(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 618 934**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/10 (2009.01)
H04W 12/12 (2009.01)
H04W 72/04 (2009.01)
H04L 9/32 (2006.01)
H04W 24/02 (2009.01)
H04W 92/10 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **24.07.2012 PCT/CN2012/079095**

(87) Fecha y número de publicación internacional: **30.01.2014 WO2014015478**

(96) Fecha de presentación y número de la solicitud europea: **24.07.2012 E 12881848 (1)**

(97) Fecha y número de publicación de la concesión europea: **28.12.2016 EP 2876839**

(54) Título: **Procedimiento, aparato y sistema de comprobación y reconfiguración**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.06.2017

(73) Titular/es:

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

(72) Inventor/es:

ZHANG, TAO;
LIN, BO y
ZHANG, DONGMEI

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Procedimiento, aparato y sistema de comprobación y reconfiguración

Campo técnico

La presente invención se refiere al campo de las comunicaciones y, en particular, a un procedimiento, aparato y sistema de comprobación y reconfiguración.

Antecedentes

Debido al rápido desarrollo de las tecnologías de comunicación, una red de Evolución a Largo Plazo (LTE) incluye algunos procesos relacionados con la seguridad. Los procesos incluyen específicamente un proceso de comprobación y un proceso de reconfiguración. El proceso de comprobación consiste principalmente en que una red existente necesita que un terminal compruebe una cantidad de datos enviados o recibidos en cada portadora radioeléctrica de datos (DRB), con el fin de detectar si un intruso ha insertado un paquete de datos entre la red y el terminal. El proceso de reconfiguración consiste principalmente en que la red existente notifica al terminal un algoritmo de seguridad que va a usarse, con el fin de actualizar un algoritmo y una clave del terminal. Cada DRB es una portadora radioeléctrica que se establece según un requisito de servicio de un usuario, y se usa para transmitir datos del usuario.

En la técnica anterior, el proceso de comprobación y el proceso de reconfiguración se completan conjuntamente mediante una estación base y un terminal. Cuando se necesita realizar una comprobación, la estación base envía información de comprobación al terminal, donde la información incluye una identidad de una DRB. Según la identidad de la DRB, el terminal compara los 25 primeros bits de un valor de cómputo de enlace ascendente de la DRB con los 25 primeros bits de un valor de cómputo de enlace ascendente de una DRB correspondiente mantenida por el propio terminal, y compara los 25 primeros bits de un valor de cómputo de enlace descendente de la DRB con los 25 primeros bits de un valor de cómputo de enlace descendente de la DRB correspondiente mantenida por el propio terminal. Cuando al menos un resultado de los resultados de las dos comparaciones es diferente, el terminal envía información de respuesta de comprobación a la estación base. Cuando se necesita realizar una reconfiguración, la estación base envía información de reconfiguración al terminal. El terminal se comunica con la estación base según un algoritmo de seguridad de la información de reconfiguración y envía información de reconfiguración completada a la estación base.

Sin embargo, el proceso de comprobación y el proceso de reconfiguración de la técnica anterior no pueden aplicarse a una arquitectura de red nueva. En la nueva arquitectura de red, una estación base que mantiene un valor de cómputo es diferente de una estación base que ejecuta un proceso de comprobación. Además, una estación base que lleva a cabo una comunicación segura con un terminal es también diferente de una estación base que ejecuta un proceso de reconfiguración. La estación base que mantiene el valor de cómputo es una estación base secundaria. La estación base que ejecuta el proceso de comprobación es una estación base primaria. La estación base que lleva a cabo realmente una comunicación segura con el terminal es la estación base secundaria. La estación base que ejecuta el proceso de reconfiguración es la estación base primaria. Si el proceso de comprobación de la técnica anterior se aplica a la nueva arquitectura de red, la estación base primaria no puede ejecutar el proceso de comprobación ya que no puede obtener información relacionada con el cómputo. Si el proceso de reconfiguración de la técnica anterior se aplica a la nueva arquitectura de red, la estación base secundaria no puede establecer una comunicación normal con el terminal ya que no puede obtener información relacionada con la seguridad.

El documento 3GPP TS 33.401, no. V11.4.0, 29 de junio de 2012, da a conocer un procedimiento. Un eNB envía un mensaje de comprobación. El mensaje de comprobación contiene las partes más significativas de los valores de cómputo de PDCP. Un UE compara los valores de cómputo de PDCP recibidos en el mensaje de comprobación con los valores de sus portadoras radioeléctricas. El eNB recibe una respuesta de comprobación que contiene uno o varios valores de cómputo de PDCP.

El documento CN101754243A, publicado el 23 de junio de 2010, da a conocer un procedimiento y un sistema de detección de seguridad. El procedimiento permite obtener un valor de cómputo; el valor de cómputo y un ID de DRB se transmiten a un UE para su comprobación; se recibe el resultado de la comprobación y, si se produce una anomalía, se guardan el valor de cómputo y el ID de DRB en el lado del UE; además, se comprueban el valor de cómputo y el ID de DRB en el lado del UE.

Resumen

Las formas de realización de la presente invención proporcionan un procedimiento, aparato y sistema de comprobación y reconfiguración aplicados a una arquitectura de red en la que una estación base primaria está desvinculada de una estación base secundaria para resolver el problema de que un proceso de comprobación y un proceso de reconfiguración no pueden implementarse en la arquitectura de red, implementándose por tanto el proceso de comprobación y el proceso de reconfiguración en la arquitectura de red en la que la estación base primaria está desvinculada de la estación base secundaria.

Según un primer aspecto, una forma de realización de la presente invención proporciona un procedimiento de comprobación, donde el procedimiento incluye: recibir, mediante una estación base, primera información de identidad y primera información de cómputo enviadas por una estación base secundaria; consultar, mediante la estación base, según la primera información de identidad, segunda información de identidad correspondiente a la primera información de identidad; extraer, mediante la estación base, segunda información de cómputo a partir de la primera información de cómputo; enviar, mediante la estación base, la segunda información de identidad y la segunda información de cómputo a un terminal, de modo que el terminal compara, según la segunda información de identidad, la segunda información de cómputo con tercera información de cómputo mantenida por propio terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación; recibir, mediante la estación base, la primera información de resultado de comparación enviada por el terminal, o la segunda información de identidad y segunda información de resultado de comparación enviadas por el terminal; y determinar, mediante la estación base, información de resultado de comprobación según la primera información de resultado de comparación recibida, o la segunda información de identidad y la segunda información de resultado de comparación recibidas.

Según un segundo aspecto, una forma de realización de la presente invención proporciona un procedimiento de comprobación, donde el procedimiento incluye: recibir, mediante un terminal, segunda información de identidad correspondiente a primera información de identidad y segunda información de cómputo extraída de primera información de cómputo, que se envían mediante una estación base primaria; comparar, mediante el terminal, según la segunda información de identidad, la segunda información de cómputo con tercera información de cómputo mantenida de manera local por el terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación; y enviar, mediante el terminal, la primera información de resultado de comparación, o la segunda información de identidad y segunda información de resultado de comparación, a la estación base primaria, de modo que la estación base primaria determina la información de resultado de comprobación según la primera información de resultado de comparación o la segunda información de resultado de comparación, donde la comparación realizada por el terminal, según la segunda información de identidad, de la segunda información de cómputo, comprendiendo la segunda información de cómputo un segundo valor de cómputo de enlace ascendente y un segundo valor de cómputo de enlace descendente, con tercera información de cómputo, comprendiendo la tercera información de cómputo un tercer valor de cómputo de enlace ascendente y un tercer valor de cómputo de enlace descendente, mantenida de manera local por el terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación, comprende específicamente:

según la segunda información de identidad, realizar una primera comparación entre el segundo valor de cómputo de enlace ascendente y el tercer valor de cómputo de enlace ascendente mantenido de manera local por el terminal y correspondiente a la segunda información de identidad, y/o realizar una segunda comparación entre el segundo valor de cómputo de enlace descendente y el tercer valor de cómputo de enlace descendente mantenido de manera local por el terminal y correspondiente a la segunda información de identidad;

cuando un resultado de comparación de la primera comparación es el mismo, y un resultado de comparación de la segunda comparación es también el mismo, obtener la primera información de resultado de comparación; cuando un resultado de comparación de la primera comparación es diferente y/o un resultado de comparación de la segunda comparación es diferente, obtener la segunda información de resultado de comparación; la primera información de resultado de comparación es información nula, la segunda información de resultado de comparación es la tercera información de cómputo.

Según un tercer aspecto, una forma de realización de la presente invención proporciona un procedimiento de comprobación, donde el procedimiento incluye: enviar primera información de identidad y primera información de cómputo a un terminal, de modo que el terminal compara, según la primera información de identidad, la primera información de cómputo con segunda información de cómputo mantenida por el propio terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación; recibir la primera información de resultado de comparación enviada por el terminal, o la primera información de identidad y la segunda información de resultado de comparación enviadas por el terminal; consultar, según la primera información de identidad, segunda información de identidad correspondiente a la primera información de identidad; y enviar la primera información de resultado de comparación o la segunda información de resultado de comparación a una estación base secundaria, de modo que la estación base secundaria determina la información de resultado de comprobación, obteniéndose así la segunda información de cómputo mantenida por el propio terminal.

Según un cuarto aspecto, una forma de realización de la presente invención proporciona un procedimiento de comprobación, donde el procedimiento incluye: recibir primera información de identidad y primera información de cómputo enviadas por una estación base primaria; comparar, según la primera información de identidad, la primera información de cómputo con segunda información de cómputo mantenida de manera local para obtener primera información de resultado de comparación o segunda información de resultado de comparación; y enviar la primera información de resultado de comparación, o la primera información de identidad y la segunda información de resultado de comparación, a la estación base primaria, de modo que la estación base primaria reenvía la primera información de identidad y segunda información de resultado de comparación a una estación base secundaria, de modo que la estación base secundaria obtiene la segunda información de cómputo mantenida por el terminal y compara la segunda información de cómputo con tercera información de cómputo mantenida por la propia estación base secundaria, determinándose así información de resultado de comprobación.

Según un quinto aspecto, una forma de realización de la presente invención proporciona un procedimiento de reconfiguración, donde el procedimiento incluye: determinar un algoritmo de cifrado según la capacidad de seguridad de un terminal; enviar al terminal información de reconfiguración que transporta el algoritmo de cifrado, de modo que el terminal actualiza una clave del propio terminal según el algoritmo de cifrado de la información de reconfiguración y se comunica con una estación base secundaria usando la clave actualizada; y recibir información de reconfiguración completada enviada por el terminal.

Según un sexto aspecto, una forma de realización de la presente invención proporciona un procedimiento de reconfiguración, donde el procedimiento incluye: recibir información de reconfiguración enviada por una estación base primaria y que transporta un algoritmo de cifrado; actualizar una clave local según el algoritmo de cifrado de la información de reconfiguración y usar el algoritmo de cifrado y la clave actualizada para establecer comunicación con una estación base secundaria; y enviar información de reconfiguración completada a la estación base primaria, de modo que la estación base primaria sabe, según la información de reconfiguración completada, que el terminal ha completado una reconfiguración.

Según un séptimo aspecto, una forma de realización de la presente invención proporciona un procedimiento de reconfiguración, donde el procedimiento incluye: recibir información de solicitud de actualización de parámetro de seguridad enviada por una estación base secundaria y que transporta un algoritmo de cifrado, donde la información de solicitud de actualización de parámetro de seguridad incluye el algoritmo de cifrado, o el algoritmo de cifrado e información de causa de solicitud de actualización de parámetro de seguridad; añadir a la información de reconfiguración el algoritmo de cifrado de la información de solicitud de actualización de parámetro de seguridad recibida; enviar a un terminal la información de reconfiguración que transporta el algoritmo de cifrado, de modo que el terminal actualiza una clave del propio terminal según el algoritmo de cifrado de la información de reconfiguración y se comunica con la estación base secundaria usando el algoritmo de cifrado y la clave actualizada; y recibir información de reconfiguración completada enviada por el terminal.

Según un octavo aspecto, una forma de realización de la presente invención proporciona un procedimiento de reconfiguración, donde el procedimiento incluye: recibir información de reconfiguración enviada por una estación base primaria y que transporta un algoritmo de cifrado; actualizar una clave local según el algoritmo de cifrado de la información de reconfiguración y usar el algoritmo de cifrado y la clave actualizada para establecer comunicación con una estación base secundaria; y enviar información de reconfiguración completada a la estación base primaria.

Según un noveno aspecto, una forma de realización de la presente invención proporciona una estación base primaria, donde la estación base primaria incluye: una primera unidad de recepción, configurada para recibir primera información de identidad y primera información de cómputo enviadas por una estación base secundaria, transmitir la primera información de identidad a una unidad de consulta, y transmitir la primera información de cómputo a una unidad de extracción; una unidad de consulta, configurada para recibir la primera información de identidad desde la primera unidad de recepción, consultar, según la primera información de identidad, segunda información de identidad correspondiente a la primera información de identidad, y transmitir la segunda información de identidad a una primera unidad de envío; una unidad de extracción, configurada para recibir la primera información de cómputo desde la primera unidad de recepción, extraer segunda información de cómputo a partir de la primera información de cómputo y transmitir la segunda información de cómputo a una primera unidad de envío; una primera unidad de envío, configurada para recibir la segunda información de identidad desde la unidad de consulta, recibir la segunda información de cómputo desde la unidad de extracción y enviar la segunda información de identidad y la segunda información de cómputo a un terminal, de manera que el terminal compara, según la segunda información de identidad, la segunda información de cómputo con tercera información de cómputo mantenida por el propio terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación; una segunda unidad de recepción, configurada para recibir la primera información de resultado de comparación enviada por el terminal, o la segunda información de identidad y segunda información de resultado de comparación enviadas por el terminal, y transmitir la primera información de resultado de comparación, o la segunda información de identidad y segunda información de resultado de comparación a una unidad de determinación; y una unidad de determinación, configurada para recibir la primera información de resultado de comparación, o la segunda información de identidad y segunda información de resultado de comparación, desde la segunda unidad de

recepción, y determinar la información de resultado de comprobación según la primera información de resultado de comparación recibida, o la segunda información de identidad y la segunda información de resultado de comparación recibidas.

Según un décimo aspecto, una forma de realización de la presente invención proporciona un terminal, donde el terminal incluye: una unidad de recepción, configurada para recibir segunda información de identidad correspondiente a primera información de identidad y segunda información de cómputo extraída de primera información de cómputo, enviadas por una estación base primaria, transmitir la segunda información de identidad a una unidad de comparación y a una unidad de envío, y transmitir la segunda información de cómputo a la unidad de comparación; una unidad de comparación, configurada para recibir la segunda información de identidad y la segunda información de cómputo desde la unidad de recepción, comparar, según la segunda información de identidad, la segunda información de cómputo con tercera información de cómputo mantenida de manera local por el terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación, y transmitir la primera información de resultado de comparación o la segunda información de resultado de comparación a una unidad de envío; y una unidad de envío, configurada para recibir la segunda información de identidad desde la unidad de recepción, recibir la primera información de resultado de comparación o la segunda información de resultado de comparación desde la unidad de comparación, y enviar la primera información de resultado de comparación, o la segunda información de identidad y la segunda información de resultado de comparación, a la estación base primaria, de modo que la estación base primaria determina la información de resultado de comprobación según la primera información de resultado de comparación o la segunda información de resultado de comparación, donde la comparación realizada por la unidad de comparación, según la segunda información de identidad, de la segunda información de cómputo, comprendiendo la segunda información de cómputo un segundo valor de cómputo de enlace ascendente y un segundo valor de cómputo de enlace descendente, con tercera información de cómputo, comprendiendo la tercera información de cómputo un tercer valor de cómputo de enlace ascendente y un tercer valor de cómputo de enlace descendente, mantenida de manera local por el terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación, comprende específicamente:

según la segunda información de identidad, realizar una primera comparación entre el segundo valor de cómputo de enlace ascendente y el tercer valor de cómputo de enlace ascendente mantenido de manera local por el terminal y correspondiente a la segunda información de identidad, y/o realizar una segunda comparación entre el segundo valor de cómputo de enlace descendente y el tercer valor de cómputo de enlace descendente mantenido de manera local por el terminal y correspondiente a la segunda información de identidad;

cuando un resultado de comparación de la primera comparación es el mismo, y un resultado de comparación de la segunda comparación es también el mismo, obtener la primera información de resultado de comparación; cuando un resultado de comparación de la primera comparación es diferente y/o un resultado de comparación de la segunda comparación es diferente, obtener la segunda información de resultado de comparación; la primera información de resultado de comparación es información nula, la segunda información de resultado de comparación es la tercera información de cómputo.

Según un décimo primer aspecto, una forma de realización de la presente invención proporciona un aparato de comprobación, donde el aparato incluye: una primera unidad de envío, configurada para enviar primera información de identidad y primera información de cómputo a un terminal, de modo que el terminal compara, según la primera información de identidad, la primera información de cómputo con segunda información de cómputo mantenida por el propio terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación; una unidad de recepción, configurada para recibir la primera información de resultado de comparación enviada por el terminal, o la primera información de identidad y segunda información de resultado de comparación enviadas por el terminal, transmitir la primera información de identidad a una unidad de consulta, y transmitir la primera información de resultado de comparación o la segunda información de resultado de comparación a una segunda unidad de envío; una unidad de consulta, configurada para recibir la primera información de identidad desde la unidad de recepción, consultar, según la primera información de identidad, segunda información de identidad correspondiente a la primera información de identidad, y transmitir la segunda información de identidad a una segunda unidad de envío; y una segunda unidad de envío, configurada para recibir la segunda información de identidad desde la unidad de consulta, recibir la primera información de resultado de comparación o la segunda información de resultado de comparación desde la unidad de recepción, y enviar la primera información de resultado de comparación, o la segunda información de identidad y la segunda información de resultado de comparación, a una estación base secundaria, de modo que la estación base secundaria determina la información de resultado de comprobación, obteniéndose así la segunda información de cómputo mantenida por el propio terminal.

Según un décimo segundo aspecto, una forma de realización de la presente invención proporciona un aparato de comprobación, donde el aparato incluye: una unidad de recepción, configurada para recibir primera información de identidad y primera información de cómputo enviadas por una estación base primaria, transmitir la primera información de identidad a una unidad de comparación y a una unidad de envío, y transmitir la primera información de cómputo a una unidad de consulta o de comparación; una unidad de consulta o de comparación, configurada

para recibir la primera información de identidad y la primera información de cómputo desde la unidad de recepción, comparar, según la primera información de identidad, la primera información de cómputo con segunda información de cómputo mantenida de manera local para obtener primera información de resultado de comparación o segunda información de resultado de comparación, y transmitir la segunda información de cómputo, o la primera información de resultado de comparación, o la segunda información de resultado de comparación a una unidad de envío; y una unidad de envío, configurada para recibir la primera información de identidad desde la unidad de recepción, recibir la primera información de resultado de comparación o la segunda información de resultado de comparación desde la unidad de consulta y de comparación, y enviar la primera información de resultado de comparación, o la primera información de identidad y segunda información de resultado de comparación a la estación base primaria, de modo que la estación base primaria reenvía la primera información de identidad y la segunda información de resultado de comparación a una estación base secundaria, y después la estación base secundaria obtiene la segunda información de cómputo mantenida por el terminal y compara la segunda información de cómputo con tercera información de cómputo mantenida por la propia estación base secundaria, determinándose así información de resultado de comprobación.

Según un décimo tercer aspecto, una forma de realización de la presente invención proporciona un aparato de reconfiguración, donde el aparato incluye: una unidad de determinación, configurada para determinar un algoritmo de cifrado según la capacidad de seguridad de un terminal, y transmitir el algoritmo de cifrado a una primera unidad de envío y una segunda unidad de envío; una primera unidad de envío, configurada para recibir el algoritmo de cifrado desde la unidad de determinación, y enviar a un terminal información de reconfiguración que transporta el algoritmo de cifrado, de modo que el terminal actualiza una clave del propio terminal según el algoritmo de cifrado de la información de reconfiguración y se comunica con una estación base secundaria usando la clave actualizada; y una primera unidad de recepción, configurada para recibir información de reconfiguración completada enviada por el terminal.

Según un décimo cuarto aspecto, una forma de realización de la presente invención proporciona un aparato de reconfiguración, donde el aparato incluye: una unidad de recepción, configurada para recibir información de reconfiguración enviada por una estación base primaria y que transporta un algoritmo de cifrado, y transmitir a una unidad de actualización la información de reconfiguración que transporta el algoritmo de cifrado; una unidad de actualización, configurada para recibir desde la unidad de recepción la información de reconfiguración que transporta el algoritmo de cifrado, actualizar una clave local según el algoritmo de cifrado de la información de reconfiguración y usar el algoritmo de cifrado y la clave actualizada para establecer comunicación con una estación base secundaria, y transmitir la información de clave actualizada a una unidad de envío; y una unidad de envío, configurada para recibir la información de clave actualizada desde la unidad de actualización, y enviar información de reconfiguración completada a la estación base primaria, de modo que la estación base primaria sabe, según la información de reconfiguración completada, que el terminal ha completado una reconfiguración.

Según un décimo quinto aspecto, una forma de realización de la presente invención proporciona un aparato de reconfiguración, donde el aparato incluye: una primera unidad de recepción, configurada para recibir información de solicitud de actualización de parámetro de seguridad enviada por una estación base secundaria y que transporta un algoritmo de cifrado, y transmitir a una unidad de adición la información de solicitud de actualización de parámetro de seguridad que transporta el algoritmo de cifrado, donde la información de solicitud de actualización de parámetro de seguridad incluye el algoritmo de cifrado, o el algoritmo de cifrado y la información de causa de solicitud de actualización de parámetro de seguridad; una unidad de adición, configurada para recibir desde la primera unidad de recepción la información de solicitud de actualización de parámetro de seguridad que transporta el algoritmo de cifrado, añadir a la información de reconfiguración el algoritmo de cifrado de la información de solicitud de actualización de parámetro de seguridad recibida, y transmitir la información de reconfiguración a una primera unidad de envío; una primera unidad de envío, configurada para recibir desde la unidad de adición la información de reconfiguración que transporta el algoritmo de cifrado, y enviar a un terminal la información de reconfiguración que transporta el algoritmo de cifrado, de modo que el terminal actualiza una clave del propio terminal según el algoritmo de cifrado de la información de reconfiguración y se comunica con la estación base secundaria usando la clave actualizada; y una segunda unidad de recepción, configurada para recibir información de reconfiguración completada enviada por el terminal.

Según un décimo sexto aspecto, una forma de realización de la presente invención proporciona un aparato de reconfiguración, donde el aparato incluye: una unidad de recepción, configurada para recibir información de reconfiguración enviada por una estación base primaria y que transporta un algoritmo de cifrado, y transmitir a una unidad de actualización la información de reconfiguración que transporta el algoritmo de cifrado; una unidad de actualización, configurada para recibir desde la unidad de recepción la información de reconfiguración que transporta el algoritmo de cifrado, actualizar una clave local según el algoritmo de cifrado de la información de reconfiguración y usar el algoritmo de cifrado y la clave actualizada para establecer comunicación con una estación base secundaria, y transmitir la información de clave actualizada a una unidad de envío; y una unidad de envío, configurada para recibir la información de clave actualizada desde la unidad de actualización, y enviar información de reconfiguración completada a la estación base primaria, de modo que la estación base primaria sabe, según la información de reconfiguración completada, que un terminal ha completado una reconfiguración.

Según un décimo séptimo aspecto, una forma de realización de la presente invención proporciona un sistema de comprobación y de reconfiguración, donde el sistema incluye: el aparato de comprobación según el noveno aspecto, el aparato de comprobación según el décimo aspecto y una estación base secundaria; o el aparato de comprobación según el décimo primer aspecto, el aparato de comprobación según el décimo segundo aspecto y una estación base secundaria; o el aparato de reconfiguración según el décimo tercer aspecto, el aparato de reconfiguración según el décimo cuarto aspecto y una estación base secundaria; o el aparato de reconfiguración según el décimo quinto aspecto, el aparato de reconfiguración según el décimo sexto aspecto y una estación base secundaria.

Según un décimo octavo aspecto, una forma de realización de la presente invención proporciona una estación base primaria, donde la estación base primaria incluye: un receptor, configurado para recibir primera información de identidad y primera información de cómputo enviadas por una estación base secundaria, y transmitir la primera información de identidad y la primera información de cómputo a un procesador; y configurado además para recibir primera información de resultado de comparación, o segunda información de identidad y segunda información de resultado de comparación enviadas por un terminal, y transmitir a un procesador la primera información de identidad y la primera información de cómputo, la primera información de resultado de comparación, o la segunda información de identidad y segunda información de resultado de comparación; un procesador, configurado para recibir la primera información de identidad y la primera información de cómputo desde el receptor, consultar, según la primera información de identidad, segunda información de identidad correspondiente a la primera información de identidad y, por otro lado, extraer segunda información de cómputo a partir de la primera información de cómputo, y transmitir la segunda información de identidad y la segunda información de cómputo a un transmisor; y configurado además para recibir la primera información de resultado de comparación, o la segunda información de identidad y segunda información de resultado de comparación desde el receptor, y determinar la información de resultado de comprobación según la primera información de resultado de comparación recibida, o la segunda información de identidad recibida y segunda información de resultado de comparación; y un transmisor, configurado para recibir la segunda información de identidad y la segunda información de cómputo desde el procesador, y enviar la segunda información de identidad y la segunda información de cómputo al terminal, de modo que el terminal compara, según la segunda información de identidad, la segunda información de cómputo con tercera información de cómputo mantenida por el propio terminal para obtener la primera información de resultado de comparación o la segunda información de resultado de comparación.

Según un décimo noveno aspecto, una forma de realización de la presente invención proporciona un terminal, donde el terminal incluye: un receptor, configurado para recibir segunda información de identidad correspondiente a primera información de identidad y segunda información de cómputo extraída de primera información de cómputo, enviadas por una estación base primaria, transmitir la segunda información de identidad a una unidad de comparación y a una unidad de envío, y transmitir la segunda información de cómputo a un procesador; un procesador, configurado para recibir la segunda información de identidad y la segunda información de cómputo desde el receptor, y comparar, según la segunda información de identidad, la segunda información de cómputo con tercera información de cómputo mantenida de manera local para obtener primera información de resultado de comparación o segunda información de resultado de comparación, y transmitir la primera información de resultado de comparación o la segunda información de resultado de comparación a un transmisor; y un transmisor, configurado para recibir la segunda información de identidad desde el receptor, recibir la primera información de resultado de comparación o la segunda información de resultado de comparación desde la unidad de comparación, y enviar la primera información de resultado de comparación, o la segunda información de identidad y la segunda información de resultado de comparación, a la estación base primaria, de modo que la estación base primaria determina la información de resultado de comprobación según la primera información de resultado de comparación o la segunda información de resultado de comparación.

Según un vigésimo aspecto, una forma de realización de la presente invención proporciona una estación base primaria, donde la estación base primaria incluye: un transmisor, configurado para enviar primera información de identidad y primera información de cómputo a un terminal, de modo que el terminal compara, según la primera información de identidad, la primera información de cómputo con segunda información de cómputo mantenida por el propio terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación; y configurado además para recibir segunda información de identidad desde un procesador, y la primera información de resultado de comparación o la segunda información de resultado de comparación, y enviar primera información de resultado de comparación, o la segunda información de identidad y la segunda información de resultado de comparación, a una estación base secundaria, de modo que la estación base secundaria determina la información de resultado de comprobación, obteniéndose así la segunda información de cómputo mantenida por el propio terminal; un receptor, configurado para recibir la primera información de resultado de comparación enviada por el terminal, o la primera información de identidad y segunda información de resultado de comparación enviadas por el terminal, transmitir la primera información de identidad al procesador, y transmitir la primera información de resultado de comparación o la segunda información de resultado de comparación al transmisor; y un procesador, configurado para recibir la primera información de identidad desde el receptor, consultar, según la primera información de identidad, la segunda información de identidad correspondiente a la primera información de identidad, y transmitir la segunda información de identidad al transmisor.

Según un vigésimo primer aspecto, una forma de realización de la presente invención proporciona un terminal, donde el terminal incluye: un receptor, configurado para recibir primera información de identidad y primera información de cómputo, enviadas por una estación base primaria, transmitir la primera información de identidad a un procesador y un transmisor, y transmitir la primera información de cómputo a un procesador; un procesador, configurado para recibir la primera información de identidad y la primera información de cómputo desde el receptor, comparar, según la primera información de identidad, la primera información de cómputo con segunda información de cómputo mantenida de manera local para obtener primera información de resultado de comparación o segunda información de resultado de comparación, y transmitir la segunda información de cómputo, o la primera información de resultado de comparación, o la segunda información de resultado de comparación, a un transmisor; y un transmisor, configurado para recibir la primera información de identidad desde el receptor, recibir la primera información de resultado de comparación o la segunda información de resultado de comparación desde el procesador, y enviar la primera información de resultado de comparación, o la primera información de identidad y segunda información de resultado de comparación a la estación base primaria, de modo que la estación base primaria envía la primera información de identidad y la segunda información de resultado de comparación a una estación base secundaria, y después la estación base secundaria obtiene la segunda información de cómputo mantenida por el terminal y compara la segunda información de cómputo con tercera información de cómputo mantenida por la propia estación base secundaria, determinándose así información de resultado de comprobación.

Según un vigésimo segundo aspecto, una forma de realización de la presente invención proporciona una estación base primaria, donde la estación base primaria incluye: un procesador, configurado para determinar un algoritmo de cifrado según la capacidad de seguridad de un terminal, y transmitir el algoritmo de cifrado a un transmisor; un transmisor, configurado para recibir el algoritmo de cifrado desde el procesador, y enviar al terminal información de reconfiguración que transporta el algoritmo de cifrado, de modo que el terminal actualiza una clave del propio terminal según el algoritmo de cifrado de la información de reconfiguración y se comunica con una estación base secundaria usando la clave actualizada; y un receptor, configurado para recibir información de reconfiguración completada enviada por el terminal.

Según un vigésimo tercer aspecto, una forma de realización de la presente invención proporciona un terminal, donde el terminal incluye: un receptor, configurado para recibir información de reconfiguración enviada por una estación base primaria y que transporta un algoritmo de cifrado, y transmitir a un procesador la información de reconfiguración que transporta el algoritmo de cifrado; un procesador, configurado para recibir desde el receptor la información de reconfiguración que transporta el algoritmo de cifrado, actualizar una clave local según el algoritmo de cifrado de la información de reconfiguración y usar el algoritmo de cifrado y la clave actualizada para establecer comunicación con una estación base secundaria, y transmitir la información de clave actualizada a un transmisor; y un transmisor, configurado para recibir la información de clave actualizada desde el procesador, y enviar información de reconfiguración completada a la estación base primaria, de modo que la estación base primaria sabe, según la información de reconfiguración completada, que el terminal ha completado una reconfiguración.

