(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 794 641**

(51) Int. CI.:

H04L 12/741 (2013.01)
H04L 12/755 (2013.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.12.2016 PCT/CN2016/111137**

(87) Fecha y número de publicación internacional: **21.09.2017 WO17157072**

(96) Fecha de presentación y número de la solicitud europea: **20.12.2016 E 16894231 (6)**

(97) Fecha y número de publicación de la concesión europea: **01.04.2020 EP 3422647**

(54) Título: **Método, controlador y sistema para detectar anormalidades de reenvío de flujos de datos**

(30) Prioridad:

15.03.2016 CN 201610147518

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.11.2020

(73) Titular/es:

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

(72) Inventor/es:

WANG, DONGHUI;
ZHOU, YADONG y
HU, CHENGCHEN

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método, controlador y sistema para detectar anormalidades de reenvío de flujos de datos

Campo técnico

La presente invención se refiere al campo de comunicaciones en una red informática y, en particular, a un método y sistema de detección de anormalidades en el reenvío de flujos de datos, y a un controlador.

Antecedentes

Con referencia a la figura 1, una red de red definida por software (SDN – Software Defined Network, en inglés) es una nueva estructura de sistema de red, que integra una pluralidad de funciones de control de una red en un controlador mediante la separación de un plano de control de un plano de reenvío de la red, y suministra información de control por medio de comunicación interactiva entre el controlador y los dispositivos de conmutación. Los dispositivos de conmutación procesan flujos de datos en base a la información de control. Específicamente, la información de control se suministra utilizando una tabla de flujos.

La tabla de flujos es una regla de procesamiento de flujos de datos suministrada por el controlador al dispositivo de conmutación, y una tabla de flujos en el dispositivo de conmutación incluye entradas de flujo. Con referencia a la figura 2, una estructura básica de datos de una entrada de flujo incluye tres partes: un campo de coincidencia, contadores e instrucciones. El campo de coincidencia incluye información de la cabecera del paquete de datos como puerto de entrada de flujo de datos, una dirección MAC (Control de acceso a medios, Media Access Control, en inglés) del origen / destino y una dirección IP (Protocolo de Internet, Internet Protocol, en inglés) del origen / destino. Cuando un flujo de datos llega al dispositivo de conmutación, el dispositivo de conmutación realiza un cotejo en las entradas de flujo en el dispositivo de conmutación en base a la información de las características de un paquete de datos, por ejemplo, la información de cabecera, y a un puerto de entrada. Una vez que se coteja una entrada de flujo, el paquete de datos es procesado de acuerdo con las operaciones especificadas en las instrucciones en la entrada de flujo. Las operaciones incluyen, por ejemplo, descartar, reenviar y modificar el paquete de datos. Además, después de que el paquete de datos coincide con la entrada de flujo, el dispositivo de conmutación actualiza los contadores correspondientes a la entrada de flujo. Es decir, el dispositivo de conmutación puede obtener, mediante la utilización de los contadores, una cantidad de flujos de datos que coincida con cada entrada de flujo, a saber, tráfico real.

Para una red de arquitectura SDN mostrada en la figura 1, cuando un atacante (por ejemplo, el atacante 14 en la figura 1) falsifica la entrada de flujo de un dispositivo de conmutación (por ejemplo, S5 en la figura 1) o la entrada de flujo del dispositivo de conmutación es anormal, una ruta correcta (por ejemplo, Anfitrión 1 -> S1 -> S5 -> S9 -> S7 -> S3 -> Anfitrión 5 que se muestra en la figura 1) desde un anfitrión de origen (por ejemplo, el Anfitrión 1 en la figura 1) hasta un anfitrión de destino (por ejemplo, el Anfitrión 5 en la figura 1) suministrado por un controlador (por ejemplo, un controlador 11 en la figura 1) es falsificada a una ruta incorrecta (por ejemplo, el Anfitrión 1 -> S1 -> S5 -> S10 -> S7 -> S3 -> Anfitrión 5 en la figura 1). El dispositivo de conmutación S9 puede ser un dispositivo de seguridad, por ejemplo, un cortafuegos o un IPS (sistema de prevención de intrusiones, Intrusion Prevention System, en inglés y en chino). Debido a dicha falsificación realizada por el atacante, el flujo de datos omite un control realizado por el dispositivo de seguridad. Una razón fundamental es que la regla de reenvío de flujos de datos suministrada por el controlador es incoherente con un estado real del reenvío de flujos de datos, y dicha incoherencia no puede ser detectada utilizando un medio técnico de la técnica anterior. Un método de detección de anormalidades en los flujos de datos se describe en el documento de la técnica anterior “Lightweight DDoS Flooding Attack Detection Using NOX/OpenFlow”.

Compendio

Las realizaciones de la presente invención proporcionan un método y un sistema de detección de anormalidades en el reenvío, y un controlador, para resolver un problema de que se debe realizar una detección cuando una regla de reenvío de flujos de datos es incoherente con un estado real del reenvío de un flujo de datos debido a una anormalidad en la tabla de flujos.

Las siguientes soluciones técnicas se utilizan en las realizaciones de la presente invención para conseguir el objetivo anterior.

De acuerdo con un primer aspecto, se proporciona un método de detección de anormalidades en el reenvío de flujos de datos. El método incluye, específicamente, las siguientes etapas:

determinar, por parte de un controlador, un dispositivo de conmutación a través del cual pasa un flujo de datos a detectar;

obtener, por parte del controlador, al menos una entrada de flujo que coincide con el flujo de datos y que esté en el dispositivo de conmutación, donde la entrada de flujo incluye tráfico real y un campo de coincidencia;

establecer, por parte del controlador, un conjunto de ecuaciones sobredeterminado en base al tráfico real y al tráfico teórico de un flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación; y

determinar, por parte del controlador, en base al conjunto de ecuaciones sobredeterminado, si al menos una entrada de flujo es anormal.

De acuerdo con el método de detección de anormalidades en el reenvío de flujos de datos proporcionado en la presente invención, el controlador determina el dispositivo de conmutación a través del cual pasa el flujo de datos a detectar; obtiene al menos una entrada de flujo que coincide con el flujo de datos y que está en el dispositivo de conmutación, donde la entrada de flujo incluye el tráfico real y el campo de coincidencia; y determina, en base al conjunto de ecuaciones sobredeterminado, si la al menos una entrada de flujo es anormal. En base al método matemático en esta realización de la presente invención, el campo de coincidencia en la entrada de flujo suministrado por el controlador corresponde a un campo de coincidencia en una entrada de flujo almacenado en el dispositivo de conmutación, el tráfico teórico del flujo de datos en el dispositivo de conmutación y el tráfico real son abstraídos como el conjunto de ecuaciones sobredeterminado, se obtiene una norma de error cuadrático utilizando una solución de mínimos cuadrados del conjunto de ecuaciones sobredeterminado, para determinar si la entrada de flujo es anormal y, si se encuentra una entrada anormal de flujos, resolver, de este modo, el problema de que se debe realizar una detección cuando una regla de reenvío de flujos de datos es incoherente con un estado real del reenvío del flujo de datos, porque la tabla de flujos está falsificada.

Con referencia al primer aspecto, en una primera implementación posible, el método de detección de anormalidades en el reenvío de flujos de datos incluye:

sustituir una solución de mínimos cuadrados del conjunto de ecuaciones sobredeterminado en un lado de vector de números incógnita del conjunto de ecuaciones sobredeterminado, para obtener un vector actualizado de términos constantes;

obtener una norma de error cuadrático en base a un vector de términos constantes del conjunto de ecuaciones sobredeterminado y el vector actualizado de términos constantes; y

comparar la norma de error cuadrático con un primer umbral, para determinar si una entrada de flujo es anormal.

Con referencia a la primera implementación posible del primer aspecto, en una segunda implementación posible, el método de detección de anormalidades en el reenvío de flujos de datos incluye:

generar un vector de diferencia calculando las diferencias entre el vector actualizado de términos constantes y el vector de términos constantes del conjunto de ecuaciones sobredeterminado, comparando cada diferencia en el vector de diferencia con un segundo umbral, y determinar una entrada anormal de flujo en las entradas de flujo correspondientes a una o más diferencias que exceden el segundo umbral y que están en las diferencias.

Con referencia al primer aspecto, en una tercera implementación posible, la entrada de flujo incluye, además, un indicador de agregación, y el indicador de agregación se utiliza para indicar si la entrada de flujo es una entrada de flujo agregado; y

la unidad de cálculo está configurada, además, para:

determinar, de acuerdo con el indicador de agregación, si la entrada de flujo es una entrada de flujo agregado;

establecer, en base a un resultado de determinación de la entrada de flujo, una ecuación mediante la igualación del tráfico teórico del flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación, con el tráfico real; y

combinar las ecuaciones establecidas en base a una pluralidad de campos de coincidencia, para generar el conjunto de ecuaciones sobredeterminado.

Con referencia a la tercera implementación posible del primer aspecto, en una cuarta implementación posible, el método de detección de anormalidades en el reenvío de flujos de datos incluye:

cuando se puede encontrar un flujo de datos coincidente mediante la utilización del campo de coincidencia, si se determina que la entrada de flujo no es una entrada de flujo agregado, lo que indica que el campo de coincidencia coincide con un flujo de datos,

establecer una ecuación mediante la igualación del tráfico teórico del flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación, con el tráfico real; o

si se determina que la entrada de flujo es una entrada de flujo agregado, lo que indica que el campo de coincidencia coincide con una pluralidad de flujos de datos,

establecer una ecuación mediante la igualación de una suma de tráficos teóricos de la pluralidad de flujos de datos que coinciden con el campo de coincidencia y que están en el dispositivo de conmutación, con el tráfico real.

Con referencia a cualquiera del primer aspecto y de la primera a la cuarta implementaciones posibles del primer aspecto, en una quinta implementación posible, el método de detección de anormalidades en el reenvío de flujos de datos incluye:

establecer el conjunto de ecuaciones sobredeterminado como

$$\begin{pmatrix} a_{11} & \cdots & a_{1p} \\ \vdots & \ddots & \vdots \\ a_{q1} & \cdots & a_{qp} \end{pmatrix} \bullet \left(m_1, m_2, m_3, ..., m_p\right)^T = \left(c_1, c_2, c_3, ..., c_q\right)^T$$

De acuerdo con un segundo aspecto, se proporciona un controlador. El controlador está configurado para realizar el método de acuerdo con cualquiera del primer aspecto o las implementaciones posibles del primer aspecto. El controlador incluye:

una unidad de detección, configurada para determinar un dispositivo de conmutación a través del cual pasa un flujo de datos a detectar;

una unidad de obtención, configurada para obtener al menos una entrada de flujo que coincide con el flujo de datos y que está en el dispositivo de conmutación determinado por la unidad de detección, donde la entrada de flujo incluye el tráfico real y un campo de coincidencia;

una unidad de cálculo, configurada para establecer un conjunto de ecuaciones sobredeterminado en base al tráfico real y al tráfico teórico de un flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación determinado por la unidad de detección;

una unidad de determinación, configurada para determinar, en base al conjunto de ecuaciones sobredeterminado establecido por la unidad de cálculo, si la al menos una entrada de flujo es anormal.

El controlador en la presente invención puede estar configurado para realizar el procedimiento del método de acuerdo con el primer aspecto y, por lo tanto, para los efectos técnicos que se pueden obtener mediante el controlador, véase el método de acuerdo con el primer aspecto. Los detalles no se describen de nuevo en la presente invención.

Con referencia al segundo aspecto, en una primera implementación posible, la unidad de cálculo está configurada, además, para:

sustituir una solución de mínimos cuadrados del conjunto de ecuaciones sobredeterminado en un lado de vector de números incógnita del conjunto de ecuaciones sobredeterminado, para obtener un vector actualizado de términos constantes;

obtener una norma de error cuadrático en base a un vector de términos constantes del conjunto de ecuaciones sobredeterminado y al vector actualizado de términos constantes; y

comparar la norma de error cuadrático con un primer umbral para determinar si una entrada de flujo es anormal.

Con referencia a la primera implementación posible del segundo aspecto, en una segunda implementación posible, la unidad de determinación está configurada, además, para:

generar un vector de diferencia calculando las diferencias entre el vector actualizado de términos constantes y el vector de términos constantes del conjunto de ecuaciones sobredeterminado, comparar cada diferencia en el vector de diferencia con un segundo umbral, y determinar una entrada anormal de flujo en las entradas de flujo correspondientes a una o más diferencias que exceden el segundo umbral y que están en las diferencias.

Con referencia al segundo aspecto, en una tercera implementación posible, la entrada de flujo incluye, además, un indicador de agregación, y el indicador de agregación se utiliza para indicar si la entrada de flujo es una entrada de flujo agregado; y

que la unidad de cálculo esté configurada, además, para establecer un conjunto de ecuaciones sobredeterminado en base al tráfico real y al tráfico teórico de un flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación incluye:

determinar, de acuerdo con el indicador de agregación, si la entrada de flujo es una entrada de flujo agregado;

establecer, en base a un resultado de determinación de la entrada de flujo, una ecuación mediante la igualación del tráfico teórico del flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación, con el tráfico real; y

combinar las ecuaciones establecidas en base a una pluralidad de campos de coincidencia, para generar el conjunto de ecuaciones sobredeterminado.

Con referencia a la tercera implementación posible del segundo aspecto, en una cuarta implementación posible, la unidad de cálculo está configurada, además, para:

cuando se puede encontrar un flujo de datos coincidente mediante la utilización del campo de coincidencia,

si se determina que la entrada de flujo no es una entrada de flujo agregado, lo que indica que el campo de coincidencia coincide con un flujo de datos,

establecer una ecuación mediante la igualación del tráfico teórico del flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación, con el tráfico real; o

si se determina que la entrada de flujo es una entrada de flujo agregado, lo que indica que el campo de coincidencia coincide con una pluralidad de flujos de datos, establecer una ecuación mediante la igualación de una suma de tráficos teóricos de la pluralidad de flujos de datos que coinciden con el campo de coincidencia y que están en el dispositivo de conmutación, con el tráfico real.

