autenticación adicionales generados mediante el uso de la segunda regla; y descifrar datos en el primer paquete mediante el uso del primer dato de autenticación adicional y la clave de sesión entre el primer nodo y el segundo nodo, donde el primer dato de autenticación adicional es igual al segundo dato de autenticación adicional.

La primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional; o

la primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

Además, la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

Asimismo, de manera opcional, el segundo paquete puede incluir además información de autenticación de mensajes de retransmisión, donde la información de autenticación de mensajes de retransmisión se genera por el segundo nodo mediante el uso de una clave de autenticación de mensajes entre el dispositivo de retransmisión y el segundo nodo; después de recibir el segundo paquete, el dispositivo de retransmisión verifica la información de autenticación de mensajes de retransmisión mediante el uso de la clave de autenticación de mensajes y envía el primer paquete al primer nodo si la verificación es exitosa.

El primer nodo es una estación y el segundo nodo es un punto de acceso; o el primer nodo es un punto de acceso y el segundo nodo es una estación.

En la presente invención, un primer nodo recibe un primer paquete enviado por un dispositivo de retransmisión, donde el primer paquete incluye datos en un segundo paquete enviado por un segundo nodo al dispositivo de retransmisión; los datos en el segundo paquete se encriptan mediante el uso de un segundo dato de autenticación adicional y una clave de sesión entre el primer nodo y el segundo nodo; el segundo dato de autenticación adicional se genera por el segundo nodo según al menos la información de dirección en un encabezado de paquete del segundo paquete mediante el uso de una segunda regla; el primer nodo genera un primer dato de autenticación adicional según al menos la información de dirección en el primer paquete mediante el uso de una primera regla, donde una secuencia de direcciones en el primer dato de autenticación adicional generado por el primer nodo según la primera regla es igual a una secuencia de direcciones en el segundo dato de autenticación adicional generado por el segundo nodo según la segunda regla; el primer nodo descifra además datos en el primer paquete mediante el uso del primer dato de autenticación adicional y la clave de sesión entre el primer nodo y el segundo nodo. De esta manera, cuando recibe el segundo paquete enviado por el segundo nodo, el dispositivo de retransmisión no necesita enviar, después de llevar a cabo, en primer lugar, el descifrado y luego llevar a cabo la encriptación en el segundo paquete, el primer paquete al primer nodo, ahorrando, por consiguiente, tiempo de procesamiento de paquetes del dispositivo de retransmisión, mejorando la utilización del canal y reduciendo el consumo de potencia adicional del dispositivo de retransmisión.

La Figura 8 es un diagrama estructural esquemático de un aparato de procesamiento de paquetes según otra realización de la presente invención, donde el aparato de procesamiento de paquetes se ubica en un lado de un segundo nodo y se aplica a un escenario en el cual un dispositivo de retransmisión reenvía un paquete entre el segundo nodo y un primer nodo, e incluye:

un módulo de generación de paquetes 81, configurado para generar un segundo paquete, donde la información de dirección en un encabezado de paquete del segundo paquete indica que una parte receptora del segundo paquete es el dispositivo de retransmisión, una parte emisora es el segundo nodo y una siguiente parte receptora es el primer nodo;

un módulo de encriptación 82, configurado para generar el segundo dato de autenticación adicional según al menos la información de dirección en el encabezado de paquete del segundo paquete mediante el uso de una segunda regla y encriptar datos en el segundo paquete mediante el uso del segundo dato de autenticación adicional y una clave de sesión entre el primer nodo y el segundo nodo; y

un módulo de envío 83, configurado para enviar el segundo paquete encriptado al dispositivo de retransmisión, de modo que después de recibir el segundo paquete, el dispositivo de retransmisión envía un primer paquete al primer nodo, donde el primer paquete incluye los datos en el segundo paquete y la información de dirección incluida en un encabezado de paquete del primer paquete indica que una parte receptora del primer paquete es el primer nodo, una parte emisora es el dispositivo de retransmisión y una parte emisora previa es el segundo nodo; después de recibir el primer paquete, el primer nodo genera el primer dato de autenticación adicional según al menos la información de dirección en el encabezado de paquete del primer paquete mediante el uso de una primera regla y descifra datos en el primer paquete mediante el uso del primer dato de autenticación adicional y la clave de sesión entre el primer nodo y el segundo nodo, donde el primer dato de autenticación adicional es igual al segundo dato de autenticación adicional.

La primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional; o

la primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

Además, la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

Asimismo, de manera opcional, el segundo paquete incluye además información de autenticación de mensajes de retransmisión, donde la información de autenticación de mensajes de retransmisión se genera por el segundo nodo mediante el uso de una clave de autenticación de mensajes entre el dispositivo de retransmisión y el segundo nodo; después de recibir el segundo paquete, el dispositivo de retransmisión verifica la información de autenticación de mensajes de retransmisión mediante el uso de la clave de autenticación de mensajes y envía el primer paquete al primer nodo si la verificación es exitosa.

El segundo nodo es una estación y el primer nodo es un punto de acceso; o el segundo nodo es un punto de acceso y el primer nodo es una estación.

En la presente realización de la presente invención, un segundo nodo genera un segundo dato de autenticación adicional según la información de dirección en un segundo paquete usando una segunda regla, encripta datos en el segundo paquete usando el segundo dato de autenticación adicional y una clave de sesión entre un primer nodo y el segundo nodo y luego envía el segundo paquete a un dispositivo de retransmisión, de modo que el dispositivo de retransmisión añade directamente los datos encriptados en el segundo paquete a un primer paquete sin descifrar los datos encriptados en el segundo paquete y envía el primer paquete al primer nodo; por lo tanto, el primer nodo genera el primer dato de autenticación adicional según la información de dirección en el primer paquete usando una primera regla, donde el primer dato de autenticación adicional generado mediante el uso de la primera regla es igual al segundo dato de autenticación adicional generado mediante el uso de la segunda regla; el primer nodo descifra los datos encriptados en el primer paquete usando el primer dato de autenticación adicional y la clave de sesión entre el primer nodo y el segundo nodo. De esta manera, el dispositivo de retransmisión puede omitir un proceso de llevar a cabo el descifrado primero y llevar a cabo la encriptación luego en un proceso de reenvío del paquete encriptado y así ahorrar tiempo de procesamiento de paquetes, mejorar la utilización del canal y reducir el consumo de potencia adicional del dispositivo de retransmisión.

La Figura 9 es un diagrama estructural esquemático de un aparato de procesamiento de paquetes según otra realización de la presente invención, donde el aparato de procesamiento de paquetes se ubica en un lado de un dispositivo de retransmisión y se aplica a un escenario en el cual el dispositivo de retransmisión reenvía un paquete entre un segundo nodo y un primer nodo, e incluye:

un módulo de recepción 91, configurado para recibir un segundo paquete enviado por el segundo nodo, donde la información de dirección en un encabezado de paquete del segundo paquete indica que una parte receptora del segundo paquete es el dispositivo de retransmisión, una parte emisora es el segundo nodo y una siguiente parte receptora es el primer nodo; los datos en el segundo paquete se encriptan mediante el uso de un segundo dato de autenticación adicional y una clave de sesión entre el primer nodo y el segundo nodo; el segundo dato de autenticación adicional se genera por el segundo nodo según al menos la información de dirección en el encabezado de paquete del segundo paquete mediante el uso de una segunda regla; y

un módulo de envío 92, configurado para enviar un primer paquete al primer nodo, donde el primer paquete incluye los datos en el segundo paquete y la información de dirección incluida en un encabezado de paquete del primer paquete indica que una parte receptora del primer paquete es el primer nodo, una parte emisora es el dispositivo de retransmisión y una parte emisora previa es el segundo nodo, de modo que el primer nodo genera el primer dato de autenticación adicional según al menos la información de dirección en el encabezado de paquete del primer paquete mediante el uso de una primera regla, y descifra datos en el primer paquete mediante el uso del primer dato de autenticación adicional y la clave de sesión entre el primer nodo y el segundo nodo, donde el primer dato de autenticación adicional es igual al segundo dato de autenticación adicional.

La primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional; o

la primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

Además, la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

Asimismo, de manera opcional, el segundo paquete puede incluir además información de autenticación de mensajes de retransmisión, donde la información de autenticación de mensajes de retransmisión se genera por el segundo nodo mediante el uso de una clave de autenticación de mensajes entre el dispositivo de retransmisión y el segundo nodo; después de recibir el segundo paquete, el dispositivo de retransmisión verifica la información de autenticación de mensajes de retransmisión mediante el uso de la clave de autenticación de mensajes y envía el primer paquete al primer nodo si la verificación es exitosa.

El primer nodo es una estación y el segundo nodo es un punto de acceso; o el primer nodo es un punto de acceso y el segundo nodo es una estación.

Cuando el dispositivo de retransmisión en la presente realización de la presente invención recibe un segundo paquete enviado por un segundo nodo, el dispositivo de retransmisión puede reensamblar directamente los datos encriptados en el segundo paquete en un primer paquete sin un proceso de llevar a cabo el descifrado primero y luego llevar a cabo la encriptación en los datos encriptados y así ahorrar tiempo de procesamiento de paquetes del dispositivo de retransmisión, mejorar la utilización del canal y reducir el consumo de potencia adicional del dispositivo de retransmisión.

La Figura 10 es un diagrama estructural esquemático de un aparato de procesamiento de paquetes según otra realización de la presente invención, donde el aparato de procesamiento de paquetes se ubica en un lado de un primer nodo y se aplica a un escenario en el cual un dispositivo de retransmisión reenvía un paquete entre el primer nodo y un segundo nodo. El aparato de procesamiento de paquetes en la presente realización puede ser, de forma específica, un punto de acceso o una estación. Como se muestra en la Figura 10, el primer nodo incluye: un procesador, una memoria y un bus de comunicaciones, donde el procesador se conecta a la memoria mediante el uso del bus de comunicaciones y la memoria guarda una orden de implementar un método de procesamiento de paquetes aplicado al escenario en el cual el dispositivo de retransmisión reenvía un paquete entre el primer nodo y el segundo nodo. Asimismo, el primer nodo incluye además una interfaz de comunicaciones y se comunica con otro dispositivo de elementos de red (por ejemplo, un dispositivo de retransmisión) mediante el uso de la interfaz de comunicaciones.

Cuando el procesador invoca la orden en la memoria, las siguientes etapas se pueden llevar a cabo:

recibir un primer paquete enviado por el dispositivo de retransmisión, donde el primer paquete incluye datos en un segundo paquete enviado por el segundo nodo al dispositivo de retransmisión, los datos en el segundo paquete se encriptan mediante el uso del segundo dato de autenticación adicional y una clave de sesión entre el primer nodo y el segundo nodo, el segundo dato de autenticación adicional se genera por el segundo nodo según al menos la información de dirección en un encabezado de paquete del segundo paquete mediante el uso de una segunda regla y la información de dirección en el encabezado de paquete del segundo paquete indica que una parte receptora del segundo paquete es el dispositivo de retransmisión, una parte emisora es el segundo nodo y una siguiente parte receptora es el primer nodo; y

generar un primer dato de autenticación adicional según al menos la información de dirección en un encabezado de paquete del primer paquete mediante el uso de una primera regla, donde la información de dirección incluida en el encabezado de paquete del primer paquete indica que una parte receptora del primer paquete es el primer nodo, una parte emisora es el dispositivo de retransmisión y una parte emisora previa es el segundo nodo, y los datos de autenticación adicionales generados mediante el uso de la primera regla son iguales a los datos de autenticación adicionales generados mediante el uso de la segunda regla; y descifrar los datos en el primer paquete mediante el uso del primer dato de autenticación adicional y la clave de sesión entre el primer nodo y el segundo nodo, donde el primer dato de autenticación adicional es igual al segundo dato de autenticación adicional.

La primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional; o

la primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

Además, la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

Asimismo, de manera opcional, el segundo paquete puede incluir además información de autenticación de mensajes de retransmisión, donde la información de autenticación de mensajes de retransmisión se genera por el segundo

nodo mediante el uso de una clave de autenticación de mensajes entre el dispositivo de retransmisión y el segundo nodo; después de recibir el segundo paquete, el dispositivo de retransmisión verifica la información de autenticación de mensajes de retransmisión mediante el uso de la clave de autenticación de mensajes y envía el primer paquete al primer nodo si la verificación es exitosa.

El primer nodo es una estación y el segundo nodo es un punto de acceso; o el primer nodo es un punto de acceso y el segundo nodo es una estación.

En la presente realización de la presente invención, un primer nodo recibe un primer paquete enviado por un dispositivo de retransmisión, donde el primer paquete incluye datos en un segundo paquete enviado por un segundo nodo al dispositivo de retransmisión; los datos en el segundo paquete se encriptan mediante el uso de un segundo dato de autenticación adicional y una clave de sesión entre el primer nodo y el segundo nodo; el segundo dato de autenticación adicional se genera por el segundo nodo según al menos la información de dirección en un encabezado de paquete del segundo paquete mediante el uso de una segunda regla; el primer nodo genera un primer dato de autenticación adicional según al menos la información de dirección en el primer paquete mediante el uso de una primera regla, donde una secuencia de direcciones en el primer dato de autenticación adicional generado por el primer nodo según la primera regla es igual a una secuencia de direcciones en el segundo dato de autenticación adicional generado por el segundo nodo según la segunda regla; el primer nodo descifra además datos en el primer paquete mediante el uso del primer dato de autenticación adicional y la clave de sesión entre el primer nodo y el segundo nodo. De esta manera, cuando recibe el segundo paquete enviado por el segundo nodo, el dispositivo de retransmisión no necesita enviar, después de llevar a cabo, en primer lugar, el descifrado y luego llevar a cabo la encriptación en el segundo paquete, el primer paquete al primer nodo y así ahorrar tiempo de procesamiento de paquetes del dispositivo de retransmisión, mejorar la utilización del canal y reducir el consumo de potencia adicional del dispositivo de retransmisión.

La Figura 11 es un diagrama estructural esquemático de un aparato de procesamiento de paquetes según otra realización de la presente invención, donde el aparato de procesamiento de paquetes se ubica en un lado de un segundo nodo y se aplica a un escenario en el cual un dispositivo de retransmisión reenvía un paquete entre un primer nodo y el segundo nodo y puede ser, específicamente, un punto de acceso PA o una estación STA. Como se muestra en la Figura 11, el segundo nodo incluye: un procesador, una memoria y un bus de comunicaciones, donde el procesador se conecta a la memoria mediante el uso del bus de comunicaciones y la memoria guarda una orden de implementar un método de procesamiento de paquetes aplicado al escenario en el cual el dispositivo de retransmisión reenvía un paquete entre el primer nodo y el segundo nodo. Asimismo, el segundo nodo incluye además una interfaz de comunicaciones y se comunica con otro dispositivo de elementos de red (por ejemplo, un dispositivo de retransmisión) mediante el uso de la interfaz de comunicaciones.

Cuando el procesador invoca la orden en la memoria, las siguientes etapas se pueden llevar a cabo:

generar un segundo paquete, donde la información de dirección en un encabezado de paquete del segundo paquete indica que una parte receptora del segundo paquete es el dispositivo de retransmisión, una parte emisora es el segundo nodo y una siguiente parte receptora es el primer nodo;

generar el segundo dato de autenticación adicional según al menos la información de dirección en el encabezado de paquete del segundo paquete mediante el uso de una segunda regla y encriptar datos en el segundo paquete mediante el uso del segundo dato de autenticación adicional y una clave de sesión entre el primer nodo y el segundo nodo; y

enviar el segundo paquete encriptado al dispositivo de retransmisión, de modo que después de recibir el segundo paquete, el dispositivo de retransmisión envía un primer paquete al primer nodo, donde el primer paquete incluye los datos en el segundo paquete y la información de dirección incluida en un encabezado de paquete del primer paquete indica que una parte receptora del primer paquete es el primer nodo, una parte emisora es el dispositivo de retransmisión y una parte emisora previa es el segundo nodo; después de recibir el primer paquete, el primer nodo genera el primer dato de autenticación adicional según al menos la información de dirección en el encabezado de paquete del primer paquete mediante el uso de una primera regla y descifra datos en el primer paquete mediante el uso del primer dato de autenticación adicional y la clave de sesión entre el primer nodo y el segundo nodo, donde el primer dato de autenticación adicional es igual al segundo dato de autenticación adicional.

La primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional; o

la primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es igual a una secuencia de direcciones en

el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

Además, la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

Asimismo, de manera opcional, el segundo paquete puede incluir además información de autenticación de mensajes de retransmisión, donde la información de autenticación de mensajes de retransmisión se genera por el segundo nodo mediante el uso de una clave de autenticación de mensajes entre el dispositivo de retransmisión y el segundo nodo; después de recibir el segundo paquete, el dispositivo de retransmisión verifica la información de autenticación de mensajes de retransmisión mediante el uso de la clave de autenticación de mensajes y envía el primer paquete al primer nodo si la verificación es exitosa.

El segundo nodo es una estación y el primer nodo es un punto de acceso; o el segundo nodo es un punto de acceso y el primer nodo es una estación.

En la presente realización de la presente invención, un segundo nodo genera un segundo dato de autenticación adicional según la información de dirección en un segundo paquete usando una segunda regla, encripta datos en el segundo paquete usando el segundo dato de autenticación adicional y una clave de sesión entre un primer nodo y el segundo nodo y luego envía el segundo paquete a un dispositivo de retransmisión, de modo que el dispositivo de retransmisión añade directamente los datos encriptados en el segundo paquete a un primer paquete sin descifrar los datos encriptados en el segundo paquete y envía el primer paquete al primer nodo; por lo tanto, el primer nodo genera el primer dato de autenticación adicional según la información de dirección en el primer paquete usando una primera regla, donde el primer dato de autenticación adicional generado mediante el uso de la primera regla es igual al segundo dato de autenticación adicional generado mediante el uso de la segunda regla; el primer nodo descifra los datos encriptados en el primer paquete usando el primer dato de autenticación adicional y la clave de sesión entre el primer nodo y el segundo nodo. De esta manera, el dispositivo de retransmisión puede omitir un proceso de llevar a cabo el descifrado primero y llevar a cabo la encriptación luego en un proceso de reenvío del paquete encriptado y así ahorrar tiempo de procesamiento de paquetes, mejorar la utilización del canal y reducir el consumo de potencia adicional del dispositivo de retransmisión.

La Figura 12 es un diagrama estructural esquemático de un aparato de procesamiento de paquetes según otra realización de la presente invención, donde el aparato de procesamiento de paquetes se ubica en un lado de un dispositivo de retransmisión y se aplica a un escenario en el cual el dispositivo de retransmisión reenvía un paquete entre un primer nodo y un segundo nodo y puede ser, específicamente, una Retransmisión. Como se muestra en la Figura 12, el dispositivo de retransmisión incluye: un procesador, una memoria y un bus de comunicaciones, donde el procesador se conecta a la memoria mediante el uso del bus de comunicaciones y la memoria guarda una orden de implementar un método de procesamiento de paquetes aplicado al escenario en el cual el dispositivo de retransmisión reenvía un paquete entre el primer nodo y el segundo nodo. Asimismo, el dispositivo de retransmisión incluye además una interfaz de comunicaciones y se comunica con otro dispositivo de elementos de red (por ejemplo, un punto de acceso o una estación) mediante el uso de la interfaz de comunicaciones.

Cuando el procesador invoca la orden en la memoria, las siguientes etapas se pueden llevar a cabo:

recibir un segundo paquete enviado por el segundo nodo, donde la información de dirección en un encabezado de paquete del segundo paquete indica que una parte receptora del segundo paquete es el dispositivo de retransmisión, una parte emisora es el segundo nodo y una siguiente parte receptora es el primer nodo; los datos en el segundo paquete se encriptan mediante el uso de un segundo dato de autenticación adicional y una clave de sesión entre el primer nodo y el segundo nodo; el segundo dato de autenticación adicional se genera por el segundo nodo según al menos la información de dirección en el encabezado de paquete del segundo paquete mediante el uso de una segunda regla; y

enviar un primer paquete al primer nodo, donde el primer paquete incluye los datos en el segundo paquete y la información de dirección incluida en un encabezado de paquete del primer paquete indica que una parte receptora del primer paquete es el primer nodo, una parte emisora es el dispositivo de retransmisión y una parte emisora previa es el segundo nodo, de modo que el primer nodo genera el primer dato de autenticación adicional según al menos la información de dirección en el encabezado de paquete del primer paquete mediante el uso de una primera regla y descifra datos en el primer paquete mediante el uso del primer dato de autenticación adicional y la clave de sesión entre el primer nodo y el segundo nodo, donde el primer dato de autenticación adicional es igual al segundo dato de autenticación adicional.

La primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional; o

la primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

Además, la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

Asimismo, de manera opcional, el segundo paquete puede además incluir información de autenticación de mensajes de retransmisión, donde la información de autenticación de mensajes de retransmisión se genera por el segundo nodo mediante el uso de una clave de autenticación de mensajes entre el dispositivo de retransmisión y el segundo nodo; después de recibir el segundo paquete, el dispositivo de retransmisión verifica la información de autenticación de mensajes de retransmisión mediante el uso de la clave de autenticación de mensajes y envía el primer paquete al primer nodo si la verificación es exitosa.

El primer nodo es una estación y el segundo nodo es un punto de acceso; o el primer nodo es un punto de acceso y el segundo nodo es una estación.

Cuando el dispositivo de retransmisión en la presente realización de la presente invención recibe un segundo paquete enviado por un segundo nodo, el dispositivo de retransmisión puede reensamblar directamente los datos encriptados en el segundo paquete en un primer paquete sin un proceso de llevar a cabo el descifrado primero y luego llevar a cabo la encriptación en los datos encriptados y así ahorrar tiempo de procesamiento de paquetes del dispositivo de retransmisión, mejorar la utilización del canal y reducir el consumo de potencia adicional del dispositivo de retransmisión.

La Figura 13 es un diagrama estructural esquemático de un sistema de procesamiento de paquetes según otra realización de la presente invención, donde el sistema de procesamiento de paquetes se aplica a un escenario en el cual un dispositivo de retransmisión reenvía un paquete entre un primer nodo y un segundo nodo. Como se muestra en la Figura 13, el sistema específicamente incluye: un dispositivo de retransmisión 11, un primer nodo 12 y un segundo nodo 13.

El primer nodo 12 incluye el aparato de procesamiento de paquetes provisto en la realización que se muestra en la Figura 7 o la Figura 10 y, para un contenido detallado, es preciso remitirse a la descripción relacionada del aparato de procesamiento de paquetes provisto en la realización que se muestra en la Figura 7 o la Figura 10.

El segundo nodo 13 incluye el aparato de procesamiento de paquetes provisto en la realización que se muestra en la Figura 8 o la Figura 11 y, para un contenido detallado, es preciso remitirse a la descripción relacionada del aparato de procesamiento de paquetes provisto en la realización que se muestra en la Figura 8 o la Figura 11.

El dispositivo de retransmisión 11 es el aparato de procesamiento de paquetes provisto en la realización que se muestra en la Figura 9 o la Figura 12 y, para un contenido detallado, es preciso remitirse a la descripción relacionada del aparato de procesamiento de paquetes provisto en la realización que se muestra en la Figura 9 o la Figura 12.

En una aplicación real, si el primer nodo es un punto de acceso PA, el segundo nodo es una estación STA; o si el primer nodo es una estación STA, el segundo nodo es un punto de acceso PA.

En la presente realización de la presente invención, un primer nodo recibe un primer paquete enviado por un dispositivo de retransmisión, donde el primer paquete incluye datos en un segundo paquete enviado por un segundo nodo al dispositivo de retransmisión; los datos en el segundo paquete se encriptan mediante el uso de un segundo dato de autenticación adicional y una clave de sesión entre el primer nodo y el segundo nodo; el segundo dato de autenticación adicional se genera por el segundo nodo según al menos la información de dirección en un encabezado de paquete del segundo paquete mediante el uso de una segunda regla; el primer nodo genera un primer dato de autenticación adicional según al menos la información de dirección en el primer paquete mediante el uso de una primera regla, donde una secuencia de direcciones en el primer dato de autenticación adicional generado por el primer nodo según la primera regla es igual a una secuencia de direcciones en el segundo dato de autenticación adicional generado por el segundo nodo según la segunda regla; el primer nodo descifra además datos en el primer paquete mediante el uso del primer dato de autenticación adicional y la clave de sesión entre el primer nodo y el segundo nodo. De esta manera, cuando recibe el segundo paquete enviado por el segundo nodo, el dispositivo de retransmisión no necesita enviar, después de llevar a cabo, en primer lugar, el descifrado y luego llevar a cabo la encriptación en el segundo paquete, el primer paquete al primer nodo, ahorrando, por consiguiente, tiempo de procesamiento de paquetes del dispositivo de retransmisión, mejorando la utilización del canal y reduciendo el consumo de potencia adicional del dispositivo de retransmisión.