Según un vigésimo cuarto aspecto, una forma de realización de la presente invención proporciona una estación base primaria, donde la estación base primaria incluye: un receptor, configurado para recibir información de solicitud de actualización de parámetro de seguridad enviada por una estación base secundaria y que transporta un algoritmo de cifrado, y transmitir a un procesador la información de solicitud de actualización de parámetro de seguridad que transporta el algoritmo de cifrado; y configurado además para recibir información completa de reconfiguración enviada por el terminal, donde la información de solicitud de actualización de parámetro de seguridad incluye el algoritmo de cifrado, o el algoritmo de cifrado e información de causa de solicitud de actualización de parámetro de seguridad; y un retransmisor, configurado para recibir desde el receptor la información de reconfiguración que transporta el algoritmo de cifrado, y reenviar al terminal la información de reconfiguración que transporta el algoritmo de cifrado, de modo que el terminal actualiza una clave del propio terminal según el algoritmo de cifrado de la información de reconfiguración y se comunica con una estación base secundaria usando la clave actualizada.

Según un vigésimo quinto aspecto, una forma de realización de la presente invención proporciona un terminal, donde el terminal incluye: un receptor, configurado para recibir información de reconfiguración enviada por una estación base primaria y que transporta un algoritmo de cifrado, y transmitir a un procesador la información de reconfiguración que transporta el algoritmo de cifrado; un procesador, configurado para recibir desde el receptor la información de reconfiguración que transporta el algoritmo de cifrado, actualizar una clave local según el algoritmo de cifrado de la información de reconfiguración y usar el algoritmo de cifrado y la clave actualizada para establecer comunicación con una estación base secundaria, y transmitir la información de clave actualizada a un transmisor; y un transmisor, configurado para recibir la información de clave actualizada desde el procesador, y enviar información de reconfiguración completa a la estación base primaria, de modo que la estación base primaria sabe, según la información de reconfiguración completada, que un terminal ha completado una reconfiguración.

Según un vigésimo sexto aspecto, una forma de realización de la presente invención proporciona un sistema de comprobación y reconfiguración, donde el sistema incluye: la estación base primaria según el décimo octavo aspecto, el terminal según el décimo noveno aspecto y una estación base secundaria; o la estación base primaria según el vigésimo aspecto, el terminal según el vigésimo primer aspecto y una estación base secundaria; o la estación base primaria según el vigésimo segundo aspecto, el terminal según el vigésimo tercer aspecto y una

estación base secundaria; o la estación base primaria según el vigésimo cuarto aspecto, el terminal según el vigésimo quinto aspecto y una estación base secundaria.

Aplicando las soluciones anteriores, las formas de realización de la presente invención implementan un proceso de comprobación y un proceso de reconfiguración en una arquitectura de red en la que una estación base primaria está desvinculada de una estación base secundaria.

Breve descripción de los dibujos

La FIG. 1 es un diagrama de una arquitectura de red de un sistema de comprobación y de reconfiguración según la forma de realización 1 de la presente invención.
La FIG. 2 es un diagrama de flujo de un procedimiento de comprobación según la forma de realización 2 de la presente invención.
La FIG. 3 es un diagrama de flujo de un procedimiento de comprobación según la forma de realización 3 de la presente invención.
La FIG. 4 es un diagrama de interacción de información de un procedimiento de comprobación según la forma de realización 4 de la presente invención.
La FIG. 5 es un diagrama de interacción de información de un procedimiento de comprobación según la forma de realización 5 de la presente invención.
La FIG. 6 es un diagrama de interacción de información de un procedimiento de comprobación según la forma de realización 6 de la presente invención.
La FIG. 7 es un diagrama de flujo de un procedimiento de comprobación según la forma de realización 7 de la presente invención.
La FIG. 8 es un diagrama de flujo de un procedimiento de comprobación según la forma de realización 8 de la presente invención.
La FIG. 9 es un diagrama de interacción de información de un procedimiento de comprobación según la forma de realización 9 de la presente invención.
La FIG. 10 es un diagrama de flujo de un procedimiento de reconfiguración según la forma de realización 10 de la presente invención.
La FIG. 11 es un diagrama de flujo de un procedimiento de reconfiguración según la forma de realización 11 de la presente invención.
La FIG. 12 es un diagrama de interacción de información de un procedimiento de reconfiguración según la forma de realización 12 de la presente invención.
La FIG. 13 es un diagrama de interacción de información de un procedimiento de reconfiguración según la forma de realización 13 de la presente invención.
La FIG. 14 es un diagrama de flujo de un procedimiento de reconfiguración según la forma de realización 14 de la presente invención.
La FIG. 15 es un diagrama de flujo de un procedimiento de reconfiguración según la forma de realización 15 de la presente invención.
La FIG. 16 es un diagrama de interacción de información de un procedimiento de reconfiguración según la forma de realización 16 de la presente invención.
La FIG. 17 es un diagrama de interacción de información de un procedimiento de reconfiguración según la forma de realización 17 de la presente invención.
La FIG. 18 es un diagrama de interacción de información de un procedimiento de reconfiguración según la forma de realización 18 de la presente invención.
La FIG. 19 es un diagrama esquemático de un aparato de comprobación según la forma de realización 19 de la presente invención.
La FIG. 20 es un diagrama esquemático de un aparato de comprobación según la forma de realización 20 de la presente invención.
La FIG. 21 es un diagrama esquemático de un aparato de comprobación según la forma de realización 21 de la presente invención.
La FIG. 22 es un diagrama esquemático de un aparato de comprobación según la forma de realización 22 de la presente invención.
La FIG. 23 es un diagrama esquemático de un aparato de reconfiguración según la forma de realización 23 de la presente invención.
La FIG. 24 es un diagrama esquemático de un aparato de reconfiguración según la forma de realización 24 de la presente invención.
La FIG. 25 es un diagrama esquemático de un aparato de reconfiguración según la forma de realización 25 de la presente invención.
La FIG. 26 es un diagrama esquemático de un aparato de reconfiguración según la forma de realización 26 de la presente invención.
La FIG. 27 es un diagrama estructural esquemático de una estación base primaria según la forma de realización 27 de la presente invención.
La FIG. 28 es un diagrama estructural esquemático de un terminal según la forma de realización 28 de la presente invención.

La FIG. 29 es un diagrama estructural esquemático de una estación base primaria según la forma de realización 29 de la presente invención.
La FIG. 30 es un diagrama estructural esquemático de un terminal según la forma de realización 30 de la presente invención.
La FIG. 31 es un diagrama estructural esquemático de una estación base primaria según la forma de realización 31 de la presente invención.
La FIG. 32 es un diagrama estructural esquemático de un terminal según la forma de realización 32 de la presente invención.
La FIG. 33 es un diagrama estructural esquemático de una estación base primaria según la forma de realización 33 de la presente invención.
La FIG. 34 es un diagrama estructural esquemático de un terminal según la forma de realización 34 de la presente invención.

Descripción de formas de realización

Para facilitar el entendimiento de los objetivos, las soluciones técnicas y las ventajas de las formas de realización de la presente invención, a continuación se describen de manera clara y completa las soluciones técnicas de las formas de realización de la presente invención haciendo referencia a los dibujos adjuntos de las formas de realización de la presente invención. Evidentemente, las formas de realización descritas son parte y no todas las formas de realización de la presente invención. Todas las demás formas de realización obtenidas por un experto en la técnica basándose en las formas de realización de la presente invención sin realizar investigaciones adicionales estarán dentro del alcance de protección de la presente invención.

La FIG. 1 es un diagrama de arquitectura de un sistema de comprobación y de reconfiguración según la forma de realización 1 de la presente invención. Como se muestra en la figura, el sistema de comprobación y reconfiguración proporcionado por la forma de realización de la presente invención incluye específicamente: una estación base primaria 11, una estación base secundaria 12 y un terminal 13.

En el sistema, la estación base primaria 11 está configurada para ejecutar un proceso de comprobación y para pedir al terminal 13 que compruebe una cantidad de datos enviados o recibidos a través de cada DRB, con el fin de detectar si un intruso ha insertado un paquete de datos entre la estación base primaria 11 y el terminal 13, y la estación base secundaria 12 está configurada para mantener un valor de cómputo. Además, la estación base primaria 11 está configurada para ejecutar un proceso de reconfiguración y para notificar al terminal 13 un algoritmo de seguridad que va a usarse, actualizando de ese modo un algoritmo y una clave del terminal, y la estación base secundaria 12 está configurada para realizar una comunicación segura con el terminal 13.

La FIG. 2 es un diagrama de flujo de un procedimiento de comprobación según la forma de realización 2 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente las siguientes etapas:

Etapa 201: Una estación base primaria recibe primera información de identidad y primera información de cómputo enviada por una estación base secundaria.
Específicamente, la primera información de identidad incluye una identidad de un terminal y una identidad de portadora de acceso radioeléctrico, E-RAB, del terminal; la primera información de cómputo incluye un primer valor de cómputo de enlace ascendente y un primer valor de cómputo de enlace descendente de la identidad E-RAB del terminal, o n primeros bits de un primer valor de cómputo de enlace ascendente y n primeros bits de un primer valor de cómputo de enlace descendente de la identidad E-RAB del terminal, donde n es un valor numérico definido por el usuario.
Etapa 202: La estación base primaria consulta, según la primera información de identidad, segunda información de identidad correspondiente a la primera información de identidad. Específicamente, una identidad DRB del terminal y correspondiente a la identidad E-RAB se consulta según la identidad del terminal y la identidad de portadora de acceso radioeléctrico, E-RAB, del terminal, donde la identidad DRB del terminal es la segunda información de identidad. Una conexión entre la estación base primaria y el terminal puede tener múltiples DRB, y una conexión entre la estación base primaria y una red central puede tener múltiples E-RAB. En un mismo terminal, cada E-RAB corresponde a una DRB única. Por lo tanto, la identidad DRB del terminal puede determinarse de manera única según la identidad del terminal y la identidad de portadora de acceso radioeléctrico, E-RAB, del terminal.
Etapa 203: La estación base primaria extrae segunda información de cómputo de la primera información de cómputo. Una pluralidad de primeros bits del primer valor de cómputo de enlace ascendente se extraen de la primera información de cómputo para usarse como segundo valor de cómputo de enlace ascendente, y una pluralidad de primeros bits del primer valor de cómputo de enlace descendente se extraen de la primera información de cómputo para usarse como segundo valor de cómputo de enlace descendente, donde el segundo valor de cómputo de enlace ascendente y el segundo valor de cómputo de enlace descendente constituyen la segunda información de cómputo.
Específicamente, si la primera información de cómputo incluye el primer valor de cómputo de enlace ascendente y el primer valor de cómputo de enlace descendente de la identidad E-RAB del terminal, m

primeros bits del primer valor de cómputo de enlace ascendente y m primeros bits del primer valor de cómputo de enlace descendente de la identidad E-RAB del terminal se extraen como segundo valor de cómputo de enlace ascendente y como segundo valor de cómputo de enlace descendente, respectivamente, donde el segundo valor de cómputo de enlace ascendente y el segundo valor de cómputo de enlace descendente constituyen la segunda información de cómputo, y m es un valor numérico definido por el usuario.

Si la primera información de cómputo incluye los n primeros bits del primer valor de cómputo de enlace ascendente y los n primeros bits del primer valor de cómputo de enlace descendente de la identidad E-RAB del terminal, m primeros bits del primer valor de cómputo de enlace ascendente y m primeros bits del primer valor de cómputo de enlace descendente de la identidad E-RAB del terminal se extraen como segundo valor de cómputo de enlace ascendente y como segundo valor de cómputo de enlace descendente, respectivamente, donde el segundo valor de cómputo de enlace ascendente y el segundo valor de cómputo de enlace descendente constituyen la segunda información de cómputo, y m es un valor numérico definido por el usuario, y m es inferior a igual a n.

Etapa 204: La estación base primaria envía la segunda información de identidad y la segunda información de cómputo al terminal, de modo que el terminal compara, según la segunda información de identidad, la segunda información de cómputo con tercera información de cómputo mantenida por el propio terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación. Según la segunda información de identidad, el terminal realiza una primera comparación entre el segundo valor de cómputo de enlace ascendente y un tercer valor de cómputo de enlace ascendente mantenido por el propio terminal y correspondiente a la segunda información de identidad, y/o realiza una segunda comparación entre el segundo valor de cómputo de enlace descendente y un tercer valor de cómputo de enlace descendente mantenido por el propio terminal y correspondiente a la segunda información de identidad; cuando un resultado de comparación de la primera comparación es el mismo, y un resultado de comparación de la segunda comparación es el mismo, obtiene la primera información de resultado de comparación; cuando un resultado de comparación de la primera comparación es diferente y/o un resultado de comparación de la segunda comparación es diferente, obtiene la segunda información de resultado de comparación; la primera información de resultado de comparación es información nula, la segunda información de resultado de comparación es la tercera información de cómputo mantenida por el propio terminal, y la tercera información de cómputo mantenida por el propio terminal incluye el tercer valor de cómputo de enlace ascendente y el tercer valor de cómputo de enlace descendente.

Específicamente, un proceso en el que el terminal compara, según la segunda información de identidad, la segunda información de cómputo con la tercera información de cómputo mantenida por el propio terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación puede realizarse según los tres modos de comparación siguientes:

1. Según la segunda información de identidad, el terminal realiza una primera comparación entre el segundo valor de cómputo de enlace ascendente y el tercer valor de cómputo de enlace ascendente mantenido por el propio terminal y correspondiente a la segunda información de identidad; cuando un resultado de comparación de la primera comparación es el mismo, el terminal realiza una segunda comparación entre el segundo valor de cómputo de enlace descendente y el tercer valor de cómputo de enlace descendente mantenido por el propio terminal y correspondiente a la segunda información de identidad; cuando un resultado de comparación de la segunda comparación es también el mismo, el terminal obtiene la primera información de resultado de comparación. La primera información de resultado de comparación es información nula.

Cuando el resultado de comparación de la primera comparación es diferente, no es necesario realizar una segunda comparación entre el segundo valor de cómputo de enlace descendente y el tercer valor de cómputo de enlace descendente mantenido por el propio terminal y correspondiente a la segunda información de identidad, y la segunda información de resultado de comparación se obtiene directamente. La segunda información de resultado de comparación es la tercera información de cómputo mantenida por el propio terminal; la tercera información de cómputo mantenida por el propio terminal incluye el tercer valor de cómputo de enlace ascendente y el tercer valor de cómputo de enlace descendente.

Cuando el resultado de comparación de la primera comparación es el mismo, pero el resultado de comparación de la segunda comparación es diferente, también se obtiene la segunda información de resultado de comparación.

2. Según la segunda información de identidad, el terminal realiza una segunda comparación entre el segundo valor de cómputo de enlace descendente y el tercer valor de cómputo de enlace descendente mantenido por el propio terminal y correspondiente a la segunda información de identidad. Cuando un resultado de comparación de la segunda comparación es el mismo, el terminal realiza una primera comparación entre el segundo valor de cómputo de enlace ascendente y el tercer valor de cómputo de enlace ascendente mantenido por el propio terminal y correspondiente a la segunda información de identidad. El resto es igual al proceso de comparación anterior, y no se repite de nuevo.

3. Según la segunda información de identidad, el terminal realiza una primera comparación entre el segundo valor de cómputo de enlace ascendente y el tercer valor de cómputo de enlace ascendente mantenido por el propio terminal y correspondiente a la segunda información de identidad, y realiza una segunda comparación

entre el segundo valor de cómputo de enlace descendente y un tercer valor de cómputo de enlace descendente mantenido por el propio terminal y correspondiente a la segunda información de identidad. Cuando un resultado de comparación de la primera comparación es el mismo, y un resultado de comparación de la segunda comparación es el mismo, se obtiene la primera información de resultado de comparación; o cuando un resultado de comparación de la primera comparación es diferente y/o un resultado de comparación de la segunda comparación es diferente, se obtiene la segunda información de resultado de comparación. La primera información de resultado de comparación es información nula, la segunda información de resultado de comparación es la tercera información de cómputo mantenida por el propio terminal, y la tercera información de cómputo mantenida por el propio terminal incluye el tercer valor de cómputo de enlace ascendente y el tercer valor de cómputo de enlace descendente.

Si el segundo valor de cómputo de enlace ascendente y el segundo valor de cómputo de enlace descendente están formados por m bits, según la identidad DRB de la segunda información de identidad, el terminal consulta la tercera información de cómputo mantenida por el propio terminal, extrae por separado m primeros bits del tercer valor de cómputo de enlace ascendente y m primeros bits del tercer valor de cómputo de enlace descendente de la tercera información de cómputo, y después realiza una primera comparación entre el segundo valor de cómputo de enlace ascendente de m bits y el tercer valor de cómputo de enlace ascendente de m bits, y/o realiza una segunda comparación entre el segundo valor de cómputo de enlace descendente de m bits y el tercer valor de cómputo de enlace descendente de m bits.

Cuando el segundo valor de cómputo de enlace ascendente de m bits es el mismo que el tercer valor de cómputo de enlace ascendente de m bits, y el segundo valor de cómputo de enlace descendente de m bits es también el mismo que el tercer valor de cómputo de enlace descendente de m bits, esto indica que la primera información de cómputo de la estación base secundaria es la misma que la tercera información de cómputo mantenida por el propio terminal, y también indica que las cantidades de paquetes de datos enviados y recibidos y correspondientes a la identidad DRB son las mismas en la estación base secundaria y el terminal. Por lo tanto, ningún intruso ha insertado un paquete de datos entre la estación base secundaria y el terminal. En este caso, la información notificada a la estación base primaria es información nula, concretamente la primera información de resultado de comparación.

Cuando el segundo valor de cómputo de enlace ascendente de m bits es diferente del tercer valor de cómputo de enlace ascendente de m bits, y/o el segundo valor de cómputo de enlace descendente de m bits es también diferente del tercer valor de cómputo de enlace descendente de m bits, esto indica que la primera información de cómputo de la estación base secundaria es diferente de la tercera información de cómputo mantenida por el propio terminal, y también indica que las cantidades de paquetes de datos enviados y recibidos y correspondientes a la identidad DRB son diferentes en la estación base secundaria y el terminal. Por lo tanto, es posible que un intruso haya insertado un paquete de datos entre la estación base secundaria y el terminal. En este caso, la información notificada a la estación base primaria es la tercera información de cómputo mantenida por el propio terminal, concretamente la segunda información de resultado de comparación.

Etapa 205: La estación base primaria recibe la primera información de resultado de comparación enviada por el terminal, o la segunda información de identidad y la segunda información de resultado de comparación enviadas por el terminal. La segunda información de identidad es la identidad DRB, la primera información de resultado de comparación es información nula, y la segunda información de resultado de comparación es la tercera información de cómputo mantenida por el propio terminal.

Específicamente, cuando el segundo valor de cómputo de enlace ascendente de m bits es el mismo que el tercer valor de cómputo de enlace ascendente de m bits, y el segundo valor de cómputo de enlace descendente de m bits es también el mismo que el tercer valor de cómputo de enlace descendente de m bits, la estación base primaria recibe la identidad DRB e información nula enviadas por el terminal.

Cuando el segundo valor de cómputo de enlace ascendente de m bits es diferente del tercer valor de cómputo de enlace ascendente de m bits, y/o el segundo valor de cómputo de enlace descendente de m bits es diferente del tercer valor de cómputo de enlace descendente de m bits, la estación base primaria recibe la identidad DRB enviada por el terminal y la tercera información de cómputo mantenida por el propio terminal.

Etapa 206: La estación base primaria determina información de resultado de comprobación según la primera información de resultado de comparación recibida, o la segunda información de identidad y la segunda información de resultado de comparación recibidas.

Específicamente, cuando se recibe la primera información de resultado de comparación, se determina que la información de resultado de comprobación indica que la primera información de cómputo es coherente con la tercera información de cómputo; cuando se recibe la segunda información de resultado de comparación, se determina que la información de resultado de comprobación indica que la primera información de cómputo no es coherente con la tercera información de cómputo.

La FIG. 3 es un diagrama de flujo de un procedimiento de comprobación según la forma de realización 3 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente las siguientes etapas:

Etapa 301: Un terminal recibe segunda información de identidad correspondiente a primera información de identidad y segunda información de cómputo extraída de la primera información de cómputo enviada por una estación base primaria.

Específicamente, la estación base primaria determina la segunda información de identidad y segunda información de cómputo según la primera información de identidad y primera información de cómputo recibidas desde una estación base secundaria. La primera información de identidad incluye una identidad del terminal y una identidad de portadora de acceso radioeléctrico, E-RAB, del terminal; la primera información de cómputo incluye un primer valor de cómputo de enlace ascendente y un primer valor de cómputo de enlace descendente de la identidad E-RAB del terminal, o n primeros bits de un primer valor de cómputo de enlace ascendente y n primeros bits de un primer valor de cómputo de enlace descendente de la identidad de E-RAB del terminal.

Además, un proceso específico en la que la estación base primaria determina la segunda información de identidad y segunda información de cómputo según la primera información de identidad y primera información de cómputo recibidas desde la estación base secundaria, es como sigue:

Una identidad DRB del terminal y correspondiente a la identidad E-RAB se consulta según la identidad del terminal y la identidad de portadora de acceso radioeléctrico, E-RAB, del terminal, donde la identidad DRB del terminal es la segunda información de identidad.

Si la primera información de cómputo incluye el primer valor de cómputo de enlace ascendente y el primer valor de cómputo de enlace descendente de la identidad E-RAB del terminal, m primeros bits del primer valor de cómputo de enlace ascendente y m primeros bits del primer valor de cómputo de enlace descendente de la identidad E-RAB del terminal se extraen como segundo valor de cómputo de enlace ascendente y como segundo valor de cómputo de enlace descendente, respectivamente, donde el segundo valor de cómputo de enlace ascendente y el segundo valor de cómputo de enlace descendente constituyen la segunda información de cómputo, y m es un valor numérico definido por el usuario.

Si la primera información de cómputo incluye los n primeros bits del primer valor de cómputo de enlace ascendente y los n primeros bits del primer valor de cómputo de enlace descendente de la identidad E-RAB del terminal, m primeros bits del primer valor de cómputo de enlace ascendente y m primeros bits del primer valor de cómputo de enlace descendente de la identidad E-RAB del terminal se extraen como segundo valor de cómputo de enlace ascendente y como segundo valor de cómputo de enlace descendente, respectivamente, donde el segundo valor de cómputo de enlace ascendente y el segundo valor de cómputo de enlace descendente constituyen la segunda información de cómputo, m es un valor numérico definido por el usuario y m es inferior a igual a n.

Etapa 302: El terminal compara, según la segunda información de identidad, la segunda información de cómputo con tercera información de cómputo mantenida por el propio terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación.

Específicamente, el proceso de comparación específico de la etapa 302 es el mismo que el de la etapa 204, y no se describe de nuevo en el presente documento.

Según la segunda información de identidad, el terminal realiza una primera comparación entre el segundo valor de cómputo de enlace ascendente y un tercer valor de cómputo de enlace ascendente mantenido por el propio terminal y correspondiente a la segunda información de identidad, y/o realiza una segunda comparación entre el segundo valor de cómputo de enlace descendente y un tercer valor de cómputo de enlace descendente mantenido por el propio terminal y correspondiente a la segunda información de identidad; cuando un resultado de comparación de la primera comparación es el mismo, y un resultado de comparación de la segunda comparación es el mismo, obtiene la primera información de resultado de comparación; cuando un resultado de comparación de la primera comparación es diferente y/o un resultado de comparación de la segunda comparación es diferente, obtiene la segunda información de resultado de comparación; la primera información de resultado de comparación es información nula, la segunda información de resultado de comparación es la tercera información de cómputo mantenida por el propio terminal, y la tercera información de cómputo mantenida por el propio terminal incluye el tercer valor de cómputo de enlace ascendente y el tercer valor de cómputo de enlace descendente.

Si el segundo valor de cómputo de enlace ascendente y el segundo valor de cómputo de enlace ascendente están formados por m bits, según la identidad DRB de la segunda información de identidad, el terminal consulta la tercera información de cómputo mantenida por el propio terminal, extrae por separado m primeros bits del tercer valor de cómputo de enlace ascendente y m primeros bits del tercer valor de cómputo de enlace descendente de la tercera información de cómputo, después realiza una primera comparación entre el segundo valor de cómputo de enlace ascendente de m bits y el tercer valor de cómputo de enlace ascendente de m bits, y, por otro lado, realiza una

segunda comparación entre el segundo valor de cómputo de enlace descendente de m bits y el tercer valor de cómputo de enlace descendente de m bits.

Cuando el segundo valor de cómputo de enlace ascendente de m bits es el mismo que el tercer valor de cómputo de enlace ascendente de m bits, y el segundo valor de cómputo de enlace descendente de m bits es también el mismo que el tercer valor de cómputo de enlace descendente de m bits, esto indica que la primera información de cómputo de la estación base secundaria es la misma que la tercera información de cómputo mantenida por el propio terminal, y también indica que una cantidad de datos enviados o recibidos y correspondientes a la identidad DRB es la misma en la estación base primaria y el terminal. Por lo tanto, ningún intruso ha insertado un paquete de datos entre la estación base primaria y el terminal. En este caso, la información notificada a la estación base primaria es información nula, concretamente la primera información de resultado de comparación.

Cuando el segundo valor de cómputo de enlace ascendente de m bits es el diferente del tercer valor de cómputo de enlace ascendente de m bits, y/o el segundo valor de cómputo de enlace descendente de m bits es también diferente del tercer valor de cómputo de enlace descendente de m bits, esto indica que la primera información de cómputo de la estación base secundaria es diferente de la tercera información de cómputo mantenida por el propio terminal, y también indica que una cantidad de datos enviados o recibidos y correspondientes a la identidad DRB es la misma en la estación base primaria y el terminal. Por lo tanto, ningún intruso ha insertado un paquete de datos entre la estación base primaria y el terminal. En este caso, la información notificada a la estación base primaria es la tercera información de cómputo mantenida por el propio terminal, concretamente la segunda información de resultado de comparación.

Etapa 303: El terminal envía la primera información de resultado de comparación, o la segunda información de identidad y la segunda información de resultado de comparación a la estación base primaria, de modo que la estación base primaria determina información de resultado de comprobación según la primera información de resultado de comparación o la segunda información de resultado de comparación. La segunda información de identidad es la identidad DRB, la primera información de resultado de comparación es información nula, y la segunda información de resultado de comparación es la tercera información de cómputo mantenida por el propio terminal.

Específicamente, cuando el segundo valor de cómputo de enlace ascendente de m bits es el mismo que el tercer valor de cómputo de enlace ascendente de m bits, y el segundo valor de cómputo de enlace descendente de m bits es también el mismo que el tercer valor de cómputo de enlace descendente de m bits, la estación base primaria recibe la identidad DRB e información nula enviadas por el terminal.

Cuando el segundo valor de cómputo de enlace ascendente de m bits es diferente del tercer valor de cómputo de enlace ascendente de m bits, y/o el segundo valor de cómputo de enlace descendente de m bits es también diferente del tercer valor de cómputo de enlace descendente de m bits, la estación base primaria recibe la identidad DRB enviada por el terminal y la tercera información de cómputo mantenida por el propio terminal.

La FIG. 4 es un diagrama de interacción de información de un procedimiento de comprobación según la forma de realización 4 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente las siguientes etapas:

Etapa 401: Una estación base secundaria envía primera información de identidad y primera información de cómputo a una estación base primaria. Esta etapa es idéntica a la etapa 201, y no se describe de nuevo en detalle en el presente documento.

Etapa 402: La estación base primaria consulta, según la primera información de identidad, segunda información de identidad correspondiente a la primera información de identidad, y extrae segunda información de cómputo a partir de la primera información de cómputo. Esta etapa incluye contenido de la etapa 202 y de la etapa 203, y no se describe de nuevo en detalle en el presente documento.

Etapa 403: La estación base primaria envía la segunda información de identidad y segunda información de cómputo a un terminal. Esta etapa es idéntica a la etapa 204, y no se describe de nuevo en detalle en el presente documento.

Etapa 404: El terminal compara, según la segunda información de identidad, la segunda información de cómputo con tercera información de cómputo mantenida por el propio terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación. Esta etapa es idéntica a la etapa 302, y no se describe de nuevo en detalle en el presente documento.

Etapa 405: El terminal envía la primera información de resultado de comparación, o la segunda información de identidad y segunda información de resultado de comparación, a la estación base primaria. Esta etapa es idéntica a la etapa 303, y no se describe de nuevo en detalle en el presente documento.

Etapa 406: La estación base primaria determina información de resultado de comprobación según la primera información de resultado de comparación recibida, o la segunda información de identidad y la segunda información de resultado de comparación recibidas. Esta etapa es idéntica a la etapa 206, y no se describe de nuevo en detalle en el presente documento.

La FIG. 5 es un diagrama de interacción de información de un procedimiento de comprobación según la forma de realización 5 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente las siguientes etapas:

Etapa 501: Una estación base primaria envía información de solicitud de transmisión de cómputo a una estación base secundaria, de modo que la estación base secundaria determina primera información de cómputo según la información de solicitud de transmisión de cómputo.
Específicamente, si la información de solicitud de transmisión de cómputo incluye solamente información de identidad de un terminal, la estación base secundaria determina, según una identidad recibida del terminal, primera información de cómputo de cada DRB transportada por el terminal para su notificación a la estación base primaria; o si la información de solicitud de transmisión de cómputo incluye información de identidad e información de identidad E-RAB de un terminal, concretamente primera información de identidad, la estación base secundaria determina, según la primera información de identidad recibida, la primera información de cómputo correspondiente a la primera información de identidad. La primera información de cómputo incluye un primer valor de cómputo de enlace ascendente y un primer valor de cómputo de enlace descendente de la identidad E-RAB del terminal, o n primeros bits de un primer valor de cómputo de enlace ascendente y n primeros bits de un primer valor de cómputo de enlace descendente de la identidad de E-RAB del terminal, donde n es un valor numérico definido por el usuario.
Las etapas 502 a 507 son idénticas a la etapas 401 a 406, y no se describen de nuevo en el presente documento.

La FIG. 6 es un diagrama de interacción de información de un procedimiento de comprobación según la forma de realización 6 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente las siguientes etapas:

Las etapas 601 a 606 son idénticas a la etapas 401 a 406, y no se describen de nuevo en el presente documento.
Etapa 607: La estación base primaria envía la primera información de resultado de comparación, o la primera información de identidad y segunda información de resultado de comparación a la estación base secundaria. La primera información de identidad es una identidad y una identidad E-RAB del terminal, la primera información de resultado de comparación es información nula, y la segunda información de resultado de comparación es tercera información de cómputo mantenida por el propio terminal
Etapa 608: La estación base secundaria determina información de resultado de comprobación según la primera información de resultado de comparación o la segunda información de resultado de comparación recibidas.

Específicamente, cuando se recibe la primera información de resultado de comparación, se determina que la información de resultado de comprobación indica que la primera información de cómputo es coherente con la tercera información de cómputo; cuando se recibe la segunda información de resultado de comparación, se determina que la información de resultado de comprobación indica que la primera información de cómputo no es coherente con la tercera información de cómputo.