Con referencia a cualquiera del segundo aspecto o a las posibles implementaciones del segundo aspecto, en una quinta implementación posible, la unidad de cálculo está configurada, además, para:

establecer el conjunto de ecuaciones sobredeterminado como

$$\begin{pmatrix} a_{11} & \cdots & a_{1p} \\ \vdots & \ddots & \vdots \\ a_{q1} & \cdots & a_{qp} \end{pmatrix} \bullet \left(m_1, m_2, m_3, \ldots, m_p\right)^T = \left(c_1, c_2, c_3, \ldots, c_q\right)^T$$

De acuerdo con un tercer aspecto, se proporciona un controlador. El controlador está configurado para realizar el método de acuerdo con cualquiera del primer aspecto o las implementaciones posibles del primer aspecto. El controlador incluye un procesador, una memoria y un bus. El procesador y la memoria se conectan mediante el bus y se completa la comunicación mutua. El procesador está configurado para ejecutar el código de programa en la memoria para realizar las siguientes operaciones:

determinar un dispositivo de conmutación a través del cual pasa un flujo de datos a detectar;

obtener al menos una entrada de flujo que coincide con el flujo de datos y que esté en el dispositivo de conmutación, donde la entrada de flujo incluye tráfico real y un campo de coincidencia;

establecer un conjunto de ecuaciones sobredeterminado en base al tráfico real y al tráfico teórico de un flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación; y

determinar, en base al conjunto de ecuaciones sobredeterminado, si la al menos una entrada de flujo es anormal.

El controlador en la presente invención puede estar configurado para realizar el procedimiento del método de acuerdo con el primer aspecto y, por lo tanto, para los efectos técnicos que pueden ser obtenidos por el controlador, véase el método de acuerdo con el primer aspecto. Los detalles no se describen de nuevo en la presente invención.

Con referencia al tercer aspecto, en una primera implementación posible, el procesador está configurado, además, para:

sustituir una solución de mínimos cuadrados en el conjunto de ecuaciones sobredeterminado en un lado de vector de números incógnita del conjunto de ecuaciones sobredeterminado, para obtener un vector actualizado de términos constantes;

obtener una norma de error cuadrático en base a un vector de términos constantes del conjunto de ecuaciones sobredeterminado y al vector actualizado de términos constantes; y

comparar la norma de error cuadrático con un primer umbral, para determinar si una entrada de flujo es anormal.

Con referencia a la primera implementación posible del tercer aspecto, en una segunda implementación posible, el procesador está configurado, además, para:

generar un vector de diferencia calculando las diferencias entre el vector actualizado de términos constantes y el vector de términos constantes del conjunto de ecuaciones sobredeterminado, comparar cada diferencia en el vector de

diferencia con un segundo umbral, y determinar una entrada anormal de flujo en las entradas de flujo correspondientes a una o más diferencias que exceden el segundo umbral y que están en las diferencias.

Con referencia al tercer aspecto, en una tercera implementación posible, el procesador está configurado, además, para:

la entrada de flujo incluye, además, un indicador de agregación, y el indicador de agregación se utiliza para indicar si la entrada de flujo es una entrada de flujo agregado; y

el establecimiento de un conjunto de ecuaciones sobredeterminado en base al tráfico real y al tráfico teórico de un flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación incluye:

determinar, de acuerdo con el indicador de agregación, si la entrada de flujo es una entrada de flujo agregado;

establecer, en base a un resultado de determinación de la entrada de flujo, una ecuación mediante la igualación del tráfico teórico del flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación, con el tráfico real; y

combinar las ecuaciones establecidas en base a una pluralidad de campos de coincidencia, para generar el conjunto de ecuaciones sobredeterminado.

Con referencia a la tercera implementación posible del tercer aspecto, en una cuarta implementación posible, el procesador está configurado, además, para:

cuando se puede encontrar un flujo de datos coincidente mediante la utilización del campo de coincidencia,

si se determina que la entrada de flujo no es una entrada de flujo agregado, lo que indica que el campo de coincidencia coincide con un flujo de datos,

establecer una ecuación mediante la igualación del tráfico teórico del flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación, con el tráfico real; o

si se determina que la entrada de flujo es una entrada de flujo agregado, lo que indica que el campo de coincidencia coincide con una pluralidad de flujos de datos,

establecer una ecuación mediante la igualación de una suma de tráficos teóricos de la pluralidad de flujos de datos que coinciden con el campo de coincidencia y que están en el dispositivo de conmutación, con el tráfico real.

Con referencia a cualquiera del tercer aspecto o las implementaciones posibles del tercer aspecto, en una quinta implementación posible, el conjunto de ecuaciones sobredeterminado es

$$\begin{pmatrix} a_{11} & \cdots & a_{1p} \\ \vdots & \ddots & \vdots \\ a_{q1} & \cdots & a_{qp} \end{pmatrix} \bullet \left(m_1, m_2, m_3, ..., m_p\right)^T = \left(c_1, c_2, c_3, ..., c_q\right)^T$$

De acuerdo con un cuarto aspecto, se proporciona un sistema de detección de anormalidades en el reenvío de flujos de datos. El sistema de detección de anormalidades de reenvío de flujos de datos incluye el controlador de acuerdo con uno cualquiera del segundo aspecto o las implementaciones posibles del segundo aspecto, o

incluye el controlador de acuerdo con uno cualquiera del tercer aspecto o las implementaciones posibles del tercer aspecto.

El sistema de detección de anormalidades en el reenvío de flujos de datos proporcionado en las realizaciones de la presente invención incluye el controlador de acuerdo con uno cualquiera del segundo aspecto o las implementaciones posibles del segundo aspecto, o incluye el controlador de acuerdo con uno cualquiera del tercer aspecto o las implementaciones posibles del tercer aspecto. Por lo tanto, para conocer los efectos técnicos que pueden ser obtenidos por el sistema de detección de anormalidades en el reenvío de flujos de datos, véanse los efectos técnicos del controlador. Los detalles no se describen de nuevo en el presente documento.

Breve descripción de los dibujos

Para describir más claramente las soluciones técnicas en las realizaciones de la presente invención o en la técnica anterior, a continuación, se describen brevemente los dibujos adjuntos necesarios para describir las realizaciones de la técnica anterior. Aparentemente, los dibujos que se acompañan en la siguiente descripción muestran simplemente algunas realizaciones de la presente invención, y una persona con conocimientos ordinarios en la materia aún puede obtener otros dibujos a partir de estos dibujos que se acompañan, sin esfuerzos creativos.

La figura 1 es un diagrama estructural, esquemático, de una red de arquitectura SDN cuya entrada de flujo es falsificada, de acuerdo con una realización de la presente invención;

la figura 2 es un diagrama estructural, esquemático, de datos de una entrada de flujo, de acuerdo con una realización de la presente invención;

la figura 3 es un diagrama esquemático, simplificado, de una red de arquitectura SDN, de acuerdo con una realización de la presente invención;

la figura 4 es un diagrama de flujo, esquemático, de un método de detección de anormalidades en el reenvío de flujos de datos, de acuerdo con una realización de la presente invención;

la figura 5 es un diagrama de flujo, esquemático, de otro método de detección de anormalidades en el reenvío de flujos de datos, de acuerdo con una realización de la presente invención;

la figura 6 es un diagrama de flujo, esquemático, de establecer una ecuación utilizando el tráfico teórico de un flujo de datos en un mismo campo de coincidencia y el tráfico real, de acuerdo con una realización de la presente invención;

la figura 7 es un diagrama de flujo, esquemático, para establecer una ecuación en base a un resultado de determinación de una entrada de flujo, de acuerdo con una realización de la presente invención;

la figura 8 es un diagrama de flujo, esquemático, para determinar si al menos una entrada de flujo es anormal en base a un conjunto de ecuaciones sobredeterminado, de acuerdo con una realización de la presente invención;

la figura 9 es un diagrama esquemático del resultado de la simulación de una anormalidad de entrada de flujo, de acuerdo con una realización de la presente invención;

la figura 10 es un diagrama estructural, esquemático, de un controlador, de acuerdo con una realización de la presente invención; y

la figura 11 es un diagrama estructural, esquemático, de otro controlador de acuerdo, con una realización de la presente invención.

Descripción de las realizaciones

Lo que sigue describe claramente las soluciones técnicas en las realizaciones de la presente invención con referencia a los dibujos adjuntos en las realizaciones de la presente invención. Aparentemente, las realizaciones descritas son simplemente algunas, pero no todas, las realizaciones de la presente invención. Todas las demás realizaciones obtenidas por una persona de habilidad ordinaria en la técnica, en base a las realizaciones de la presente invención sin esfuerzos creativos, caerán dentro del alcance de protección de la presente invención.

Las realizaciones de la presente invención proporcionan un sistema de detección de anormalidades en el reenvío de flujos de datos. Con referencia a la figura 1, el sistema de detección de anormalidades en el reenvío de flujos de datos incluye un controlador 11, un dispositivo de conmutación 12 y un anfitrión 13. Las realizaciones de la presente invención se aplican principalmente a una red SDN / OpenFlow (nombre chino: OpenFlow). Es necesario que, en una ruta a través de la cual pasa un flujo de datos, al menos un dispositivo de conmutación no sea atacado y pueda funcionar normalmente. Una entrada de tráfico de la red puede coincidir con precisión con todos los flujos de datos, es decir, no se agregan entradas de flujo en un dispositivo de conmutación de entrada. Además, los relojes de los dispositivos de conmutación en la red son síncronos, lo que garantiza que la información leída de la tabla de flujos sea coherente.

Para simplificar la descripción que se muestra a continuación, haciendo referencia a la figura 3, se describe un modo de transmisión de flujos de datos de una red de arquitectura SDN mediante la utilización de un ejemplo en el que la red de arquitectura SDN tiene un controlador, dos conmutadores y dos anfitriones. En primer lugar, el controlador, un primer dispositivo de conmutación y un segundo dispositivo de conmutación son conectados entre sí mediante la utilización de la red. La red puede ser Internet o una red de área local. Un primer anfitrión y un segundo anfitrión no están conectados directamente, pero se conectan utilizando el primer dispositivo de conmutación y el segundo dispositivo de conmutación. Además, el controlador no se comunica directamente con los anfitriones. El controlador tiene una unidad de procesamiento y una unidad de comunicaciones, el primer dispositivo de conmutación y el segundo dispositivo de conmutación tienen, asimismo, una unidad de procesamiento y una unidad de comunicaciones, y el primer anfitrión y el segundo anfitrión tienen, asimismo, una unidad de procesamiento y una unidad de comunicaciones. Cada dispositivo accede a la red utilizando la unidad de comunicaciones, y la unidad de procesamiento de cada dispositivo está configurada para procesar la información del flujo de datos. Antes de que el primer anfitrión envíe un flujo de datos al segundo anfitrión, el controlador suministra, en primer lugar, una tabla de flujos al primer dispositivo de conmutación y al segundo dispositivo de conmutación, para indicar una ruta de enrutamiento del flujo de datos. Posteriormente, el flujo de datos enviado por el primer anfitrión es enviado, en primer lugar, al primer dispositivo de conmutación y, a continuación, es reenviado al segundo dispositivo de conmutación en base a la tabla de flujos en el primer dispositivo de conmutación, y a continuación, es reenviado al segundo anfitrión

en base a la tabla de flujos en el segundo dispositivo de conmutación. De esta manera, finaliza un proceso de reenvío de flujo de datos completo.

Una idea principal de la presente invención radica en que: debido a que un atacante no puede obtener un permiso de control de cada dispositivo de red, una cantidad de dispositivos de conmutación falsificados por el atacante debe formar parte de una cantidad de dispositivos de conmutación en la ruta correcta suministrada por el controlador. Por lo tanto, para una red relativamente compleja mostrada en la figura 1, si los dispositivos de conmutación no son falsificados, cuando un flujo de datos fluye a través de una ruta s1 -> s5 -> s9 -> s7 -> s3, los valores estadísticos del flujo de datos en todos los dispositivos de conmutación deben ser coherentes. No obstante, cuando el dispositivo de conmutación s5 es falsificado y una ruta a través de la cual fluye realmente el flujo de datos es s1 -> s5 -> s10 -> s7 -> s3, existe un error de tráfico en los valores estadísticos del flujo de datos en todos los dispositivos de conmutación en la ruta correcta original s1 -> s5 -> s9 -> s7 -> s3. En esta solución, se proporciona un método para localizar un dispositivo de conmutación anormal y la entrada de flujo mediante el análisis de los errores de tráfico de un flujo de datos en los dispositivos de conmutación en cada ruta en todos los casos.

Una realización de la presente invención proporciona un método de detección de anormalidades en el reenvío de flujos de datos. Con referencia a la figura 4, el método incluye las siguientes etapas.

S101. Un controlador determina un dispositivo de conmutación a través del cual pasa un flujo de datos a detectar.

En base a una tabla de flujos suministrada correspondiente a cada flujo de datos, el controlador puede aprender de cada dispositivo de conmutación a través del cual fluye teóricamente cada flujo de datos a detectar.

S102. El controlador obtiene al menos una entrada de flujo que coincide con el flujo de datos y que está en el dispositivo de conmutación, donde la entrada de flujo incluye tráfico real y un campo de coincidencia, y el tráfico real es un valor de un contador que está en el dispositivo de conmutación y que corresponde a un flujo de datos que corresponde al campo de coincidencia.

La tabla de flujos incluye al menos una entrada de flujo. El controlador obtiene una tabla de flujos almacenada localmente del dispositivo de conmutación, para obtener al menos una entrada de flujo en la tabla de flujos y obtener, en consecuencia, un campo de coincidencia y un contador en la al menos una entrada de flujo. Tal como se muestra en la figura 2, cada entrada de flujo corresponde a un campo de coincidencia y a un contador. Por lo tanto, el tráfico real de un flujo de datos coincidente correspondiente a un campo de coincidencia en el dispositivo de conmutación se puede conocer mediante la utilización del contador.

Debido a que una cantidad de flujos de datos es, normalmente, menor que una cantidad de entradas de flujo, se pueden encontrar cero o uno o más flujos de datos correspondientes mediante la utilización del campo de coincidencia. Si ningún flujo de datos correspondiente al campo de coincidencia fluye a través del dispositivo de conmutación, se puede encontrar el flujo de datos correspondiente a cero mediante la utilización del campo de coincidencia. Si se determina que un flujo de datos correspondiente al campo de coincidencia fluye a través del dispositivo de conmutación, existen dos casos: para un campo de coincidencia en una entrada de flujo no agregado, se puede encontrar un flujo de datos correspondiente utilizando un campo de coincidencia; para un campo de coincidencia en una entrada de flujo agregado, se pueden encontrar una pluralidad de flujos de datos correspondientes utilizando el mismo campo de coincidencia. Por ejemplo, se supone que una dirección IP de un campo de coincidencia en una entrada de flujo agregado es 10.0.0.0/8, todos los flujos de datos cuyas cabeceras de paquetes de datos incluyen una dirección IP 10.*.*.* pueden coincidir con el campo de coincidencia.