Una persona con experiencia en la técnica podrá comprender de forma clara que, a los fines de una descripción conveniente y breve, para un proceso de trabajo detallado del sistema, aparato y unidad anterior, se puede hacer referencia a un proceso correspondiente en las realizaciones anteriores del método y los detalles no se describen nuevamente en la presente memoria.

En las diversas realizaciones provistas en la presente solicitud, se debe comprender que el sistema, aparato y método descritos pueden implementarse de otras maneras. Por ejemplo, la realización del aparato descrita es meramente a modo de ejemplo. Por ejemplo, la división de unidad es meramente una división de función lógica y en la implementación real la división puede ser otra. Por ejemplo, se pueden combinar o integrar en otro sistema múltiples unidades o componentes, o algunas características se pueden ignorar o no llevar a cabo. Además, los acoplamientos mutuos representados o descritos o los acoplamientos directos o conexiones de comunicaciones se pueden implementar a través de algunas interfaces. Los acoplamientos indirectos o conexiones de comunicación entre los aparatos o unidades se pueden implementar de forma electrónica, mecánica u otras.

Las unidades descritas como partes separadas pueden o pueden no estar físicamente separadas y las partes que se muestran como unidades pueden o pueden no ser unidades físicas, pueden estar ubicadas en una posición, o pueden distribuirse en múltiples unidades de red. Algunas o todas las unidades se pueden seleccionar según las necesidades reales para lograr los objetivos de las soluciones de las realizaciones.

Además, las unidades funcionales en las realizaciones de la presente invención se pueden integrar en una unidad de procesamiento, o cada una de las unidades puede existir sola físicamente, o dos o más unidades se integran en una unidad. La unidad integrada se puede implementar en forma de hardware o se puede implementar en forma de hardware además de una unidad funcional de software.

Cuando la unidad integrada anterior se implementa en la forma de una unidad funcional de software, la unidad integrada se puede almacenar en un medio de almacenamiento legible por ordenador. La unidad funcional de software está almacenada en un medio de almacenamiento e incluye diversas instrucciones para indicar a un dispositivo informático (que puede ser un ordenador, un servidor o un dispositivo de red) que realice algunas de las etapas de los métodos descritos en las realizaciones de la presente invención. Los medios de almacenamiento anteriores incluyen: cualquier medio que pueda almacenar un código de programa como, por ejemplo, una memoria USB, un disco duro removible, una memoria de solo lectura (ROM, memoria de sólo lectura), una memoria de acceso aleatorio (RAM, memoria de acceso aleatorio), un disco magnético o un disco óptico.

REIVINDICACIONES

1. Un método de procesamiento de paquetes, aplicado a un escenario en el cual un dispositivo de retransmisión (11) reenvía un paquete entre un primer nodo (12) y un segundo nodo (13), que comprende:

recibir (301), por el primer nodo (12), un primer paquete enviado por el dispositivo de retransmisión (11), en donde el primer paquete comprende datos en un segundo paquete enviado por el segundo nodo (13) al dispositivo de retransmisión (11), los datos en el segundo paquete se encriptan mediante el uso de un segundo dato de autenticación adicional y una clave de sesión entre el primer nodo (12) y el segundo nodo (13), el segundo dato de autenticación adicional se genera por el segundo nodo (13) según al menos la información de dirección en un encabezado de paquete del segundo paquete mediante el uso de una segunda regla y la información de dirección en el encabezado de paquete del segundo paquete indica que una parte receptora del segundo paquete es el dispositivo de retransmisión (11), una parte emisora es el segundo nodo (13) y una siguiente parte receptora es el primer nodo (12);

generar (302), por el primer nodo (12), el primer dato de autenticación adicional según al menos la información de dirección en un encabezado de paquete del primer paquete mediante el uso de una primera regla, en donde la información de dirección comprendida en el encabezado de paquete del primer paquete indica que una parte receptora del primer paquete es el primer nodo (12), una parte emisora es el dispositivo de retransmisión (11) y una parte emisora previa es el segundo nodo (13) y el primer dato de autenticación adicional es igual al segundo dato de autenticación adicional; y

descifrar (303), por el primer nodo (12), los datos en el primer paquete usando el primer dato de autenticación adicional y la clave de sesión entre el primer nodo (12) y el segundo nodo (13); en donde la primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional; o

la primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

2. El método según la reivindicación 1, en donde la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

3. El método según cualquiera de las reivindicaciones 1 a 2, en donde el segundo paquete comprende además información de autenticación de mensajes de retransmisión, en donde la información de autenticación de mensajes de retransmisión se genera por el segundo nodo mediante el uso de una clave de autenticación de mensajes entre el dispositivo de retransmisión y el segundo nodo; después de recibir el segundo paquete, el dispositivo de retransmisión verifica la información de autenticación de mensajes de retransmisión mediante el uso de la clave de autenticación de mensajes y envía el primer paquete al primer nodo si la verificación es exitosa.

4. Un método de procesamiento de paquetes, aplicado a un escenario en el cual un dispositivo de retransmisión (11) reenvía un paquete entre un primer nodo (12) y un segundo nodo (13), que comprende:

generar (501), por el segundo nodo (13), un segundo paquete, en donde la información de dirección en un encabezado de paquete del segundo paquete indica que una parte receptora del segundo paquete es el dispositivo de retransmisión (11), una parte emisora es el segundo nodo (13) y una siguiente parte receptora es el primer nodo (12);

generar (502), por el segundo nodo, el segundo dato de autenticación adicional según al menos la información de dirección en el encabezado de paquete del segundo paquete mediante el uso de una segunda regla y encriptar datos en el segundo paquete mediante el uso del segundo dato de autenticación adicional y una clave de sesión entre el primer nodo (12) y el segundo nodo (13); y

enviar (503), por el segundo nodo (13), el segundo paquete encriptado al dispositivo de retransmisión (11), de modo que después de recibir el segundo paquete, el dispositivo de retransmisión (11) envía un primer paquete al primer nodo (12), en donde el primer paquete comprende los datos en el segundo paquete y la información de dirección comprendida en un encabezado de paquete del primer paquete indica que una parte receptora del primer paquete es el primer nodo (12), una parte emisora es el dispositivo de retransmisión (11) y una parte emisora previa es el segundo nodo (13); después de recibir el primer paquete, el primer nodo (12) genera el primer dato de autenticación adicional según al menos la información de dirección en el encabezado de paquete del primer paquete mediante el

uso de una primera regla y descifra datos en el primer paquete mediante el uso del primer dato de autenticación adicional y la clave de sesión entre el primer nodo (12) y el segundo nodo (13), en donde el primer dato de autenticación adicional es igual al segundo dato de autenticación adicional; en donde

la primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional; o

la primera regla es que una secuencia de direcciones en el primer dato de autenticación adicional es diferente de una secuencia de direcciones en el encabezado de paquete del primer paquete y la segunda regla es que una secuencia de direcciones en el segundo dato de autenticación adicional es igual a una secuencia de direcciones en el encabezado de paquete del segundo paquete, de modo que la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

5. El método según la reivindicación 4, en donde la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

6. El método según cualquiera de las reivindicaciones 4 a 5, en donde el segundo paquete comprende además información de autenticación de mensajes de retransmisión, en donde la información de autenticación de mensajes de retransmisión se genera por el segundo nodo mediante el uso de una clave de autenticación de mensajes entre el dispositivo de retransmisión y el segundo nodo; después de recibir el segundo paquete, el dispositivo de retransmisión verifica la información de autenticación de mensajes de retransmisión mediante el uso de la clave de autenticación de mensajes y envía el primer paquete al primer nodo si la verificación es exitosa.