La forma de realización 5 y la forma de realización 6 anteriores de la presente invención proporcionan dos procedimientos de comprobación diferentes. Además, otra forma de realización a modo de ejemplo incluye las etapas 501 a 507 de la forma de realización 5 de la presente invención y las etapas 607 y 608 de la forma de realización 6 de la presente invención. El contenido específico de cada etapa ya está descrito en detalle en la forma de realización 5 o la forma de realización 6 de la presente invención, y no se repite de nuevo.

Por lo tanto, en los procedimientos de comprobación anteriores proporcionados por la formas de realización 2 a 6 de la presente invención, una estación base primaria recibe primera información de identidad y primera información de cómputo desde una estación base secundaria, y convierte la primera información de identidad en segunda información de identidad y, por otro lado, extrae segunda información de cómputo a partir de la primera información de cómputo y envía la segunda información de cómputo a un terminal, de manera que el terminal realiza una comparación con tercera información de cómputo mantenida por el propio terminal y notifica primera información de comparación o segunda información de comparación a la estación base primaria; la estación base primaria determina un resultado de comprobación, implementándose así un proceso de comprobación en una arquitectura de red en la que una estación base primaria está desvinculada de una estación base secundaria.

La FIG. 7 es un diagrama de flujo de un procedimiento de comprobación según la forma de realización 7 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente las siguientes etapas:

Etapa 701: Una estación base primaria envía primera información de identidad, o primera información de identidad y primera información de cómputo a un terminal, de modo que el terminal consulta, según la primera información de identidad, segunda información de cómputo mantenida por el propio terminal, o compara, según la primera información de identidad, la primera información de cómputo con segunda información de

cómputo mantenida por el propio terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación. Según la primera información de identidad, el terminal realiza una primera comparación entre un primer valor de cómputo de enlace ascendente y un segundo valor de cómputo de enlace ascendente mantenido por el propio terminal y correspondiente a la primera información de identidad, y/o realiza una segunda comparación entre un primer valor de cómputo de enlace descendente y un segundo valor de cómputo de enlace descendente mantenido por el propio terminal y correspondiente a la primera información de identidad; cuando un resultado de comparación de la primera comparación es el mismo, y un resultado de comparación de la segunda comparación es el mismo, obtiene la primera información de resultado de comparación; o cuando un resultado de comparación de la primera comparación es diferente y/o un resultado de comparación de la segunda comparación es diferente, obtiene la segunda información de resultado de comparación; la primera información de resultado de comparación es información nula, la segunda información de resultado de comparación es la segunda información de cómputo mantenida por el propio terminal, y la segunda información de cómputo mantenida por el propio terminal incluye el segundo valor de cómputo de enlace ascendente y el segundo valor de cómputo de enlace descendente.

Específicamente, cuando la estación base primaria envía la primera información de identidad al terminal, el terminal consulta, según la primera información de identidad recibida, segunda información de cómputo mantenida por el propio terminal y correspondiente a la primera información de identidad, y usa la segunda información de cómputo como información para su notificación a la estación base primaria.

Cuando la estación base primaria envía la primera información de identidad y primera información de cómputo al terminal, la primera información de identidad es una identidad DRB del terminal. La primera información de cómputo incluye m bits del primer valor de cómputo de enlace ascendente y enlace descendente y m bits del primer valor de cómputo de enlace descendente, donde m es un valor definido por el usuario. Además, la primera información de cómputo es un valor aleatorio decidido por la estación base primaria o un valor fijo preestablecido por un sistema. Por ejemplo, el primer valor de cómputo de enlace ascendente contiene m 0_S, y el primer valor de cómputo de enlace descendente también contiene m 0_S. La posibilidad de que el valor aleatorio sea igual a la segunda información de cómputo mantenida por el propio terminal es muy pequeña. Un objetivo del procedimiento de comprobación es que la estación base primaria necesite obtener la segunda información de cómputo mantenida por el propio terminal y envíe la segunda información de cómputo a una estación base secundaria, de modo que la estación base secundaria realice una comparación.

Si el primer valor de cómputo de enlace ascendente y el primer valor de cómputo de enlace descendente están formados por m bits, según la identidad DRB de la primera información de identidad, el terminal consulta la segunda información de cómputo mantenida por el propio terminal, extrae por separado m primeros bits del segundo valor de cómputo de enlace ascendente y m primeros bits del segundo valor de cómputo de enlace descendente de la segunda información de cómputo, después realiza una primera comparación entre el primer valor de cómputo de enlace ascendente de m bits y el segundo valor de cómputo de enlace ascendente de m bits, y, por otro lado, realiza una segunda comparación entre el primer valor de cómputo de enlace descendente de m bits y el segundo valor de cómputo de enlace descendente de m bits.

Cuando el primer valor de cómputo de enlace ascendente de m bits es el mismo que el segundo valor de cómputo de enlace ascendente de m bits, y el primer valor de cómputo de enlace descendente de m bits es también el mismo que el segundo valor de cómputo de enlace descendente de m bits, la información notificada a la estación base primaria es información nula, concretamente la primera información de resultado de comparación. Sin embargo, la posibilidad de que se produzca este caso es muy pequeña.

Cuando el primer valor de cómputo de enlace ascendente de m bits es diferente del segundo valor de cómputo de enlace ascendente de m bits, y/o el primer valor de cómputo de enlace descendente de m bits es diferente del segundo valor de cómputo de enlace descendente de m bits, la información notificada a la estación base primaria es la segunda información de cómputo mantenida por el propio terminal, concretamente la segunda información de resultado de comparación.

Etapa 702: La estación base primaria recibe la primera información de identidad y segunda información de cómputo enviada por el terminal, o la primera información de resultado de comparación enviada por el terminal, o la primera información de identidad y la segunda información de resultado de comparación enviadas por el terminal. La primera información de resultado de comparación es información nula, y la segunda información de resultado de comparación es la segunda información de cómputo mantenida por el propio terminal.

Etapa 703: La estación base primaria consulta, según la primera información de identidad, segunda información de identidad correspondiente a la primera información de identidad. La segunda información de identidad es una identidad del terminal y una identidad E-RAB del terminal.

Específicamente, una conexión entre la estación base primaria y el terminal puede tener múltiples DRB, y una conexión entre la estación base primaria y una red central puede tener múltiples E-RAB. En un mismo terminal, cada DRB corresponde a una E-RAB única.

Etapa 704: La estación base primaria envía la segunda información de identidad y la segunda información de cómputo, o la primera información de resultado de comparación, o la segunda información de identidad y segunda información de resultado de comparación, a una estación base secundaria, de modo que la estación base secundaria obtiene la segunda información de cómputo mantenida por el propio terminal y compara la segunda información de cómputo con tercera información de cómputo mantenida por la propia estación base secundaria, determinándose así información de resultado de comprobación final. La segunda información de identidad es la identidad del terminal y la identidad E-RAB del terminal, y la tercera información de cómputo mantenida por la propia estación base secundaria incluye un tercer valor de cómputo de enlace ascendente y un tercer valor de cómputo de enlace descendente.

La FIG. 8 es un diagrama de flujo de un procedimiento de comprobación según la forma de realización 8 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente las siguientes etapas:

Etapa 801: Recibir primera información de identidad y primera información de cómputo enviadas por una estación de base primaria, donde la primera información de identidad es una identidad DRB de un terminal.
Etapa 802: Comparar, según la primera información de identidad, la primera información de cómputo con segunda información de cómputo mantenida de manera local para obtener primera información de resultado de comparación o segunda información de resultado de comparación.

Según la primera información de identidad, el terminal realiza una primera comparación entre un primer valor de cómputo de enlace ascendente y un segundo valor de cómputo de enlace ascendente mantenido por el propio terminal y correspondiente a la primera información de identidad, y, por otro lado, realiza una segunda comparación entre un primer valor de cómputo de enlace descendente y un segundo valor de cómputo de enlace descendente mantenido por el propio terminal y correspondiente a la primera información de identidad; cuando un resultado de comparación de la primera comparación es el mismo, y un resultado de comparación de la segunda comparación es el mismo, obtiene la primera información de resultado de comparación; cuando un resultado de comparación de la primera comparación es diferente y/o un resultado de comparación de la segunda comparación es diferente, obtiene la segunda información de resultado de comparación; la primera información de resultado de comparación es información nula, la segunda información de resultado de comparación es la segunda información de cómputo mantenida por el propio terminal, y la segunda información de cómputo mantenida por el propio terminal incluye el segundo valor de cómputo de enlace ascendente y el segundo valor de cómputo de enlace descendente.

Específicamente, si el primer valor de cómputo de enlace ascendente y el primer valor de cómputo de enlace descendente están formados por m bits, el terminal consulta la segunda información de cómputo mantenida por el propio terminal según la identidad DRB de la primera información de identidad, extrae por separado m primeros bits del segundo valor de cómputo de enlace ascendente y m primeros bits del segundo valor de cómputo de enlace descendente a partir de la segunda información de cómputo, después realiza una primera comparación entre el primer valor de cómputo de enlace ascendente de m bits y el segundo valor de cómputo de enlace ascendente de m bits, y, por otro lado, realiza una segunda comparación entre el primer valor de cómputo de enlace descendente de m bits y el segundo valor de cómputo de enlace descendente de m bits.

Cuando el primer valor de cómputo de enlace ascendente de m bits es el mismo que el segundo valor de cómputo de enlace ascendente de m bits, y el primer valor de cómputo de enlace descendente de m bits es también el mismo que el segundo valor de cómputo de enlace descendente de m bits, la información notificada a la estación base primaria es información nula, concretamente la primera información de resultado de comparación. Sin embargo, la posibilidad de que se produzca este caso es muy pequeña.

Cuando el primer valor de cómputo de enlace ascendente de m bits es diferente del segundo valor de cómputo de enlace ascendente de m bits, y/o el primer valor de cómputo de enlace descendente de m bits es también diferente del segundo valor de cómputo de enlace descendente de m bits, la información notificada a la estación base primaria es la segunda información de cómputo mantenida por el propio terminal, concretamente la segunda información de resultado de comparación.

Etapa 803: El terminal envía la primera información de resultado de comparación, o la primera información de identidad y segunda información de resultado de comparación a la estación base primaria, de modo que la estación base primaria reenvía la primera información de resultado de comparación o segunda información de resultado de comparación a una estación base secundaria, de modo que la estación base secundaria determina, según la primera información de resultado de comparación o segunda información de resultado de comparación, información de resultado de comprobación y obtiene la segunda información de cómputo mantenida por el propio terminal.

La FIG. 9 es un diagrama de interacción de información de un procedimiento de comprobación según la forma de realización 9 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente las siguientes etapas:

Etapa 901: Una estación base primaria envía primera información de identidad, o primera información de identidad y primera información de cómputo, a un terminal. Esta etapa es idéntica a la etapa 701, y no se describe de nuevo en detalle en el presente documento.

Etapa 902: El terminal consulta, según la primera información de identidad, segunda información de cómputo mantenida por el propio terminal, o compara, según la primera información de identidad, la primera información de cómputo con segunda información de cómputo mantenida por el propio terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación. Esta etapa es idéntica a la etapa 802, y no se describe de nuevo en detalle en el presente documento.

Etapa 903: El terminal envía la primera información de identidad y segunda información de cómputo, o la primera información de resultado de comparación o la primera información de identidad y segunda información de resultado de comparación, a la estación base primaria. Esta etapa es idéntica a la etapa 803, y no se describe de nuevo en detalle en el presente documento.

Etapa 904: La estación base primaria consulta, según la primera información de identidad, segunda información de identidad correspondiente a la primera información de identidad. Esta etapa es idéntica a la etapa 703, y no se describe de nuevo en detalle en el presente documento.

Etapa 905: La estación base primaria envía la segunda información de identidad y segunda información de cómputo, o la primera información de resultado de comparación, o la segunda información de identidad y segunda información de resultado de comparación, a una estación base secundaria. La primera información de resultado de comparación es información nula, y la segunda información de resultado de comparación es la segunda información de cómputo mantenida por el propio terminal. Esta etapa es idéntica a la etapa 704, y no se describe de nuevo en detalle en el presente documento.

Etapa 906: La estación base secundaria obtiene, según la segunda información de cómputo o segunda información de resultado de comparación, la segunda información de cómputo mantenida por el propio terminal, y compara la segunda información de cómputo con tercera información de cómputo mantenida por la propia estación base secundaria, determinándose así información de resultado de comprobación.

Por lo tanto, en los procedimientos de comprobación anteriores proporcionados por las formas de realización 7 a 9 de la presente invención, una estación base primaria fija previamente primera información de cómputo a un valor aleatorio y envía primera información de identidad y la primera información de cómputo prefijada a un terminal, de modo que el terminal realiza una comparación con segunda información de cómputo mantenida por el propio terminal y notifica primera información de comparación o segunda información de comparación a la estación base primaria; después, la estación base primaria reenvía la primera información de comparación o segunda información de comparación a una estación base secundaria, de modo que la estación base secundaria determina un resultado de comprobación y obtiene la segunda información de cómputo mantenida por el propio terminal, implementándose así un proceso de comprobación en una arquitectura de red en la que una estación base primaria está desvinculada de una estación base secundaria.

La FIG. 10 es un diagrama de flujo de un procedimiento de reconfiguración según la forma de realización 10 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente las siguientes etapas:

Etapa 101: Una estación base primaria determina, según la capacidad de seguridad de un terminal, un algoritmo de cifrado usado por una estación base secundaria y el terminal. Existen múltiples algoritmos de cifrado, por ejemplo eea0, eea1 y eea2. La estación base primaria puede determinar el algoritmo de cifrado según una condición real del terminal, donde el algoritmo de cifrado no solo puede aplicarse al terminal, sino que también puede aplicarse a la estación base secundaria.

Etapa 102: La estación base primaria envía a la estación base secundaria información de actualización de parámetro de seguridad que transporta el algoritmo de cifrado, de modo que la estación base secundaria se comunica con el terminal usando el algoritmo de cifrado de la información de actualización de parámetro de seguridad. El algoritmo de cifrado es determinado por la estación base primaria. Para garantizar una comunicación segura entre el terminal y la estación base secundaria, la estación base primaria notifica el algoritmo de cifrado a la estación base secundaria.

Etapa 103: La estación base primaria envía al terminal información de reconfiguración que transporta el algoritmo de cifrado, de modo que el terminal actualiza una clave del propio terminal según el algoritmo de cifrado de la información de reconfiguración y se comunica con la estación base secundaria usando el algoritmo de cifrado y la clave actualizada. El algoritmo de cifrado es determinado por la estación base primaria. Para garantizar una comunicación segura entre el terminal y la estación base secundaria, la estación base primaria no solo notifica el algoritmo de cifrado a la estación base secundaria, sino que también notifica el algoritmo de cifrado al terminal, de modo que el terminal genera una clave de nuevo usando el algoritmo de cifrado y realiza una comunicación segura con la estación base secundaria usando el algoritmo de cifrado y la clave.

Etapa 104: La estación base primaria recibe información de reconfiguración completada enviada por el terminal. Tras completar la actualización de la clave, el terminal puede notificar información de actualización completada a la estación base primaria, de modo que la estación base primaria sabe que el terminal ha completado una reconfiguración y puede realizar una comunicación segura con la estación base secundaria.

Primero se ejecuta la etapa 102 y después la etapa 103; o primero se ejecuta la etapa 103 y después la 102; o las etapas 102 y 103 se ejecutan simultáneamente; o la etapa 102 se ejecuta tras llevarse a cabo las etapas 103 y 104. Un proceso de implementación específico de las etapas no se describirá en mayor detalle.

La FIG. 11 es un diagrama de flujo de un procedimiento de reconfiguración según la forma de realización 11 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente las siguientes etapas:

Etapa 111: Un terminal recibe información de reconfiguración enviada por una estación base primaria y que transporta un algoritmo de cifrado. El algoritmo de cifrado es determinado por la estación base primaria. Para garantizar una comunicación segura entre el terminal y una estación base secundaria, la estación base primaria no solo notifica el algoritmo de cifrado a la estación base secundaria, sino que también notifica el algoritmo de cifrado al terminal, de modo que el terminal genera una clave de nuevo usando el algoritmo de cifrado y realiza una comunicación segura con la estación base secundaria usando la clave.

Etapa 112: El terminal actualiza la clave del terminal según el algoritmo de cifrado de la información de reconfiguración y usa el algoritmo de cifrado y la clave actualizada para comunicarse con una estación base secundaria.

Específicamente, el terminal genera una clave de nuevo usando el algoritmo de cifrado de la información de reconfiguración y realiza una comunicación segura con la estación base secundaria usando la clave.

Etapa 113: El terminal envía información de reconfiguración completada a la estación base primaria.

Específicamente, tras completar una actualización de la clave, el terminal notifica información de actualización completada a la estación base primaria, de modo que la estación base primaria sabe que el terminal ha completado una reconfiguración y puede realizar una comunicación segura con la estación base secundaria.

La FIG. 12 es un diagrama de interacción de información de un procedimiento de reconfiguración según la forma de realización 12 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente las siguientes etapas:

Etapa 121: Una estación base primaria determina, según la capacidad de seguridad de un terminal, un algoritmo de cifrado usado por una estación base secundaria y el terminal. Esta etapa es idéntica a la etapa 101, y no se describe de nuevo en detalle en el presente documento.

Etapa 122: La estación base primaria envía a la estación base secundaria información de actualización de parámetro de seguridad que transporta el algoritmo de cifrado.

Etapa 123: La estación base secundaria se comunica con el terminal usando el algoritmo de cifrado de la información de actualización de parámetro de seguridad recibida, donde el algoritmo de cifrado es determinado por la estación base primaria.

Etapa 124: La estación base primaria envía al terminal información de reconfiguración que transporta el algoritmo de cifrado.

Etapa 125: Tras recibir la información de reconfiguración que transporta el algoritmo de cifrado, el terminal actualiza una clave del terminal según el algoritmo de cifrado de la información de reconfiguración y se comunica con la estación base secundaria usando el algoritmo de cifrado y la clave actualizada. El algoritmo de cifrado es determinado por la estación base primaria.

Etapa 126: El terminal envía información de reconfiguración completada a la estación base primaria.

La FIG. 13 es un diagrama de interacción de información de un procedimiento de reconfiguración según la forma de realización 13 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente las siguientes etapas:

Etapa 131: Una estación base secundaria envía información de solicitud de actualización de parámetro de seguridad a una estación base primaria. La información de solicitud de actualización de parámetro de seguridad incluye una causa de solicitud de actualización de parámetro de seguridad. La causa de solicitud de actualización de parámetro de seguridad es que se supere un valor de cómputo mantenido por la estación base secundaria o que un valor de cómputo mantenido por la estación base secundaria sea incorrecto. Cuando el valor de cómputo mantenido por la estación base secundaria es diferente de un valor de cómputo mantenido por el propio terminal y correspondiente al valor de cómputo mantenido por la estación base secundaria, se considera que el valor de cómputo mantenido por la estación base secundaria es incorrecto.

Las etapas 132 a 137 son idénticas a la etapas 121 a 126, y no se describen de nuevo en el presente documento.

Por lo tanto, en los procedimientos de reconfiguración anteriores proporcionados por las formas de realización 10 a 13 de la presente invención, una estación base primaria determina un algoritmo de cifrado usado por una estación base secundaria y un terminal, y envía el algoritmo de cifrado a la estación base secundaria y al terminal, respectivamente; el terminal envía información de reconfiguración completada a la estación base primaria tras actualizar una clave usando el algoritmo de cifrado, de modo que la estación base secundaria realiza una comunicación segura con el terminal usando el algoritmo de cifrado y la clave actualizada, implementándose así un proceso de reconfiguración en una arquitectura de red en la que una estación base primaria está desvinculada de una estación base secundaria.

La FIG. 14 es un diagrama de flujo de un procedimiento de reconfiguración según la forma de realización 14 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente las siguientes etapas:

Etapa 141: Una estación base primaria recibe información de solicitud de actualización de parámetro de seguridad enviada por una estación base secundaria y que transporta un algoritmo de cifrado. El algoritmo de cifrado es determinado por la estación base secundaria. En la actualidad existen múltiples algoritmos de cifrado, por ejemplo eea0, eea1 y eea2. La estación base secundaria puede determinar un algoritmo de cifrado según una condición real de un terminal, donde el algoritmo de cifrado no solo puede aplicarse a la estación base secundaria, sino que también puede aplicarse al terminal. Además, la información de solicitud de actualización de parámetro de seguridad puede incluir además una causa de solicitud de actualización de parámetro de seguridad. La causa de solicitud de actualización de parámetro de seguridad es que se supere un valor de cómputo mantenido por la estación base secundaria o que un valor de cómputo mantenido por la estación base secundaria sea incorrecto. Cuando el valor de cómputo mantenido por la estación base secundaria es diferente de un valor de cómputo mantenido por el propio terminal y correspondiente al valor de cómputo, se considera que el valor de cómputo mantenido por la estación base secundaria es incorrecto. La información de solicitud de actualización de parámetro de seguridad incluye el algoritmo de cifrado, o el algoritmo de cifrado y la información de causa de solicitud de actualización de parámetro de seguridad. La información de causa de solicitud de actualización de parámetro de seguridad incluye que se supere un valor de cómputo mantenido por la estación base secundaria o que un resultado de comprobación sea incorrecto.
Etapa 142: La estación base primaria añade a la información de reconfiguración el algoritmo de cifrado de la información de solicitud de actualización de parámetro de seguridad recibida.
Etapa 143: La estación base primaria envía a un terminal la información de reconfiguración que transporta el algoritmo de cifrado, de modo que el terminal actualiza una clave del propio terminal según el algoritmo de cifrado de la información de reconfiguración y se comunica con la estación base secundaria usando el algoritmo de cifrado y la clave actualizada.
Etapa 144: La estación base primaria recibe información de reconfiguración completada enviada por el terminal.

La FIG. 15 es un diagrama de flujo de un procedimiento de reconfiguración según la forma de realización 15 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente las siguientes etapas:

Etapa 151: Un terminal recibe información de reconfiguración reenviada por una estación base primaria y que transporta un algoritmo de cifrado.
Etapa 152: El terminal actualiza una clave del terminal según el algoritmo de cifrado de la información de reconfiguración y se comunica con una estación base secundaria usando el algoritmo de cifrado y la clave actualizada.
Etapa 153: El terminal envía información de reconfiguración completada a la estación base primaria.

La FIG. 16 es un diagrama de interacción de información de un procedimiento de reconfiguración según la forma de realización 16 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente las siguientes etapas:

Etapa 161: Una estación base secundaria determina un algoritmo de cifrado usado por la estación base secundaria y un terminal.
Etapa 162: La estación base secundaria envía información de solicitud de actualización de parámetro de seguridad que transporta el algoritmo de cifrado, donde la información de solicitud de actualización de parámetro de seguridad transporta el algoritmo de cifrado, y puede incluir además información de causa de solicitud de actualización de parámetro de seguridad. La causa de solicitud de actualización de parámetro de seguridad es que se supere un valor de cómputo mantenido por la estación base secundaria o que un valor de cómputo mantenido por la estación base secundaria sea incorrecto. Cuando el valor de cómputo mantenido por la estación base secundaria es diferente de un valor de cómputo mantenido por el propio terminal y correspondiente al valor de cómputo, se considera que el valor de cómputo mantenido por la estación base secundaria es incorrecto.
Etapa 163: Una estación base primaria añade el algoritmo de cifrado a la información de reconfiguración.

Etapa 164: Enviar al terminal la información de reconfiguración que transporta el algoritmo de cifrado. El algoritmo de cifrado es determinado por la estación base secundaria.
Etapa 165: Tras recibir la información de reconfiguración que transporta el algoritmo de cifrado, el terminal actualiza una clave del terminal según el algoritmo de cifrado de la información de reconfiguración y se comunica con la estación base secundaria usando el algoritmo de cifrado y la clave actualizada.
Etapa 166: El terminal envía información de reconfiguración completada a la estación base primaria.

La FIG. 17 es un diagrama de interacción de información de un procedimiento de reconfiguración según la forma de realización 17 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente las siguientes etapas:

Etapa 171: Una estación base primaria envía información de capacidad de seguridad de un terminal a una estación base secundaria.
Etapa 172: La estación base secundaria determina, según la información de capacidad de seguridad recibida del terminal, un algoritmo de cifrado usado por la propia estación base secundaria para establecer comunicación con el terminal.
Las etapas 173 a 177 son idénticas a la etapas 162 a 166, y no se describen de nuevo en el presente documento.

La FIG. 18 es un diagrama de interacción de información de un procedimiento de reconfiguración según la forma de realización 18 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente las siguientes etapas:

Etapa 181: Una estación base secundaria envía información de causa de solicitud de actualización de parámetro de seguridad a una estación base primaria. La información de causa de solicitud de actualización de parámetro de seguridad es que se supere un valor de cómputo mantenido por la estación base secundaria o que un valor de cómputo mantenido por la estación base secundaria sea incorrecto. Cuando el valor de cómputo mantenido por la estación base secundaria es diferente de un valor de cómputo mantenido por el propio terminal y correspondiente al valor de cómputo, se considera que el valor de cómputo mantenido por la estación base secundaria es incorrecto.
Las etapas 182 a 188 son idénticas a la etapas 171 a 177, y no se describen de nuevo en el presente documento. En esta forma de realización, la información de solicitud de actualización de parámetro de seguridad incluye solamente un algoritmo de cifrado.

Por lo tanto, en los procedimientos de reconfiguración anteriores proporcionados por las formas de realización 14 a 18 de la presente invención, una estación base secundaria determina un algoritmo de cifrado usado por la propia estación base secundaria y un terminal, y envía el algoritmo de cifrado a una estación base primaria; después, la estación base primaria envía el algoritmo de cifrado al terminal; el terminal envía información de reconfiguración completada a la estación base primaria tras actualizar una clave usando el algoritmo de cifrado, de modo que la estación base secundaria realiza una comunicación segura con el terminal usando el algoritmo de cifrado y la clave actualizada, implementándose así un proceso de reconfiguración en una arquitectura de red en la que una estación base primaria está desvinculada de una estación base secundaria.

La FIG. 19 es un diagrama esquemático de un aparato de comprobación según la forma de realización 19 de la presente invención. Este aparato está configurado para ejecutar el procedimiento de comprobación proporcionado por cualquiera de las formas de realización 2, 4, 5 y 6 de la presente invención. Como se muestra en la figura, el aparato de comprobación proporcionado por la forma de realización de la presente invención incluye específicamente: una primera unidad de recepción 191, una unidad de consulta 192, una unidad de extracción 193, una primera unidad de envío 194, una segunda unidad de recepción 195 y una unidad de determinación 196.

La primera unidad de recepción 191 está configurada para recibir primera información de identidad y primera información de cómputo enviada por una estación base secundaria, y transmitir la primera información de identidad a la unidad de consulta 192, y transmitir la primera información de cómputo a la unidad de extracción 193. La primera información de identidad incluye una identidad de un terminal y una identidad de portadora de acceso radioeléctrico, E-RAB, del terminal; la primera información de cómputo incluye un primer valor de cómputo de enlace ascendente y un primer valor de cómputo de enlace descendente de la identidad E-RAB del terminal, o n primeros bits de un primer valor de cómputo de enlace ascendente y n primeros bits de un primer valor de cómputo de enlace descendente de la identidad de E-RAB del terminal.

La unidad de consulta 192 está configurada para recibir la primera información de identidad desde la primera unidad de recepción, consultar, según la primera información de identidad, segunda información de identidad correspondiente a la primera información de identidad, y transmitir la segunda información de identidad a la primera unidad de envío 194.

Específicamente, una identidad de portadora radioeléctrica de datos, DRB, del terminal y correspondiente a la identidad E-RAB se consulta según la identidad del terminal y la identidad de portadora de acceso radioeléctrico, E-RAB, del terminal, donde la identidad DRB del terminal es la segunda información de identidad.

La unidad de extracción 193 está configurada para recibir la primera información de cómputo desde la primera unidad de recepción, extraer segunda información de cómputo a partir de la primera información de cómputo y transmitir la segunda información de cómputo a la primera unidad de envío 194.

Específicamente, una pluralidad de primeros bits se extraen del primer valor de cómputo de enlace ascendente para usarse como segundo valor de cómputo de enlace ascendente, y una pluralidad de primeros bits se extraen del primer valor de cómputo de enlace descendente para usarse como segundo valor de cómputo de enlace descendente, donde el segundo valor de cómputo de enlace ascendente y el segundo valor de cómputo de enlace descendente constituyen la segunda información de cómputo. Además, m primeros bits también pueden extraerse de n primeros bits del primer valor de cómputo de enlace ascendente para usarse como segundo valor de cómputo de enlace ascendente, y, simultáneamente, m primeros bits se extraen de n primeros bits del primer valor de cómputo de enlace descendente para usarse como segundo valor de cómputo de enlace descendente, donde m es inferior o igual a n. En este caso, el segundo valor de cómputo de enlace ascendente y el segundo valor de cómputo de enlace descendente constituyen la segunda información de cómputo.

La primera unidad de envío 194 está configurada para recibir la segunda información de identidad desde la unidad de consulta, recibir la segunda información de cómputo desde la unidad de extracción, y enviar la segunda información de identidad y la segunda información de cómputo al terminal, de modo que el terminal compara, según la segunda información de identidad, la segunda información de cómputo con tercera información de cómputo mantenida por el propio terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación.

Específicamente, según la segunda información de identidad, el terminal realiza una primera comparación entre el segundo valor de cómputo de enlace ascendente y un tercer valor de cómputo de enlace ascendente mantenido por el propio terminal y correspondiente a la segunda información de identidad, y/o realiza una segunda comparación entre el segundo valor de cómputo de enlace descendente y un tercer valor de cómputo de enlace descendente mantenido por el propio terminal y correspondiente a la segunda información de identidad; cuando un resultado de comparación de la primera comparación es el mismo, y un resultado de comparación de la segunda comparación es el mismo, obtiene la primera información de resultado de comparación; cuando un resultado de comparación de la primera comparación es diferente y/o un resultado de comparación de la segunda comparación es diferente, obtiene la segunda información de resultado de comparación; la primera información de resultado de comparación es información nula, la segunda información de resultado de comparación es la tercera información de cómputo mantenida por el propio terminal, y la tercera información de cómputo mantenida por el propio terminal incluye el tercer valor de cómputo de enlace ascendente y el tercer valor de cómputo de enlace descendente.

La segunda unidad de recepción 195 está configurada para recibir la primera información de resultado de comparación enviada por el terminal, o la segunda información de identidad y segunda información de resultado de comparación enviadas por el terminal, y transmitir la primera información de resultado de comparación, o la segunda información de identidad y segunda información de resultado de comparación a la unidad de determinación 196.

La unidad de determinación 196 está configurada para recibir la primera información de resultado de comparación, o la segunda información de identidad y segunda información de resultado de comparación desde la segunda unidad de recepción 195, y determinar información de resultado de comprobación según la primera información de resultado de comparación recibida, o la segunda información de identidad recibida y segunda información de resultado de comparación.