Se establece que el tráfico real, de cero o uno o más flujos de datos correspondientes que corresponden al campo de coincidencia, generado en el dispositivo de conmutación es c.

S103. El controlador establece un conjunto de ecuaciones sobredeterminado en base al tráfico real y al tráfico teórico de un flujo de datos que coincide con el campo de coincidencia y que se encuentra en el dispositivo de conmutación, donde el tráfico teórico forma un vector de números incógnita del conjunto de ecuaciones sobredeterminado y el tráfico real forma un vector de términos constantes del conjunto de ecuaciones sobredeterminado.

La tabla de flujos suministrada por el controlador incluye una entrada de flujo, y la entrada de flujo incluye un campo de coincidencia. En un caso normal en el que el dispositivo de conmutación no está falsificado y atacado, un flujo de datos corresponde a un campo de coincidencia en una entrada de flujo y, en consecuencia, los campos de coincidencia correspondientes en todos los dispositivos de conmutación a través de los cuales el fluye el flujo de datos deben ser iguales.

Además, suponiendo que el tráfico teórico de un flujo de datos es m, el tráfico teórico generado por el flujo de datos en cada dispositivo de conmutación a través del cual el flujo de datos fluye teóricamente también es m.

Se puede encontrar un flujo de datos correspondiente y un tráfico teórico m del flujo de datos en cada dispositivo de conmutación mediante la utilización de un campo de coincidencia.

Para cada entrada de flujo en el dispositivo de conmutación, el controlador puede buscar un mismo campo de coincidencia en la entrada de flujo en una tabla de flujos suministrada mediante la utilización del campo de coincidencia de la entrada de flujo, encontrar un flujo de datos correspondiente en base al campo de coincidencia y, a continuación, encontrar el tráfico teórico m del flujo de datos en el dispositivo de conmutación y establecer una ecuación mediante la igualación del tráfico teórico m con el tráfico real c.

Específicamente, si no se puede encontrar un flujo de datos correspondiente utilizando un campo de coincidencia, se puede formular una ecuación 0 * m = c. En el caso de una entrada de flujo no agregado, y cuando se puede encontrar un flujo de datos correspondiente mediante la utilización de un campo de coincidencia, se puede formular una ecuación m = c. En el caso de una entrada de flujo agregado, cuando se pueden encontrar una pluralidad de flujos de datos correspondientes mediante la utilización de un campo de coincidencia, se puede formular una ecuación m1 + m2 + ... + mk = c, donde k representa que se pueden encontrar k flujos de datos correspondientes mediante la utilización de un campo de coincidencia.

Por ejemplo, se puede formular al menos una de las siguientes ecuaciones:

$0 * m1 = c1$

$m1 + m2 + ... + mk = c2$

Debido a que cada entrada de flujo corresponde a un campo de coincidencia, cada entrada de flujo corresponde a una ecuación.

El controlador construye un conjunto de ecuaciones utilizando todas las ecuaciones, utiliza el tráfico teórico m1, m2, ... de todas las ecuaciones como una parte de las incógnitas del conjunto de ecuaciones, y utiliza el tráfico real c1, c2, ... de todas las ecuaciones como una parte de términos constantes del conjunto de ecuaciones. El conjunto de ecuaciones está representado por AM = C en forma de vectores. A es una matriz de coeficientes del conjunto de ecuaciones, M es un vector de números incógnita formado por el tráfico teórico, y C es un vector de términos constantes formado por el tráfico real.

Debido a que la cantidad de flujos de datos es normalmente menor que la cantidad de entradas de flujo, el conjunto de ecuaciones es un conjunto de ecuaciones sobredeterminado.

S104. El controlador determina, en base al conjunto de ecuaciones sobredeterminado, si la al menos una entrada de flujo es anormal.

Debido a que el conjunto de ecuaciones sobredeterminado no tiene una solución fija, se obtiene una solución de mínimos cuadrados m* resolviendo el conjunto de ecuaciones sobredeterminado, y la solución de mínimos cuadrados m* es una solución aproximada.

La solución de mínimos cuadrados m* se sustituye en el lado de vector de números incógnita del conjunto de ecuaciones sobredeterminado original para obtener un vector actualizado de términos constantes C*, y se obtiene una norma de error cuadrático en base al vector actualizado de términos constantes C* y al vector original de términos constantes C. Si la norma de error cuadrático es mayor que un primer umbral, se puede determinar completamente que la entrada de flujo que construye la ecuación es anormal.

Además, se calculan las diferencias entre C* y C para obtener un vector de diferencia C* - C. En base a cada diferencia del vector de diferencia C* - C, una entrada de flujo que corresponde a una o más diferencias relativamente grandes que exceden un segundo umbral es muy probablemente una entrada anormal de flujo.

De acuerdo con el método de detección de anormalidades en el reenvío de flujos de datos proporcionado en la presente invención, el controlador determina el dispositivo de conmutación a través del cual fluyen los datos a detectar; obtiene al menos una entrada de flujo que coincide con el flujo de datos y que está en el dispositivo de conmutación, donde la entrada de flujo incluye el tráfico real y el campo de coincidencia, y el tráfico real es el valor del contador correspondiente al campo de coincidencia; establece el conjunto de ecuaciones sobredeterminado en base al tráfico real y al tráfico teórico del flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación, donde el tráfico teórico forma el vector de números incógnita del conjunto de ecuaciones sobredeterminado y el tráfico real forma el vector de términos constantes del conjunto de ecuaciones sobredeterminado; y determina, en base al conjunto de ecuaciones sobredeterminado, si la al menos una entrada de flujo es anormal. En base al método matemático en esta realización de la presente invención, el campo de coincidencia en la entrada de flujo suministrado por el controlador corresponde a un campo de coincidencia en una entrada de flujo almacenada en el dispositivo de conmutación, el tráfico teórico del flujo de datos en el dispositivo de conmutación y el tráfico real son abstraídos como el conjunto de ecuaciones sobredeterminado, la norma de error cuadrático se obtiene utilizando la solución de mínimos cuadrados del conjunto de ecuaciones sobredeterminado, para determinar si la entrada de flujo es anormal y, si se encuentra una entrada anormal de flujo, resolver de este modo el problema que se debe realizar una detección cuando una regla de reenvío del flujo de datos es incoherente con un estado real del reenvío del flujo de datos porque la tabla de flujos está falsificada.

Con referencia a la figura 5, una realización de la presente invención proporciona un método de detección de anormalidades en el reenvío de flujos de datos, y el método incluye, específicamente las siguientes etapas.

S201. Un controlador determina un dispositivo de conmutación a través del cual pasa un flujo de datos a detectar, para generar una tabla de información de flujos que se muestra en la Tabla 1.

En base a una tabla de flujos suministrada correspondiente a cada flujo de datos, el controlador obtiene cada dispositivo de conmutación a través del cual fluye teóricamente cada flujo de datos a detectar. Para completar la comunicación entre dos sitios, el controlador se comunica con cada conmutador en un enlace para completar la adición de la tabla de flujos. Por lo tanto, el controlador puede conocer de antemano todos los dispositivos de conmutación a través de los cuales fluye el flujo de datos en el enlace.

En base a la tabla de flujos correspondiente a cada flujo de datos y a al menos un dispositivo de conmutación a través del cual pasa, teóricamente, el flujo de datos, el controlador genera una tabla de información de flujos (Flow info table, en inglés) que se muestra en la Tabla 1, y actualiza cada entrada en la tabla de información de flujos en tiempo real en base a un cambio dinámico de la tabla de flujos. La tabla de información de flujos incluye un campo de coincidencia correspondiente (un campo de coincidencia en la Tabla 1) en cada dispositivo de conmutación a través del cual fluye cada flujo de datos, y el tráfico teórico (tráfico teórico en la Tabla 1) de cada flujo de datos en cada dispositivo de conmutación a través del cual fluye el flujo de datos.

Además, en la Tabla 1, un número de secuencia de flujo se refiere a un número de secuencia de un flujo de datos; el tráfico teórico representa el tráfico teórico de cada flujo de datos, y los valores de tráfico teórico de diferentes flujos de datos están representados por m1, m2, m3 y similares; un campo de coincidencia representa un campo de coincidencia de una entrada de flujo mostrada en la figura 2, SrcIP se refiere a una dirección IP de origen, DstIP se refiere a una dirección IP de destino; una ruta representa los nombres de todos los dispositivos de conmutación a través de los cuales pasa el flujo de datos y los nombres están representados por S1, S5 y similares; y un número de conmutador en la entrada de flujo representa un nombre de cada dispositivo de conmutación a través del cual fluye el flujo de datos, y el contenido de entrada de flujo en la entrada de flujo representa el contenido en una instrucción de la entrada de flujo mostrada en la figura 2, y las elipses "..." en la tabla representan otro contenido omitido.

Se puede deducir de la tabla que un flujo de datos corresponde a un campo de coincidencia en una entrada de flujo; en consecuencia, los campos de coincidencia correspondientes al flujo de datos en todos los dispositivos de conmutación a través de los cuales fluye el flujo de datos son iguales; y el tráfico teórico del flujo de datos generado en los dispositivos de conmutación a través de los cuales fluye el flujo de datos es el mismo.

Por ejemplo, un campo de coincidencia correspondiente a un flujo de datos cuyo número de secuencia de flujo es 1 es SrcIP: 10.0.0.1, DstIP: 10.0.0.4, ...; los campos de coincidencia correspondientes del flujo de datos en los dispositivos de conmutación S1, S5, S9, S7 y S3 a través de los cuales fluye el flujo de datos son iguales; y el tráfico teórico del flujo de datos generado en los dispositivos de conmutación S1, S5, S9, S7 y S3 a través de los cuales fluye el flujo de datos es el mismo y es m1.

Tabla 1

<table>
<tr><th rowspan="2">Número de secuencia de flujo</th><th rowspan="2">Tráfico teórico</th><th rowspan="2">Campo de coincidencia</th><th colspan="2">Entrada de flujo</th><th rowspan="2">Ruta</th></tr>
<tr><th>Número de conmutador</th><th>Contenido de entrada de flujo</th></tr>
<tr><td rowspan="5">1</td><td rowspan="5">m1</td><td rowspan="5">SrcIP: 10.0.0.1,
DstIP: 10.0.0.4, …</td><td>S1</td><td>…</td><td rowspan="5">S1, S5, S9, S7, S3</td></tr>
<tr><td>S5</td><td>…</td></tr>
<tr><td>S9</td><td>…</td></tr>
<tr><td>S7</td><td>…</td></tr>
<tr><td>S3</td><td>…</td></tr>
<tr><td>2</td><td>m2</td><td>SrcIP: 10.0.0.2,
DstIP: 10.0.0.3, …</td><td colspan="2">…</td><td>S1, S5, S2</td></tr>
<tr><td>3</td><td>m3</td><td>SrcIP: 10.0.0.2,
DstIP: 10.0.0.3, …</td><td colspan="2">…</td><td>S1, S5, S2</td></tr>
<tr><td>…</td><td>…</td><td>…</td><td colspan="2">…</td><td>…</td></tr>
</table>

S202. El controlador obtiene al menos una entrada de flujo que coincide con el flujo de datos y que está en el dispositivo de conmutación, donde la entrada de flujo incluye tráfico real y un campo de coincidencia, y el tráfico real es un valor de un contador que está en el dispositivo de conmutación y que corresponde a un flujo de datos que corresponde al

campo de coincidencia; y genera una tabla de contadores (Counter table, en inglés) mostrada en la Tabla 2 en base, al menos, a una entrada de flujo.

La tabla de contadores generada incluye el contenido principal de la entrada de flujo mostrada en la figura 2, e incluye, específicamente, un contador y un campo de coincidencia en el mismo. Un valor del contador está representado por c1, c2 y similares y, el campo de coincidencia en la tabla de contadores y un campo de coincidencia en la tabla de información de flujos tienen el mismo formato, de modo que se puede encontrar el campo de coincidencia en la tabla de información de flujos mediante la utilización del campo de coincidencia en la tabla de contadores. Los puntos suspensivos "..." en la tabla representan otro contenido omitido.

La entrada de flujo en la Tabla 2 incluye, además, un indicador de agregación, utilizado para indicar si la entrada de flujo es una entrada de flujo agregado. Un valor del indicador de agregación incluye: Falso (Falso, en chino), que indica que la entrada de flujo no es una entrada de flujo agregado; y Verdadero (Verdadero, en chino), que indica que la entrada de flujo es una entrada de flujo agregado.

Tabla 2

Número de conmutador	Entrada de flujo		
	Campo de coincidencia	Contador	Indicador de agregación
S1	SrcIP: 10.0.0.1, DstIP: 10.0.0.4, …	c1	Falso
	SrcIP: 10.0.0.2, DstIP: 10.0.0.3, …	c2	Verdadero
S2	SrcIP: 10.0.0.2, DstIP: 10.0.0.4, …	c3	Verdadero
	…	…	…
…	…	…	…

S203. Establecer un conjunto de ecuaciones sobredeterminado en base al tráfico real y al tráfico teórico de un flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación, donde cada entrada de flujo en la tabla de contadores corresponde a una ecuación en el conjunto de ecuaciones sobredeterminado.

Para cada entrada de flujo en la tabla de contadores, el controlador puede buscar un mismo campo de coincidencia en la entrada de flujo en la tabla de información de flujos mediante la utilización del campo de coincidencia de la entrada de flujo, encontrar un flujo de datos correspondiente en base al campo de coincidencia, encontrar el tráfico teórico m del flujo de datos en el dispositivo de conmutación y establecer una ecuación mediante la igualación del tráfico teórico m con el tráfico real c. Específicamente, haciendo referencia a la figura 6, la etapa S203 incluye la etapa S2031 a la etapa S2034.

S2031. Leer un campo de coincidencia, un contador y un indicador de agregación en una entrada de flujo en la tabla de contadores.

Por ejemplo, se lee la primera entrada de flujo en la tabla de contadores, es decir, un campo de coincidencia de un dispositivo de conmutación S1 es SrcIP: 10.0.0.1, DstIP: 10.0.0.4, ..., un contador, es decir, el tráfico real es c1, y un indicador de agregación es Falso. No obstante, cuando la segunda entrada de flujo en la tabla de contadores se lee en un bucle en la siguiente vez, se lee que el campo de coincidencia del dispositivo de conmutación S1 es "SrcIP: 10.0.0.2, DstIP: 10.0.0.3, ...", el contador, es decir, el tráfico real, es c2, y el indicador de agregación es Verdadero.