7. Un aparato de procesamiento de paquetes, ubicado en un lado de un primer nodo (12), aplicado a un escenario en el cual un dispositivo de retransmisión (11) reenvía un paquete entre el primer nodo (12) y un segundo nodo (13), que comprende:

un módulo de recepción (71), configurado para recibir un primer paquete enviado por el dispositivo de retransmisión (11), en donde el primer paquete comprende datos en un segundo paquete enviado por el segundo nodo (13) al dispositivo de retransmisión (11), los datos en el segundo paquete se encriptan mediante el uso del segundo dato de autenticación adicional y una clave de sesión entre el primer nodo (12) y el segundo nodo (13), el segundo dato de autenticación adicional se genera por el segundo nodo (13) según al menos información de dirección en un encabezado de paquete del segundo paquete mediante el uso de una segunda regla y la información de dirección en el encabezado de paquete del segundo paquete indica que una parte receptora del segundo paquete es el dispositivo de retransmisión (11), una parte emisora es el segundo nodo (13) y una siguiente parte receptora es el primer nodo (12); y

un módulo de descifrado (72), configurado para generar el primer dato de autenticación adicional según al menos la información de dirección en un encabezado de paquete del primer paquete mediante el uso de una primera regla, en donde la información de dirección comprendida en el encabezado de paquete del primer paquete indica que una parte receptora del primer paquete es el primer nodo (12), una parte emisora es el dispositivo de retransmisión (11) y una parte emisora previa es el segundo nodo (13) y los datos de autenticación adicionales generados mediante el uso de la primera regla son iguales a los datos de autenticación adicionales generados mediante el uso de la segunda regla; y descifrar los datos en el primer paquete mediante el uso del primer dato de autenticación adicional y la clave de sesión entre el primer nodo (12) y el segundo nodo (13), en donde el primer dato de autenticación adicional es igual al segundo dato de autenticación adicional; en donde el aparato de procesamiento de paquetes se configura para llevar a cabo el método según cualquiera de las reivindicaciones 1 a 3.

8. El aparato según la reivindicación 7, en donde la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

9. El aparato según cualquiera de las reivindicaciones 7 a 8, en donde el segundo paquete comprende además información de autenticación de mensajes de retransmisión, en donde la información de autenticación de mensajes de retransmisión se genera por el segundo nodo mediante el uso de una clave de autenticación de mensajes entre el dispositivo de retransmisión y el segundo nodo; después de recibir el segundo paquete, el dispositivo de retransmisión verifica la información de autenticación de mensajes de retransmisión mediante el uso de la clave de autenticación de mensajes y envía el primer paquete al primer nodo si la verificación es exitosa.

10. Un aparato de procesamiento de paquetes, ubicado en un lado de un segundo nodo (13), aplicado a un escenario en el cual un dispositivo de retransmisión (11) reenvía un paquete entre el segundo nodo (13) y un primer nodo (12), que comprende:

un módulo de generación de paquetes (81), configurado para generar un segundo paquete, en donde la información de dirección en un encabezado de paquete del segundo paquete indica que una parte receptora del segundo paquete es el dispositivo de retransmisión (11), una parte emisora es el segundo nodo (12) y una siguiente parte receptora es el primer nodo (12);

un módulo de encriptación (82), configurado para generar el segundo dato de autenticación adicional según al menos la información de dirección en el encabezado de paquete del segundo paquete mediante el uso de una segunda regla y encriptar datos en el segundo paquete mediante el uso del segundo dato de autenticación adicional y una clave de sesión entre el primer nodo (12) y el segundo nodo (13); y

un módulo de envío (83), configurado para enviar el segundo paquete encriptado al dispositivo de retransmisión (11), en donde el aparato de procesamiento de paquetes se configura para llevar a cabo el método según cualquiera de las reivindicaciones 4 a 6.

11. El aparato según la reivindicación 10, en donde la secuencia de las direcciones en el segundo dato de autenticación adicional es igual a la secuencia de las direcciones en el primer dato de autenticación adicional.

12. El aparato según cualquiera de las reivindicaciones 10 a 11, en donde el segundo paquete comprende además información de autenticación de mensajes de retransmisión, en donde la información de autenticación de mensajes de retransmisión se genera por el segundo nodo mediante el uso de una clave de autenticación de mensajes entre el dispositivo de retransmisión y el segundo nodo; después de recibir el segundo paquete, el dispositivo de retransmisión verifica la información de autenticación de mensajes de retransmisión mediante el uso de la clave de autenticación de mensajes y envía el primer paquete al primer nodo si la verificación es exitosa.

13. Un sistema de procesamiento de paquetes, aplicado a un escenario en el cual un dispositivo de retransmisión (11) reenvía un paquete entre un primer nodo (12) y un segundo nodo (13), caracterizado por que comprende: el dispositivo de retransmisión (11), el primer nodo (12) y el segundo nodo (13), en donde el primer nodo (12) comprende el aparato de procesamiento de paquetes según cualquiera de las reivindicaciones 7 a 9; y el segundo nodo (13) comprende el aparato de procesamiento de paquetes según cualquiera de las reivindicaciones 10 a 12.