Específicamente, cuando se recibe la primera información de resultado de comparación, se determina que la información de resultado de comprobación indica que la primera información de cómputo es coherente con la tercera información de cómputo; cuando se recibe la segunda información de resultado de comparación, se determina que la información de resultado de comprobación indica que la primera información de cómputo no es coherente con la tercera información de cómputo.

En una forma de realización a modo de ejemplo, el aparato de comprobación proporcionado por la forma de realización de la presente invención incluye además una segunda unidad de envío 197.

La segunda unidad de envío 197 está configurada para enviar información de solicitud de transmisión de cómputo, de modo que la estación base secundaria determina la primera información de cómputo según la información de solicitud de transmisión de cómputo. La información de solicitud de transmisión de cómputo incluye la identidad del terminal, o la identidad del terminal y la identidad E-RAB del terminal.

En otra forma de realización a modo de ejemplo, preferentemente el aparato de comprobación proporcionado por la forma de realización de la presente invención incluye además una tercera unidad de envío 198.

La tercera unidad de envío 198 está configurada para recibir desde la segunda unidad de recepción 195 la primera información de resultado de comparación, o la segunda información de identidad y segunda información de resultado de comparación, obtener la primera información de identidad según la segunda información de identidad, y enviar la primera información de resultado de comparación, o la primera información de identidad y segunda información de resultado de comparación a la estación base secundaria, de manera que la estación base secundaria determina información de resultado de comprobación según la primera información de resultado de comparación o segunda información de resultado de comparación recibidas.

En otra forma de realización adicional a modo de ejemplo, el aparato de comprobación proporcionado por la forma de realización de la presente invención incluye además la segunda unidad de envío 197 y la tercera unidad de envío 198.

La FIG. 20 es un diagrama esquemático de un aparato de comprobación según la forma de realización 20 de la presente invención. Este aparato está configurado para ejecutar el procedimiento de comprobación proporcionado por cualquiera de las formas de realización 3, 4, 5 y 6 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente: una unidad de recepción 201, una unidad de comparación 202 y una unidad de envío 203.

La unidad de recepción 201 está configurada para recibir segunda información de identidad correspondiente a primera información de identidad y segunda información de cómputo extraída de primera información de cómputo enviada por una estación base primaria, y transmitir la segunda información de identidad a la unidad de comparación 202 y la unidad de envío 203, y transmitir la segunda información de cómputo a la unidad de comparación 202. La primera información de cómputo incluye un primer valor de cómputo de enlace ascendente y un primer valor de cómputo de enlace descendente de la identidad E-RAB de un terminal, o un primer valor de cómputo de enlace ascendente y un primer valor de cómputo de enlace descendente de la identidad E-RAB de un terminal.

Específicamente, la identidad DRB del terminal y correspondiente a la identidad E-RAB se consulta según la identidad del terminal y la identidad de portadora de acceso radioeléctrico, E-RAB, del terminal, donde la identidad DRB es la segunda información de identidad; y una pluralidad de primeros bits se extraen del primer valor de cómputo de enlace ascendente para usarse como segundo valor de cómputo de enlace ascendente, y una pluralidad de primeros bits se extraen del primer valor de cómputo de enlace descendente para usarse como segundo valor de cómputo de enlace descendente, donde el segundo valor de cómputo de enlace ascendente y el segundo valor de cómputo de enlace descendente constituyen la segunda información de cómputo.

La unidad de comparación 202 está configurada para recibir la segunda información de identidad y la segunda información de cómputo desde la unidad de recepción 201, y comparar, según la segunda información de identidad, la segunda información de cómputo con tercera información de cómputo mantenida de manera local para obtener primera información de resultado de comparación o segunda información de resultado de comparación, y transmitir la primera información de resultado de comparación o la segunda información de resultado de comparación a la unidad de envío 203.

Específicamente, según la segunda información de identidad, se realiza una primera comparación entre el segundo valor de cómputo de enlace ascendente y un tercer valor de cómputo de enlace ascendente mantenido de manera local y correspondiente a la segunda información de identidad, y/o se realiza una segunda comparación entre el segundo valor de cómputo de enlace descendente y un tercer valor de cómputo de enlace descendente mantenido de manera local y correspondiente a la segunda información de identidad; cuando un resultado de comparación de la primera comparación es el mismo, y un resultado de comparación de la segunda comparación es también el mismo, se obtiene la primera información de resultado de comparación; cuando un resultado de comparación de la primera comparación es diferente y/o un resultado de comparación de la segunda comparación es diferente, se obtiene la segunda información de resultado de comparación; la primera información de resultado de comparación es información nula, la segunda información de resultado de comparación es la tercera información de cómputo mantenida de manera local, y la tercera información de cómputo mantenida de manera local incluye el tercer valor de cómputo de enlace ascendente y el tercer valor de cómputo de enlace descendente.

La unidad de envío 203 está configurada para recibir la segunda información de identidad desde la unidad de recepción 201, recibir la primera información de resultado de comparación o la segunda información de resultado de comparación desde la unidad de comparación 202, y enviar la primera información de resultado de comparación, o la segunda información de identidad y segunda información de resultado de comparación a la estación base primaria, de manera que la estación base primaria determina información de resultado de comprobación según la primera información de resultado de comparación o la segunda información de resultado de comparación.

Específicamente, cuando la estación base primaria recibe la primera información de resultado de comparación, se determina que la información de resultado de comprobación indica que la primera información de cómputo es coherente con la tercera información de cómputo; cuando se recibe la segunda información de resultado de

comparación, se determina que la información de resultado de comprobación indica que la primera información de cómputo no es coherente con la tercera información de cómputo.

Por lo tanto, usando los aparatos de comprobación anteriores proporcionados por la formas de realización 19 y 20 de la presente invención, una estación base primaria recibe primera información de identidad y primera información de cómputo desde una estación base secundaria, y convierte la primera información de identidad en segunda información de identidad y, por otro lado, extrae segunda información de cómputo a partir de la primera información de cómputo y envía la segunda información de cómputo a un terminal, de modo que el terminal realiza una comparación con tercera información de cómputo mantenida por el propio terminal y notifica primera información de comparación o segunda información de comparación a la estación base primaria; la estación base primaria determina un resultado de comprobación, implementándose así un proceso de comprobación en una arquitectura de red en la que una estación base primaria está desvinculada de una estación base secundaria.

La FIG. 21 es un diagrama esquemático de un aparato de comprobación según la forma de realización 20 de la presente invención. Este aparato está configurado para ejecutar el procedimiento de comprobación proporcionado por cualquiera de las formas de realización 7 y 9 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente: una primera unidad de envío 211, una unidad de recepción 212, una unidad de consulta 213 y una segunda unidad de envío 214.

La primera unidad de envío 211 está configurada para enviar primera información de identidad, o primera información de identidad y primera información de cómputo a un terminal, de modo que el terminal consulta, según la primera información de identidad, segunda información de cómputo mantenida por el propio terminal, o compara, según la primera información de identidad, la primera información de cómputo con segunda información de cómputo mantenida por el propio terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación. La primera información de identidad es una identidad DRB del terminal, y la primera información de cómputo es un valor de cómputo prefijado.

Específicamente, según la primera información de identidad, el terminal realiza una primera comparación entre un primer valor de cómputo de enlace ascendente y un segundo valor de cómputo de enlace ascendente mantenido por el propio terminal y correspondiente a la primera información de identidad, y/o realiza una segunda comparación entre un primer valor de cómputo de enlace descendente y un segundo valor de cómputo de enlace descendente mantenido por el propio terminal y correspondiente a la primera información de identidad; cuando un resultado de comparación de la primera comparación es el mismo, y un resultado de comparación de la segunda comparación es el mismo, obtiene la primera información de resultado de comparación; cuando un resultado de comparación de la primera comparación es diferente y/o un resultado de comparación de la segunda comparación es diferente, obtiene la segunda información de resultado de comparación; la primera información de resultado de comparación es información nula, la segunda información de resultado de comparación es la segunda información de cómputo mantenida por el propio terminal, y la segunda información de cómputo mantenida por el propio terminal incluye el segundo valor de cómputo de enlace ascendente y el segundo valor de cómputo de enlace descendente.

La unidad de recepción 212 está configurada para recibir la primera información de identidad y la segunda información de cómputo enviadas por el terminal, o la primera información de resultado de comparación enviada por el terminal, o la primera información de identidad y la segunda información de resultado de comparación enviadas por el terminal, transmitir la primera información de identidad a la unidad de consulta 213, y transmitir la segunda información de cómputo, o la primera información de resultado de comparación, o la segunda información de resultado de comparación a la segunda unidad de envío 214.

La unidad de consulta 213 está configurada para recibir la primera información de identidad desde la unidad de recepción 212, consultar, según la primera información de identidad, segunda información de identidad correspondiente a la primera información de identidad, y transmitir la segunda información de identidad a la segunda unidad de envío 214. La segunda información de identidad es información de identidad del terminal y una identidad E-RAB del terminal.

La segunda unidad de envío 214 está configurada para recibir la segunda información de identidad desde la unidad de consulta 213, y recibir la segunda información de cómputo, o la primera información de resultado de comparación, o la segunda información de resultado de comparación, desde la unidad de recepción 212, y enviar la segunda información de identidad y la segunda información de cómputo, o la primera información de resultado de comparación, o la segunda información de identidad y la segunda información de resultado de comparación, a una estación base secundaria, de modo que la estación base secundaria obtiene la segunda información de cómputo mantenida por el propio terminal y compara la segunda información de cómputo con tercera información de cómputo mantenida por la propia estación base secundaria, determinándose así información de resultado de comprobación.

La FIG. 22 es un diagrama esquemático de un aparato de comprobación según la forma de realización 22 de la presente invención. Este aparato está configurado para ejecutar el procedimiento de comprobación proporcionado por cualquiera de las formas de realización 8 y 9 de la presente invención. Como se muestra en la figura, la forma de

realización de la presente invención incluye específicamente: una unidad de recepción 221, una unidad de consulta o de comparación 222 y una unidad de envío 223.

La unidad de recepción 221 está configurada para recibir primera información de identidad, o primera información de identidad y primera información de cómputo, enviadas por una estación base primaria, y transmitir la primera información de identidad a la unidad de consulta o de comparación 222 y a la unidad de envío 223, y transmitir la primera información de cómputo a la unidad de consulta o de comparación 222. La primera información de identidad es una identidad DRB de un terminal; la primera información de cómputo es un valor de cómputo prefijado; y la primera información de cómputo incluye un primer valor de cómputo de enlace ascendente y un primer valor de cómputo de enlace descendente.

La unidad de consulta o de comparación 222 está configurada para recibir la primera información de identidad y la primera información de cómputo desde la unidad de recepción 221, consultar, según la primera información de identidad, segunda información de cómputo mantenida de manera local, o comparar, según la primera información de identidad, la primera información de cómputo con segunda información de cómputo mantenida de manera local para obtener primera información de resultado de comparación o segunda información de resultado de comparación, y transmitir la segunda información de cómputo, o la primera información de resultado de comparación, o la segunda información de resultado de comparación, a la unidad de envío 223. La primera información de cómputo incluye el primer valor de cómputo de enlace ascendente y el primer valor de cómputo de enlace descendente.

Específicamente, según la primera información de identidad, se realiza una primera comparación entre el primer valor de cómputo de enlace ascendente y un segundo valor de cómputo de enlace ascendente mantenido de manera local y correspondiente a la primera información de identidad, y/o se realiza una segunda comparación entre el primer valor de cómputo de enlace descendente y un segundo valor de cómputo de enlace descendente mantenido por el propio terminal y correspondiente a la primera información de identidad; cuando un resultado de comparación de la primera comparación es el mismo, y un resultado de comparación de la segunda comparación es el mismo, se obtiene la primera información de resultado de comparación; cuando un resultado de comparación de la primera comparación es diferente y/o un resultado de comparación de la segunda comparación es diferente, se obtiene la segunda información de resultado de comparación; la primera información de resultado de comparación es información nula, la segunda información de resultado de comparación es la segunda información de cómputo mantenida por el propio terminal, y la segunda información de cómputo mantenida por el propio terminal incluye el segundo valor de cómputo de enlace ascendente y el segundo valor de cómputo de enlace descendente.

La unidad de envío 223 está configurada para recibir la primera información de identidad desde la unidad de recepción 221, y recibir la segunda información de cómputo, o la primera información de resultado de comparación, o la segunda información de resultado de comparación, desde la unidad de consulta o comparación 222, y enviar la primera información de identidad y la segunda información de cómputo, o la primera información de resultado de comparación, o la primera información de identidad y la segunda información de resultado de comparación, a la estación base primaria, de manera que la estación base primaria envía la segunda información de cómputo, o la primera información de identidad, o la segunda información de resultado de comparación, a una estación base secundaria, y después la estación base secundaria determina la información de resultado de comprobación según la segunda información de cómputo, o la primera información de resultado de comparación, o la segunda información de resultado de comparación, y obtiene la segunda información de cómputo mantenida por el propio terminal.

Por lo tanto, usando los anteriores aparatos de comprobación proporcionados por las formas de realización 21 y 22 de la presente invención, una estación base primaria fija previamente primera información de cómputo a un valor aleatorio y envía primera información de identidad y la primera información de cómputo prefijada a un terminal, de modo que el terminal realiza una comparación con segunda información de cómputo mantenida por el propio terminal y notifica primera información de comparación o segunda información de comparación a la estación base primaria; después, la estación base primaria reenvía la primera información de comparación o segunda información de comparación a una estación base secundaria, de modo que la estación base secundaria determina un resultado de comprobación y obtiene la segunda información de cómputo mantenida por el propio terminal, implementándose así un proceso de comprobación en una arquitectura de red en la que una estación base primaria está desvinculada de una estación base secundaria.

La FIG. 23 es un diagrama esquemático de un aparato de reconfiguración según la forma de realización 23 de la presente invención. Este aparato está configurado para ejecutar el procedimiento de reconfiguración proporcionado por cualquiera de las formas de realización 10, 12 y 13 de la presente invención. Como se muestra en la figura, el aparato de reconfiguración proporcionado por la forma de realización de la presente invención incluye específicamente: una unidad de determinación 231, una primera unidad de envío 232, una segunda unidad de envío 233 y una primera unidad de recepción 234.

La unidad de determinación 231 está configurada para determinar un algoritmo de cifrado según la capacidad de seguridad de un terminal, y transmitir el algoritmo de cifrado a la primera unidad de envío 232 y la segunda unidad de envío 233.

La primera unidad de envío 232 está configurada para recibir el algoritmo de cifrado desde la unidad de determinación 231, y enviar información de reconfiguración que transporta el algoritmo de cifrado al terminal, de modo que el terminal actualiza una clave del propio terminal según el algoritmo de cifrado de la información de reconfiguración y usa el algoritmo de cifrado y la clave actualizada para comunicarse con una estación base secundaria.

La segunda unidad de envío 233 está configurada para recibir el algoritmo de cifrado desde la unidad de determinación 231, y enviar información de actualización de parámetro de seguridad que transporta el algoritmo de cifrado a la estación base secundaria, de modo que la estación base secundaria se comunica con el terminal usando el algoritmo de cifrado de la información de actualización de parámetro de seguridad.

La primera unidad de recepción 234 recibe información de reconfiguración completada enviada por el terminal.

Preferentemente, el aparato de reconfiguración proporcionado por la forma de realización de la presente invención incluye además una segunda unidad de recepción 235, configurada para recibir información de solicitud de actualización de parámetro de seguridad enviada por la estación base secundaria, y transmitir la información de solicitud de actualización de parámetro de seguridad a la unidad de determinación 231, de modo que la unidad de determinación 231 determina el algoritmo de cifrado según la capacidad de seguridad del terminal después de recibirse la información de solicitud de actualización de parámetro de seguridad. La información de solicitud de actualización de parámetro de seguridad incluye que se supere un valor de cómputo mantenido por la estación base secundaria o que un resultado de comprobación no sea coherente.

La FIG. 24 es un diagrama esquemático de un aparato de reconfiguración según la forma de realización 24 de la presente invención. Este aparato está configurado para ejecutar el procedimiento de reconfiguración proporcionado por cualquiera de las formas de realización 11, 12 y 13 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente: una unidad de recepción 241, una unidad de actualización 242 y una unidad de envío 243.

La unidad de recepción 241 está configurada para recibir información de configuración enviada por una estación base primaria y que transporta un algoritmo de cifrado, y transmitir la información de reconfiguración que transporta el algoritmo de cifrado a la unidad de actualización 242, donde el algoritmo de cifrado es un algoritmo de cifrado determinado por la estación base primaria según la capacidad de seguridad de un terminal.

La unidad de actualización 242 está configurada para recibir desde la unidad de recepción 241 la información de reconfiguración que transporta el algoritmo de cifrado, actualizar una clave local según el algoritmo de cifrado de la información de reconfiguración y usar el algoritmo de cifrado y la clave actualizada para comunicarse con una estación base secundaria, y transmitir información de clave actualizada a la unidad de envío 243.

La unidad de envío 243 está configurada para recibir la información de clave actualizada desde la unidad de actualización 242, y enviar información de reconfiguración completada a la estación base primaria, de modo que la estación base primaria sabe, según la información de reconfiguración completada, que un terminal ha completado una reconfiguración.

Por lo tanto, usando los anteriores aparatos de reconfiguración proporcionados por las formas de realización 23 y 24 de la presente invención, una estación base primaria determina un algoritmo de cifrado usado por una estación base secundaria y un terminal, y envía el algoritmo de cifrado a la estación base secundaria y al terminal, respectivamente; el terminal envía información de reconfiguración completada a la estación base primaria tras actualizar una clave usando el algoritmo de cifrado, de modo que la estación base secundaria realiza una comunicación segura con el terminal usando el algoritmo de cifrado y la clave actualizada, implementándose así un proceso de reconfiguración en una arquitectura de red en la que una estación base primaria está desvinculada de una estación base secundaria.

La FIG. 25 es un diagrama esquemático de un aparato de reconfiguración según la forma de realización 25 de la presente invención. Este aparato está configurado para ejecutar el procedimiento de reconfiguración proporcionado por cualquiera de las formas de realización 14 y 16 a 18 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente: una primera unidad de recepción 251, una unidad de adición 252, una primera unidad de envío 253 y una segunda unidad de recepción 254.

La primera unidad de recepción 251 está configurada para recibir información de solicitud de actualización de parámetro de seguridad enviada por una estación base secundaria y que transporta un algoritmo de cifrado, y transmitir la información de solicitud de actualización de parámetro de seguridad que transporta el algoritmo de cifrado a la unidad de adición 252, donde la información de solicitud de actualización de parámetro de seguridad incluye el algoritmo de cifrado, o el algoritmo de cifrado e información de causa de solicitud de actualización de parámetro de seguridad. La información de causa de solicitud de actualización de parámetro de seguridad incluye que se supere un valor de cómputo mantenido por la estación base secundaria o que un resultado de comprobación no sea coherente.

La unidad de adición 252 está configurada para añadir a la información de reconfiguración el algoritmo de cifrado de la información de solicitud de actualización de parámetro de seguridad recibida.

La primera unidad de envío 253 está configurada para recibir desde la unidad de adición 252 la información de reconfiguración que transporta el algoritmo de cifrado, y enviar la información de reconfiguración que transporta el algoritmo de cifrado a un terminal, de modo que el terminal actualiza una clave del propio terminal según el algoritmo de cifrado de la información de reconfiguración y se comunica con la estación base secundaria usando el algoritmo de cifrado y la clave actualizada.

La segunda unidad de recepción 254 está configurada para recibir información de reconfiguración completada enviada por el terminal.

Además, el aparato de reconfiguración proporcionado por la forma de realización 25 de la presente invención incluye además:

una segunda unidad de envío, configurada para enviar información de capacidad de seguridad del terminal a la estación base secundaria, de modo que la estación base secundaria determina el algoritmo de cifrado según la información de capacidad de seguridad del terminal; y

una tercera unidad de recepción, configurada para recibir información de causa de solicitud de actualización de parámetro de seguridad enviada por la estación base secundaria cuando la información de solicitud de actualización de parámetro de seguridad recibida desde la primera unidad de recepción 251 incluye solamente el algoritmo de cifrado, y transmitir la información de causa de solicitud de actualización de parámetro de seguridad a la segunda unidad de envío. La información de causa de solicitud de actualización de parámetro de seguridad es que se supere un valor de cómputo mantenido por la estación base secundaria o que un valor de cómputo mantenido por la estación base secundaria sea incorrecto. Cuando el valor de cómputo mantenido por la estación base secundaria es diferente de un valor de cómputo mantenido por el propio terminal y correspondiente al valor de cómputo, se considera que el valor de cómputo mantenido por la estación base secundaria es incorrecto.

La FIG. 26 es un diagrama esquemático de un aparato de reconfiguración según la forma de realización 26 de la presente invención. Este aparato está configurado para ejecutar el procedimiento de reconfiguración proporcionado por cualquiera de las formas de realización 15 y 16 a 18 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente: una unidad de recepción 261, una unidad de actualización 262 y una unidad de envío 263.

La unidad de recepción 261 está configurada para recibir información de reconfiguración enviada por una estación base primaria y que transporta un algoritmo de cifrado de una estación base secundaria, y transmitir a la unidad de actualización 262 la información de reconfiguración que transporta el algoritmo de cifrado. El algoritmo de cifrado es un algoritmo de cifrado obtenido por la estación base primaria a partir de la información de solicitud de actualización de parámetro de seguridad enviada por la estación base secundaria.

La unidad de actualización 262 está configurada para recibir desde la unidad de recepción 261 la información de reconfiguración que transporta el algoritmo de cifrado, actualizar una clave local según el algoritmo de cifrado de la información de reconfiguración y comunicarse con la estación base secundaria usando el algoritmo de cifrado y la clave actualizada, y transmitir información de clave actualizada a la unidad de envío 263.

La unidad de envío 263 está configurada para recibir la información de clave actualizada desde la unidad de actualización 262, y enviar información de reconfiguración completada a la estación base primaria, de modo que la estación base primaria sabe, según la información de reconfiguración completada, que un terminal ha completado una reconfiguración.

Por lo tanto, usando los anteriores aparatos de reconfiguración proporcionados por las formas de realización 25 y 26 de la presente invención, una estación base secundaria determina un algoritmo de cifrado usado por la propia estación base secundaria y un terminal, y envía el algoritmo de cifrado a una estación base primaria; después, la estación base primaria envía el algoritmo de cifrado al terminal; el terminal envía información de reconfiguración completada a la estación base primaria tras actualizar una clave usando el algoritmo de cifrado, de modo que la estación base secundaria realiza una comunicación segura con el terminal usando el algoritmo de cifrado y la clave actualizada, implementándose así un proceso de reconfiguración en una arquitectura de red en la que una estación base primaria está desvinculada de una estación base secundaria.

Una forma de realización de la presente invención proporciona un sistema de comprobación y reconfiguración, donde el sistema incluye: el aparato de comprobación proporcionado por una cualquiera de las forma de realización 19 a 22, el aparato de reconfiguración proporcionado por una cualquiera de las formas de realización 23 a 26 y una estación base secundaria relacionada con el aparato de comprobación y el aparato de reconfiguración.

La FIG. 27 es un diagrama estructural esquemático de una estación base primaria según la forma de realización 27 de la presente invención. Esta estación base primaria está configurada para ejecutar el procedimiento de comprobación proporcionado por cualquiera de las formas de realización 2, 4, 5 y 6 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente: un receptor 271, un procesador 272 y un transmisor 273.

El receptor 271 está configurado para recibir primera información de identidad y primera información de cómputo enviadas por una estación base secundaria, y transmitir la primera información de identidad y la primera información de cómputo al procesador 272; y está configurado además para recibir primera información de resultado de comparación, o segunda información de identidad y segunda información de resultado de comparación enviadas por un terminal, y transmitir la primera información de identidad y la primera información de cómputo, la primera información de resultado de comparación, o la segunda información de identidad y segunda información de resultado de comparación, al procesador 272.

El procesador 272 está configurado para recibir la primera información de identidad y la primera información de cómputo desde el receptor 271, consultar, según la primera información de identidad, segunda información de identidad correspondiente a la primera información de identidad, y/o extraer segunda información de cómputo a partir de la primera información de cómputo, y transmitir la segunda información de identidad y la segunda información de cómputo al transmisor 273; y está configurado además para recibir desde el receptor la primera información de resultado de comparación, o la segunda información de identidad y segunda información de resultado de comparación, y determinar información de resultado de comprobación según la primera información de resultado de comparación recibida o la segunda información de identidad y la segunda información de resultado de comparación recibidas. La primera información de identidad incluye una identidad del terminal y una identidad de portadora de acceso radioeléctrico, E-RAB, del terminal; la primera información de cómputo incluye un primer valor de cómputo de enlace ascendente y un primer valor de cómputo de enlace descendente de la identidad E-RAB del terminal, o n primeros bits de un primer valor de cómputo de enlace ascendente y n primeros bits de un primer valor de cómputo de enlace descendente de la identidad E-RAB del terminal.

Específicamente, extraer segunda información de cómputo a partir de la primera información de cómputo comprende específicamente: extraer una pluralidad de primeros bits del primer valor de cómputo de enlace ascendente que se usarán como segundo valor de cómputo de enlace ascendente, y extraer una pluralidad de primeros bits del primer valor de cómputo de enlace descendente que se usarán como segundo valor de cómputo de enlace descendente, donde el segundo valor de cómputo de enlace ascendente y el segundo valor de cómputo de enlace descendente constituyen la segunda información de cómputo. Además, m primeros bits también pueden extraerse de n primeros bits del primer valor de cómputo de enlace ascendente para usarse como segundo valor de cómputo de enlace ascendente, y, simultáneamente, m primeros bits se extraen de n primeros bits del primer valor de cómputo de enlace descendente para usarse como segundo valor de cómputo de enlace descendente, donde m es inferior o igual a n. En este caso, el segundo valor de cómputo de enlace ascendente y el segundo valor de cómputo de enlace descendente constituyen la segunda información de cómputo.

El transmisor 273 está configurado para recibir la segunda información de identidad y la segunda información de cómputo desde el procesador 272, y enviar la segunda información de identidad y la segunda información de cómputo al terminal, de modo que el terminal compara, según la segunda información de identidad, la segunda información de cómputo con tercera información de cómputo mantenida por el propio terminal para obtener la primera información de resultado de comparación o la segunda información de resultado de comparación.

La comparación realizada por el terminal, según la segunda información de identidad, de la segunda información de cómputo con tercera información de cómputo mantenida por el propio terminal para obtener la primera información de resultado de comparación o la segunda información de resultado de comparación, comprende específicamente lo siguiente: según la segunda información de identidad, el terminal realiza una primera comparación entre el segundo valor de cómputo de enlace ascendente y un tercer valor de cómputo de enlace ascendente mantenido por el propio terminal y correspondiente a la segunda información de identidad, y, por otro lado, realiza una segunda comparación entre el segundo valor de cómputo de enlace descendente y un tercer valor de cómputo de enlace descendente mantenido por el propio terminal y correspondiente a la segunda información de identidad; cuando un resultado de comparación de la primera comparación es el mismo, y un resultado de comparación de la segunda comparación es el mismo, obtiene la primera información de resultado de comparación; cuando un resultado de comparación de la primera comparación es diferente y/o un resultado de comparación de la segunda comparación es diferente, obtiene la segunda información de resultado de comparación; la primera información de resultado de comparación es información nula, la segunda información de resultado de comparación es la tercera información de cómputo mantenida por el propio terminal, y la tercera información de cómputo mantenida por el propio terminal incluye el tercer valor de cómputo de enlace ascendente y el tercer valor de cómputo de enlace descendente.

La determinación de la información de resultado de comprobación según la primera información de resultado de comparación recibida, o la segunda información de identidad y segunda información de resultado de comparación recibidas, comprende específicamente lo siguiente: cuando se recibe la primera información de resultado de comparación, determinar que la información de resultado de comprobación indica que la primera información de

cómputo es coherente con la tercera información de cómputo; cuando se recibe la segunda información de resultado de comparación, determinar que la información de resultado de comprobación indica que la primera información de cómputo no es coherente con la tercera información de cómputo.

Preferentemente, el transmisor 273 está configurado además para enviar información de solicitud de transmisión de cómputo, de modo que la estación base secundaria determina la primera información de cómputo según la información de solicitud de transmisión de cómputo. La información de solicitud de transmisión de cómputo incluye la identidad del terminal y la identidad E-RAB del terminal.

Preferentemente, el transmisor 273 está configurado además para recibir la primera información de identidad y la primera información de resultado de comparación o segunda información de resultado de comparación desde el receptor, y enviar la primera información de resultado de comparación, o la primera información de identidad y segunda información de resultado de comparación a la estación base secundaria, de modo que la estación base secundaria determina información de resultado de comprobación según la primera información de resultado de comparación o la segunda información de resultado de comparación recibidas.

La FIG. 28 es un diagrama estructural esquemático de un terminal según la forma de realización 28 de la presente invención. Este terminal está configurado para ejecutar el procedimiento de comprobación proporcionado por cualquiera de las formas de realización 3, 4, 5 y 6 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente: un receptor 281, un procesador 282 y un transmisor 283.

El receptor 281 está configurado para recibir segunda información de identidad correspondiente a primera información de identidad y segunda información de cómputo extraída de primera información de cómputo, enviadas por una estación base primaria, transmitir la segunda información de identidad a una unidad de comparación y a una unidad de envío, y transmitir la segunda información de cómputo al procesador 282. La primera información de identidad incluye una identidad del terminal y una identidad de portadora de acceso radioeléctrico, E-RAB, del terminal; la primera información de cómputo incluye un primer valor de cómputo de enlace ascendente y un primer valor de cómputo de enlace descendente de la identidad E-RAB del terminal.

Específicamente, el envío, por medio de una estación base primaria, de segunda información de identidad correspondiente a primera información de identidad y segunda información de cómputo extraída de primera información de cómputo, comprende específicamente: consultar, mediante la estación base primaria según la identidad del terminal y la identidad de portadora de acceso radioeléctrico, E-RAB, del terminal, una identidad DRB del terminal y correspondiente a la identidad E-RAB, donde la identidad DRB es la segunda información de identidad; y extraer una pluralidad de primeros bits del primer valor de cómputo de enlace ascendente que se usarán como segundo valor de cómputo de enlace ascendente, y extraer una pluralidad de primeros bits del primer valor de cómputo de enlace descendente que se usarán como segundo valor de cómputo de enlace descendente, donde el segundo valor de cómputo de enlace ascendente y el segundo valor de cómputo de enlace descendente constituyen la segunda información de cómputo.

El procesador 282 está configurado para recibir la segunda información de identidad y la segunda información de cómputo desde el receptor 281, y comparar, según la segunda información de identidad, la segunda información de cómputo con tercera información de cómputo mantenida de manera local para obtener primera información de resultado de comparación o segunda información de resultado de comparación, y transmitir la primera información de resultado de comparación o la segunda información de resultado de comparación al transmisor 283.