S2032. Determinar, de acuerdo con el indicador de agregación, si la entrada de flujo es una entrada de flujo agregado.

Por ejemplo, debido a que el indicador de agregación de la primera entrada de flujo en la tabla de contadores es Falso, la entrada de flujo no es una entrada de flujo agregado. No obstante, debido a que el indicador de agregación en la segunda entrada de flujo en la tabla de contadores es Verdadero, la entrada de flujo es una entrada de flujo agregado.

S2033. Establecer, en base a un resultado de determinación de la entrada de flujo, una ecuación, mediante la igualación del tráfico teórico del flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación, con el tráfico real.

Específicamente, con referencia a la figura 7, la etapa S2033 incluye la etapa S20331 a la etapa S20334. Si la entrada de flujo no es una entrada de flujo agregado, se realiza la etapa S20331; en caso contrario, se realiza la etapa S20333.

S20331. Cuando se puede encontrar un flujo de datos correspondiente mediante la utilización del campo de coincidencia, si se determina que la entrada de flujo no es una entrada de flujo agregado, lo que indica que el campo

de coincidencia corresponde a un flujo de datos, como máximo, leer el tráfico teórico del flujo de datos correspondiente al campo de coincidencia en una tabla de información de flujos.

Por ejemplo, en esta realización, un flujo de datos cuyo número de secuencia de flujo correspondiente es 1 se puede encontrar en la tabla de información de flujos mediante la utilización de un campo de coincidencia “SrcIP: 10.0.0.1, DstIP: 10.0.0.4, ...”, y el tráfico teórico del flujo de datos es m1.

Además, cuando no se puede encontrar un flujo de datos correspondiente mediante la utilización del campo de coincidencia, en este caso, un coeficiente antes de que el tráfico teórico m se establezca en 0, es decir, 0 * m, y posteriormente, cuando se genera un conjunto de ecuaciones, m, en este caso, se amplía.

S20332. Si se determina que la entrada de flujo no es una entrada de flujo agregado, establecer una ecuación mediante la igualación del tráfico teórico de un flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación, con el tráfico real y, a continuación, ir a la etapa S2034.

Específicamente, la ecuación se establece mediante la igualación del tráfico teórico en la tabla de información de flujos con un contador correspondiente (es decir, tráfico real) en la tabla de contadores.

Por ejemplo, en esta realización, se puede establecer una ecuación m1 = c1 mediante la utilización del campo de coincidencia “SrcIP: 10.0.0.1, DstIP: 10.0.0.4, ...”.

Además, si no se puede encontrar un flujo de datos correspondiente mediante la utilización del campo de coincidencia “SrcIP: 10.0.0.1, DstIP: 10.0.0.4, ...”, se formula una ecuación 0 * m = c1.

S20333. Cuando se puede encontrar un flujo de datos correspondiente mediante la utilización del campo de coincidencia, si se determina que la entrada de flujo es una entrada de flujo agregado, lo que indica que el campo de coincidencia coincide con una pluralidad de flujos de datos, leer el tráfico teórico de la pluralidad de flujos de datos correspondiente al campo de coincidencia en la tabla de información de flujos.

Por ejemplo, si se puede encontrar un flujo de datos correspondiente mediante la utilización del campo de coincidencia, en esta realización, se pueden encontrar dos flujos de datos cuyos números de secuencia de flujo son 2 y 3 en la tabla de información de flujos mediante la utilización de un campo de coincidencia “SrcIP: 10.0.0.2, DstIP: 10.0.0.3, ...”, y el tráfico teórico de los dos flujos de datos es m2 y m3.

Además, cuando no se puede encontrar un flujo de datos correspondiente mediante la utilización del campo de coincidencia, en este caso, un coeficiente antes de que el tráfico teórico m se establezca en 0, es decir, 0 * m, y posteriormente, cuando se genera un conjunto de ecuaciones, m en este caso, se amplía.

S20334. Si se determina que la entrada de flujo es una entrada de flujo agregado, establecer una ecuación mediante la igualación de una suma de tráficos teóricos de la pluralidad de flujos de datos que coinciden con el campo de coincidencia y que están en el dispositivo de conmutación, con el tráfico real y, a continuación, ir a etapa S2034.

Por ejemplo, si se puede encontrar un flujo de datos correspondiente mediante la utilización del campo de coincidencia, en este caso, se puede establecer una ecuación m2 + m3 = c2 mediante la utilización de un campo de coincidencia “SrcIP: 10.0.0.2, DstIP: 10.0.0.3, ...”.

Además, si no se puede encontrar un flujo de datos correspondiente mediante la utilización del campo de coincidencia “SrcIP: 10.0.0.2, DstIP: 10.0.0.3, ...”, se formula una ecuación 0 * m = c2.

S2034. El controlador combina ecuaciones establecidas en bade a una pluralidad de campos de coincidencia, para generar el conjunto de ecuaciones sobredeterminado, donde el tráfico teórico forma un vector de números incógnita del conjunto de ecuaciones sobredeterminado, y el tráfico real forma un vector de términos constantes del conjunto de ecuaciones sobredeterminado.

Se supone que, en las etapas anteriores, además de las dos ecuaciones m1 = c1 y m2 + m3 = c2 en los ejemplos, se obtiene una tercera ecuación 0 * m = c3 y una cuarta ecuación m3 = c4. En este caso, la tercera ecuación 0 * m = c3 se amplía a 0 * m1 + 0 * m2 + 0 * m3 = c3 en base al tráfico teórico m1, m2, m3 que se pueden encontrar.

$$\begin{pmatrix} a_{11} & \cdots & a_{1p} \\ \vdots & \ddots & \vdots \\ a_{q1} & \cdots & a_{qp} \end{pmatrix} \bullet \left(m_1, m_2, m_3, ..., m_p\right)^T = \left(c_1, c_2, c_3, ..., c_q\right)^T$$

fórmula (1)

a es un coeficiente que tiene un valor de solo 0 o 1, *m* representa el vector de números incógnita del tráfico teórico, *c* representa el vector de términos constantes del tráfico real, *p* es una cantidad de flujos de datos y *q* es una cantidad de entrada de flujo. En general, *q* >= *p*.

Posteriormente, el tráfico teórico m1, m2 y m3 de la cuarta ecuación se utiliza como una parte de las incógnitas del conjunto de ecuaciones, y el tráfico real c1, c2, c3 y c4 de todas las ecuaciones se utiliza como una parte de términos constantes del conjunto de ecuaciones. El conjunto de ecuaciones está representado por AM = C en una forma de vectores. A es una matriz de coeficientes del conjunto de ecuaciones, M es un vector de números incógnita formado por el tráfico teórico, y C es un vector de términos constantes formado por el tráfico real. Para más detalles, véase la fórmula (1). Las cuatro ecuaciones anteriores se representan como un conjunto de ecuaciones de una forma vectorial:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \bullet \left(m_1, m_2, m_3\right)^T = \left(c_1, c_2, c_3, c_4\right)^T$$

S204. Determinar, en base al conjunto de ecuaciones sobredeterminado, si la al menos una entrada de flujo es anormal. Específicamente, con referencia a la figura 8, la etapa S204 incluye las etapas S2041 a S2045.

S2041. Resolver el conjunto de ecuaciones sobredeterminado para obtener una solución de mínimos cuadrados más aproximada m*.

Debido a que el conjunto de ecuaciones sobredeterminado no tiene una solución fija, la solución de mínimos cuadrados m* se obtiene resolviendo el conjunto de ecuaciones sobredeterminado, y la solución de mínimos cuadrados m* es una solución aproximada.

S2042. Sustituir la solución de mínimos cuadrados m* del conjunto de ecuaciones sobredeterminado en el lado de vector de números incógnita del conjunto de ecuaciones sobredeterminado, para obtener un vector actualizado de términos constantes C*.

Es decir, la solución de mínimos cuadrados obtenida m* se sustituye en el lado izquierdo del conjunto de ecuaciones que se muestra en la fórmula 1, para obtener un nuevo vector C* del conjunto de ecuaciones en el lado derecho.

S2043. Obtener una norma de error cuadrático en base al vector de términos constantes C del conjunto de ecuaciones sobredeterminado y al vector actualizado de términos constantes C*, tal como se muestra en la fórmula (2).

$$\varepsilon = \sqrt{\sum_{i=0}^{q} (c_i^* - c_i)^2}$$

fórmula (2)

q es una cantidad de entradas de flujo, c_i^* es una de C*, y c_i es una de C.

S2044. Comparar la norma de error cuadrático con un primer umbral para determinar si una entrada de flujo es anormal.

Cuando la norma de error cuadrático es mayor que el primer umbral, se considera que el estado real del reenvío en una red es incoherente con una regla suministrada por el controlador, es decir, una entrada de flujo en el dispositivo de conmutación es anormal.

S2045. Generar un vector de diferencia C* - C calculando las diferencias entre el vector actualizado de términos constantes C* y el vector de términos constantes C del conjunto de ecuaciones sobredeterminado, comparar cada diferencia en el vector de diferencia C* - C con un segundo umbral, determinar una entrada anormal de flujo en las entradas de flujo correspondientes a una o más diferencias que exceden el segundo umbral y que están en las diferencias del vector de diferencia C* - C, y localizar un dispositivo de conmutación correspondiente y una entrada de flujo en el dispositivo de conmutación.

Específicamente, haciendo referencia a la figura 9, la figura 9 es un diagrama esquemático de un resultado de simulación de anormalidad de una entrada de flujo. Una coordenada horizontal es un número de un dispositivo de conmutación, y una coordenada vertical es una diferencia en el vector de diferencia C* - C. Se puede ver, a partir de la figura, que las diferencias E1, E2 y E3 correspondientes a los dispositivos de conmutación 8, 30 y 42 son relativamente grandes, y se puede deducir que las entradas de flujo en los tres dispositivos de conmutación probablemente son anormales, de modo que se puede realizar una verificación adicional de manera manual.

De acuerdo con el método de detección de anormalidades en el reenvío de flujos de datos proporcionado en la presente invención, el controlador determina el dispositivo de conmutación a través del cual fluyen los datos a detectar; obtiene al menos una entrada de flujo que coincide con el flujo de datos y que se encuentra en el dispositivo de

conmutación, donde la entrada de flujo incluye el tráfico real y el campo de coincidencia, y el tráfico real es el valor del contador correspondiente al campo de coincidencia; establece el conjunto de ecuaciones sobredeterminado en base al tráfico real y al tráfico teórico del flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación, donde el tráfico teórico forma el vector de números incógnita del conjunto de ecuaciones sobredeterminado y el tráfico real forma el vector de términos constantes del conjunto de ecuaciones sobredeterminado; y determina, en base al conjunto de ecuaciones sobredeterminado, si la al menos una entrada de flujo es anormal. En base al método matemático en esta realización de la presente invención, el campo de coincidencia en la entrada de flujo suministrado por el controlador corresponde a un campo de coincidencia en una entrada de flujo almacenada en el dispositivo de conmutación, el tráfico teórico del flujo de datos en el dispositivo de conmutación y el tráfico real son abstraídos como el conjunto de ecuaciones sobredeterminado, la norma de error cuadrático se obtiene mediante la utilización de la solución de mínimos cuadrados del conjunto de ecuaciones sobredeterminado, para determinar si la entrada de flujo es anormal y, si se encuentra una entrada anormal de flujo, resolver, de este modo, el problema de que se debe realizar una detección cuando una regla de reenvío de flujos de datos es incoherente con un estado real del reenvío del flujo de datos porque la tabla de flujos está falsificada.

La presente invención proporciona un controlador. El controlador está configurado para realizar el método de detección de anormalidades en el reenvío de flujos de datos anterior. Con referencia a la figura 10, el controlador incluye:

una unidad de detección 111, configurada para determinar un dispositivo de conmutación a través del cual pasa un flujo de datos a detectar;

una unidad de obtención 112, configurada para obtener al menos una entrada de flujo que coincide con el flujo de datos y que está en el dispositivo de conmutación, donde la entrada de flujo incluye tráfico real y un campo de coincidencia; y el tráfico real es un valor de un contador correspondiente al campo de coincidencia;

una unidad de cálculo 113, configurada para establecer un conjunto de ecuaciones sobredeterminado en base al tráfico real y al tráfico teórico de un flujo de datos que coincide con el campo de coincidencia y que se encuentra en el dispositivo de conmutación, donde el tráfico teórico forma un vector de números incógnita del conjunto de ecuaciones sobredeterminado y el tráfico real forma un vector de términos constantes del conjunto de ecuaciones sobredeterminado; y

una unidad de determinación 114, configurada para determinar, en base al conjunto de ecuaciones sobredeterminado, si la al menos una entrada de flujo es anormal.

Debido a que el controlador en esta realización de la presente invención puede estar configurado para realizar los procedimientos del método indicados anteriormente, para los efectos técnicos que pueden ser obtenidos por el controlador, véanse las realizaciones del método anterior, y los detalles no se describen de nuevo en esta realización de la presente invención.

En un ejemplo proporcionado, la unidad de cálculo 113 está configurada, además, para:

sustituir una solución de mínimos cuadrados del conjunto de ecuaciones sobredeterminado en el lado de vector de números incógnita del conjunto de ecuaciones sobredeterminado, para obtener un vector actualizado de términos constantes;

obtener una norma de error cuadrático en base al vector de términos constantes del conjunto de ecuaciones sobredeterminado y al vector actualizado de términos constantes; y

comparar la norma de error cuadrático con un primer umbral para determinar si una entrada de flujo es anormal.

En un ejemplo proporcionado, la unidad de determinación 114 está configurada, además, para:

generar un vector de diferencia calculando las diferencias entre el vector actualizado de términos constantes y el vector de términos constantes del conjunto de ecuaciones sobredeterminado, comparar cada diferencia en el vector de diferencia con un segundo umbral, y determinar una entrada anormal de flujo en las entradas de flujo correspondientes a una o más diferencias que exceden el segundo umbral y que están en las diferencias.

En un ejemplo proporcionado,

la entrada de flujo incluye, además, un indicador de agregación, y el indicador de agregación se utiliza para indicar si la entrada de flujo es una entrada de flujo agregado; y

la unidad de cálculo 113 está configurada, además, para:

determinar, de acuerdo con el indicador de agregación, si la entrada de flujo es una entrada de flujo agregado;

establecer, en base a un resultado de determinación de la entrada de flujo, una ecuación, mediante la igualación del tráfico teórico del flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación, con el tráfico real; y

combinar las ecuaciones establecidas en base a una pluralidad de campos de coincidencia, para generar el conjunto de ecuaciones sobredeterminado.