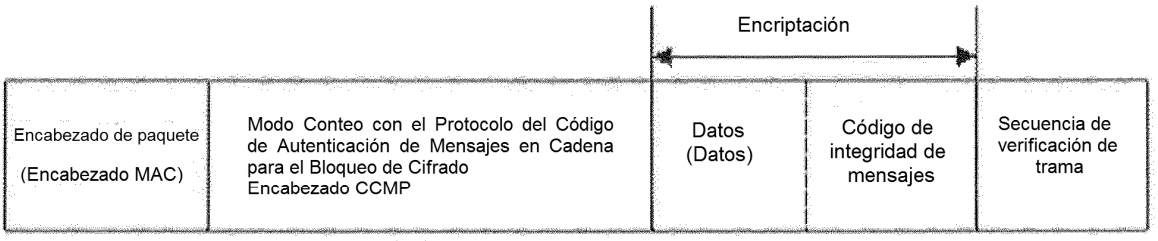

FIG. 1

Control de trama	D1	D2	D3	Control de secuencia	D4	Calidad de control de servicio

FIG. 2

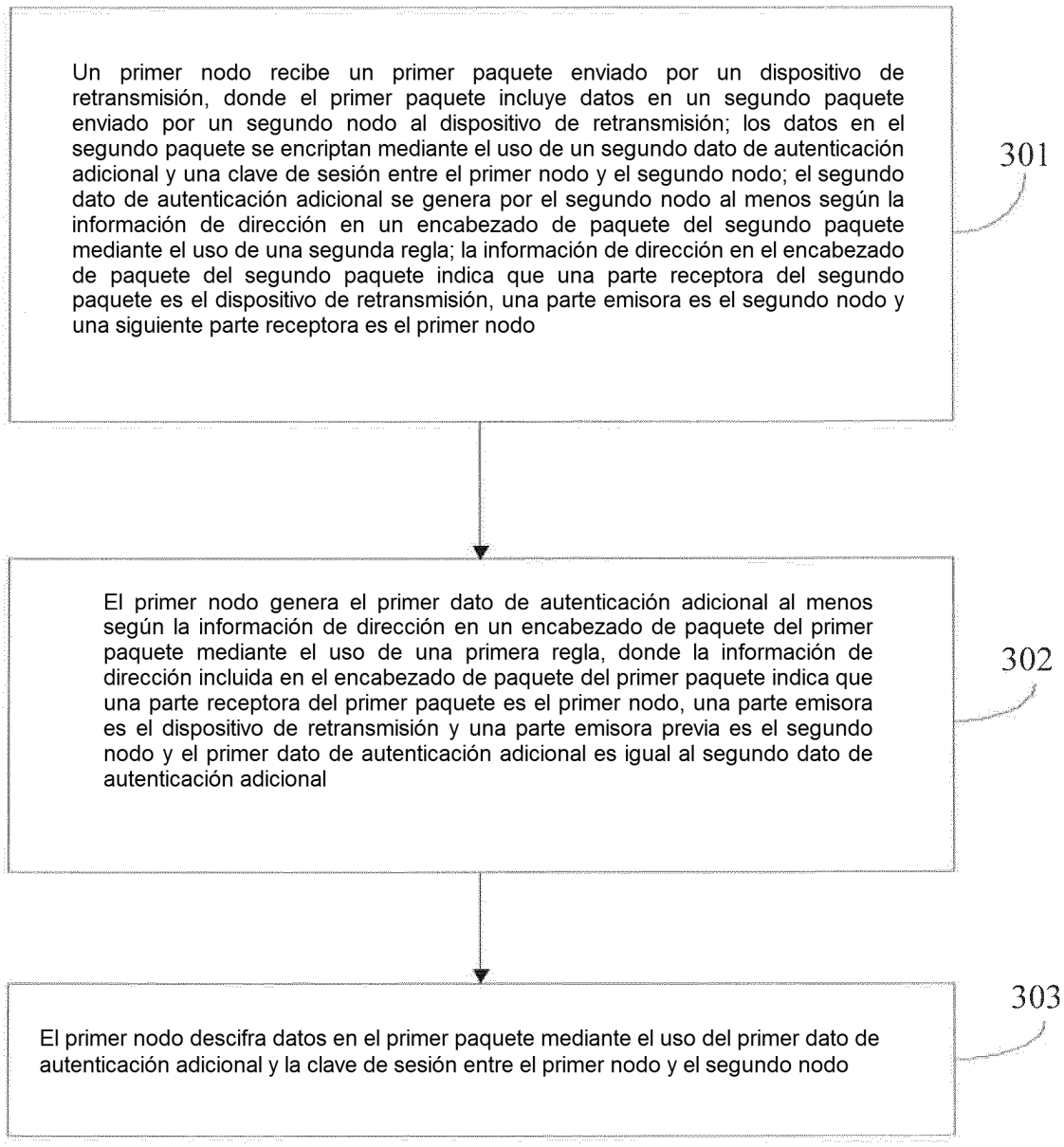
Un primer nodo recibe un primer paquete enviado por un dispositivo de retransmisión, donde el primer paquete incluye datos en un segundo paquete enviado por un segundo nodo al dispositivo de retransmisión; los datos en el segundo paquete se encriptan mediante el uso de un segundo dato de autenticación adicional y una clave de sesión entre el primer nodo y el segundo nodo; el segundo dato de autenticación adicional se genera por el segundo nodo al menos según la información de dirección en un encabezado de paquete del segundo paquete mediante el uso de una segunda regla; la información de dirección en el encabezado de paquete del segundo paquete indica que una parte receptora del segundo paquete es el dispositivo de retransmisión, una parte emisora es el segundo nodo y una siguiente parte receptora es el primer nodo
301
El primer nodo genera el primer dato de autenticación adicional al menos según la información de dirección en un encabezado de paquete del primer paquete mediante el uso de una primera regla, donde la información de dirección incluida en el encabezado de paquete del primer paquete indica que una parte receptora del primer paquete es el primer nodo, una parte emisora es el dispositivo de retransmisión y una parte emisora previa es el segundo nodo y el primer dato de autenticación adicional es igual al segundo dato de autenticación adicional
302
El primer nodo descifra datos en el primer paquete mediante el uso del primer dato de autenticación adicional y la clave de sesión entre el primer nodo y el segundo nodo
303

FIG. 3


Segundo paquete
Primer paquete
Estación
Dispositivo de retransmisión
Punto de acceso

FIG. 4

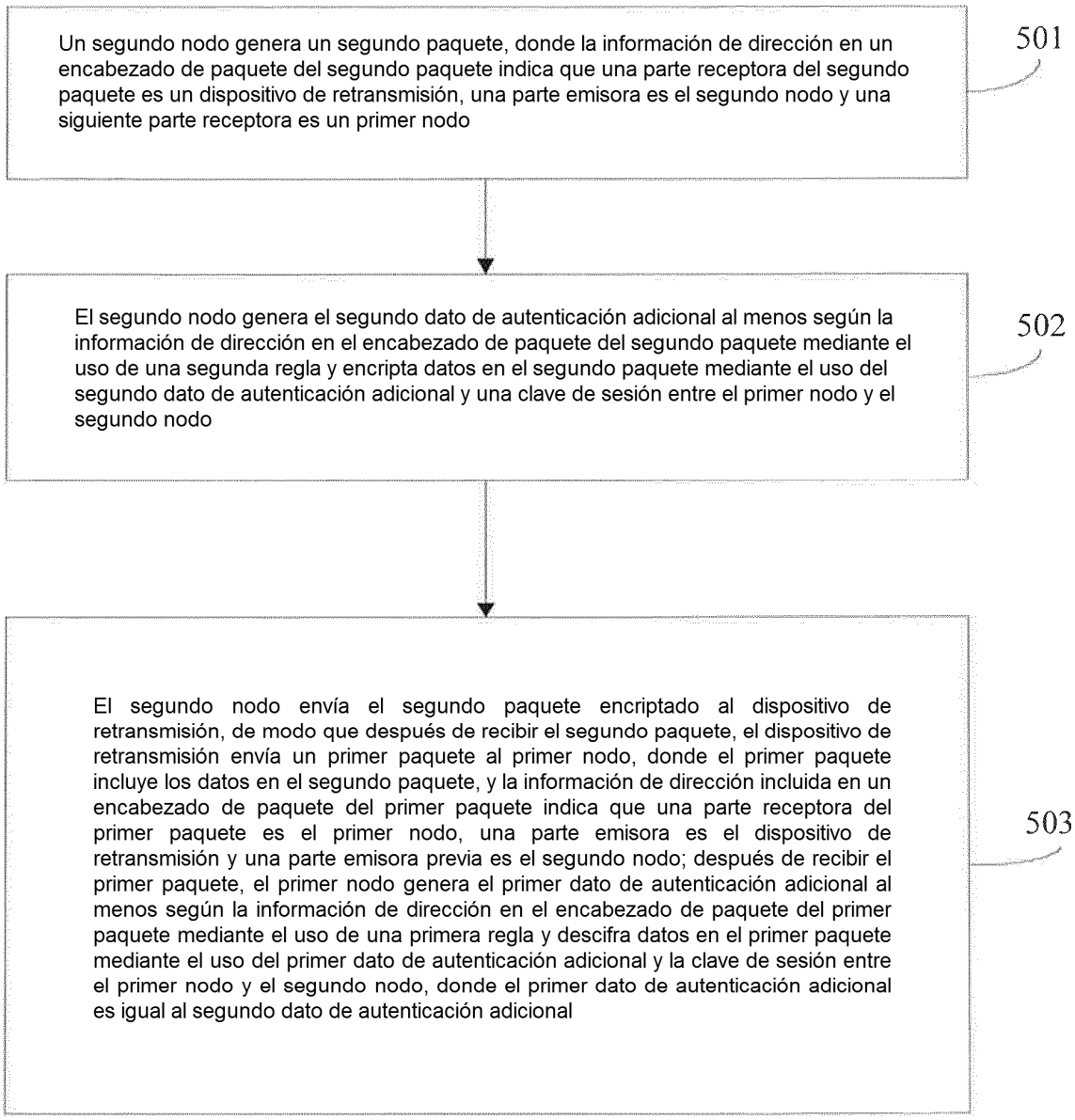
Un segundo nodo genera un segundo paquete, donde la información de dirección en un encabezado de paquete del segundo paquete indica que una parte receptora del segundo paquete es un dispositivo de retransmisión, una parte emisora es el segundo nodo y una siguiente parte receptora es un primer nodo
501
El segundo nodo genera el segundo dato de autenticación adicional al menos según la información de dirección en el encabezado de paquete del segundo paquete mediante el uso de una segunda regla y encripta datos en el segundo paquete mediante el uso del segundo dato de autenticación adicional y una clave de sesión entre el primer nodo y el segundo nodo
502
El segundo nodo envía el segundo paquete encriptado al dispositivo de retransmisión, de modo que después de recibir el segundo paquete, el dispositivo de retransmisión envía un primer paquete al primer nodo, donde el primer paquete incluye los datos en el segundo paquete, y la información de dirección incluida en un encabezado de paquete del primer paquete indica que una parte receptora del primer paquete es el primer nodo, una parte emisora es el dispositivo de retransmisión y una parte emisora previa es el segundo nodo; después de recibir el primer paquete, el primer nodo genera el primer dato de autenticación adicional al menos según la información de dirección en el encabezado de paquete del primer paquete mediante el uso de una primera regla y descifra datos en el primer paquete mediante el uso del primer dato de autenticación adicional y la clave de sesión entre el primer nodo y el segundo nodo, donde el primer dato de autenticación adicional es igual al segundo dato de autenticación adicional
503