Específicamente, la comparación, según la segunda información de identidad, de la segunda información de cómputo con tercera información de cómputo mantenida de manera local para obtener primera información de resultado de comparación o segunda información de resultado de comparación, comprende específicamente:

según la segunda información de identidad, realizar una primera comparación entre el segundo valor de cómputo de enlace ascendente y un tercer valor de cómputo de enlace ascendente mantenido de manera local y correspondiente a la segunda información de identidad, y, por otro lado, realizar una segunda comparación entre el segundo valor de cómputo de enlace descendente y un tercer valor de cómputo de enlace descendente mantenido de manera local y correspondiente a la segunda información de identidad; cuando un resultado de comparación de la primera comparación es el mismo, y un resultado de comparación de la segunda comparación es también el mismo, obtener la primera información de resultado de comparación; cuando un resultado de comparación de la primera comparación es diferente y/o un resultado de comparación de la segunda comparación es diferente, obtener la segunda información de resultado de comparación; la primera información de resultado de comparación es información nula, la segunda información de resultado de comparación es la tercera información de cómputo mantenida de manera local, y la tercera información de cómputo mantenida de manera local incluye el tercer valor de cómputo de enlace ascendente y el tercer valor de cómputo de enlace descendente.

El transmisor 283 está configurado para recibir la segunda información de identidad desde el receptor, recibir la primera información de resultado de comparación o la segunda información de resultado de comparación desde la unidad de comparación, y enviar la primera información de resultado de comparación, o la segunda información de identidad y segunda información de resultado de comparación, a la estación base primaria, de manera que la estación base primaria determina información de resultado de comprobación según la primera información de resultado de comparación o la segunda información de resultado de comparación.

La determinación de la información de resultado de comprobación según la primera información de resultado de comparación, o la segunda información de resultado de comparación, comprende específicamente lo siguiente: cuando se recibe la primera información de resultado de comparación, determinar que la información de resultado de comprobación indica que la primera información de cómputo es coherente con la tercera información de cómputo; cuando se recibe la segunda información de resultado de comparación, determinar que la información de resultado de comprobación indica que la primera información de cómputo no es coherente con la tercera información de cómputo.

Por lo tanto, usando la anterior estación base primaria proporcionada por la forma de realización 27 y el terminal proporcionado por la forma de realización 28 de la presente invención, la estación base primaria recibe primera información de identidad y primera información de cómputo desde una estación base secundaria, y convierte la primera información de identidad en segunda información de identidad y, por otro lado, extrae segunda información de cómputo a partir de la primera información de cómputo y envía la segunda información de cómputo al terminal, de manera que el terminal realiza una comparación con tercera información de cómputo mantenida por el propio terminal y notifica primera información de comparación o segunda información de comparación a la estación base primaria; la estación base primaria determina un resultado de comprobación, implementándose así un proceso de comprobación en una arquitectura de red en la que una estación base primaria está desvinculada de una estación base secundaria.

La FIG. 29 es un diagrama estructural esquemático de una estación base primaria según la forma de realización 29 de la presente invención. Esta estación base primaria está configurada para ejecutar el procedimiento de comprobación proporcionado por cualquiera de las formas de realización 7 y 9 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente: un transmisor 291, un receptor 292 y un procesador 293.

El transmisor 291 está configurado para enviar primera información de identidad, o primera información de identidad y primera información de cómputo, a un terminal, de modo que el terminal consulta, según la primera información de identidad, segunda información de cómputo mantenida por el propio terminal, o compara, según la primera información de identidad, la primera información de cómputo con segunda información de cómputo mantenida por el propio terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación; y está configurado además para recibir segunda información de identidad desde el procesador 293, y la segunda información de cómputo, o la primera información de resultado de comparación, o la segunda información de resultado de comparación, y enviar la segunda información de identidad y la segunda información de cómputo, o la primera información de resultado de comparación, o la segunda información de identidad y la segunda información de resultado de comparación, a una estación base secundaria, de modo que la estación base secundaria obtiene la segunda información de cómputo mantenida por el propio terminal y compara la segunda información de cómputo con tercera información de cómputo mantenida por la propia estación base secundaria, determinándose así información de resultado de comprobación. La primera información de identidad es una identidad DRB del terminal; la primera información de cómputo es un valor de cómputo prefijado; la segunda información de identidad es información de identidad del terminal y una identidad E-RAB del terminal. La primera información de cómputo incluye un primer valor de cómputo de enlace ascendente y un primer valor de cómputo de enlace descendente.

Específicamente, la comparación realizada por el terminal, según la primera información de identidad, de la primera información de cómputo con segunda información de cómputo mantenida por el propio terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación, comprende específicamente lo siguiente: según la primera información de identidad, el terminal realiza una primera comparación entre el primer valor de cómputo de enlace ascendente y un segundo valor de cómputo de enlace ascendente mantenido por el propio terminal y correspondiente a la primera información de identidad, y/o realiza una segunda comparación entre el primer valor de cómputo de enlace descendente y un segundo valor de cómputo de enlace descendente mantenido por el propio terminal y correspondiente a la primera información de identidad; cuando un resultado de comparación de la primera comparación es el mismo, y un resultado de comparación de la segunda comparación es el mismo, obtiene la primera información de resultado de comparación; cuando un resultado de comparación de la primera comparación es diferente y/o un resultado de comparación de la segunda comparación es diferente, obtiene la segunda información de resultado de comparación; la primera información de resultado de comparación es información nula, la segunda información de resultado de comparación es la segunda información de cómputo mantenida por el propio terminal, y la segunda información de cómputo mantenida por el propio terminal incluye el segundo valor de cómputo de enlace ascendente y el segundo valor de cómputo de enlace descendente.

El receptor 292 está configurado para recibir la primera información de identidad y la segunda información de cómputo enviadas por el terminal, o la primera información de resultado de comparación enviada por el terminal, o la primera información de identidad y la segunda información de resultado de comparación enviadas por el terminal, transmitir la primera información de identidad al procesador, y transmitir la segunda información de cómputo, o la primera información de resultado de comparación, o la segunda información de resultado de comparación, al transmisor 291.

El procesador 293 está configurado para recibir la primera información de identidad desde el receptor, consultar, según la primera información de identidad, segunda información de identidad correspondiente a la primera información de identidad, y transmitir la segunda información de identidad al transmisor 291.

La FIG. 30 es un diagrama estructural esquemático de un terminal según la forma de realización 30 de la presente invención. Este terminal está configurado para ejecutar el procedimiento de comprobación proporcionado por cualquiera de las formas de realización 8 y 9 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente: un receptor 301, un procesador 302 y un transmisor 303.

El receptor 301 está configurado para recibir primera información de identidad o primera información de identidad y primera información de cómputo, enviadas por una estación base primaria, y transmitir la primera información de identidad al procesador y al transmisor, y transmitir la primera información de cómputo al procesador 302. La primera información de identidad es una identidad DRB del terminal, y la primera información de cómputo es un valor de cómputo prefijado.

El procesador 302 está configurado para recibir la primera información de identidad, o la primera información de identidad y la primera información de cómputo desde el receptor 301, consultar, según la primera información de identidad, segunda información de cómputo mantenida de manera local, o comparar, según la primera información de identidad, la primera información de cómputo con segunda información de cómputo mantenida de manera local para obtener primera información de resultado de comparación o segunda información de resultado de comparación, y transmitir la segunda información de cómputo, o la primera información de resultado de comparación, o la segunda información de resultado de comparación, al transmisor 303. La primera información de cómputo incluye un primer valor de cómputo de enlace ascendente y un primer valor de cómputo de enlace descendente.

Específicamente, según la primera información de identidad, se realiza una primera comparación entre el primer valor de cómputo de enlace ascendente y un segundo valor de cómputo de enlace ascendente mantenido por el propio terminal y correspondiente a la primera información de identidad, y/o se realiza una segunda comparación entre el primer valor de cómputo de enlace descendente y un segundo valor de cómputo de enlace descendente mantenido por el propio terminal y correspondiente a la primera información de identidad; cuando un resultado de comparación de la primera comparación es el mismo, y un resultado de comparación de la segunda comparación es también el mismo, se obtiene la primera información de resultado de comparación; cuando un resultado de comparación de la primera comparación es diferente y/o un resultado de comparación de la segunda comparación es diferente, se obtiene la segunda información de resultado de comparación; la primera información de resultado de comparación es información nula, la segunda información de resultado de comparación es la segunda información de cómputo mantenida por el propio terminal, y la segunda información de cómputo mantenida por el propio terminal incluye el segundo valor de cómputo de enlace ascendente y el segundo valor de cómputo de enlace descendente.

El transmisor 303 está configurado para recibir la primera información de identidad desde el receptor 301, y recibir la segunda información de cómputo, o la primera información de resultado de comparación, o la segunda información de resultado de comparación, desde el procesador 302, y enviar la primera información de identidad y la segunda información de cómputo, o la primera información de resultado de comparación, o la primera información de identidad y la segunda información de resultado de comparación, a la estación base primaria, de manera que la estación base primaria reenvía la segunda información de cómputo, o la primera información de resultado de comparación y la segunda información de resultado de comparación, a una estación base secundaria, de modo que la estación base secundaria determina información de resultado de comprobación según la segunda información de cómputo, o la primera información de resultado de comparación, o la segunda información de resultado de comparación, y obtiene la segunda información de cómputo mantenida por el propio terminal.

Por lo tanto, usando la anterior estación base primaria proporcionada por la forma de realización 29 y el terminal proporcionado por la forma de realización 30 de la presente invención, la estación base primaria fija previamente primera información de cómputo a un valor aleatorio y envía primera información de identidad y la primera información de cómputo prefijada al terminal, de modo que el terminal realiza una comparación con segunda información de cómputo mantenida por el propio terminal y notifica primera información de comparación o segunda información de comparación a la estación base primaria; después, la estación base primaria reenvía la primera información de comparación o segunda información de comparación a una estación base secundaria, de modo que la estación base secundaria determina un resultado de comprobación y obtiene la segunda información de cómputo mantenida por el propio terminal, implementándose así un proceso de comprobación en una arquitectura de red en la que una estación base primaria está desvinculada de una estación base secundaria.

La FIG. 31 es un diagrama estructural esquemático de una estación base primaria según la forma de realización 31 de la presente invención. Esta estación base primaria está configurada para ejecutar el procedimiento de reconfiguración proporcionado por cualquiera de las formas de realización 10, 12 y 13 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente: un procesador 311, un transmisor 312 y un receptor 313.

El procesador 311 está configurado para determinar un algoritmo de cifrado según la capacidad de seguridad de un terminal, y transmitir el algoritmo de cifrado al transmisor 312.

El transmisor 312 está configurado para recibir el algoritmo de cifrado desde el procesador 311, y enviar al terminal información de reconfiguración que transporta el algoritmo de cifrado, de modo que el terminal actualiza una clave del propio terminal según el algoritmo de cifrado de la información de reconfiguración y se comunica con una estación base secundaria usando el algoritmo de cifrado y la clave actualizada.

El receptor 313 está configurado para recibir información de reconfiguración completada enviada por el terminal.

Preferentemente, el transmisor 312 está configurado además para recibir el algoritmo de cifrado desde el procesador 311, y enviar a la estación base secundaria información de actualización de parámetro de seguridad que transporta el algoritmo de cifrado, de modo que la estación base secundaria se comunica con el terminal usando el algoritmo de cifrado de la información de actualización de parámetro de seguridad.

El receptor 313 está configurado además para recibir información de solicitud de actualización de parámetro de seguridad enviada por la estación base secundaria, y transmitir la información de solicitud de actualización de parámetro de seguridad al procesador 311, de modo que el procesador 311 determina el algoritmo de cifrado según la capacidad de seguridad del terminal después de recibirse la información de solicitud de actualización de parámetro de seguridad. La información de solicitud de actualización de parámetro de seguridad incluye que se supere un valor de cómputo mantenido por la estación base secundaria o que un resultado de comprobación no sea coherente.

La FIG. 32 es un diagrama estructural esquemático de un terminal según la forma de realización 32 de la presente invención. Este terminal está configurado para ejecutar el procedimiento de reconfiguración proporcionado por cualquiera de las formas de realización 11, 12 y 13 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente: un receptor 321, un procesador 322 y un transmisor 323.

El receptor 321 está configurado para recibir información de reconfiguración enviada por una estación base primaria y que transporta un algoritmo de cifrado, y transmitir al procesador 322 la información de reconfiguración que transporta el algoritmo de cifrado.

El procesador 322 está configurado para recibir desde el receptor la información de reconfiguración que transporta el algoritmo de cifrado, actualizar una clave local según el algoritmo de cifrado de la información de reconfiguración y comunicarse con una estación base secundaria usando el algoritmo de cifrado y la clave actualizada, y transmitir la información de clave actualizada al transmisor 323.

El transmisor 323 está configurado para recibir la información de clave actualizada desde el procesador 322, y enviar información de reconfiguración completada a la estación base primaria, de modo que la estación base primaria sabe, según la información de reconfiguración completada, que un terminal ha completado una reconfiguración.

Por lo tanto, usando la anterior estación base primaria proporcionada por la forma de realización 31 y el terminal proporcionado por la forma de realización 32 de la presente invención, la estación base primaria determina un algoritmo de cifrado usado por una estación base secundaria y el terminal, y envía el algoritmo de cifrado a la estación base secundaria y al terminal, respectivamente; el terminal envía información de reconfiguración completada a la estación base primaria tras actualizar una clave usando el algoritmo de cifrado, de modo que la estación base secundaria realiza una comunicación segura con el terminal usando el algoritmo de cifrado y la clave actualizada, implementándose así un proceso de reconfiguración en una arquitectura de red en la que una estación base primaria está desvinculada de una estación base secundaria.

La FIG. 33 es un diagrama estructural esquemático de una estación base primaria según la forma de realización 33 de la presente invención. Esta estación base primaria está configurada para ejecutar el procedimiento de reconfiguración proporcionado por cualquiera de las formas de realización 14 y 16 a 18 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente: un receptor 331, un procesador 332 y un transmisor 333.

El receptor 331 está configurado para recibir información de solicitud de actualización de parámetro de seguridad enviada por una estación base secundaria y que transporta un algoritmo de cifrado, y transmitir al procesador 332 la

información de solicitud de actualización de parámetro de seguridad que transporta el algoritmo de cifrado; y está configurado además para recibir información de reconfiguración completada enviada por un terminal, donde la información de solicitud de actualización de parámetro de seguridad incluye el algoritmo de cifrado, o el algoritmo de cifrado e información de causa de solicitud de actualización de parámetro de seguridad.

El procesador 332 está configurado para recibir desde el receptor 331 la información de solicitud de actualización de parámetro de seguridad que transporta el algoritmo de cifrado, añadir a la información de reconfiguración el algoritmo de cifrado de la información de solicitud de actualización de parámetro de seguridad recibida, y transmitir la información de reconfiguración al transmisor 333.

El transmisor 333 está configurado para recibir desde el procesador 332 la información de reconfiguración que transporta el algoritmo de cifrado, y enviar al terminal la información de reconfiguración que transporta el algoritmo de cifrado, de modo que el terminal actualiza una clave del propio terminal según el algoritmo de cifrado de la información de reconfiguración y se comunica con la estación base secundaria usando la clave actualizada.

Preferentemente, la estación base primaria proporcionada por la forma de realización de la presente invención incluye además: el transmisor 333, configurado para enviar información de capacidad de seguridad del terminal a la estación base secundaria, de modo que la estación base secundaria determina el algoritmo de cifrado según la información de capacidad de seguridad del terminal.

Preferentemente, el receptor 331 está configurado además para recibir información de causa de solicitud de actualización de parámetro de seguridad enviada por la estación base secundaria cuando la información de solicitud de actualización de parámetro de seguridad recibida transporta solamente el algoritmo de cifrado, y transmitir la información de causa de solicitud de actualización de parámetro de seguridad al transmisor. La información de causa de solicitud de actualización de parámetro de seguridad indica que se supera un valor de cómputo mantenido por la estación base secundaria o que un valor de cómputo mantenido por la estación base secundaria es incorrecto. Cuando el valor de cómputo mantenido por la estación base secundaria es diferente de un valor de cómputo mantenido por el propio terminal y correspondiente al valor de cómputo, se considera que el valor de cómputo mantenido por la estación base secundaria es incorrecto.

La FIG. 34 es un diagrama estructural esquemático de un terminal según la forma de realización 34 de la presente invención. Este terminal está configurado para ejecutar el procedimiento de reconfiguración proporcionado por cualquiera de las formas de realización 15 y 16 a 18 de la presente invención. Como se muestra en la figura, la forma de realización de la presente invención incluye específicamente: un receptor 341, un procesador 342 y un transmisor 343.

El receptor 341 está configurado para recibir información de reconfiguración enviada por una estación base primaria y que transporta un algoritmo de cifrado de una estación base secundaria, y transmitir al procesador 342 la información de reconfiguración que transporta el algoritmo de cifrado. El algoritmo de cifrado es un algoritmo de cifrado obtenido por la estación base primaria a partir de la información de solicitud de actualización de parámetro de seguridad enviada por la estación base secundaria.

El procesador 342 está configurado para recibir desde el receptor 341 la información de reconfiguración que transporta el algoritmo de cifrado, actualizar una clave local según el algoritmo de cifrado de la información de reconfiguración y comunicarse con la estación base secundaria usando el algoritmo de cifrado y la clave actualizada, y transmitir la información de clave actualizada al transmisor 343.

El transmisor 343 está configurado para recibir la información de clave actualizada desde el procesador 342, y enviar información de reconfiguración completada a la estación base primaria, de modo que la estación base primaria sabe, según la información de reconfiguración completada, que un terminal ha completado una reconfiguración.

Por lo tanto, usando la anterior estación base primaria proporcionada por la forma de realización 33 y el terminal proporcionado por la forma de realización 34 de la presente invención, una estación base secundaria determina un algoritmo de cifrado usado por la estación base secundaria y el terminal, y envía el algoritmo de cifrado a la estación base primaria; después, la estación base primaria envía el algoritmo de cifrado al terminal; el terminal envía información de reconfiguración completada a la estación base primaria tras actualizar una clave usando el algoritmo de cifrado, de modo que la estación base secundaria realiza una comunicación segura con el terminal usando el algoritmo de cifrado y la clave actualizada, implementándose así un proceso de reconfiguración en una arquitectura de red en la que una estación base primaria está desvinculada de una estación base secundaria.

Una forma de realización de la presente invención proporciona un sistema de comprobación y reconfiguración, donde el sistema incluye: la estación base primaria proporcionada por la forma de realización 27 de la presente invención, el terminal proporcionado por la forma de realización 28 de la presente invención, y una estación base secundaria que lleva a cabo una interacción de información con la estación base primaria; o la estación base primaria proporcionada por la forma de realización 29 de la presente invención, el terminal proporcionado por la forma de realización 30 de la presente invención, y una estación base secundaria que lleva a cabo una interacción

de información con la estación base primaria; o la estación base primaria proporcionada por la forma de realización 31 de la presente invención, el terminal proporcionado por la forma de realización 32 de la presente invención, y una estación base secundaria que lleva a cabo una interacción de información con la estación base primaria; o la estación base primaria proporcionada por la forma de realización 33 de la presente invención, el terminal proporcionado por la forma de realización 34 de la presente invención, y una estación base secundaria que lleva a cabo una interacción de información con la estación base primaria.

Un experto en la técnica puede percatarse además de que, en combinación con los ejemplos descritos en las formas de realización dadas a conocer en esta memoria descriptiva, las unidades y etapas de algoritmo pueden implementarse mediante hardware electrónico, software informático o una combinación de los mismos. Para describir claramente la intercambiabilidad entre el hardware y el software, lo expuesto anteriormente ha descrito composiciones y etapas de cada ejemplo según las funciones. El que las funciones se implementen en hardware o en software depende de las aplicaciones particulares y de las restricciones de diseño de las soluciones técnicas. Un experto en la técnica puede usar diferentes procedimientos para implementar las funciones descritas para cada aplicación particular, pero no debe considerarse que la implementación va más allá del alcance de la presente invención.

Las etapas de los procedimientos o algoritmos descritos en las formas de realización dadas a conocer en esta memoria descriptiva pueden implementarse en hardware, un módulo de software ejecutado mediante un procesador, o una combinación de los mismos. El módulo de software puede residir en una memoria de acceso aleatorio (RAM), una memoria, una memoria de solo lectura (ROM), una ROM eléctricamente programable, una ROM eléctricamente programable y borrable, un registro, un disco duro, un disco extraíble, un CD-ROM o cualquier otra forma de medio de almacenamiento conocida en la técnica.

En los anteriores modos de implementación específicos se han descrito en detalle los objetivos, las soluciones técnicas y los beneficios de la presente invención. Debe observarse que las descripciones anteriores son simplemente modos de implementación específicos de la presente invención, y no pretenden limitar el alcance de protección de la presente invención. Cualquier modificación, sustitución equivalente o mejora realizada sin apartarse de los principios de la presente invención estará dentro del alcance de protección de la presente invención.

REIVINDICACIONES

1. Un procedimiento de comprobación, que comprende:

recibir (201), mediante una estación base primaria, primera información de identidad y primera información de cómputo enviada por una estación base secundaria;
consultar (202), mediante la estación base primaria, según la primera información de identidad, segunda información de identidad correspondiente a la primera información de identidad;
extraer (203), mediante la estación base primaria, segunda información de cómputo a partir de la primera información de cómputo;
enviar (204), mediante la estación base primaria, la segunda información de identidad y la segunda información de cómputo a un terminal;
recibir (205), mediante la estación base primaria, la primera información de resultado de comparación enviada por el terminal, o la segunda información de identidad y segunda información de resultado de comparación enviadas por el terminal, donde la primera información de resultado de comparación o la segunda información de resultado de comparación corresponde a un resultado de comparar la segunda información de cómputo con una tercera información de cómputo mantenida por el terminal; y
determinar (206), mediante la estación base primaria, información de resultado de comprobación según la primera información de resultado de comparación, o la segunda información de identidad recibida y la segunda información de resultado de comparación.

2. El procedimiento de comprobación según la reivindicación 1, en el que la primera información de identidad comprende una identidad del terminal y una identidad de portadora de acceso radioeléctrico, E-RAB, del terminal.

3. El procedimiento de comprobación según la reivindicación 2, en el que la primera información de cómputo comprende un primer valor de cómputo de enlace ascendente y un primer valor de cómputo de enlace descendente de la identidad E-RAB del terminal.

4. El procedimiento de comprobación según la reivindicación 3, en el que consultar, mediante la estación base primaria, según la primera información de identidad, segunda información de identidad correspondiente a la primera información de identidad, comprende específicamente:

consultar, mediante la estación base primaria, según la identidad del terminal y la identidad de portadora de acceso radioeléctrico, E-RAB, del terminal, una identidad de portadora radioeléctrica de datos, DRB, del terminal y correspondiente a la identidad E-RAB, donde la identidad DRB del terminal es la segunda información de identidad.

5. El procedimiento de comprobación según una cualquiera de las reivindicaciones 3 o 4, en el que extraer, mediante la estación base primaria, segunda información de cómputo a partir de la primera información de cómputo comprende específicamente:

extraer, mediante la estación base primaria, una pluralidad de primeros bits del primer valor de cómputo de enlace ascendente que se usarán como segundo valor de cómputo de enlace ascendente, y extraer una pluralidad de primeros bits del primer valor de cómputo de enlace descendente que se usarán como segundo valor de cómputo de enlace descendente, donde el segundo valor de cómputo de enlace ascendente y el segundo valor de cómputo de enlace descendente constituyen la segunda información de cómputo.

6. Un procedimiento de comprobación, en el que el procedimiento comprende:

recibir (301), mediante un terminal, desde una estación base primaria, segunda información de identidad correspondiente a primera información de identidad y segunda información de cómputo extraída de primera información de cómputo;
comparar (302), mediante el terminal, según la segunda información de identidad, la segunda información de cómputo con tercera información de cómputo mantenida de manera local por el terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación; y
enviar (302), mediante el terminal, la primera información de resultado de comparación, o la segunda información de identidad y segunda información de resultado de comparación, a la estación base primaria;

donde comparar (302), mediante el terminal, según la segunda información de identidad, la segunda información de cómputo, comprendiendo la segunda información de cómputo un segundo valor de cómputo de enlace ascendente y un segundo valor de cómputo de enlace descendente, con tercera información de cómputo, comprendiendo la tercera información de cómputo un tercer valor de cómputo de enlace ascendente y un tercer valor de cómputo de enlace descendente, mantenida de manera local por el terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación, comprende específicamente:

según la segunda información de identidad, realizar una primera comparación entre el segundo valor de cómputo de enlace ascendente y el tercer valor de cómputo de enlace ascendente mantenido de manera local por el terminal y correspondiente a la segunda información de identidad, y/o realizar una segunda comparación entre el segundo valor de cómputo de enlace descendente y el tercer valor de cómputo de enlace descendente mantenido de manera local por el terminal y correspondiente a la segunda información de identidad;

cuando un resultado de comparación de la primera comparación es el mismo, y un resultado de comparación de la segunda comparación es también el mismo, obtener la primera información de resultado de comparación; cuando un resultado de comparación de la primera comparación es diferente y/o un resultado de comparación de la segunda comparación es diferente, obtener la segunda información de resultado de comparación; la primera información de resultado de comparación es información nula, la segunda información de resultado de comparación es la tercera información de cómputo.

7. Una estación base primaria, que comprende:

una primera unidad de recepción (191), configurada para recibir primera información de identidad y primera información de cómputo enviadas por una estación base secundaria, y transmitir la primera información de identidad a una unidad de consulta, y transmitir la primera información de cómputo a una unidad de extracción;

una unidad de consulta (192), configurada para recibir la primera información de identidad desde la primera unidad de recepción, consultar, según la primera información de identidad, segunda información de identidad correspondiente a la primera información de identidad, y transmitir la segunda información de identidad a una primera unidad de envío;

una unidad de extracción (193), configurada para recibir la primera información de cómputo desde la primera unidad de recepción, extraer segunda información de cómputo a partir de la primera información de cómputo, y transmitir la segunda información de cómputo a la primera unidad de envío;

una primera unidad de envío (194), configurada para recibir la segunda información de identidad desde la unidad de consulta, y recibir la segunda información de cómputo desde la unidad de extracción, y enviar la segunda información de identidad y la segunda información de cómputo a un terminal;

una segunda unidad de recepción (197), configurada para recibir la primera información de resultado de comparación, o la segunda información de identidad y segunda información de resultado de comparación enviadas por el terminal, y transmitir la primera información de resultado de comparación, o la segunda información de identidad y segunda información de resultado de comparación, a una unidad de determinación, donde la primera información de resultado de comparación o la segunda información de resultado de comparación corresponde a un resultado de comparar la segunda información de cómputo con una tercera información de cómputo mantenida por el terminal; y

una unidad de determinación (196) configurada para recibir la primera información de resultado de comparación, o la segunda información de identidad y segunda información de resultado de comparación, desde la segunda unidad de recepción, y determinar información de resultado de comprobación según la primera información de resultado de comparación recibida, o la segunda información de identidad y la segunda información de resultado de comparación recibidas.

8. La estación base primaria según la reivindicación 7, en la que la primera información de identidad comprende una identidad del terminal y una identidad de portadora de acceso radioeléctrico, E-RAB, del terminal.

9. La estación base primaria según la reivindicación 8, en la que la primera información de cómputo comprende un primer valor de cómputo de enlace ascendente y un primer valor de cómputo de enlace descendente de la identidad E-RAB del terminal.

10. La estación base primaria según la reivindicación 9, en la que consultar, mediante la unidad de consulta según la primera información de identidad, segunda información de identidad correspondiente a la primera información de identidad, comprende específicamente:

consultar, según la identidad del terminal y la identidad de portadora de acceso radioeléctrico, E-RAB, del terminal, una identidad de portadora radioeléctrica de datos, DRB, del terminal y correspondiente a la identidad E-RAB, donde la identidad DRB del terminal es la segunda información de identidad.

11. La estación base primaria según la reivindicación 10, en la que extraer, mediante la unidad de extracción, segunda información de cómputo a partir de la primera información de cómputo comprende específicamente:

extraer una pluralidad de primeros bits del primer valor de cómputo de enlace ascendente que se usarán como segundo valor de cómputo de enlace ascendente, y extraer una pluralidad de primeros bits del primer valor de cómputo de enlace descendente que se usarán como segundo valor de cómputo de enlace descendente, donde el segundo valor de cómputo de enlace ascendente y el segundo valor de cómputo de enlace descendente constituyen la segunda información de cómputo.

12. Un terminal, que comprende:

una unidad de recepción (201), configurada para recibir segunda información de identidad correspondiente a primera información de identidad y segunda información de cómputo extraída de primera información de cómputo, enviadas por una estación base primaria, transmitir la segunda información de identidad a una unidad de comparación y una unidad de envío, y transmitir la segunda información de cómputo a la unidad de comparación;
una unidad de comparación (202), configurada para recibir la segunda información de identidad y la segunda información de cómputo desde la unidad de recepción, y comparar, según la segunda información de identidad, la segunda información de cómputo con tercera información de cómputo mantenida de manera local por el terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación, y transmitir la primera información de resultado de comparación o la segunda información de resultado de comparación a una unidad de envío; y
una unidad de envío (203, configurada para recibir la segunda información de identidad desde la unidad de recepción, recibir la primera información de resultado de comparación o la segunda información de resultado de comparación desde la unidad de comparación, y enviar la primera información de resultado de comparación, o la segunda información de identidad y segunda información de resultado de comparación a la estación base primaria;

donde comparar, mediante la unidad de comparación, según la segunda información de identidad, la segunda información de cómputo, comprendiendo la segunda información de cómputo un segundo valor de cómputo de enlace ascendente y un segundo valor de cómputo de enlace descendente, con tercera información de cómputo, comprendiendo la tercera información de cómputo un tercer valor de cómputo de enlace ascendente y un tercer valor de cómputo de enlace descendente, mantenida de manera local por el terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación, comprende específicamente:

según la segunda información de identidad, realizar una primera comparación entre el segundo valor de cómputo de enlace ascendente y el tercer valor de cómputo de enlace ascendente mantenido de manera local por el terminal y correspondiente a la segunda información de identidad, y/o realizar una segunda comparación entre el segundo valor de cómputo de enlace descendente y el tercer valor de cómputo de enlace descendente mantenido de manera local por el terminal y correspondiente a la segunda información de identidad;
cuando un resultado de comparación de la primera comparación es el mismo, y un resultado de comparación de la segunda comparación es también el mismo, obtener la primera información de resultado de comparación; cuando un resultado de comparación de la primera comparación es diferente y/o un resultado de comparación de la segunda comparación es diferente, obtener la segunda información de resultado de comparación; la primera información de resultado de comparación es información nula, la segunda información de resultado de comparación es la tercera información de cómputo.