En un ejemplo proporcionado, la unidad de cálculo 113 está configurada, además, para:

cuando se puede encontrar un flujo de datos coincidente mediante la utilización del campo de coincidencia, si se determina que la entrada de flujo no es una entrada de flujo agregado, lo que indica que el campo de coincidencia coincide un flujo de datos, establecer una ecuación mediante la igualación del tráfico teórico del flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación, con el tráfico real; o

si se determina que la entrada de flujo es una entrada de flujo agregado, lo que indica que el campo de coincidencia coincide con una pluralidad de flujos de datos, establecer una ecuación mediante la igualación de una suma de tráficos teóricos de la pluralidad de flujos de datos que coinciden con el campo de coincidencia y que están en el dispositivo de conmutación, con el tráfico real.

En un ejemplo proporcionado, la unidad de cálculo 113 está configurada, además, para:

establecer el conjunto de ecuaciones sobredeterminado como

$$\begin{pmatrix} a_{11} & \cdots & a_{1p} \\ \vdots & \ddots & \vdots \\ a_{q1} & \cdots & a_{qp} \end{pmatrix} \bullet \left(m_1, m_2, m_3, ..., m_p\right)^T = \left(c_1, c_2, c_3, ..., c_q\right)^T$$

, donde *a* es un coeficiente que tiene un valor de solo 0 o 1, *m* representa el vector de números incógnita del tráfico teórico, *c* representa el vector de términos constantes del contador, *p* es una cantidad de flujos de datos y *q* es una cantidad de entradas de flujo.

Debido a que el controlador en esta realización de la presente invención puede estar configurado para realizar los procedimientos del método citados anteriormente, para los efectos técnicos que pueden ser obtenidos por el controlador, véanse las realizaciones del método anterior, y los detalles no se describen de nuevo en esta realización de la presente invención.

Se debe observar que la unidad de detección, la unidad de obtención, la unidad de cálculo y la unidad de determinación pueden ser procesadores dispuestos de manera independiente, o pueden estar integrados en un procesador en el controlador para su implementación. Además, la unidad de detección, la unidad de obtención, la unidad de cálculo y la unidad de determinación pueden estar almacenadas en una memoria del controlador en forma de código de programa, y ser invocadas por un procesador del controlador para realizar las funciones de la unidad de detección, la unidad de obtención, la unidad de cálculo y la unidad de determinación. El procesador, en este caso, puede ser una unidad de procesamiento central (Central Processing Unit, nombre completo en inglés, CPU, para abreviar) o un circuito integrado específico de la aplicación (Application Specific Integrated Circuit, nombre completo en inglés, ASIC, para abreviar), o puede ser uno o más circuitos integrados configurados para implementar esta realización de la presente invención.

La presente invención proporciona un controlador que está configurado para realizar el método de detección de anormalidades en el reenvío de flujos de datos. Con referencia a la figura 11, el aparato puede ser un controlador en una red SDN y puede incluir un procesador 1101, una memoria 1102 y un bus 1103. El procesador 1101 y la memoria 1102 están conectados y completan la comunicación mutua utilizando el bus 1103.

Se debe observar que el procesador 1101, en este caso, puede ser un procesador, o puede ser el término general de una pluralidad de elementos de procesamiento. Por ejemplo, el procesador puede ser una unidad central de procesamiento, CPU, puede ser un circuito integrado específico de la aplicación, ASIC, o puede ser uno o más circuitos integrados configurados para implementar esta realización de la presente invención, por ejemplo, uno o más microprocesadores, tales como el procesador de señal digital (DSP - Digital Signal Processor, en inglés), o una o más matrices de puertas programables en campo (FPGA - Field Programmable Gate Array, en inglés).

La memoria 1102 puede ser un aparato de almacenamiento, o puede ser un término general de una pluralidad de elementos de almacenamiento, y está configurada para almacenar código de programa ejecutable, o parámetros, datos y similares necesarios para ejecutar el código de programa ejecutable o un dispositivo de gestión la red de acceso. La memoria 1102 puede incluir una memoria de acceso aleatorio (RAM - Random Access Memory, en inglés), o puede incluir una memoria no volátil (NVRAM - Non Volatile RAM, en inglés), por ejemplo, un almacenamiento en disco magnético o una memoria rápida (Flash, en inglés).

El bus 1103 puede ser un bus de arquitectura estándar industrial (ISA - Industry Standard Architecture, en inglés), un bus de interconexión de componentes periféricos (PCIt - Peripheral Component Interconnect, en inglés), un bus de arquitectura estándar industrial extendido (EISA - Extended Industry Standard, en inglés) o similares. El bus 1103 se puede clasificar en un bus de direcciones, un bus de datos, un bus de control y similares. Para facilitar la indicación,

el bus se indica utilizando solo una línea en negrita en la figura 11. No obstante, no indica que solo haya un bus o solo un tipo de bus.

El procesador 1101 está configurado para ejecutar el código de programa almacenado en el mismo, para realizar el método proporcionado en las realizaciones de método anteriores.

Específicamente, el procesador 1101 está configurado para ejecutar el programa en la memoria para realizar las funciones de la unidad de detección, la unidad de obtención, la unidad de cálculo y la unidad de determinación del controlador en las realizaciones anteriores. Los detalles no se describen de nuevo en el presente documento.

El controlador en esta realización de la presente invención puede estar configurado para realizar el proceso del método anterior. Por lo tanto, para un efecto técnico que puede ser obtenido por el controlador, véanse las realizaciones del método citadas anteriormente, y los detalles no se describen de nuevo en esta realización de la presente invención.

Una persona de habilidad ordinaria en la materia puede ser consciente de que las unidades y las etapas del algoritmo en los ejemplos descritos con referencia a las realizaciones descritas en esta memoria descriptiva pueden ser implementadas mediante hardware electrónico o una combinación de software y hardware electrónico. Si las funciones se realizan en forma de hardware o software depende de las aplicaciones particulares y de las condiciones de limitación de diseño de las soluciones técnicas. Una persona experta en la materia puede utilizar diferentes métodos para implementar las funciones descritas para cada aplicación particular, pero no se debe considerar que la implementación va más allá del alcance de la presente invención.

Una persona experta en la materia puede comprender claramente que, a efectos de una descripción conveniente y breve, para un proceso de trabajo detallado del sistema, aparato y unidad, se debe consultar un proceso correspondiente en las realizaciones del método. Los detalles no se describen de nuevo en el presente documento.

En las diversas realizaciones proporcionadas en esta solicitud, se debe comprender que el sistema, dispositivo y método dados a conocer pueden ser implementados de otras maneras. Por ejemplo, la realización del dispositivo descrita es simplemente un ejemplo. Por ejemplo, la división de unidades es simplemente una división de función lógica y puede ser otra división en una implementación real. Por ejemplo, una pluralidad de unidades o componentes pueden ser combinados o integrados en otro sistema, o algunas características pueden ser ignoradas o no realizarse. Además, los acoplamientos mutuos mostrados o explicados o los acoplamientos directos o las conexiones de comunicación pueden ser implementados por medio de algunas interfaces. Los acoplamientos indirectos o las conexiones de comunicación entre los dispositivos o unidades pueden ser implementados en forma electrónica, mecánica o en otras formas.

Las unidades descritas como partes separadas pueden o no estar físicamente separadas, y las partes mostradas como unidades pueden o no ser unidades físicas, pueden estar ubicadas en una posición o pueden estar distribuidas en una pluralidad de unidades de red. Algunas o todas las unidades pueden ser seleccionadas de acuerdo con las necesidades reales para conseguir los objetivos de las soluciones de las realizaciones.

Además, las unidades funcionales en las realizaciones de la presente invención pueden estar integradas en una unidad de procesamiento, o cada una de las unidades puede existir solo físicamente, o dos o más unidades pueden estar integradas en una unidad.

Cuando las funciones están implementadas en forma de una unidad funcional de software y se venden o utilizan como un producto independiente, las funciones pueden estar almacenadas en un medio de almacenamiento legible por ordenador. En base a dicha comprensión, las soluciones técnicas de la presente invención, esencialmente, o la parte que contribuye a la técnica anterior, o algunas de las soluciones técnicas, pueden estar implementadas en forma de un producto de software. El producto de software se almacena en un medio de almacenamiento e incluye varias instrucciones para indicar a un dispositivo informático (que puede ser un ordenador personal, un servidor, un dispositivo de red o similar) que realice todas o algunas de las etapas de los métodos descritas en las realizaciones de la presente invención. El medio de almacenamiento indicado anteriormente incluye: cualquier medio que pueda almacenar código de programa, tal como una unidad flash USB, un disco duro extraíble, una memoria de solo lectura (ROM - Read Only Memory, en inglés), una memoria de acceso aleatorio (RAM - Random Access Memory, en inglés), un disco magnético o un disco óptico.

Las descripciones son solo implementaciones específicas de la presente invención, pero no pretenden limitar el alcance de protección de la presente invención. Cualquier variación o sustitución fácilmente configurada por una persona experta en la materia dentro del alcance técnico dado a conocer en la presente invención caerá dentro del alcance de protección de la presente invención. Por lo tanto, el alcance de protección de la presente invención estará sujeto al alcance de protección de las reivindicaciones.

REIVINDICACIONES

1. Un método de detección de anormalidades en el reenvío de flujos de datos por parte de un controlador, caracterizado por:

determinar, un dispositivo de conmutación a través del cual pasa un flujo de datos a detectar;

obtener al menos una entrada de flujo que coincide con el flujo de datos y que esté en el dispositivo de conmutación, donde la entrada de flujo comprende tráfico real y un campo de coincidencia; y el tráfico real es un valor de un contador correspondiente al campo de coincidencia;

establecer un conjunto de ecuaciones sobredeterminado en base al tráfico real y al tráfico teórico de un flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación, en donde el tráfico teórico forma un vector de números incógnita del conjunto de ecuaciones sobredeterminado y el tráfico real forma un vector de términos constantes del conjunto de ecuaciones sobredeterminado; y

determinar, en base al conjunto de ecuaciones sobredeterminado, si la al menos una entrada de flujo es anormal.

2. El método de acuerdo con la reivindicación 1, en el que la determinación, en base al conjunto de ecuaciones sobredeterminado de si la al menos una entrada de flujo es anormal, comprende:

sustituir una solución de mínimos cuadrados del conjunto de ecuaciones sobredeterminado en el vector de números incógnita del conjunto de ecuaciones sobredeterminado, para obtener un vector actualizado de términos constantes;

obtener una norma de error cuadrático en base al vector de términos constantes del conjunto de ecuaciones sobredeterminado y al vector actualizado de términos constantes; y

comparar la norma de error cuadrático con un primer umbral, para determinar si una entrada de flujo es anormal.

3. El método de acuerdo con la reivindicación 2, en el que la determinación, en base al conjunto de ecuaciones sobredeterminado, de si la al menos una entrada de flujo es anormal comprende, además:

generar un vector de diferencia calculando las diferencias entre el vector actualizado de términos constantes y el vector de términos constantes del conjunto de ecuaciones sobredeterminado, comparando cada diferencia en el vector de diferencia con un segundo umbral, y determinar una entrada anormal de flujo en las entradas de flujo correspondientes a una o más diferencias que exceden el segundo umbral y que están en las diferencias.

4. El método de acuerdo con la reivindicación 1, en el que

la entrada de flujo comprende, además, un indicador de agregación, y el indicador de agregación se utiliza para indicar si la entrada de flujo es una entrada de flujo agregado; y

el establecimiento de un conjunto de ecuaciones sobredeterminado en base al tráfico real y al tráfico teórico de un flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación comprende:

determinar, de acuerdo con el indicador de agregación, si la entrada de flujo es una entrada de flujo agregado;

establecer, en base a un resultado de determinación de la entrada de flujo, una ecuación mediante la igualación del tráfico teórico del flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación, con el tráfico real; y

combinar las ecuaciones establecidas en base a una pluralidad de campos de coincidencia, para generar el conjunto de ecuaciones sobredeterminado.

5. El método de acuerdo con la reivindicación 4, en el que el establecimiento, en base a un resultado de determinación de la entrada de flujo, de una ecuación mediante la igualación del tráfico teórico del flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación, con el tráfico real, comprende:

cuando se puede encontrar un flujo de datos coincidente mediante la utilización del campo de coincidencia,

si se determina que la entrada de flujo no es una entrada de flujo agregado, lo que indica que el campo de coincidencia coincide con un flujo de datos,

establecer una ecuación mediante la igualación del tráfico teórico del flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación, con el tráfico real; o

si se determina que la entrada de flujo es una entrada de flujo agregado, lo que indica que el campo de coincidencia coincide con una pluralidad de flujos de datos,

establecer una ecuación mediante la igualación de una suma de tráficos teóricos de la pluralidad de flujos de datos que coinciden con el campo de coincidencia y que están en el dispositivo de conmutación, con el tráfico real.

6. El método de acuerdo con una cualquiera de las reivindicaciones 1 a 5, en el que el conjunto de ecuaciones sobredeterminado es $\begin{pmatrix} a_{11} & \cdots & a_{1p} \\ \vdots & \ddots & \vdots \\ a_{q1} & \cdots & a_{qp} \end{pmatrix} \bullet \left(m_1, m_2, m_3, ..., m_p\right)^T = \left(c_1, c_2, c_3, ..., c_q\right)^T$

a es un coeficiente que tiene un valor de solo 0 o 1, *m* representa el vector de números incógnita del tráfico teórico, *c* representa el vector de términos constantes del contador, *p* es una cantidad de flujos de datos y *q* es una cantidad de entradas de flujo.

7. Un controlador, caracterizado por que comprende:

una unidad de detección, configurada para determinar un dispositivo de conmutación a través del cual pasan los datos a detectar;

una unidad de obtención, configurada para obtener al menos una entrada de flujo que coincide con el flujo de datos y que está en el dispositivo de conmutación determinado por la unidad de detección, en donde la entrada de flujo comprende tráfico real y un campo de coincidencia; y el tráfico real es un valor de un contador correspondiente al campo de coincidencia;

una unidad de cálculo, configurada para establecer un conjunto de ecuaciones sobredeterminado en base al tráfico real y al tráfico teórico de un flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación determinado por la unidad de detección, en donde el tráfico teórico forma un vector de números incógnita del conjunto de ecuaciones sobredeterminado y el tráfico real forma un vector de términos constantes del conjunto de ecuaciones sobredeterminado; y

una unidad de determinación, configurada para determinar, en base al conjunto de ecuaciones sobredeterminado establecido por la unidad de cálculo, si la al menos una entrada de flujo es anormal.