FIG. 5

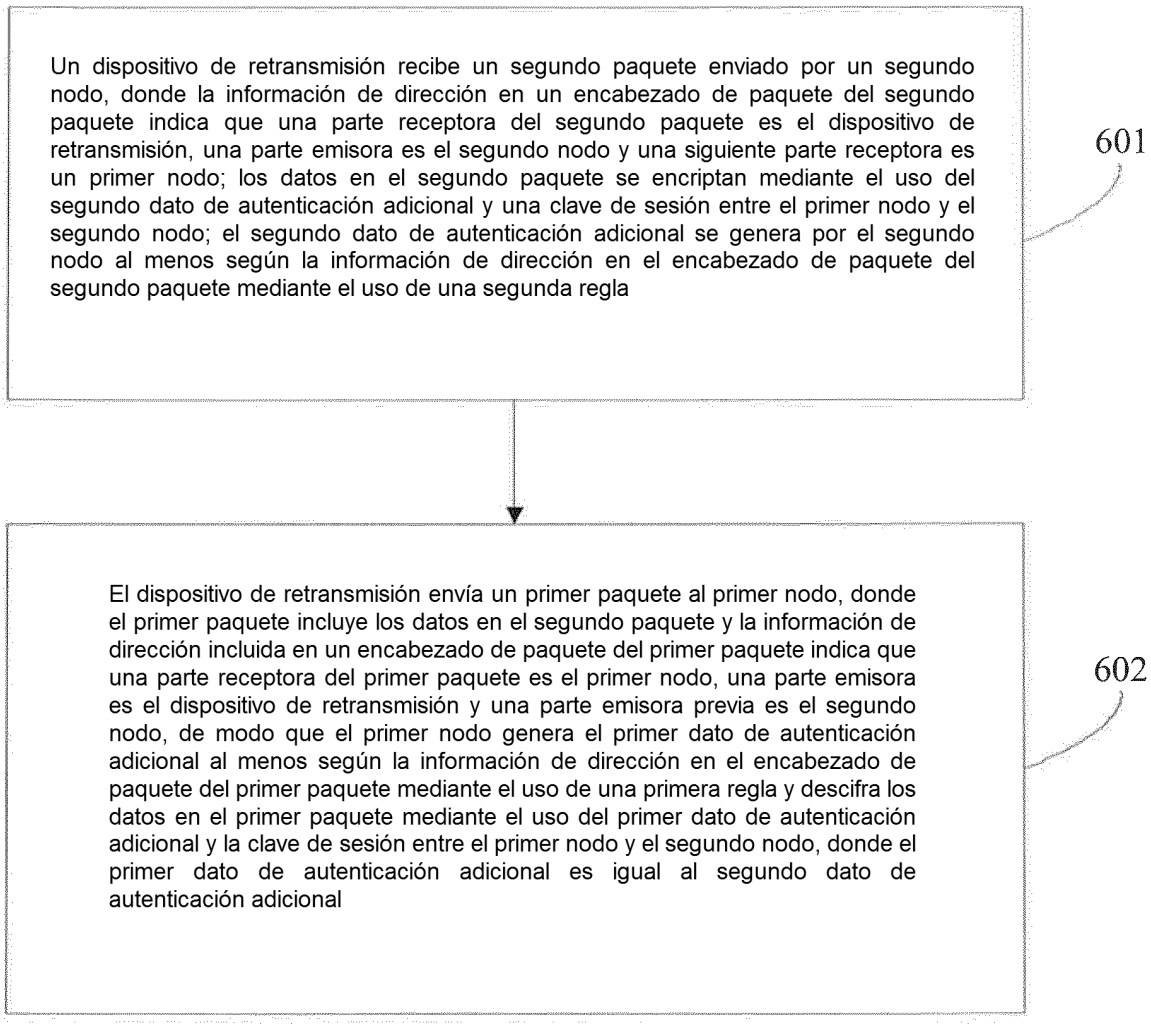
Un dispositivo de retransmisión recibe un segundo paquete enviado por un segundo nodo, donde la información de dirección en un encabezado de paquete del segundo paquete indica que una parte receptora del segundo paquete es el dispositivo de retransmisión, una parte emisora es el segundo nodo y una siguiente parte receptora es un primer nodo; los datos en el segundo paquete se encriptan mediante el uso del segundo dato de autenticación adicional y una clave de sesión entre el primer nodo y el segundo nodo; el segundo dato de autenticación adicional se genera por el segundo nodo al menos según la información de dirección en el encabezado de paquete del segundo paquete mediante el uso de una segunda regla
601
El dispositivo de retransmisión envía un primer paquete al primer nodo, donde el primer paquete incluye los datos en el segundo paquete y la información de dirección incluida en un encabezado de paquete del primer paquete indica que una parte receptora del primer paquete es el primer nodo, una parte emisora es el dispositivo de retransmisión y una parte emisora previa es el segundo nodo, de modo que el primer nodo genera el primer dato de autenticación adicional al menos según la información de dirección en el encabezado de paquete del primer paquete mediante el uso de una primera regla y descifra los datos en el primer paquete mediante el uso del primer dato de autenticación adicional y la clave de sesión entre el primer nodo y el segundo nodo, donde el primer dato de autenticación adicional es igual al segundo dato de autenticación adicional
602

FIG. 6

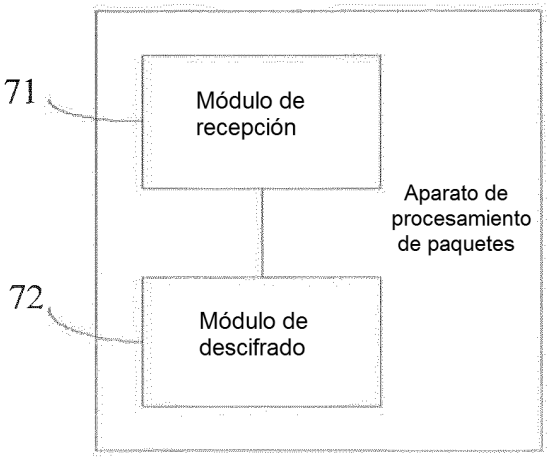
71
Módulo de recepción
Aparato de procesamiento de paquetes
72
Módulo de descifrado

FIG. 7

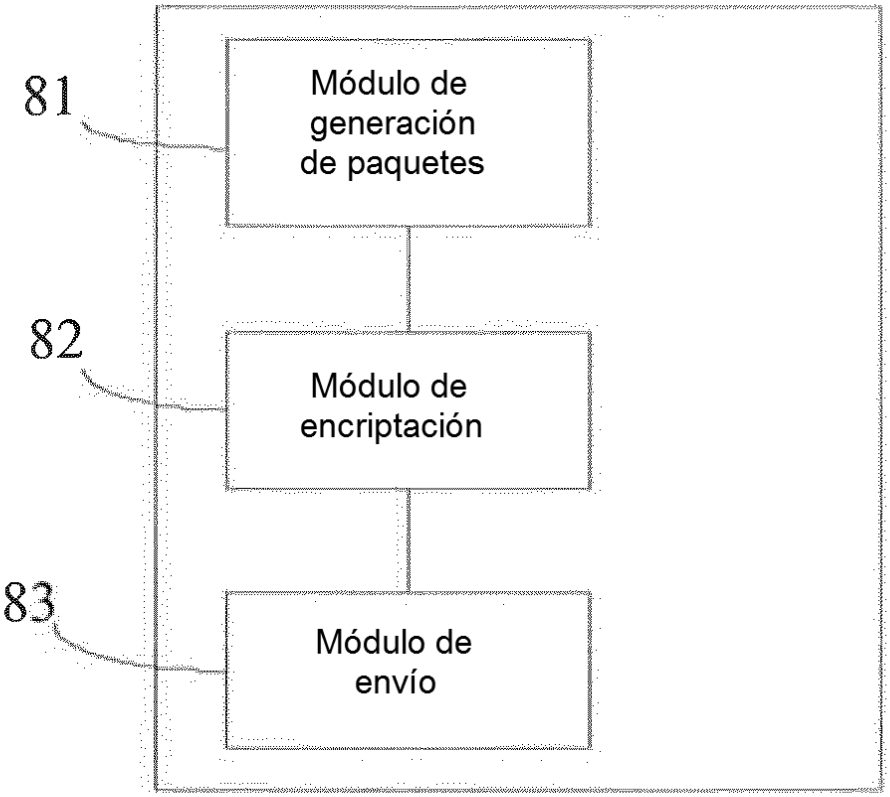
81
Módulo de generación de paquetes
82
Módulo de encriptación
83
Módulo de envío