13. Un sistema de comprobación y de reconfiguración, que comprende: una estación base primaria según una cualquiera de las reivindicaciones 7 a 11, y un terminal, que comprende:

una unidad de recepción (201), configurada para recibir segunda información de identidad correspondiente a primera información de identidad y segunda información de cómputo extraída de primera información de cómputo, enviadas por una estación base primaria, y transmitir la segunda información de identidad a una unidad de comparación y una unidad de envío, y transmitir la segunda información de cómputo a una unidad de comparación;
una unidad de comparación (202), configurada para recibir la segunda información de identidad y la segunda información de cómputo desde la unidad de recepción, y comparar, según la segunda información de identidad, la segunda información de cómputo con tercera información de cómputo mantenida de manera local para obtener primera información de resultado de comparación o segunda información de resultado de comparación, y transmitir la primera información de resultado de comparación o la segunda información de resultado de comparación a una unidad de envío; y
una unidad de envío (203), configurada para recibir la segunda información de identidad desde la unidad de recepción, recibir la primera información de resultado de comparación o la segunda información de resultado de comparación desde la unidad de comparación, y enviar la primera información de resultado de comparación, o la segunda información de identidad y segunda información de resultado de comparación, a la estación base primaria.

14. El sistema de comprobación y reconfiguración según la reivindicación 13, en el que comparar, mediante la unidad de comparación, según la segunda información de identidad, la segunda información de cómputo, comprendiendo la segunda información de cómputo un segundo valor de cómputo de enlace ascendente y un segundo valor de cómputo de enlace descendente, con tercera información de cómputo, comprendiendo la tercera información de cómputo un tercer valor de cómputo de enlace ascendente y un tercer valor de cómputo de enlace

descendente, mantenida de manera local por el terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación, comprende específicamente:

según la segunda información de identidad, realizar una primera comparación entre el segundo valor de cómputo de enlace ascendente y el tercer valor de cómputo de enlace ascendente mantenido de manera local por el terminal y correspondiente a la segunda información de identidad, y/o realizar una segunda comparación entre el segundo valor de cómputo de enlace descendente y el tercer valor de cómputo de enlace descendente mantenido de manera local por el terminal y correspondiente a la segunda información de identidad;

cuando un resultado de comparación de la primera comparación es el mismo, y un resultado de comparación de la segunda comparación es también el mismo, obtener la primera información de resultado de comparación; cuando un resultado de comparación de la primera comparación es diferente y/o un resultado de comparación de la segunda comparación es diferente, obtener la segunda información de resultado de comparación; la primera información de resultado de comparación es información nula, la segunda información de resultado de comparación es la tercera información de cómputo.

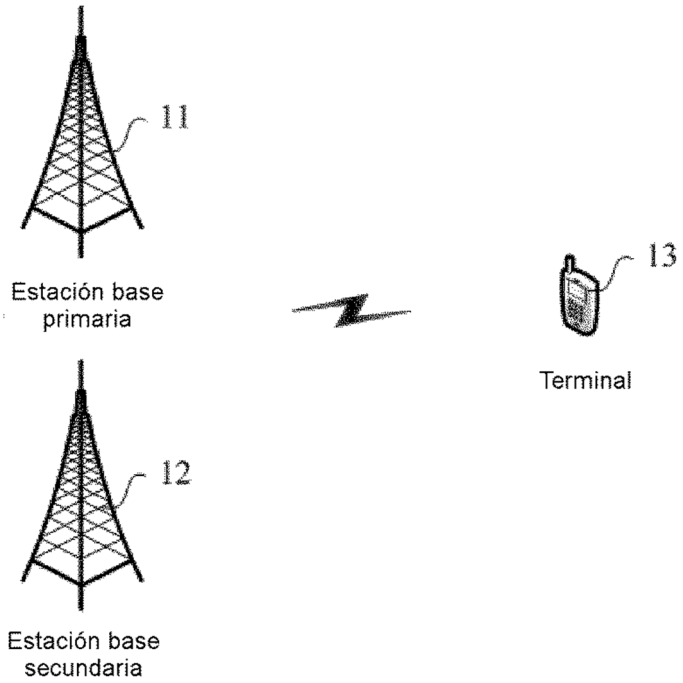
11
Estación base primaria
13
Terminal
12
Estación base secundaria

FIG. 1

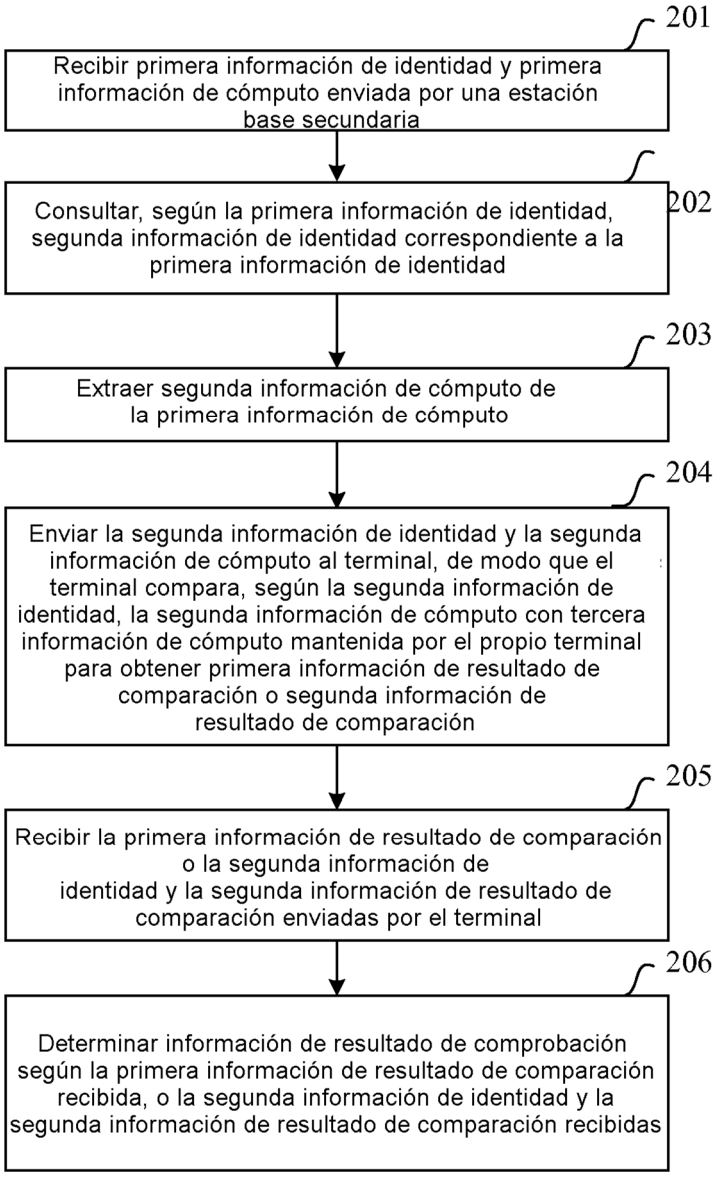
201
Recibir primera información de identidad y primera información de cómputo enviada por una estación base secundaria
202
Consultar, según la primera información de identidad, segunda información de identidad correspondiente a la primera información de identidad
203
Extraer segunda información de cómputo de la primera información de cómputo
204
Enviar la segunda información de identidad y la segunda información de cómputo al terminal, de modo que el terminal compara, según la segunda información de identidad, la segunda información de cómputo con tercera información de cómputo mantenida por el propio terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación
205
Recibir la primera información de resultado de comparación o la segunda información de identidad y la segunda información de resultado de comparación enviadas por el terminal
206
Determinar información de resultado de comprobación según la primera información de resultado de comparación recibida, o la segunda información de identidad y la segunda información de resultado de comparación recibidas

FIG. 2

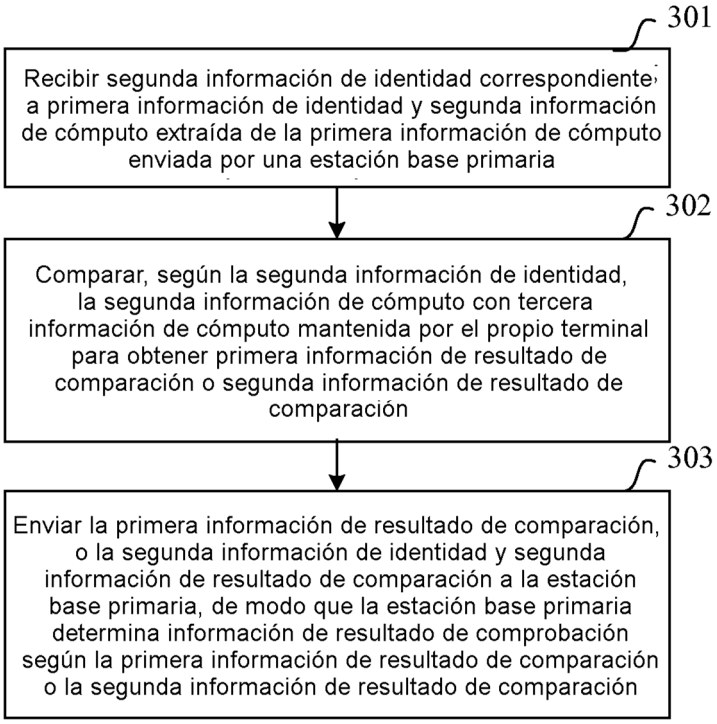
301
Recibir segunda información de identidad correspondiente a primera información de identidad y segunda información de cómputo extraída de la primera información de cómputo enviada por una estación base primaria
302
Comparar, según la segunda información de identidad, la segunda información de cómputo con tercera información de cómputo mantenida por el propio terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación
303
Enviar la primera información de resultado de comparación, o la segunda información de identidad y segunda información de resultado de comparación a la estación base primaria, de modo que la estación base primaria determina información de resultado de comprobación según la primera información de resultado de comparación o la segunda información de resultado de comparación

FIG. 3

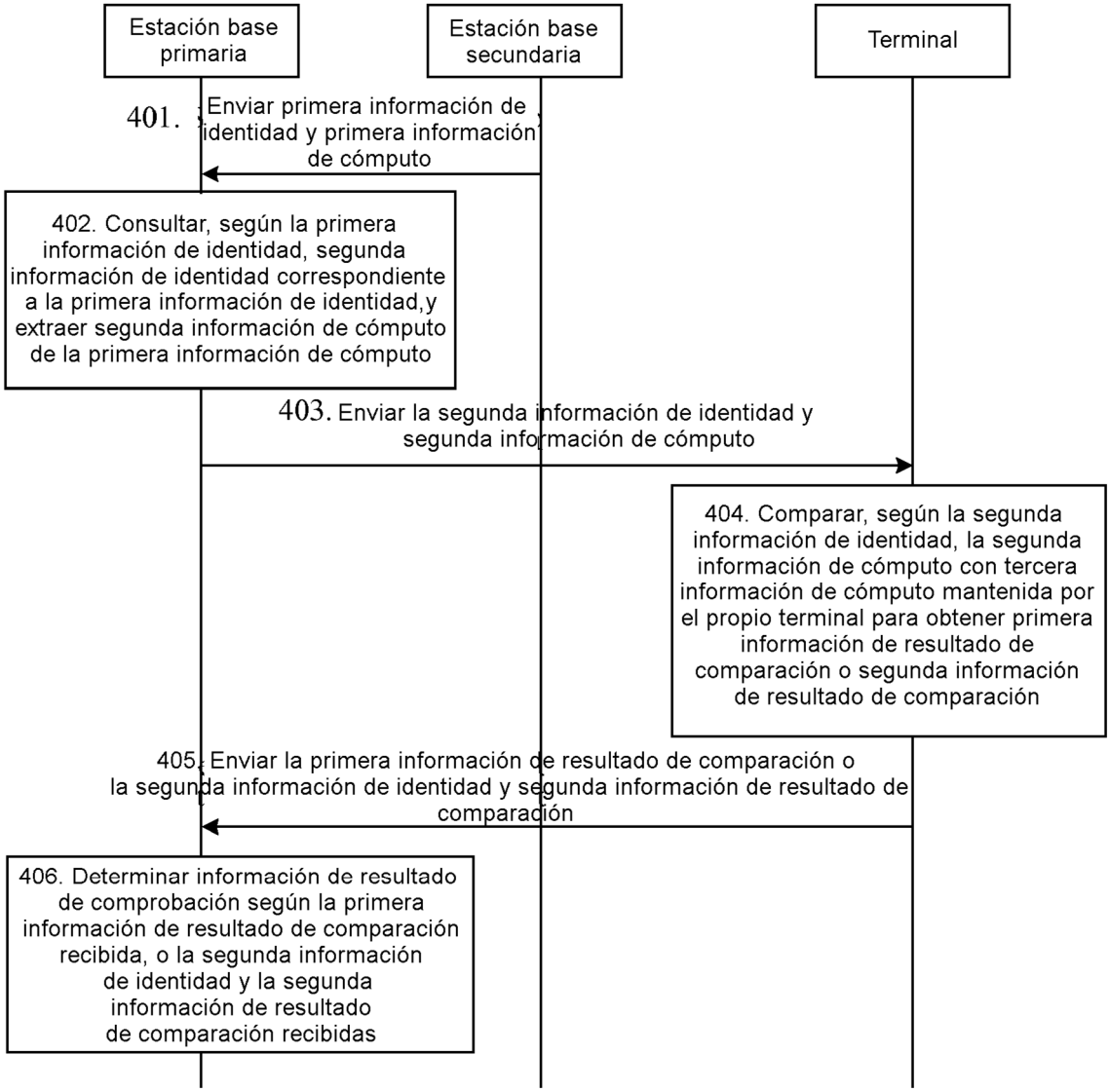
Estación base primaria
Estación base secundaria
Terminal
401. Enviar primera información de identidad y primera información de cómputo
402. Consultar, según la primera información de identidad, segunda información de identidad correspondiente a la primera información de identidad,y extraer segunda información de cómputo de la primera información de cómputo
403. Enviar la segunda información de identidad y segunda información de cómputo
404. Comparar, según la segunda información de identidad, la segunda información de cómputo con tercera información de cómputo mantenida por el propio terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación
405. Enviar la primera información de resultado de comparación o la segunda información de identidad y segunda información de resultado de comparación
406. Determinar información de resultado de comprobación según la primera información de resultado de comparación recibida, o la segunda información de identidad y la segunda información de resultado de comparación recibidas

FIG. 4

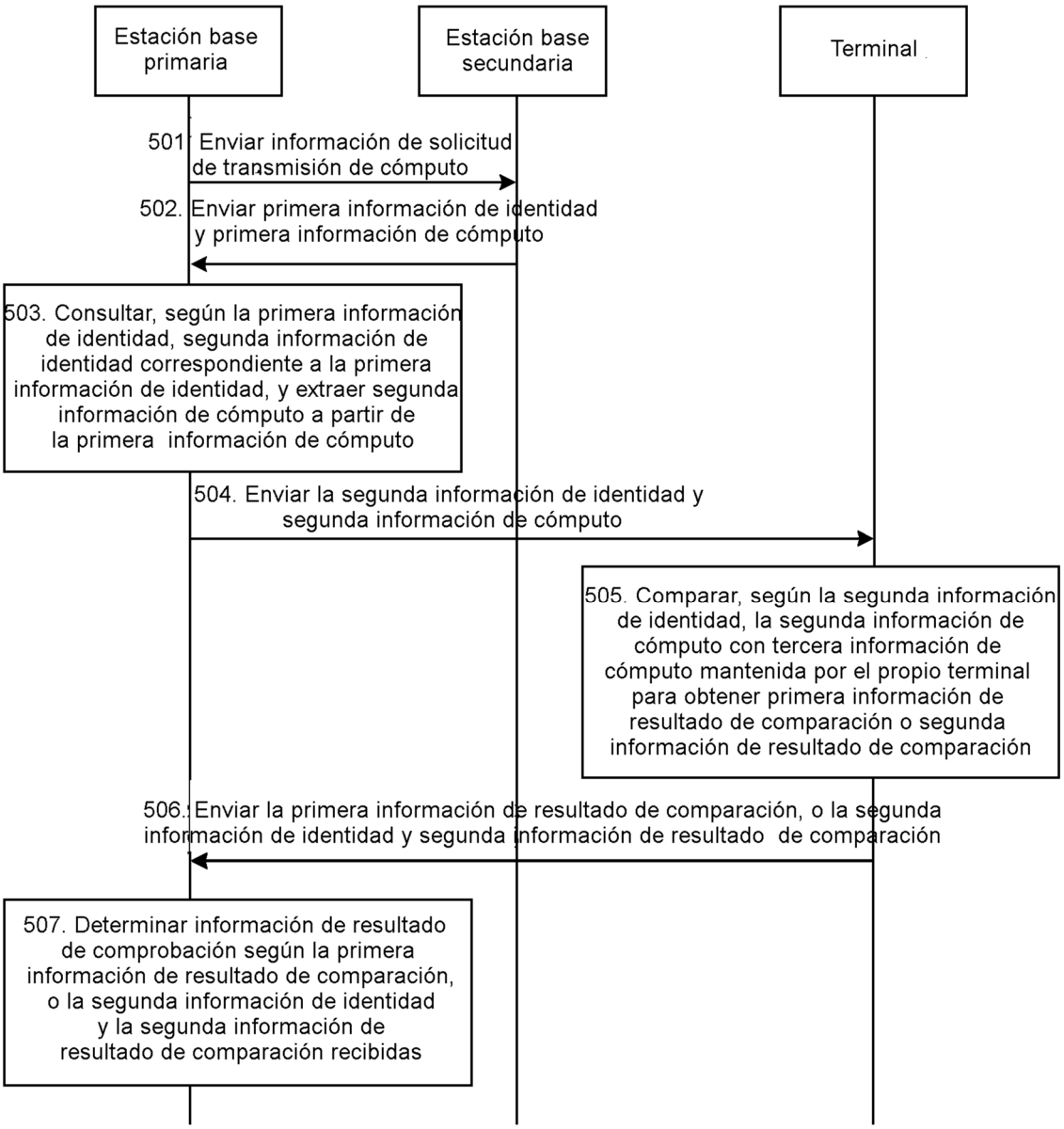
Estación base primaria
Estación base secundaria
Terminal
501. Enviar información de solicitud de transmisión de cómputo
502. Enviar primera información de identidad y primera información de cómputo
503. Consultar, según la primera información de identidad, segunda información de identidad correspondiente a la primera información de identidad, y extraer segunda información de cómputo a partir de la primera información de cómputo
504. Enviar la segunda información de identidad y segunda información de cómputo
505. Comparar, según la segunda información de identidad, la segunda información de cómputo con tercera información de cómputo mantenida por el propio terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación
506. Enviar la primera información de resultado de comparación, o la segunda información de identidad y segunda información de resultado de comparación
507. Determinar información de resultado de comprobación según la primera información de resultado de comparación, o la segunda información de identidad y la segunda información de resultado de comparación recibidas

FIG. 5

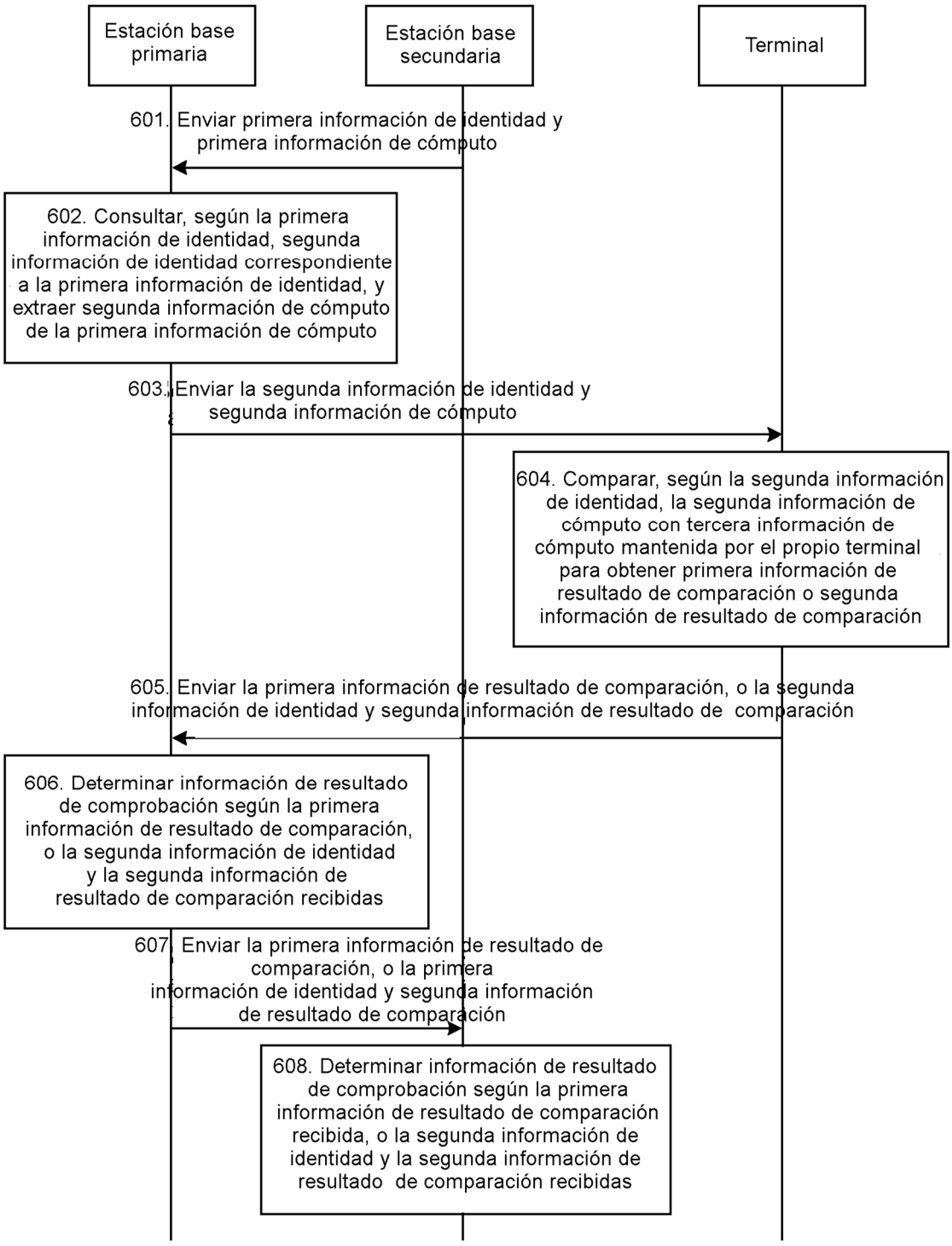
Estación base primaria
Estación base secundaria
Terminal
601. Enviar primera información de identidad y primera información de cómputo
602. Consultar, según la primera información de identidad, segunda información de identidad correspondiente a la primera información de identidad, y extraer segunda información de cómputo de la primera información de cómputo
603. Enviar la segunda información de identidad y segunda información de cómputo
604. Comparar, según la segunda información de identidad, la segunda información de cómputo con tercera información de cómputo mantenida por el propio terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación
605. Enviar la primera información de resultado de comparación, o la segunda información de identidad y segunda información de resultado de comparación
606. Determinar información de resultado de comprobación según la primera información de resultado de comparación, o la segunda información de identidad y la segunda información de resultado de comparación recibidas
607. Enviar la primera información de resultado de comparación, o la primera información de identidad y segunda información de resultado de comparación
608. Determinar información de resultado de comprobación según la primera información de resultado de comparación recibida, o la segunda información de identidad y la segunda información de resultado de comparación recibidas

FIG. 6

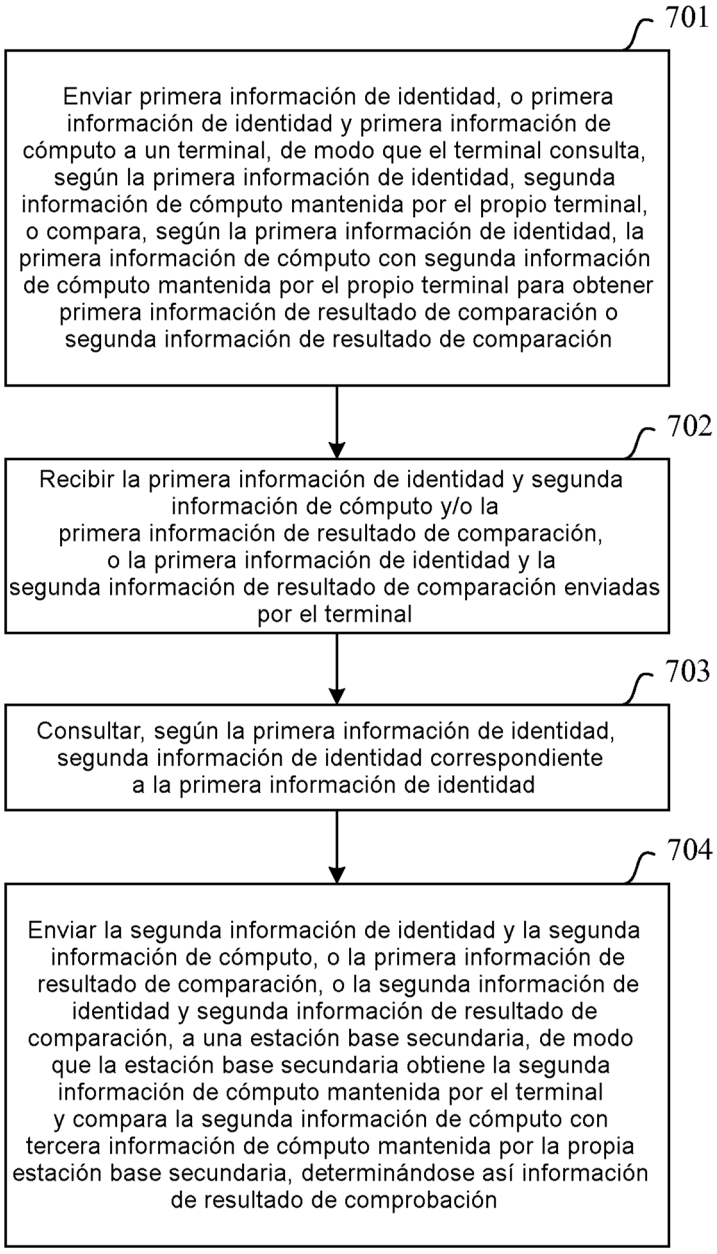
701
Enviar primera información de identidad, o primera información de identidad y primera información de cómputo a un terminal, de modo que el terminal consulta, según la primera información de identidad, segunda información de cómputo mantenida por el propio terminal, o compara, según la primera información de identidad, la primera información de cómputo con segunda información de cómputo mantenida por el propio terminal para obtener primera información de resultado de comparación o segunda información de resultado de comparación
702
Recibir la primera información de identidad y segunda información de cómputo y/o la primera información de resultado de comparación, o la primera información de identidad y la segunda información de resultado de comparación enviadas por el terminal
703
Consultar, según la primera información de identidad, segunda información de identidad correspondiente a la primera información de identidad
704
Enviar la segunda información de identidad y la segunda información de cómputo, o la primera información de resultado de comparación, o la segunda información de identidad y segunda información de resultado de comparación, a una estación base secundaria, de modo que la estación base secundaria obtiene la segunda información de cómputo mantenida por el terminal y compara la segunda información de cómputo con tercera información de cómputo mantenida por la propia estación base secundaria, determinándose así información de resultado de comprobación

FIG. 7

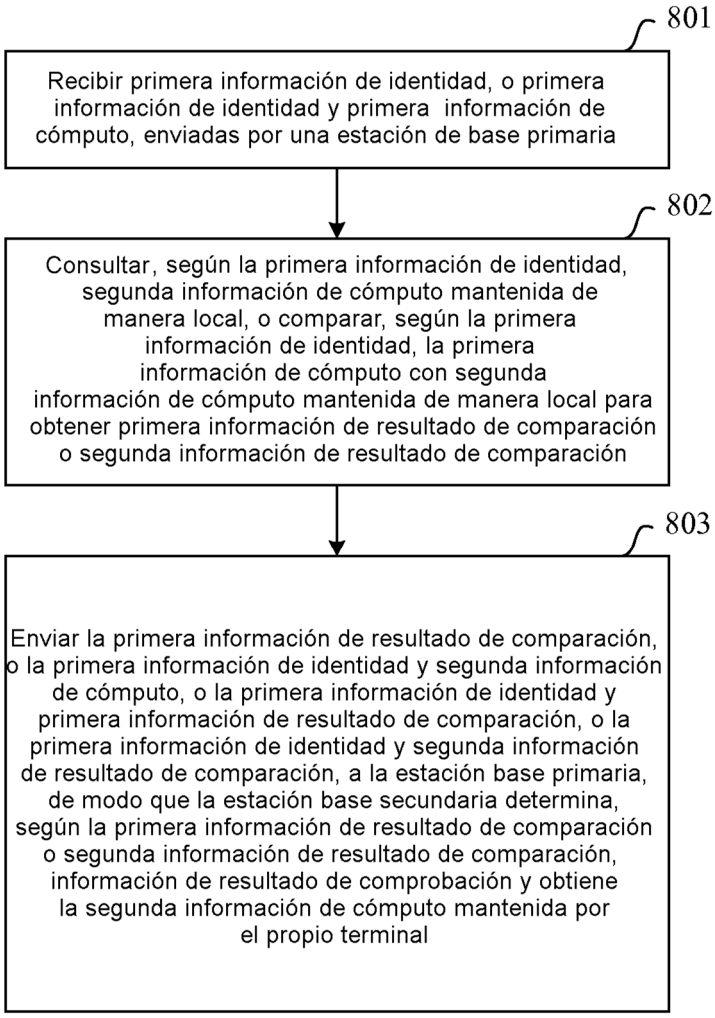
801
Recibir primera información de identidad, o primera información de identidad y primera información de cómputo, enviadas por una estación de base primaria
802
Consultar, según la primera información de identidad, segunda información de cómputo mantenida de manera local, o comparar, según la primera información de identidad, la primera información de cómputo con segunda información de cómputo mantenida de manera local para obtener primera información de resultado de comparación o segunda información de resultado de comparación
803
Enviar la primera información de resultado de comparación, o la primera información de identidad y segunda información de cómputo, o la primera información de identidad y primera información de resultado de comparación, o la primera información de identidad y segunda información de resultado de comparación, a la estación base primaria, de modo que la estación base secundaria determina, según la primera información de resultado de comparación o segunda información de resultado de comparación, información de resultado de comprobación y obtiene la segunda información de cómputo mantenida por el propio terminal