8. El controlador de acuerdo con la reivindicación 7, en el que la unidad de cálculo está configurada, además, para:

sustituir una solución de mínimos cuadrados del conjunto de ecuaciones sobredeterminado en el lado de vector de números incógnita del conjunto de ecuaciones sobredeterminado, para obtener un vector actualizado de términos constantes;

obtener una norma de error cuadrático en base al vector de términos constantes del conjunto de ecuaciones sobredeterminado y al vector actualizado de términos constantes; y

comparar la norma de error cuadrático con un primer umbral para determinar si una entrada de flujo es anormal.

9. El controlador de acuerdo con la reivindicación 8, en el que la unidad de determinación está configurada, además, para:

generar un vector de diferencia calculando las diferencias entre el vector actualizado de términos constantes y el vector de términos constantes del conjunto de ecuaciones sobredeterminado, comparar cada diferencia en el vector de diferencia con un segundo umbral, y determinar una entrada anormal de flujo en las entradas de flujo correspondientes a una o más diferencias que exceden el segundo umbral y que están en las diferencias.

10. El controlador de acuerdo con la reivindicación 7, en el que

la entrada de flujo comprende, además, un indicador de agregación, y el indicador de agregación se utiliza para indicar si la entrada de flujo es una entrada de flujo agregado; y

la unidad de cálculo está configurada, además, para:

determinar, de acuerdo con el indicador de agregación, si la entrada de flujo es una entrada de flujo agregado;

establecer, en base a un resultado de determinación de la entrada de flujo, una ecuación mediante la igualación del tráfico teórico del flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación, con el tráfico real; y

combinar las ecuaciones establecidas en base a una pluralidad de campos de coincidencia, para generar el conjunto de ecuaciones sobredeterminado.

11. El controlador de acuerdo con la reivindicación 10, en el que la unidad de cálculo está configurada, además, para:

cuando se puede encontrar un flujo de datos coincidente mediante la utilización del campo de coincidencia,

si se determina que la entrada de flujo no es una entrada de flujo agregado, lo que indica que el campo de coincidencia coincide con un flujo de datos,

establecer una ecuación mediante la igualación del tráfico teórico del flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación, con el tráfico real; o

si se determina que la entrada de flujo es una entrada de flujo agregado, lo que indica que el campo de coincidencia coincide con una pluralidad de flujos de datos, establecer una ecuación mediante la igualación de una suma de tráficos teóricos de la pluralidad de flujos de datos que coinciden con el campo de coincidencia y que están en el dispositivo de conmutación, con el tráfico real.

12. El controlador de acuerdo con una cualquiera de las reivindicaciones 7 a 11, en el que la unidad de cálculo está configurada, además, para:

establecer el conjunto de ecuaciones sobredeterminado como

$$\begin{pmatrix} a_{11} & \cdots & a_{1p} \\ \vdots & \ddots & \vdots \\ a_{q1} & \cdots & a_{qp} \end{pmatrix} \bullet \left(m_1, m_2, m_3, ..., m_p\right)^T = \left(c_1, c_2, c_3, ..., c_q\right)^T$$

, en donde *a* es un coeficiente que tiene un valor de solo 0 o 1, *m* representa el vector de números incógnita del tráfico teórico, *c* representa el vector de términos constantes del contador, *p* es una cantidad de flujos de datos, y *q* es una cantidad de entradas de flujo.

13. Un sistema de detección de anormalidades en el reenvío de flujos de datos, que comprende el controlador de acuerdo con una cualquiera de las reivindicaciones 7 a 12.

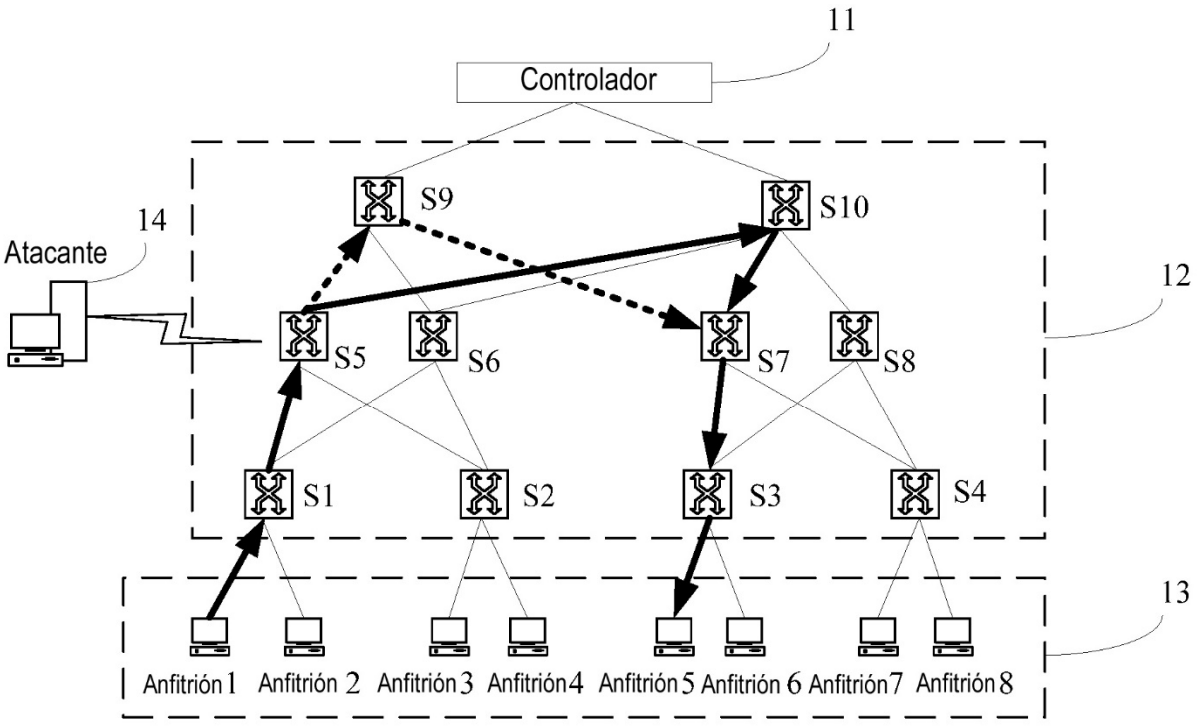
11
Controlador
S9
S10
14
Atacante
12
S5
S6
S7
S8
S1
S2
S3
S4
13
Anfitrión 1
Anfitrión 2
Anfitrión 3
Anfitrión 4
Anfitrión 5
Anfitrión 6
Anfitrión 7
Anfitrión 8

FIG. 1

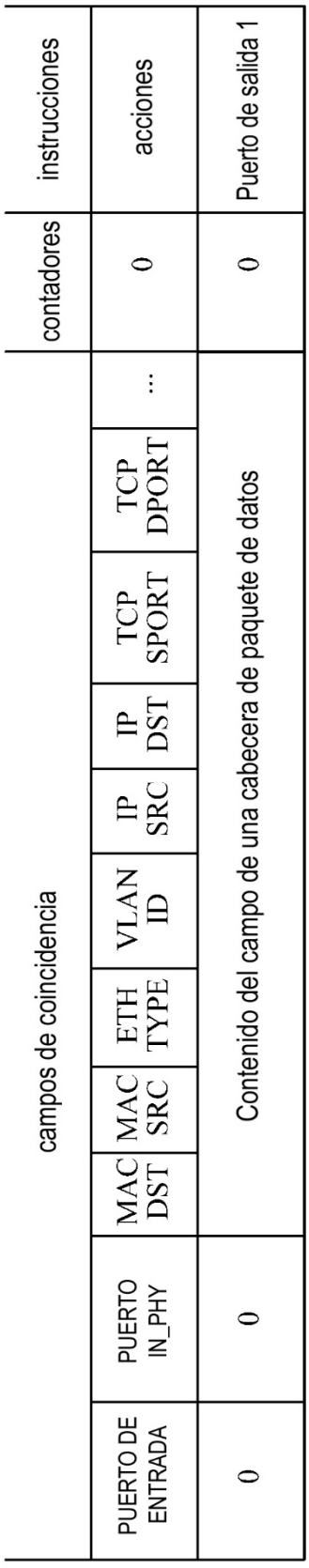
campos de coincidencia
contadores
instrucciones
PUERTO DE ENTRADA
PUERTO IN_PHY
MAC DST
MAC SRC
ETH TYPE
VLAN ID
IP SRC
IP DST
TCP SPORT
TCP DPORT
...
0
0
Contenido del campo de una cabecera de paquete de datos
0
acciones
0
Puerto de salida 1

FIG. 2

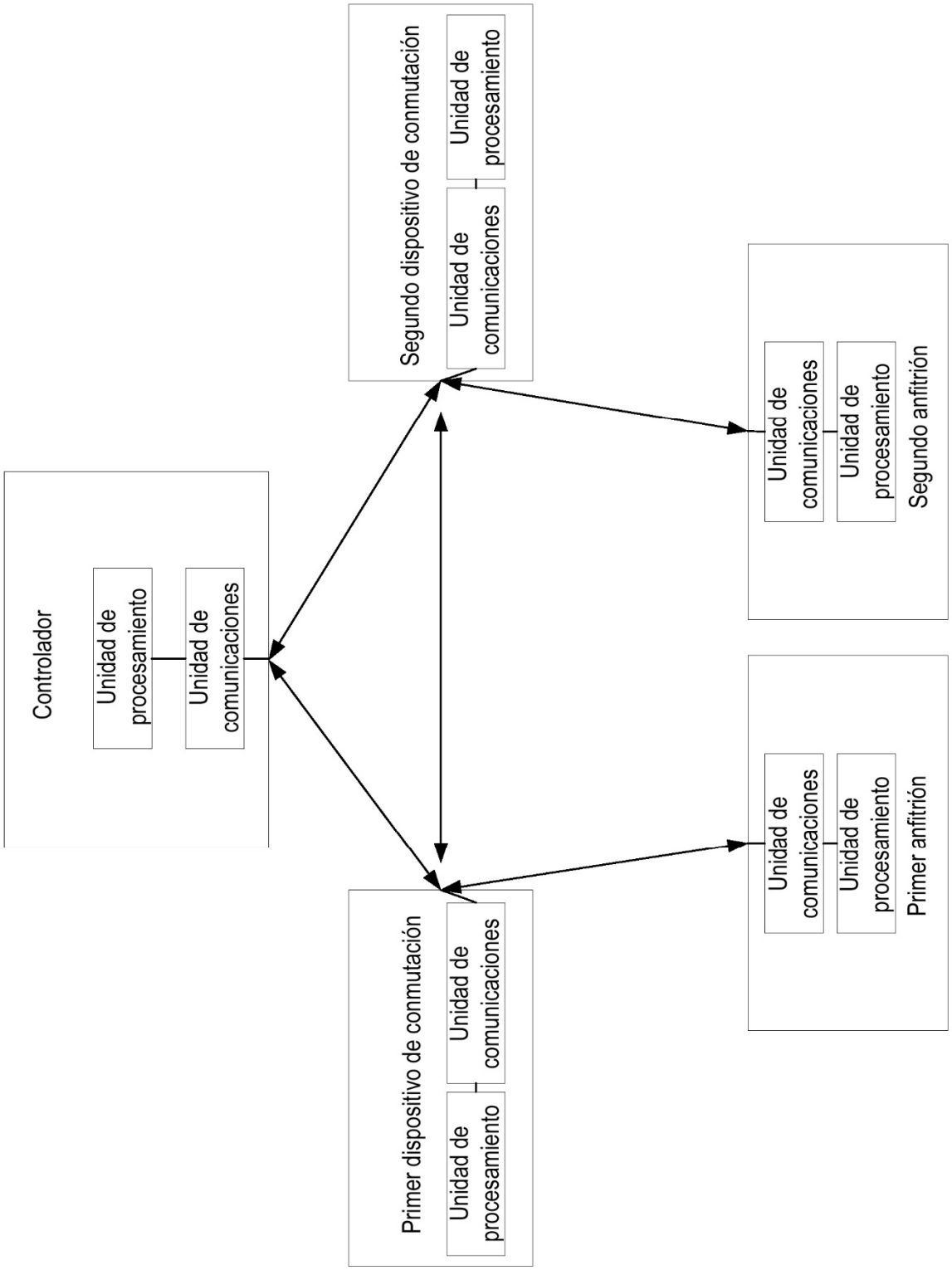
Controlador
Unidad de procesamiento
Unidad de comunicaciones
Segundo dispositivo de conmutación
Unidad de procesamiento
Unidad de comunicaciones
Primer dispositivo de conmutación
Unidad de procesamiento
Unidad de comunicaciones
Unidad de comunicaciones
Unidad de procesamiento
Segundo anfitrión
Unidad de comunicaciones
Unidad de procesamiento
Primer anfitrión