FIG. 8

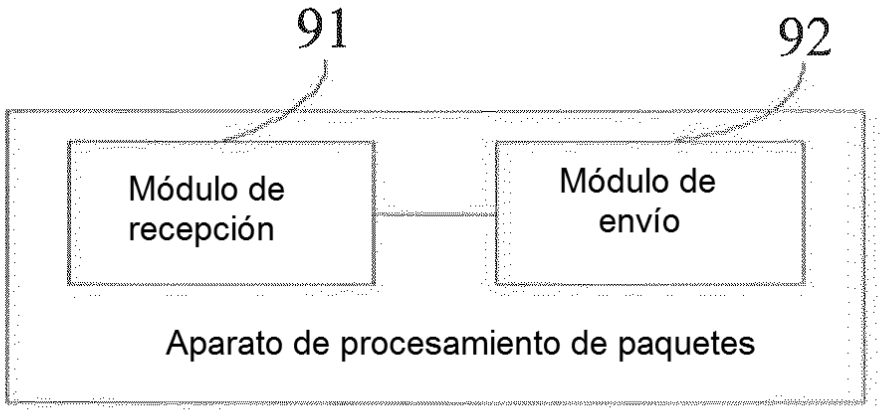
91
92
Módulo de recepción
Módulo de envío
Aparato de procesamiento de paquetes

FIG. 9

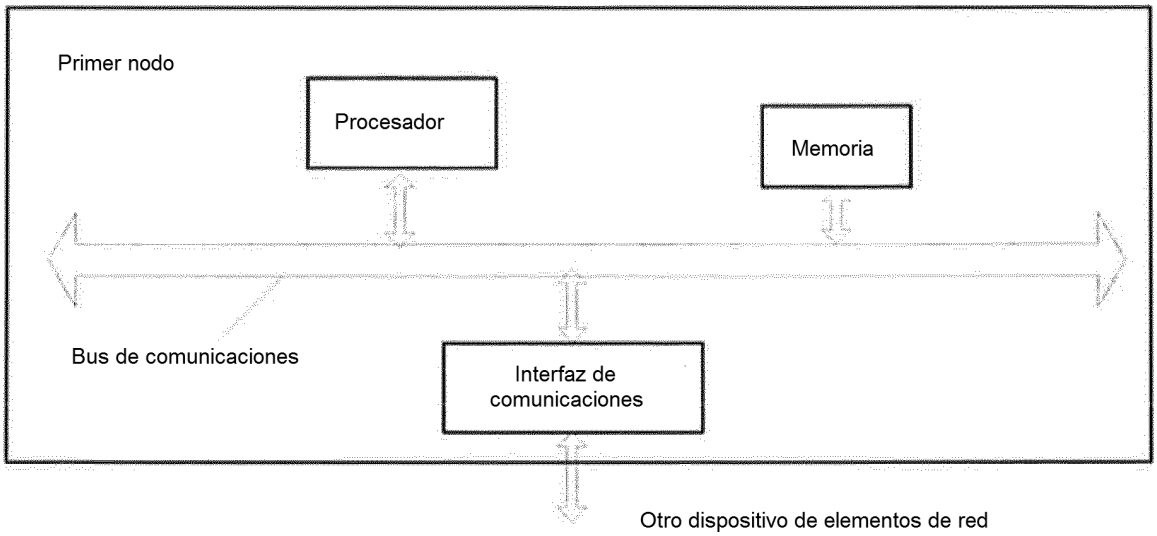
Primer nodo
Procesador
Memoria
Bus de comunicaciones
Interfaz de comunicaciones
Otro dispositivo de elementos de red

FIG. 10

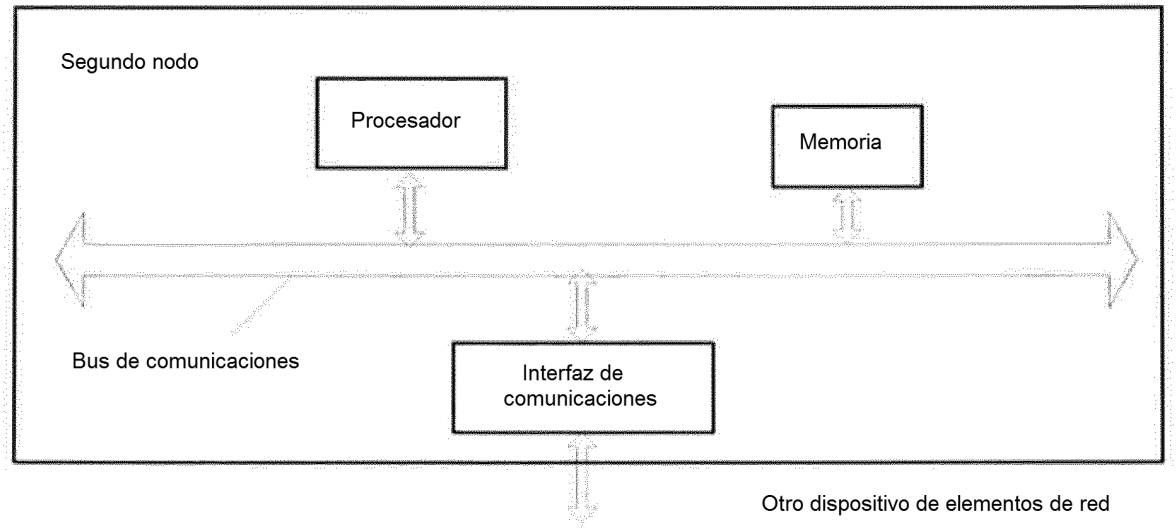
Segundo nodo
Procesador
Memoria
Bus de comunicaciones
Interfaz de comunicaciones
Otro dispositivo de elementos de red

FIG. 11

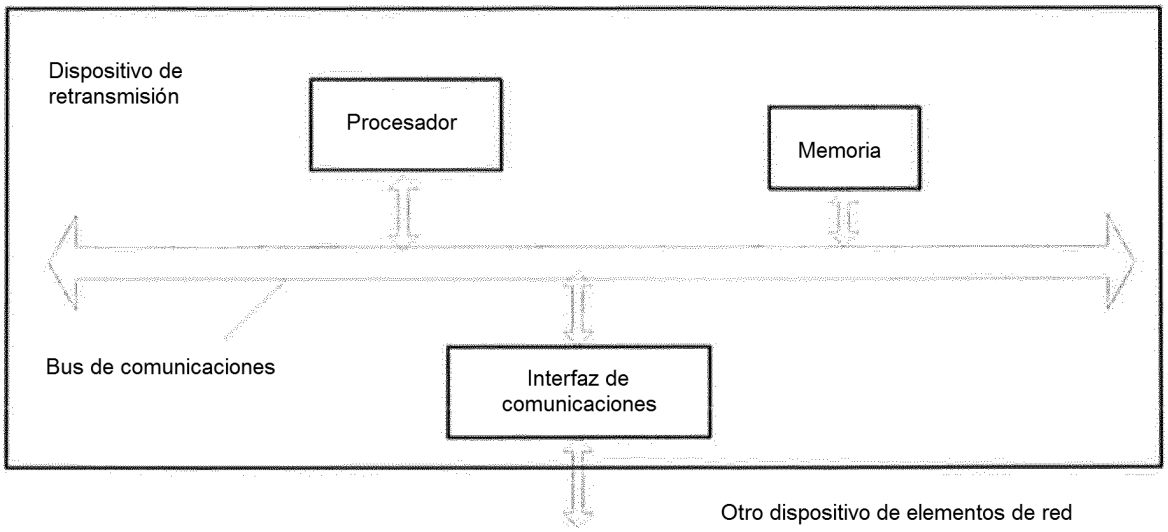
Dispositivo de retransmisión
Procesador
Memoria
Bus de comunicaciones
Interfaz de comunicaciones
Otro dispositivo de elementos de red

FIG. 12


13
11
12
Segundo nodo
Dispositivo de retransmisión
Primer nodo

FIG. 13