FIG. 8

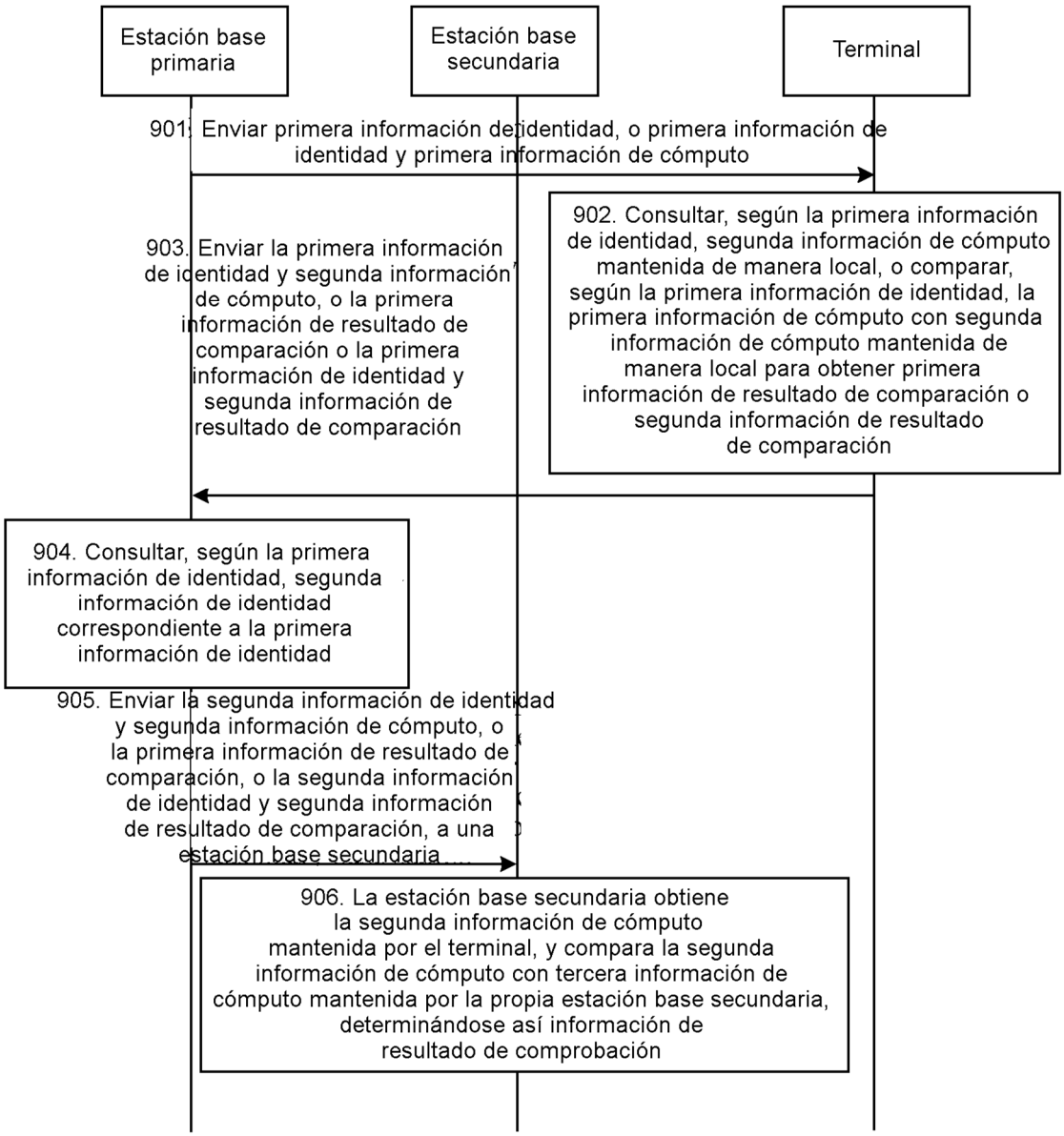
Estación base primaria
Estación base secundaria
Terminal
901. Enviar primera información de identidad, o primera información de identidad y primera información de cómputo
902. Consultar, según la primera información de identidad, segunda información de cómputo mantenida de manera local, o comparar, según la primera información de identidad, la primera información de cómputo con segunda información de cómputo mantenida de manera local para obtener primera información de resultado de comparación o segunda información de resultado de comparación
903. Enviar la primera información de identidad y segunda información de cómputo, o la primera información de resultado de comparación o la primera información de identidad y segunda información de resultado de comparación
904. Consultar, según la primera información de identidad, segunda información de identidad correspondiente a la primera información de identidad
905. Enviar la segunda información de identidad y segunda información de cómputo, o la primera información de resultado de comparación, o la segunda información de identidad y segunda información de resultado de comparación, a una estación base secundaria
906. La estación base secundaria obtiene la segunda información de cómputo mantenida por el terminal, y compara la segunda información de cómputo con tercera información de cómputo mantenida por la propia estación base secundaria, determinándose así información de resultado de comprobación

FIG. 9

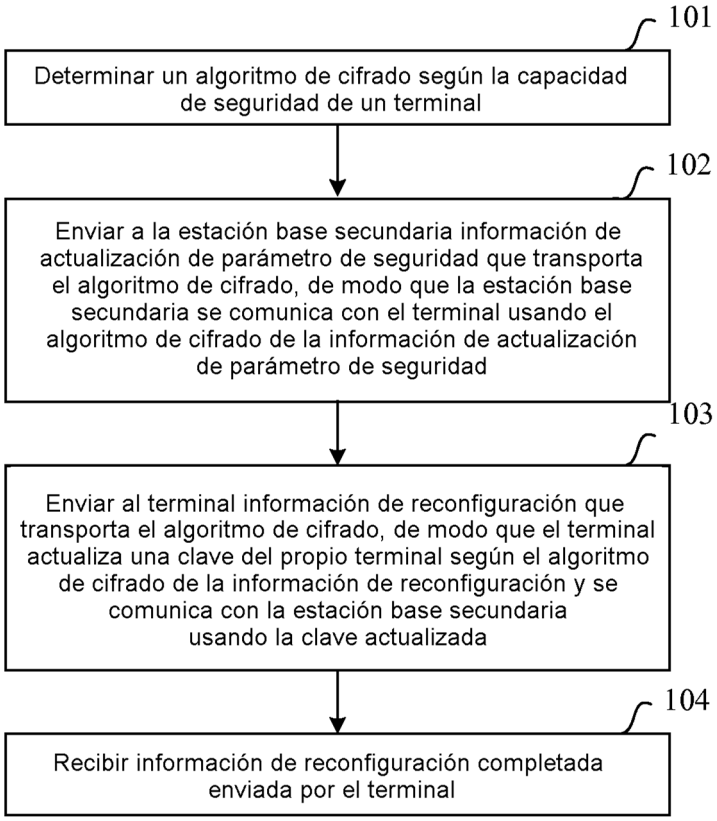
101
Determinar un algoritmo de cifrado según la capacidad de seguridad de un terminal
102
Enviar a la estación base secundaria información de actualización de parámetro de seguridad que transporta el algoritmo de cifrado, de modo que la estación base secundaria se comunica con el terminal usando el algoritmo de cifrado de la información de actualización de parámetro de seguridad
103
Enviar al terminal información de reconfiguración que transporta el algoritmo de cifrado, de modo que el terminal actualiza una clave del propio terminal según el algoritmo de cifrado de la información de reconfiguración y se comunica con la estación base secundaria usando la clave actualizada
104
Recibir información de reconfiguración completada enviada por el terminal

FIG. 10

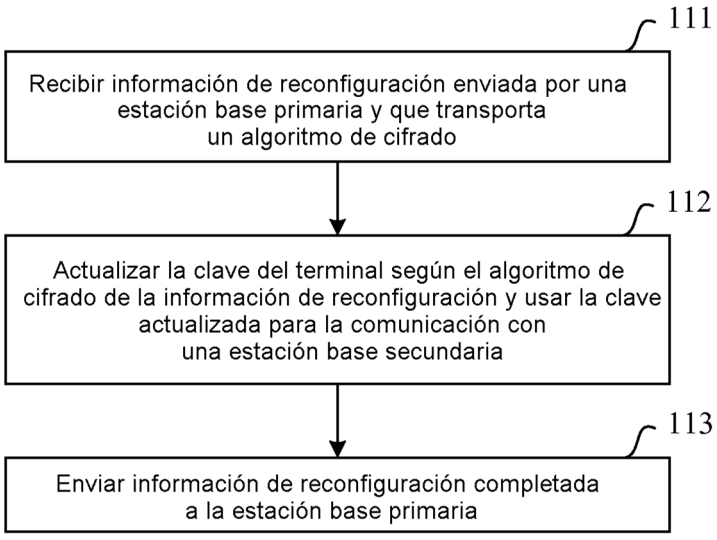
111
Recibir información de reconfiguración enviada por una estación base primaria y que transporta un algoritmo de cifrado
112
Actualizar la clave del terminal según el algoritmo de cifrado de la información de reconfiguración y usar la clave actualizada para la comunicación con una estación base secundaria
113
Enviar información de reconfiguración completada a la estación base primaria

FIG. 11

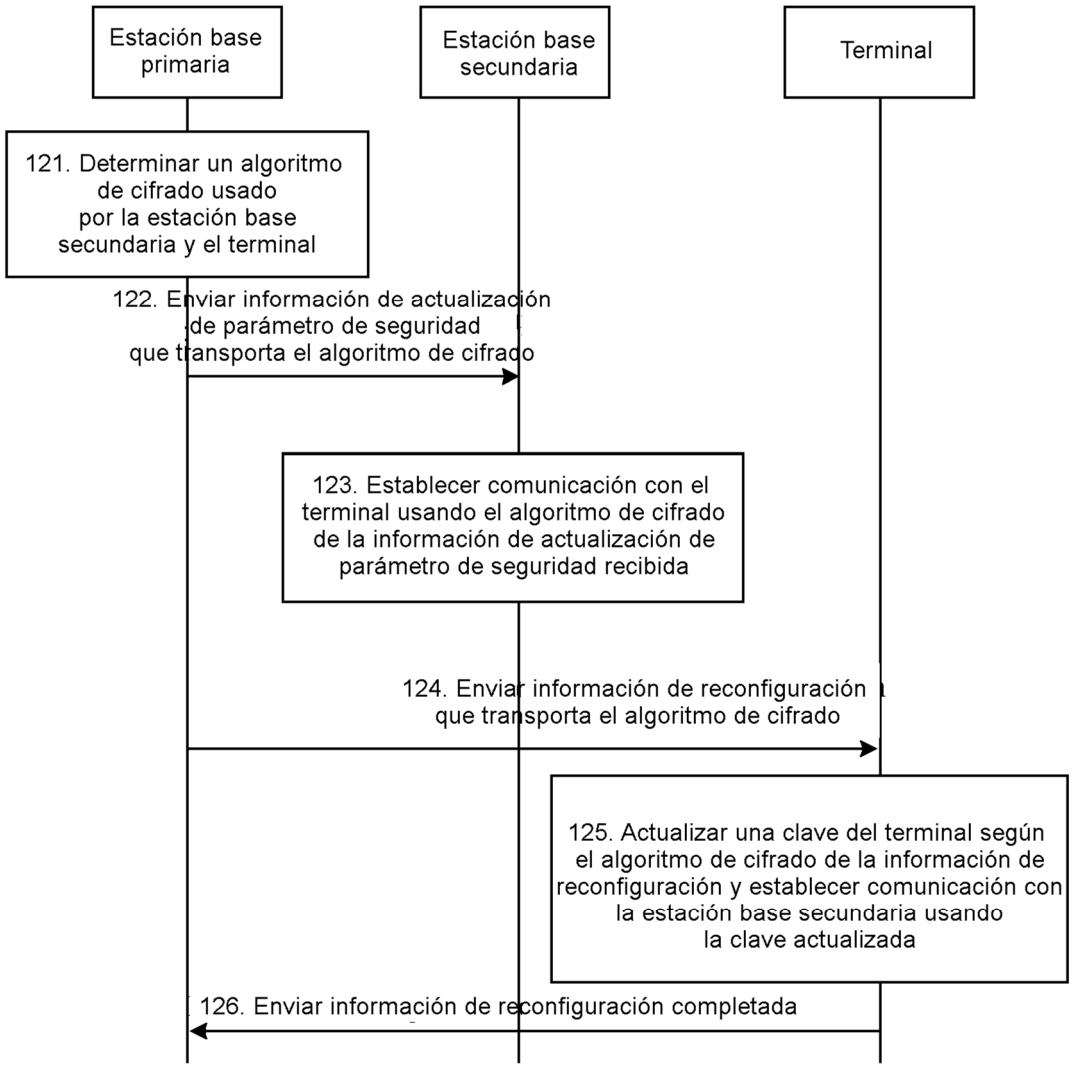
Estación base primaria
Estación base secundaria
Terminal
121. Determinar un algoritmo de cifrado usado por la estación base secundaria y el terminal
122. Enviar información de actualización de parámetro de seguridad que transporta el algoritmo de cifrado
123. Establecer comunicación con el terminal usando el algoritmo de cifrado de la información de actualización de parámetro de seguridad recibida
124. Enviar información de reconfiguración que transporta el algoritmo de cifrado
125. Actualizar una clave del terminal según el algoritmo de cifrado de la información de reconfiguración y establecer comunicación con la estación base secundaria usando la clave actualizada
126. Enviar información de reconfiguración completada

FIG. 12

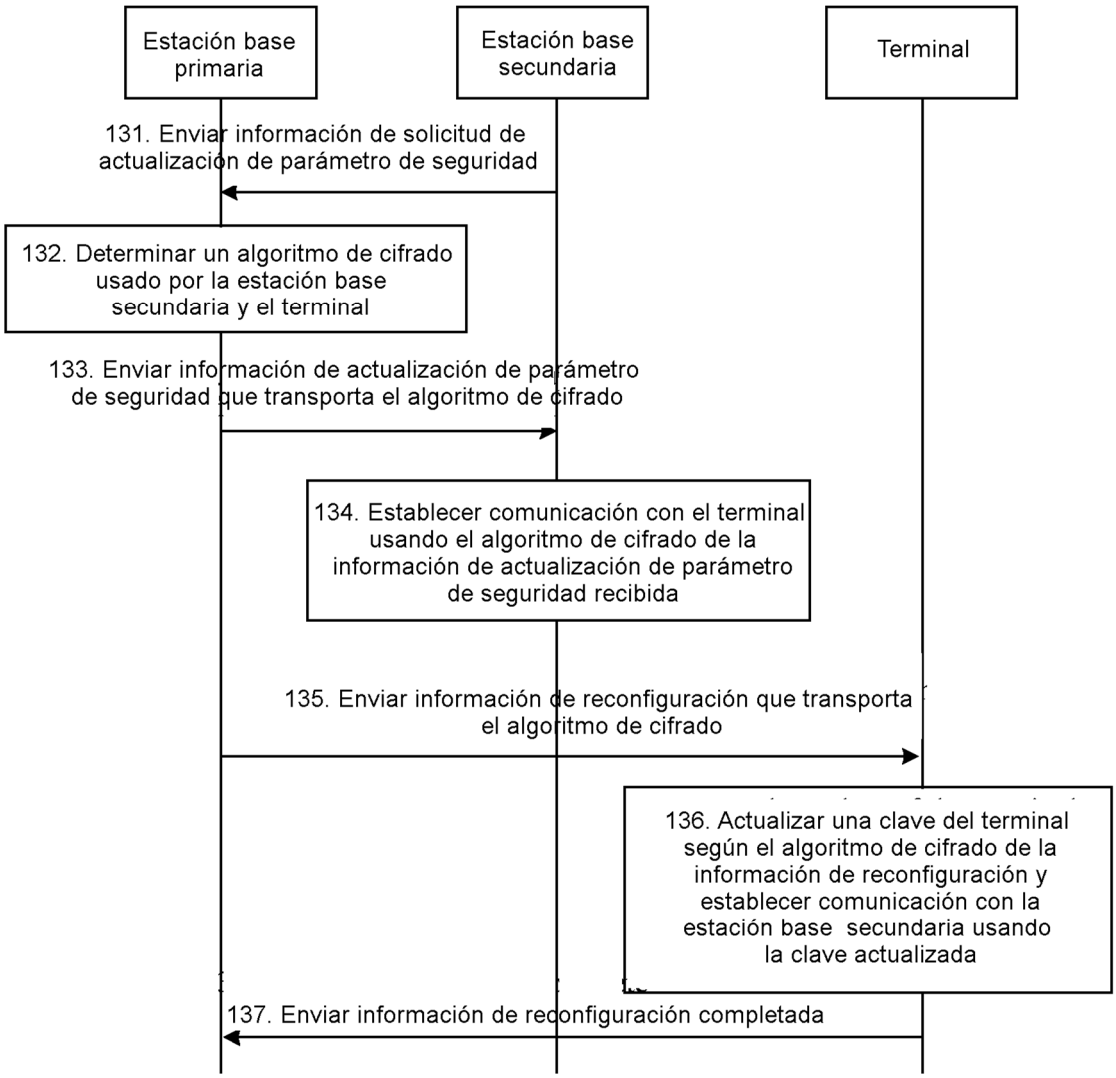
Estación base primaria
Estación base secundaria
Terminal
131. Enviar información de solicitud de actualización de parámetro de seguridad
132. Determinar un algoritmo de cifrado usado por la estación base secundaria y el terminal
133. Enviar información de actualización de parámetro de seguridad que transporta el algoritmo de cifrado
134. Establecer comunicación con el terminal usando el algoritmo de cifrado de la información de actualización de parámetro de seguridad recibida
135. Enviar información de reconfiguración que transporta el algoritmo de cifrado
136. Actualizar una clave del terminal según el algoritmo de cifrado de la información de reconfiguración y establecer comunicación con la estación base secundaria usando la clave actualizada
137. Enviar información de reconfiguración completada

FIG. 13

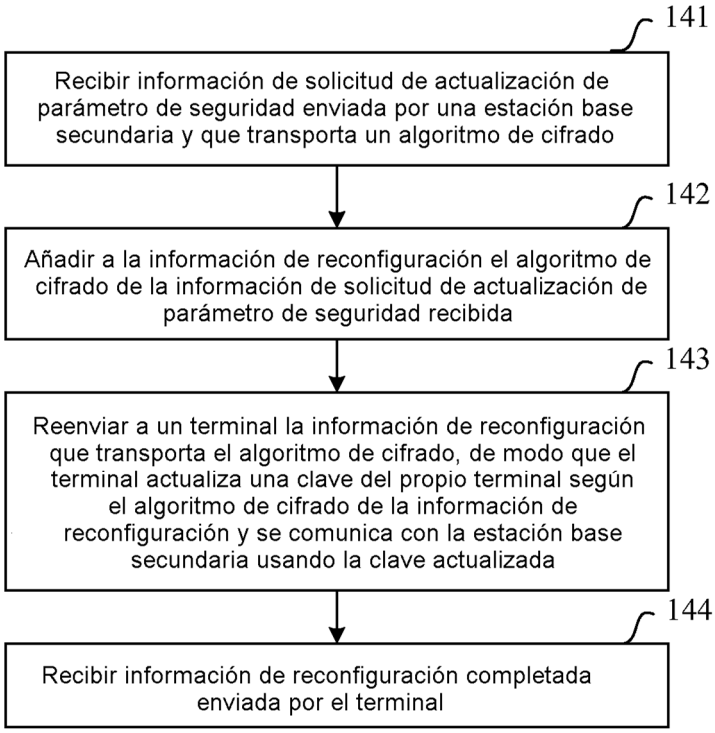
141
Recibir información de solicitud de actualización de parámetro de seguridad enviada por una estación base secundaria y que transporta un algoritmo de cifrado
142
Añadir a la información de reconfiguración el algoritmo de cifrado de la información de solicitud de actualización de parámetro de seguridad recibida
143
Reenviar a un terminal la información de reconfiguración que transporta el algoritmo de cifrado, de modo que el terminal actualiza una clave del propio terminal según el algoritmo de cifrado de la información de reconfiguración y se comunica con la estación base secundaria usando la clave actualizada
144
Recibir información de reconfiguración completada enviada por el terminal

FIG. 14

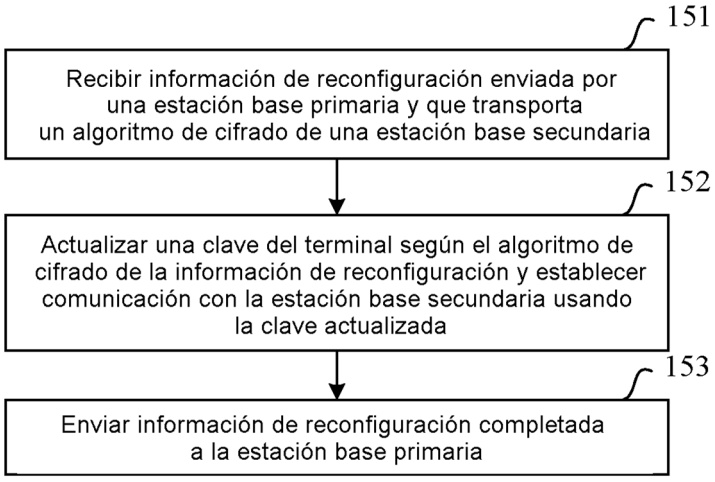
151
Recibir información de reconfiguración enviada por una estación base primaria y que transporta un algoritmo de cifrado de una estación base secundaria
152
Actualizar una clave del terminal según el algoritmo de cifrado de la información de reconfiguración y establecer comunicación con la estación base secundaria usando la clave actualizada
153
Enviar información de reconfiguración completada a la estación base primaria

FIG. 15

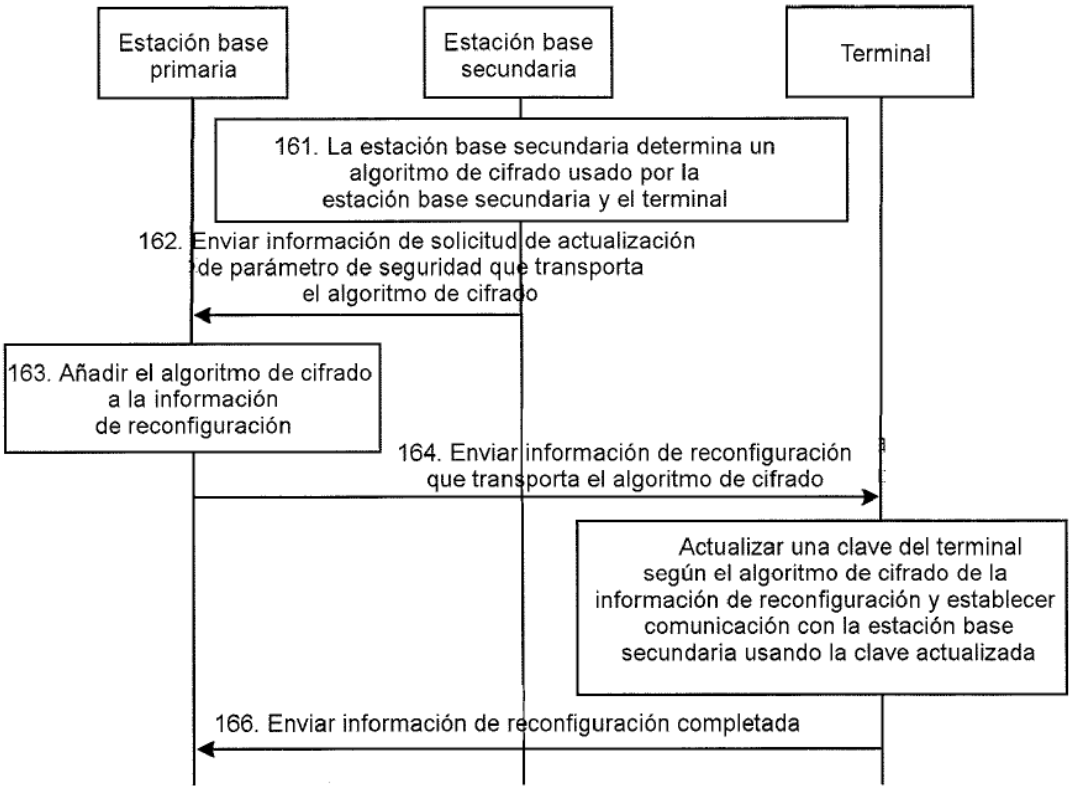
Estación base primaria
Estación base secundaria
Terminal
161. La estación base secundaria determina un algoritmo de cifrado usado por la estación base secundaria y el terminal
162. Enviar información de solicitud de actualización de parámetro de seguridad que transporta el algoritmo de cifrado
163. Añadir el algoritmo de cifrado a la información de reconfiguración
164. Enviar información de reconfiguración que transporta el algoritmo de cifrado
Actualizar una clave del terminal según el algoritmo de cifrado de la información de reconfiguración y establecer comunicación con la estación base secundaria usando la clave actualizada
166. Enviar información de reconfiguración completada

FIG. 16

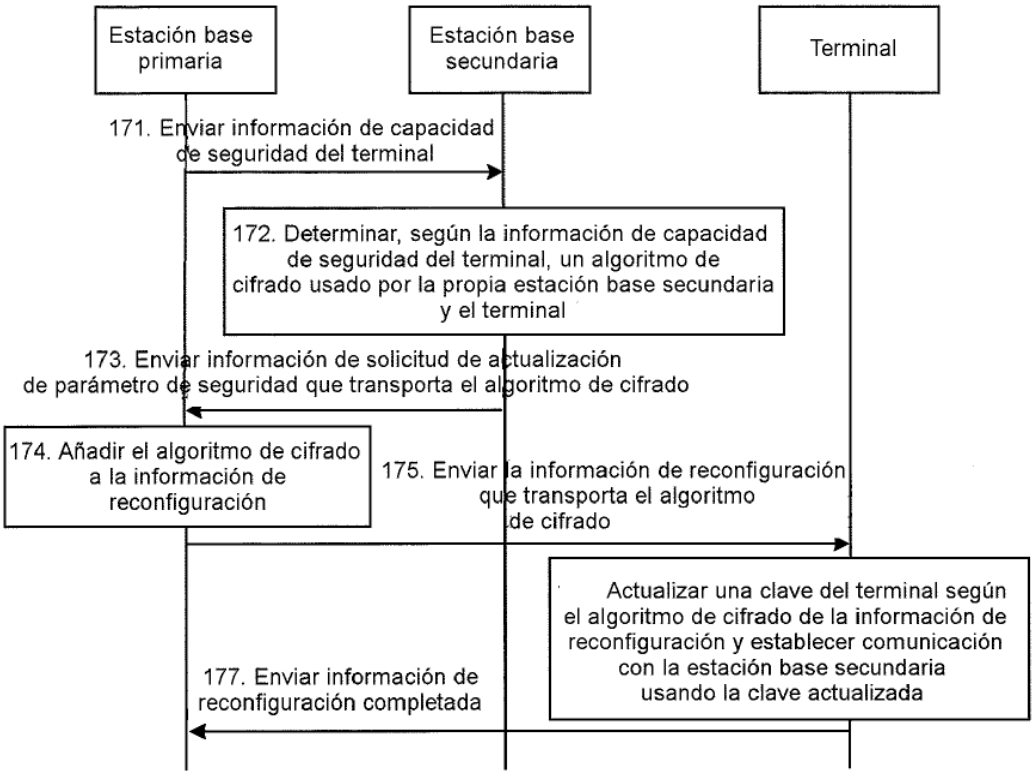
Estación base primaria
Estación base secundaria
Terminal
171. Enviar información de capacidad de seguridad del terminal
172. Determinar, según la información de capacidad de seguridad del terminal, un algoritmo de cifrado usado por la propia estación base secundaria y el terminal
173. Enviar información de solicitud de actualización de parámetro de seguridad que transporta el algoritmo de cifrado
174. Añadir el algoritmo de cifrado a la información de reconfiguración
175. Enviar la información de reconfiguración que transporta el algoritmo de cifrado
Actualizar una clave del terminal según el algoritmo de cifrado de la información de reconfiguración y establecer comunicación con la estación base secundaria usando la clave actualizada
177. Enviar información de reconfiguración completada

FIG. 17

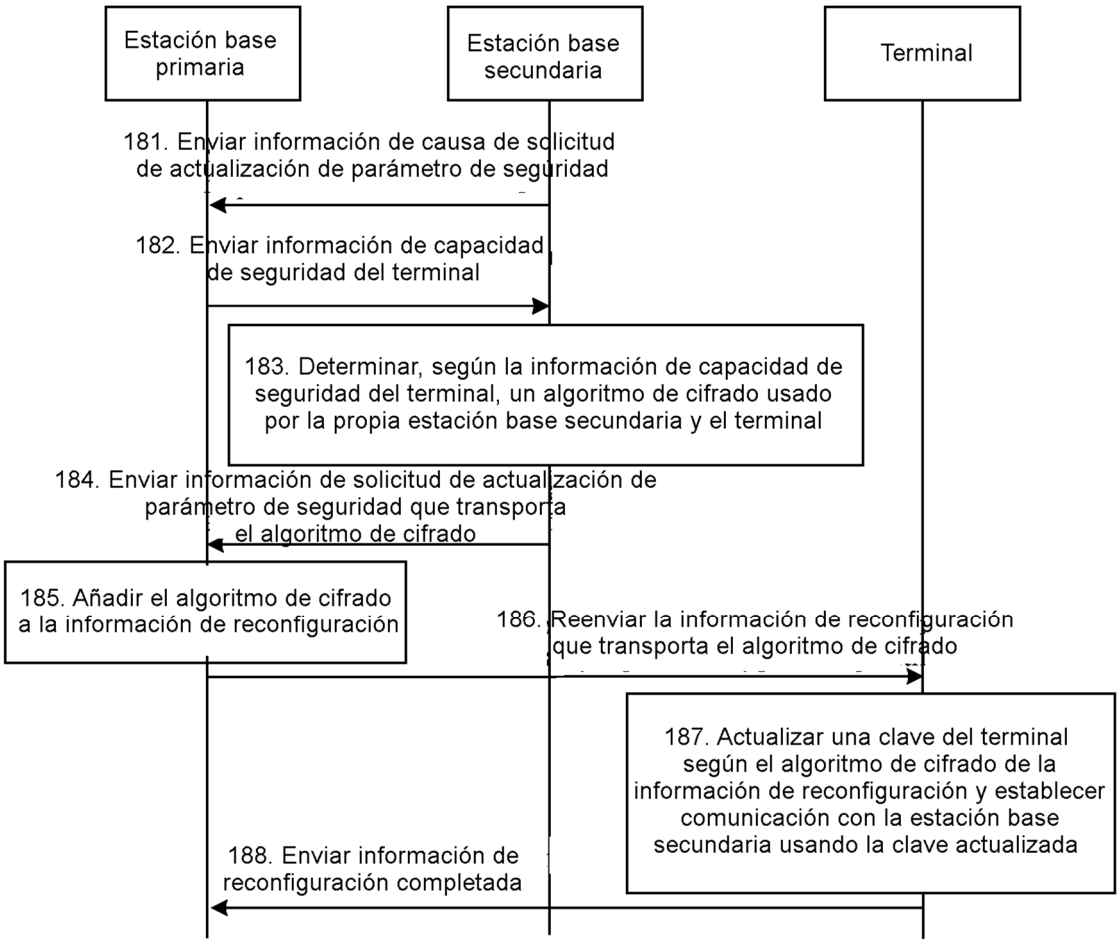
Estación base primaria
Estación base secundaria
Terminal
181. Enviar información de causa de solicitud de actualización de parámetro de seguridad
182. Enviar información de capacidad de seguridad del terminal
183. Determinar, según la información de capacidad de seguridad del terminal, un algoritmo de cifrado usado por la propia estación base secundaria y el terminal
184. Enviar información de solicitud de actualización de parámetro de seguridad que transporta el algoritmo de cifrado
185. Añadir el algoritmo de cifrado a la información de reconfiguración
186. Reenviar la información de reconfiguración que transporta el algoritmo de cifrado
187. Actualizar una clave del terminal según el algoritmo de cifrado de la información de reconfiguración y establecer comunicación con la estación base secundaria usando la clave actualizada
188. Enviar información de reconfiguración completada