FIG. 3

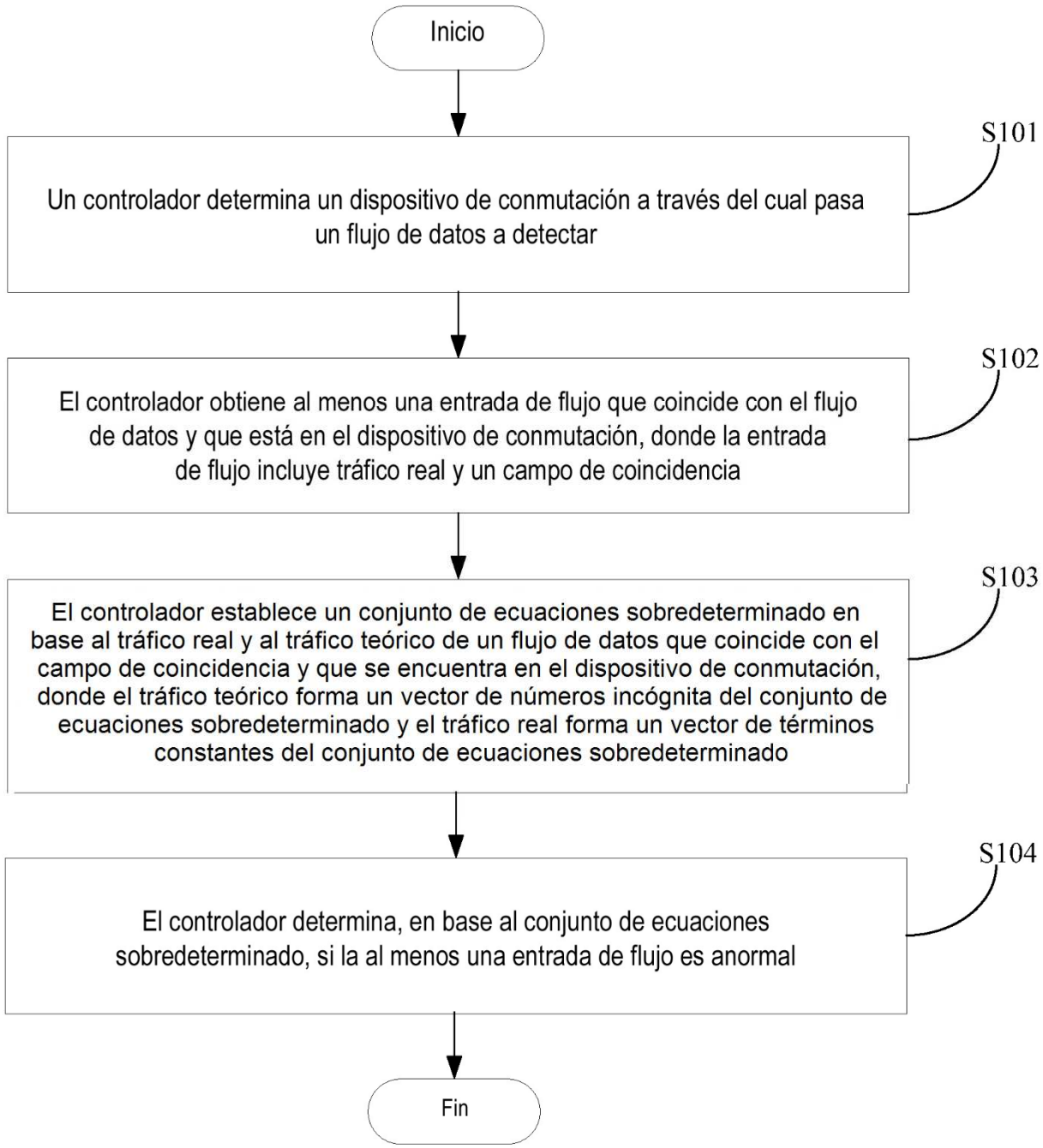
Inicio
S101
Un controlador determina un dispositivo de conmutación a través del cual pasa un flujo de datos a detectar
S102
El controlador obtiene al menos una entrada de flujo que coincide con el flujo de datos y que está en el dispositivo de conmutación, donde la entrada de flujo incluye tráfico real y un campo de coincidencia
S103
El controlador establece un conjunto de ecuaciones sobredeterminado en base al tráfico real y al tráfico teórico de un flujo de datos que coincide con el campo de coincidencia y que se encuentra en el dispositivo de conmutación, donde el tráfico teórico forma un vector de números incógnita del conjunto de ecuaciones sobredeterminado y el tráfico real forma un vector de términos constantes del conjunto de ecuaciones sobredeterminado
S104
El controlador determina, en base al conjunto de ecuaciones sobredeterminado, si la al menos una entrada de flujo es anormal
Fin

FIG. 4

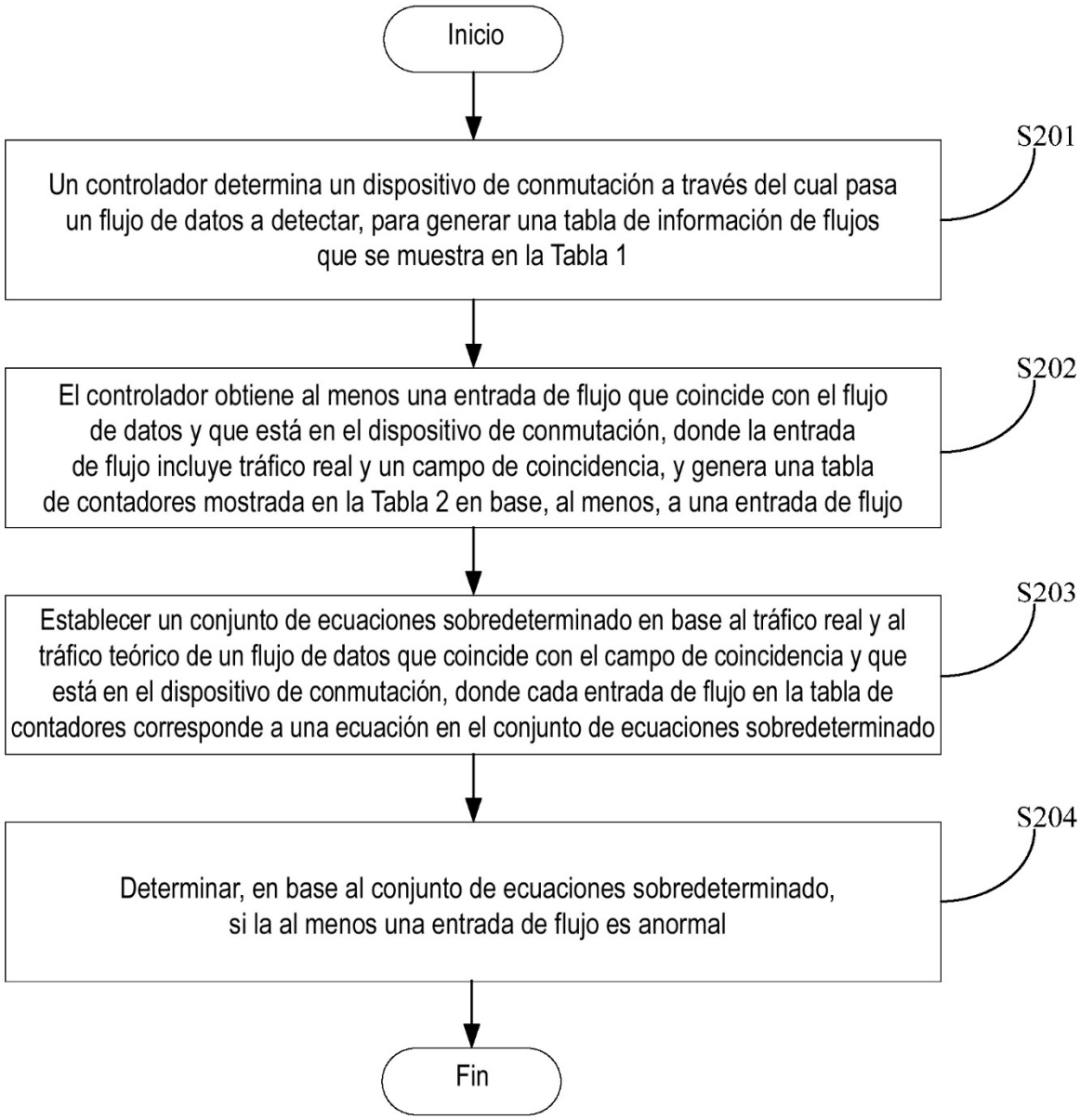
Inicio
S201
Un controlador determina un dispositivo de conmutación a través del cual pasa un flujo de datos a detectar, para generar una tabla de información de flujos que se muestra en la Tabla 1
S202
El controlador obtiene al menos una entrada de flujo que coincide con el flujo de datos y que está en el dispositivo de conmutación, donde la entrada de flujo incluye tráfico real y un campo de coincidencia, y genera una tabla de contadores mostrada en la Tabla 2 en base, al menos, a una entrada de flujo
S203
Establecer un conjunto de ecuaciones sobredeterminado en base al tráfico real y al tráfico teórico de un flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación, donde cada entrada de flujo en la tabla de contadores corresponde a una ecuación en el conjunto de ecuaciones sobredeterminado
S204
Determinar, en base al conjunto de ecuaciones sobredeterminado, si la al menos una entrada de flujo es anormal
Fin

FIG. 5

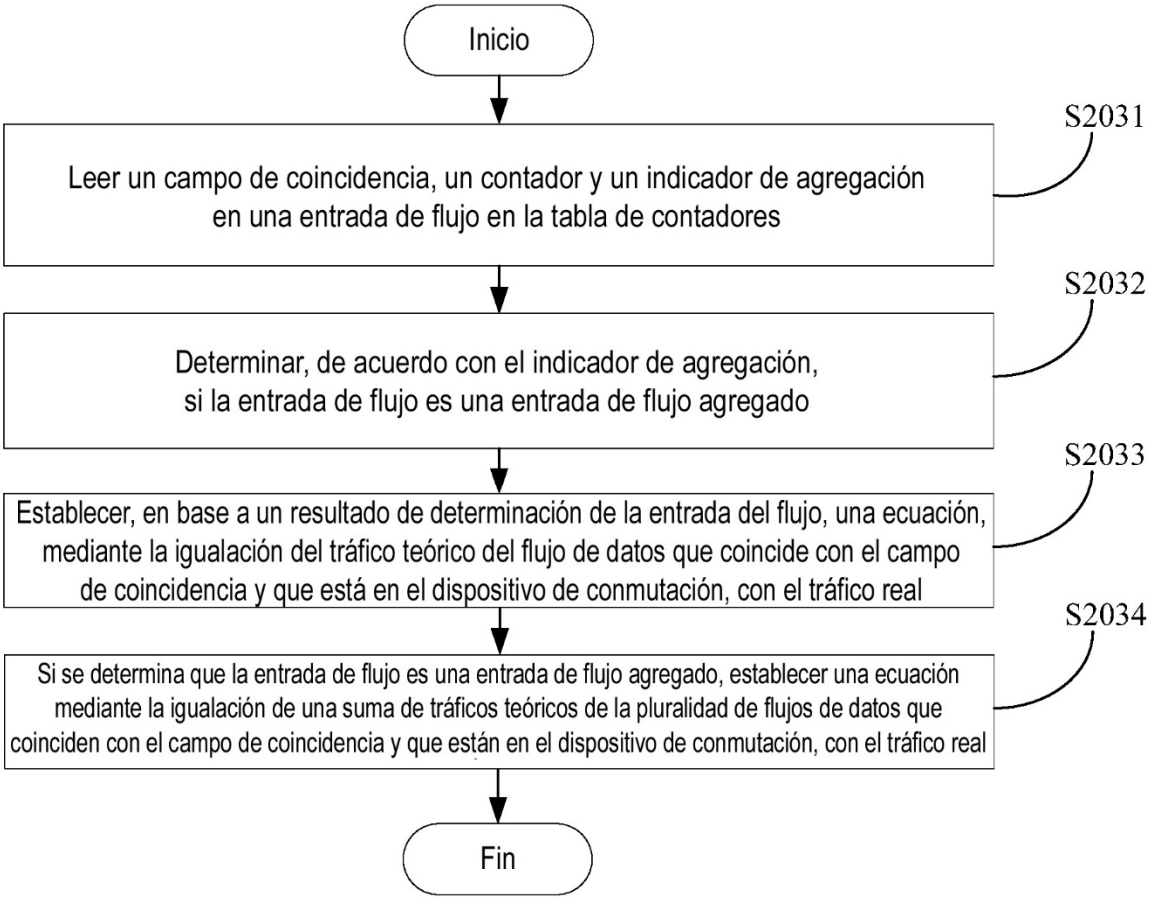
Inicio
S2031
Leer un campo de coincidencia, un contador y un indicador de agregación en una entrada de flujo en la tabla de contadores
S2032
Determinar, de acuerdo con el indicador de agregación, si la entrada de flujo es una entrada de flujo agregado
S2033
Establecer, en base a un resultado de determinación de la entrada del flujo, una ecuación, mediante la igualación del tráfico teórico del flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación, con el tráfico real
S2034
Si se determina que la entrada de flujo es una entrada de flujo agregado, establecer una ecuación mediante la igualación de una suma de tráficos teóricos de la pluralidad de flujos de datos que coinciden con el campo de coincidencia y que están en el dispositivo de conmutación, con el tráfico real
Fin