FIG. 18

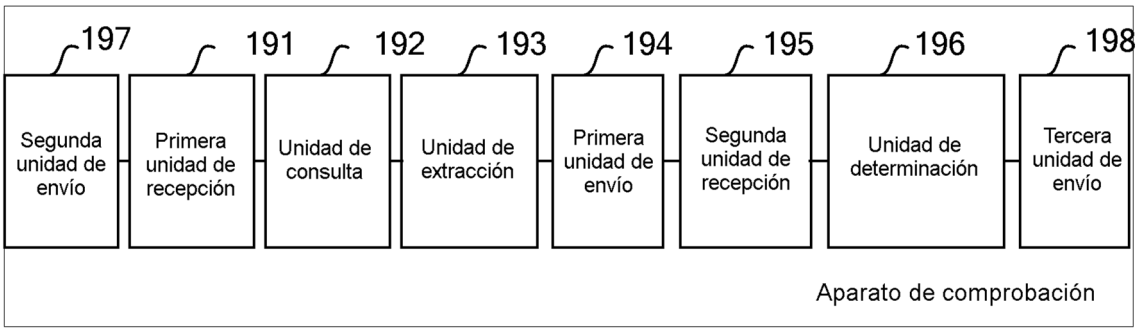
197
191
192
193
194
195
196
198
Segunda unidad de envío
Primera unidad de recepción
Unidad de consulta
Unidad de extracción
Primera unidad de envío
Segunda unidad de recepción
Unidad de determinación
Tercera unidad de envío
Aparato de comprobación

FIG. 19

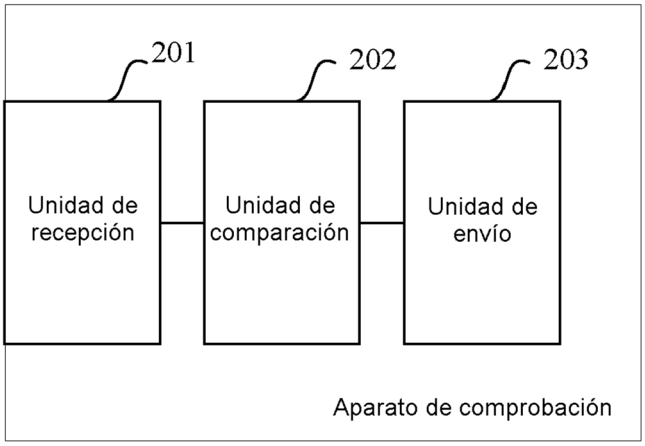
201
202
203
Unidad de recepción
Unidad de comparación
Unidad de envío
Aparato de comprobación

FIG. 20

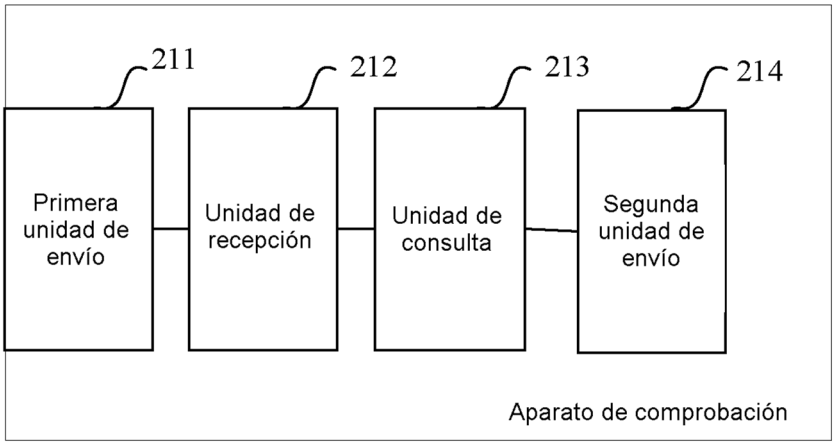
211
212
213
214
Primera unidad de envío
Unidad de recepción
Unidad de consulta
Segunda unidad de envío
Aparato de comprobación

FIG. 21

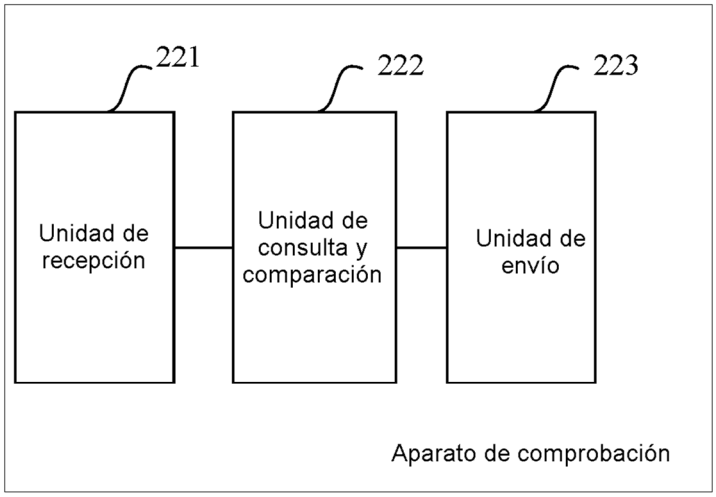
221
222
223
Unidad de recepción
Unidad de consulta y comparación
Unidad de envío
Aparato de comprobación

FIG. 22

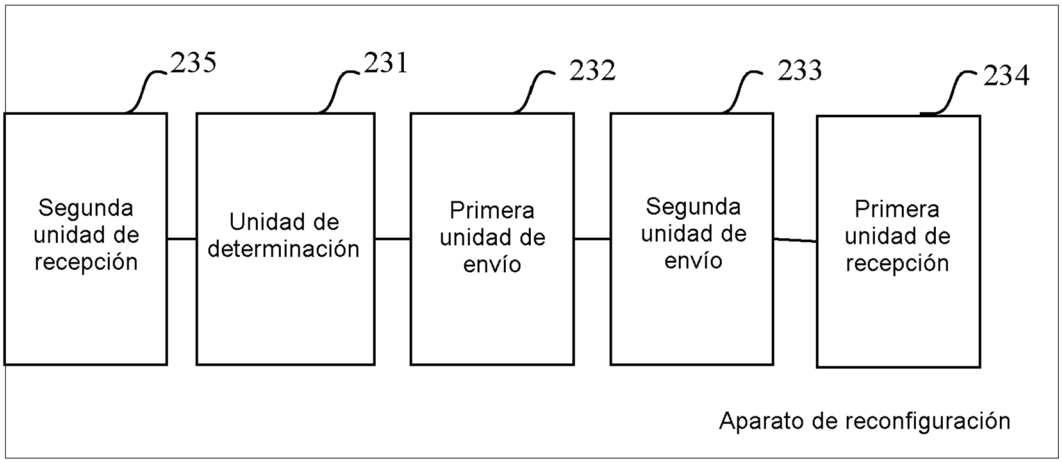
235
231
232
233
234
Segunda unidad de recepción
Unidad de determinación
Primera unidad de envío
Segunda unidad de envío
Primera unidad de recepción
Aparato de reconfiguración

FIG. 23

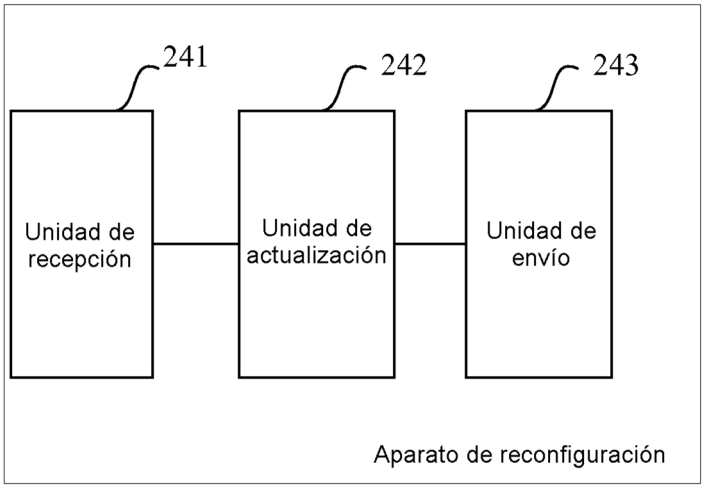
241
242
243
Unidad de recepción
Unidad de actualización
Unidad de envío
Aparato de reconfiguración

FIG. 24

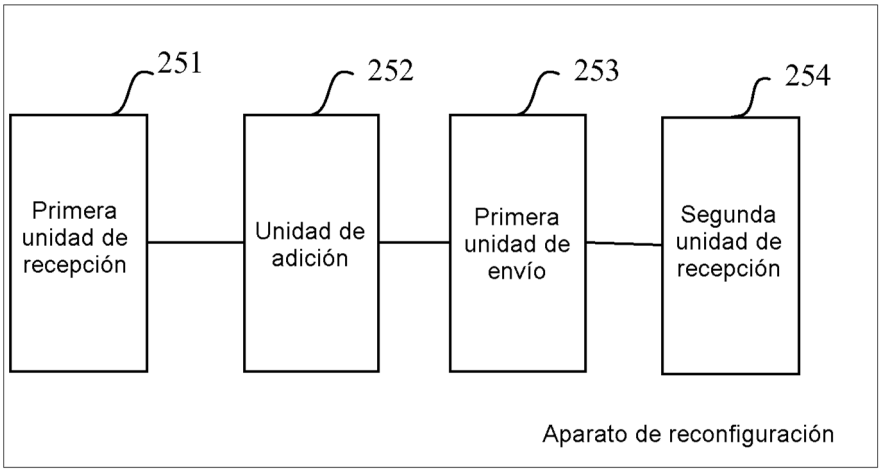
251
252
253
254
Primera unidad de recepción
Unidad de adición
Primera unidad de envío
Segunda unidad de recepción
Aparato de reconfiguración

FIG. 25

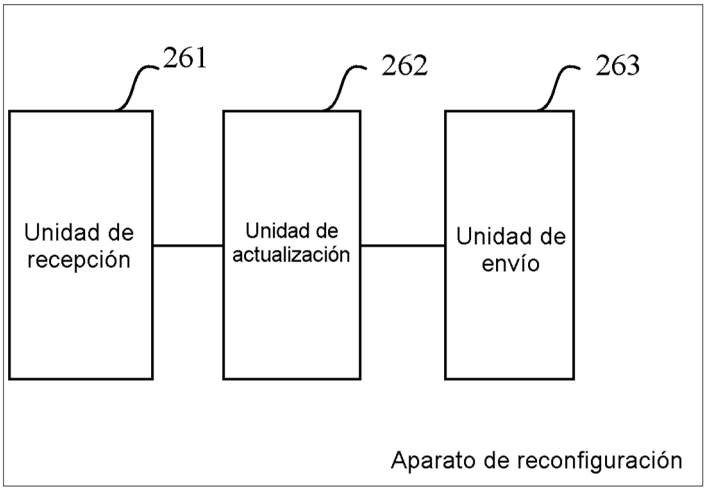
261
262
263
Unidad de recepción
Unidad de actualización
Unidad de envío
Aparato de reconfiguración

FIG. 26

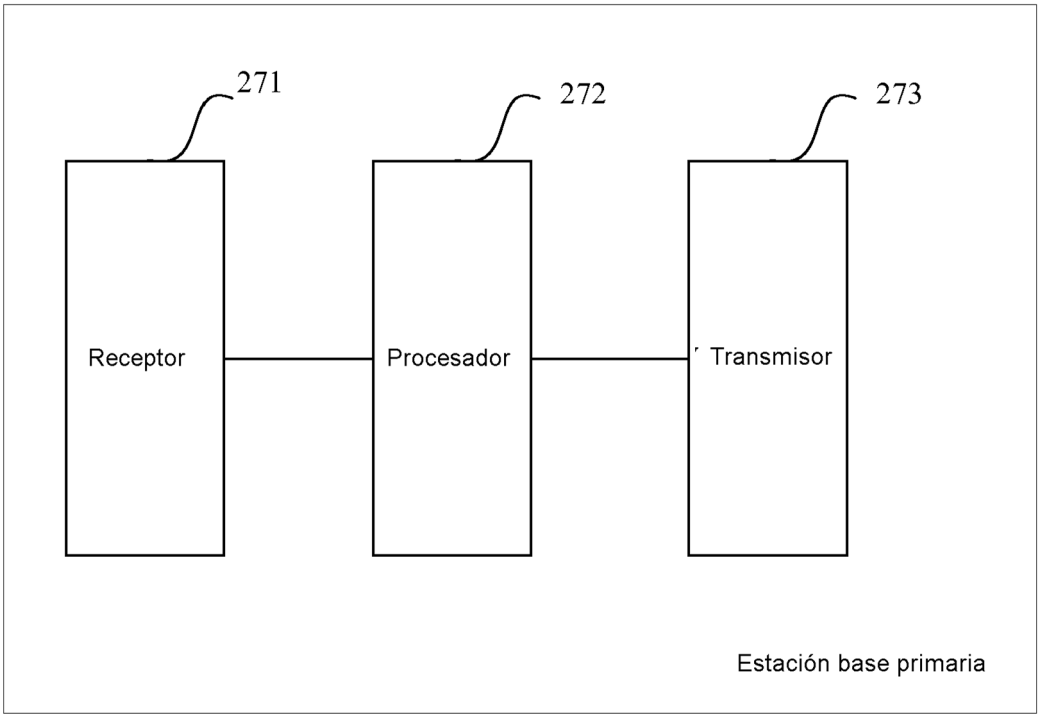
271
272
273
Receptor
Procesador
Transmisor
Estación base primaria

FIG. 27

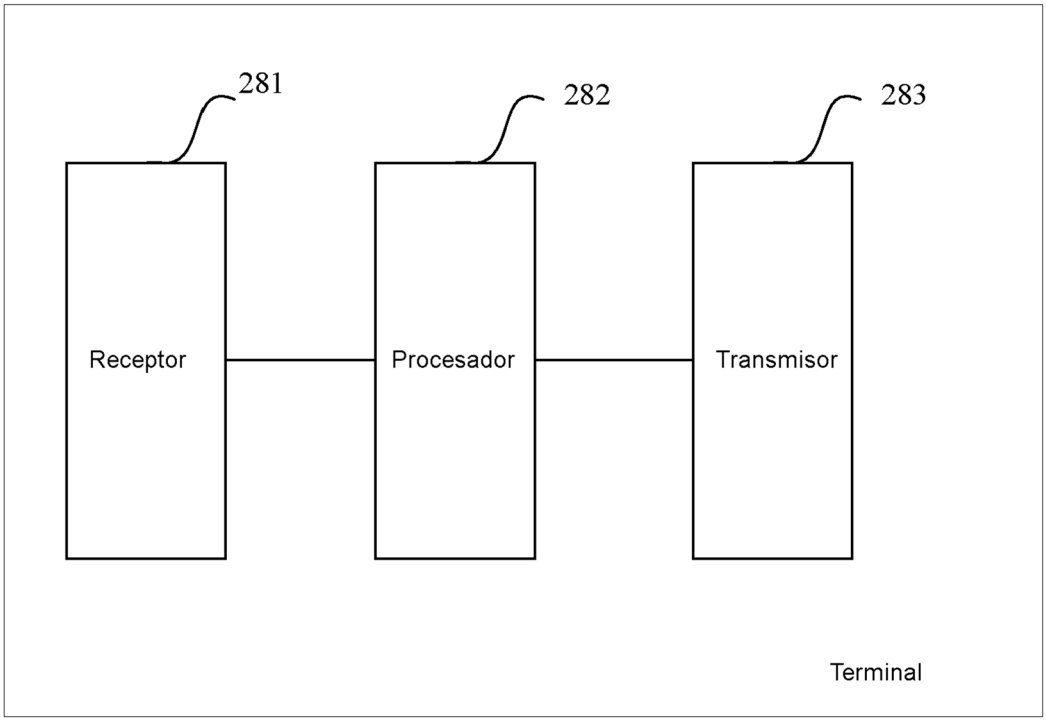
281
282
283
Receptor
Procesador
Transmisor
Terminal

FIG. 28

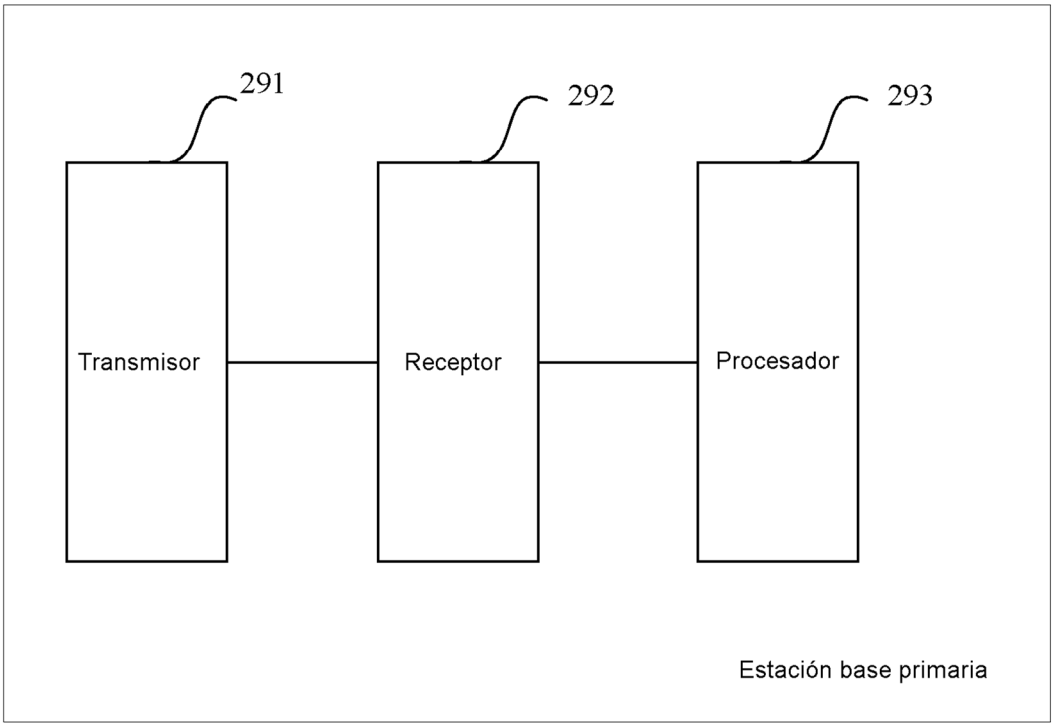
291
292
293
Transmisor
Receptor
Procesador
Estación base primaria

FIG. 29

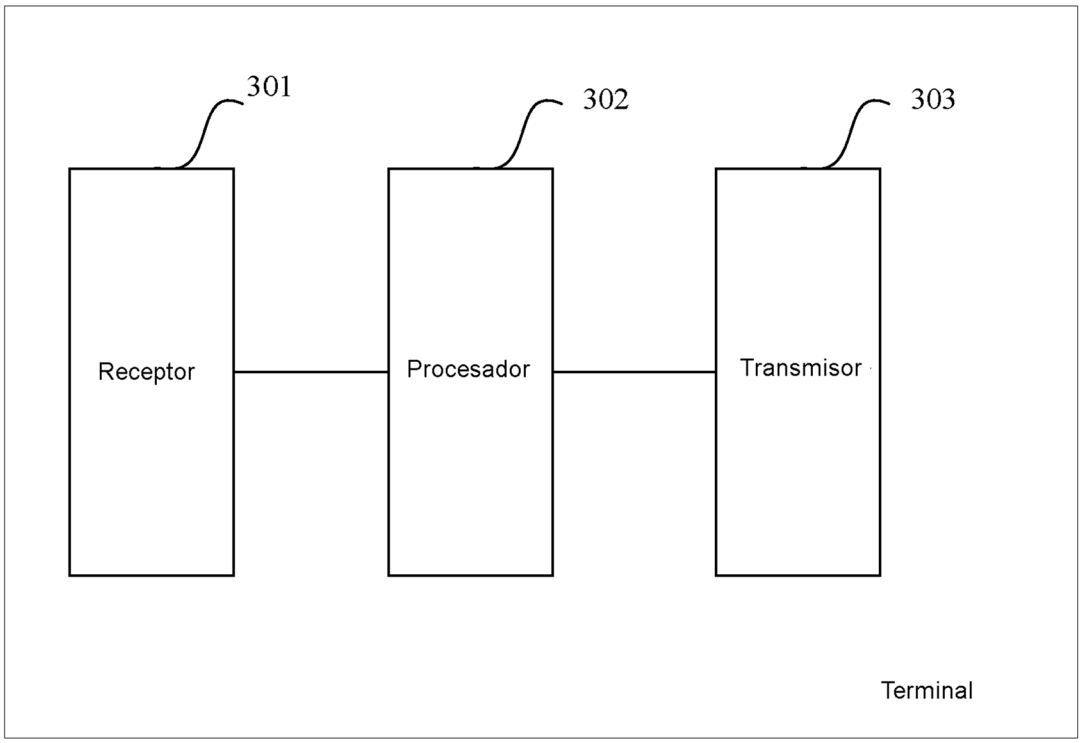
301
302
303
Receptor
Procesador
Transmisor
Terminal

FIG. 30

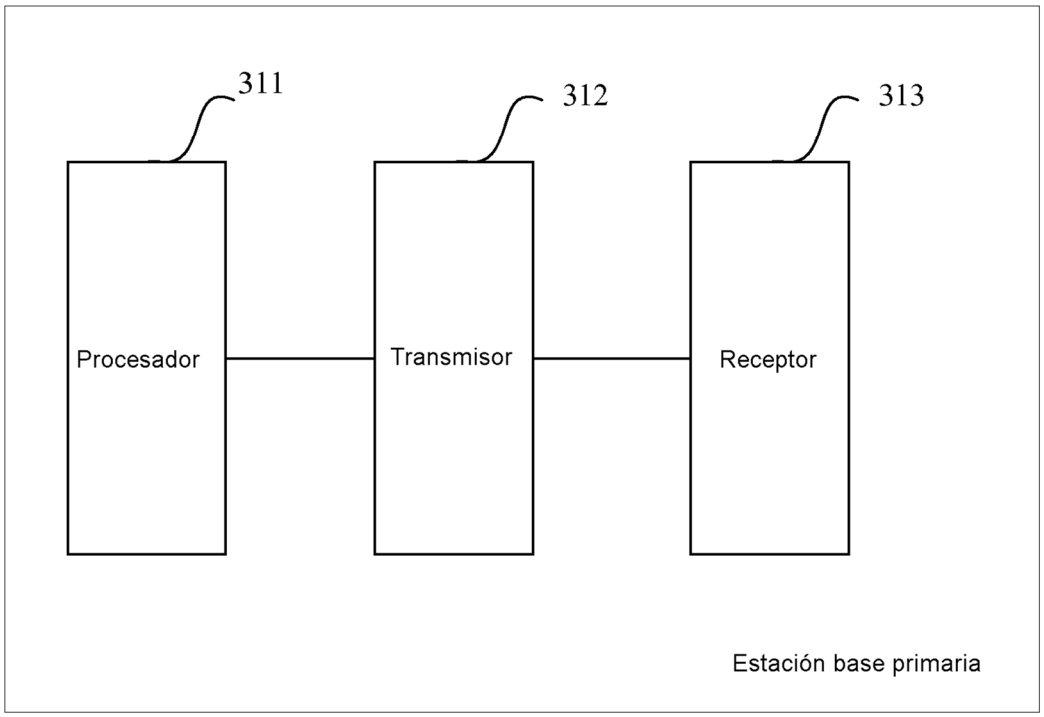
311
312
313
Procesador
Transmisor
Receptor
Estación base primaria

FIG. 31

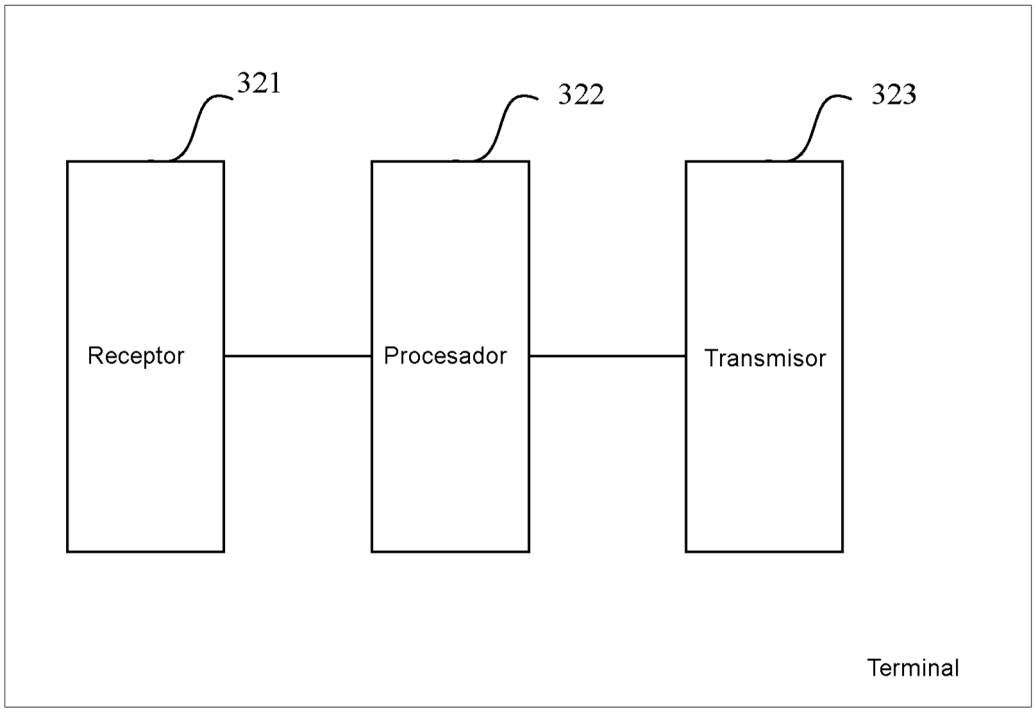
321
322
323
Receptor
Procesador
Transmisor
Terminal

FIG. 32

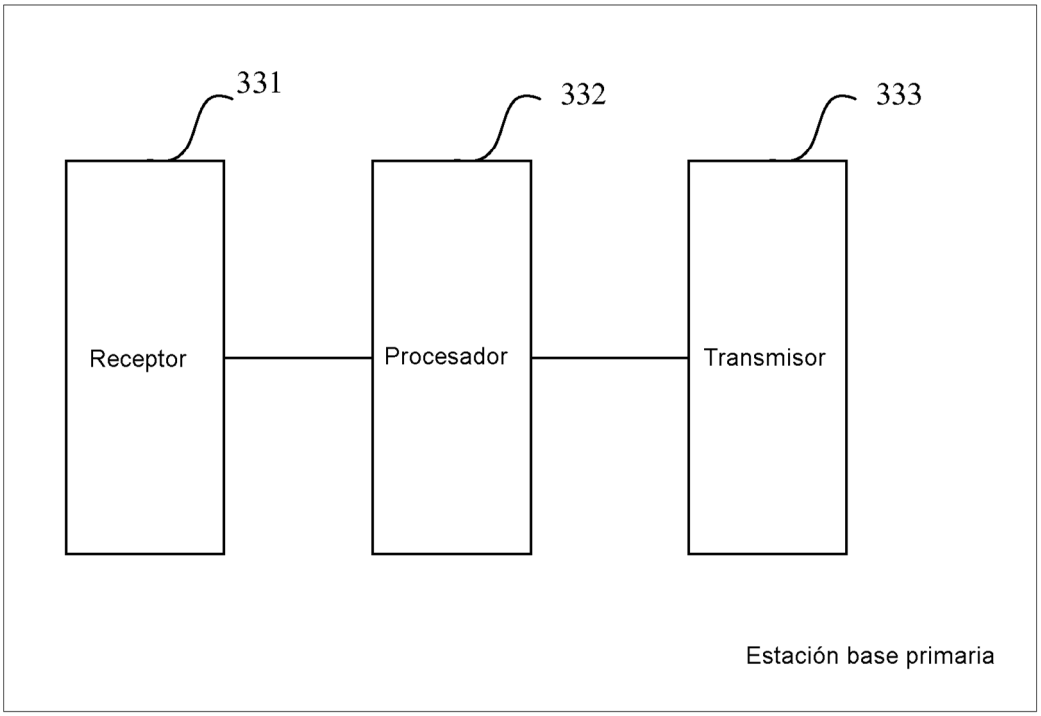
331
332
333
Receptor
Procesador
Transmisor
Estación base primaria

FIG. 33

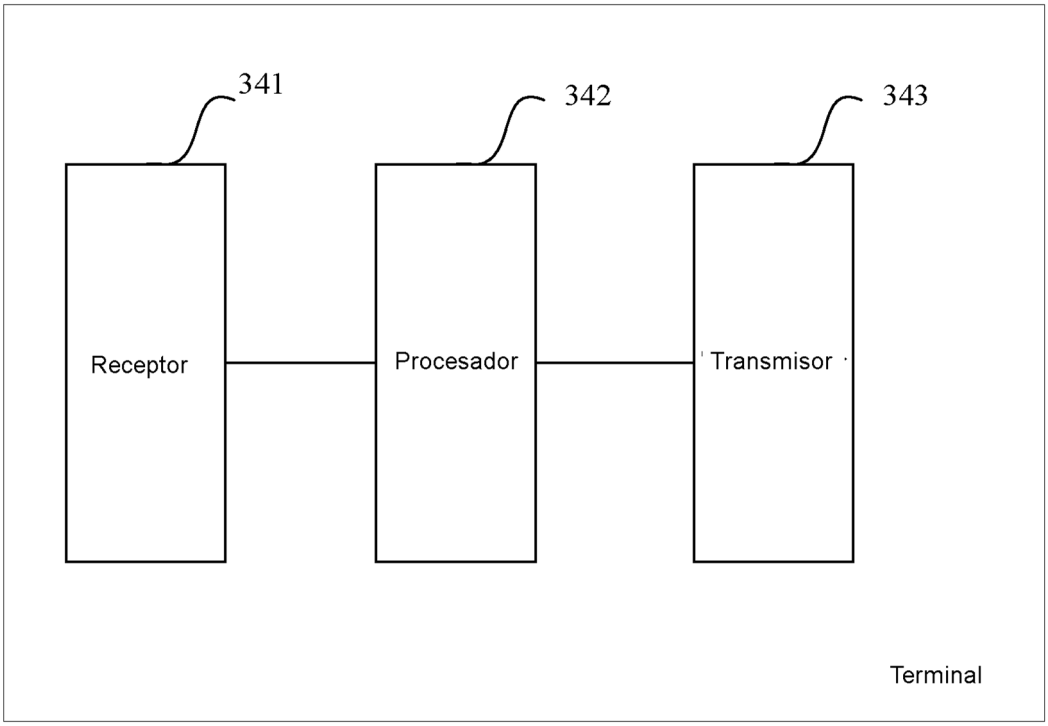

FIG. 34