FIG. 6

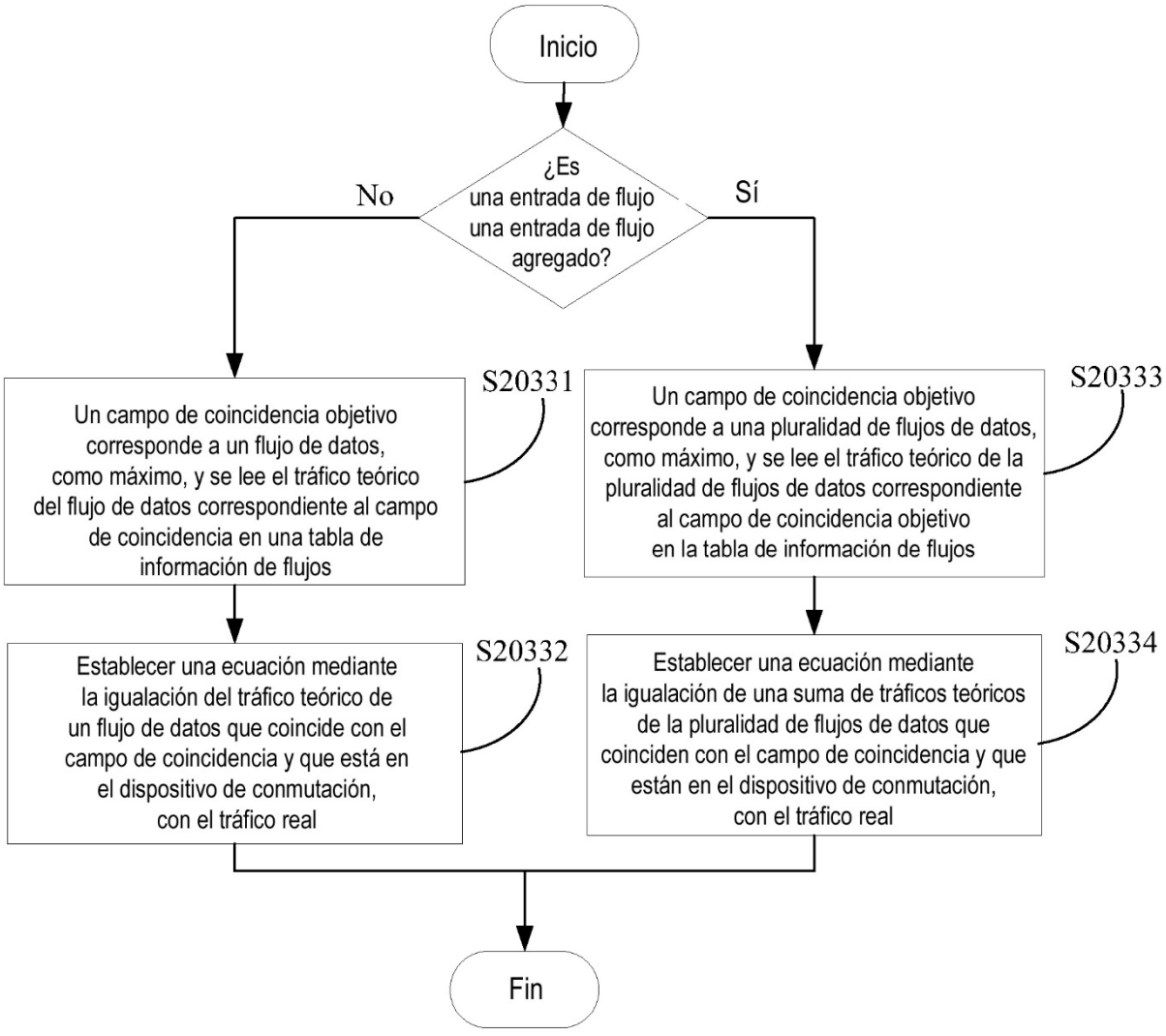
Inicio
¿Es una entrada de flujo una entrada de flujo agregado?
No
Sí
S20331
Un campo de coincidencia objetivo corresponde a un flujo de datos, como máximo, y se lee el tráfico teórico del flujo de datos correspondiente al campo de coincidencia en una tabla de información de flujos
S20333
Un campo de coincidencia objetivo corresponde a una pluralidad de flujos de datos, como máximo, y se lee el tráfico teórico de la pluralidad de flujos de datos correspondiente al campo de coincidencia objetivo en la tabla de información de flujos
S20332
Establecer una ecuación mediante la igualación del tráfico teórico de un flujo de datos que coincide con el campo de coincidencia y que está en el dispositivo de conmutación, con el tráfico real
S20334
Establecer una ecuación mediante la igualación de una suma de tráficos teóricos de la pluralidad de flujos de datos que coinciden con el campo de coincidencia y que están en el dispositivo de conmutación, con el tráfico real
Fin

FIG. 7

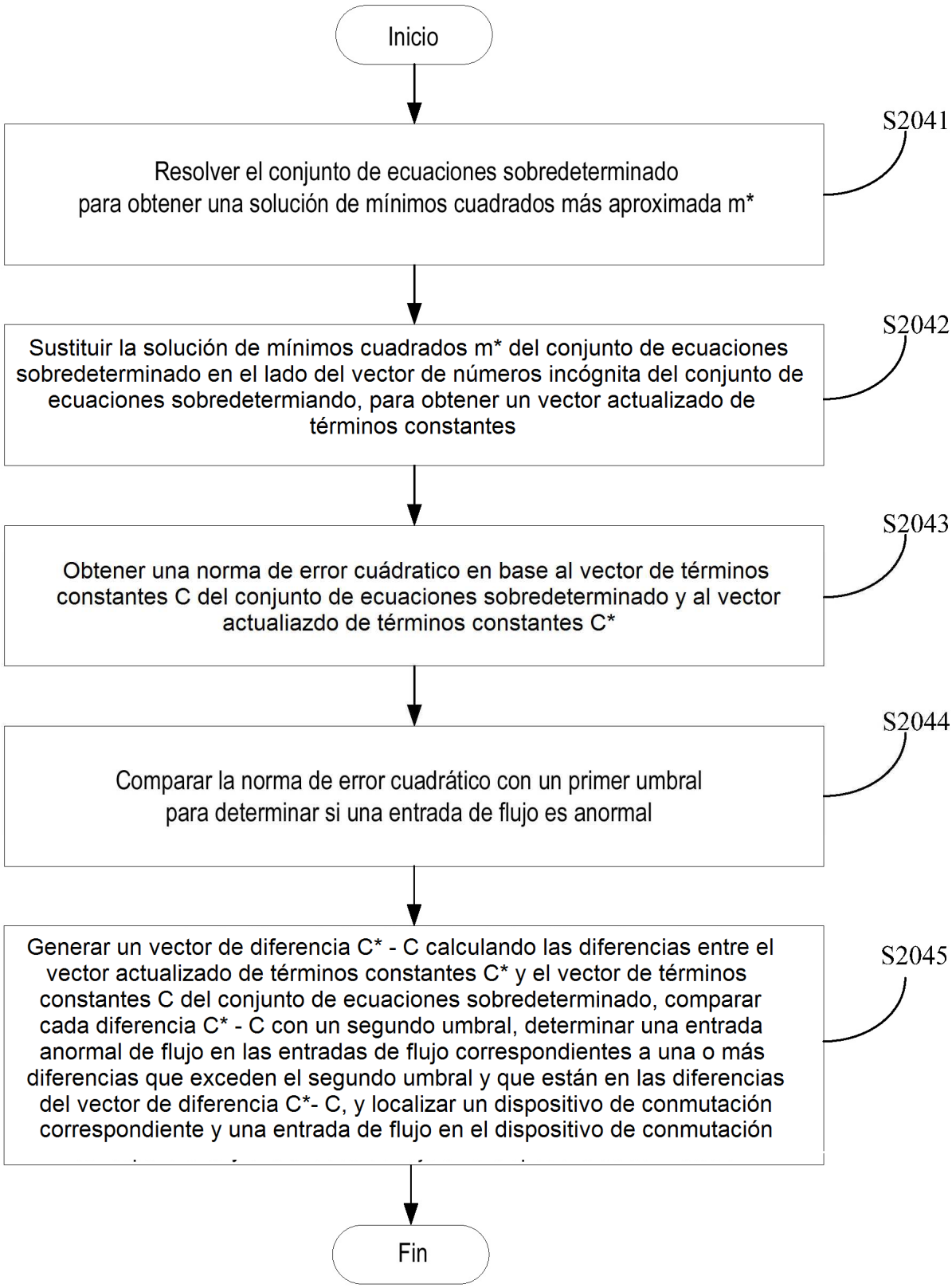
Inicio
S2041
Resolver el conjunto de ecuaciones sobredeterminado para obtener una solución de mínimos cuadrados más aproximada m*
S2042
Sustituir la solución de mínimos cuadrados m* del conjunto de ecuaciones sobredeterminado en el lado del vector de números incógnita del conjunto de ecuaciones sobredetermiando, para obtener un vector actualizado de términos constantes
S2043
Obtener una norma de error cuádratico en base al vector de términos constantes C del conjunto de ecuaciones sobredeterminado y al vector actualiazdo de términos constantes C*
S2044
Comparar la norma de error cuadrático con un primer umbral para determinar si una entrada de flujo es anormal
S2045
Generar un vector de diferencia C* - C calculando las diferencias entre el vector actualizado de términos constantes C* y el vector de términos constantes C del conjunto de ecuaciones sobredeterminado, comparar cada diferencia C* - C con un segundo umbral, determinar una entrada anormal de flujo en las entradas de flujo correspondientes a una o más diferencias que exceden el segundo umbral y que están en las diferencias del vector de diferencia C*- C, y localizar un dispositivo de conmutación correspondiente y una entrada de flujo en el dispositivo de conmutación
Fin

FIG. 8

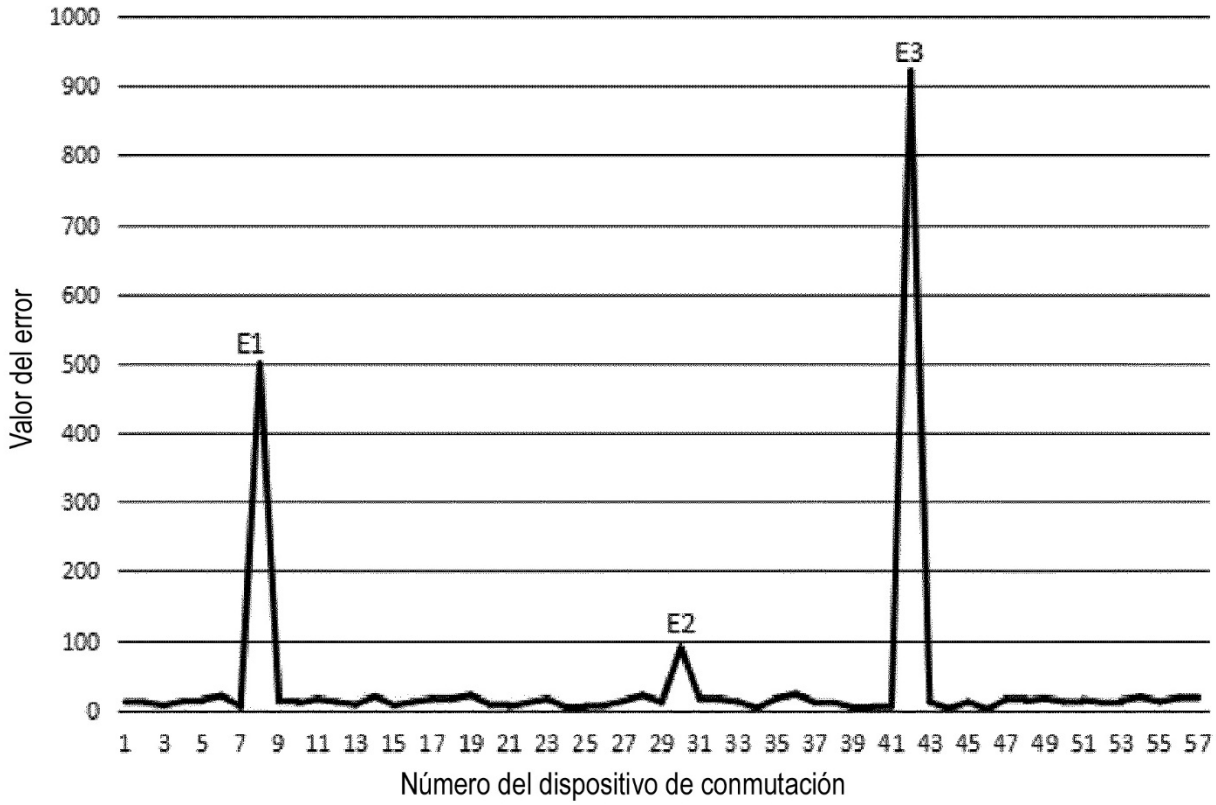
1000
900
800
700
600
500
400
300
200
100
0
Valor del error
E1
E2
E3
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 49 51 53 55 57
Número del dispositivo de conmutación

FIG. 9

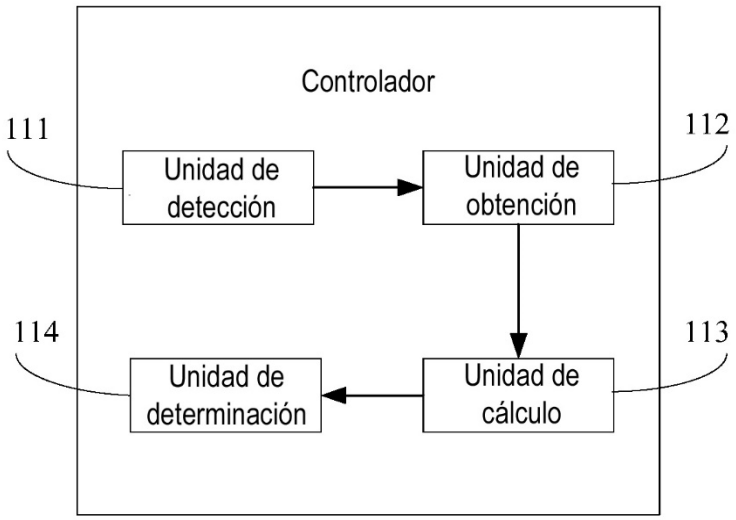
Controlador
111
Unidad de detección
112
Unidad de obtención
114
Unidad de determinación
113
Unidad de cálculo

FIG. 10

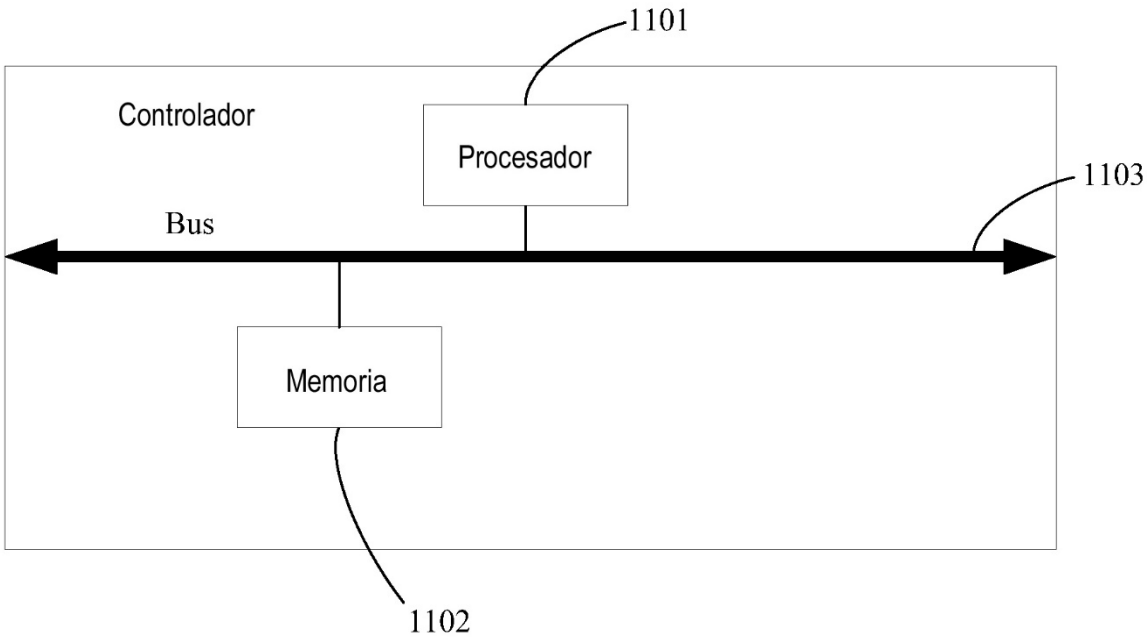

FIG. 11