(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 911 555**

(51) Int. CI.:

H04W 12/102 (2011.01)
H04W 12/104 (2011.01)
H04W 12/106 (2011.01)
H04L 29/06 (2006.01)
H04W 88/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **27.04.2018 PCT/CN2018/084820**

(87) Fecha y número de publicación internacional: **01.11.2018 WO18196852**

(96) Fecha de presentación y número de la solicitud europea: **27.04.2018 E 18791933 (7)**

(97) Fecha y número de publicación de la concesión europea: **23.03.2022 EP 3618480**

(54) Título: **Método de verificación de integridad, terminal y dispositivo de red**

(30) Prioridad:

28.04.2017 CN 201710297656

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.05.2022

(73) Titular/es:

VIVO MOBILE COMMUNICATION CO., LTD. (100.0%)
283 BBK Road, Wusha
Chang'An, Dongguan, Guangdong 523860, CN

(72) Inventor/es:

YANG, XIAODONG

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método de verificación de integridad, terminal y dispositivo de red

Campo técnico

La presente descripción se refiere a la tecnología de comunicación inalámbrica, en particular a un método de verificación de integridad, un terminal y un equipo del lado de la red.

Antecedentes

Actualmente, en el campo de la comunicación inalámbrica, con una mayor demanda en la seguridad de la comunicación, se ha vuelto cada vez más importante mejorar las medidas de seguridad durante la comunicación. Las medidas de seguridad aplicadas en los sistemas de comunicación convencionales incluyen principalmente autenticación, cifrado y verificación de integridad.

En un sistema de Evolución a Largo Plazo (LTE), un mensaje de control de recursos de radio (RRC) se cifra antes de la transmisión. Mientras tanto, se realiza una verificación de integridad adicional en el mensaje de RRC para evitar la alteración de datos.

Sin embargo, en un sistema LTE, durante la transmisión y recepción de datos del plano de usuario, solo se realiza el cifrado y descifrado de los datos del plano de usuario, por lo que no se puede garantizar la seguridad de los datos del plano de usuario.

El documento EP 2 528 369 A1 describe un método y un sistema para realizar la protección de la integridad. El método incluye: se restablece una conexión de radio entre una estación base y un terminal, y la estación base notifica al terminal la información de configuración de protección de integridad incluida en una primera señalización de reconfiguración de la conexión de Control de Recursos de Radio (RRC) después de que se restablece la conexión de radio.

El documento US 2017/005795 A1 describe un método de generación de claves, un eNodoB maestro, un eNodoB secundario y un UE. El método de generación de claves incluye: determinar un parámetro clave correspondiente a una portadora de radio de datos DRB; enviar el parámetro clave al UE correspondiente a la DRB, para que el UE genere una clave del plano de usuario según el parámetro clave y una clave básica generada por el UE; recibir una clave básica generada por un eNodoB maestro y enviada por el eNodoB maestro; y generar la clave del plano de usuario según el parámetro clave y la clave básica generada por el eNodoB maestro.

El documento US 2011/188408 A1 describe un método para aplicar selectivamente una función PDCP en un Sistema Universal de Telecomunicaciones Móviles Evolucionado (E-UMTS) evolucionado a partir de un UMTS, Sistema de Evolución a Largo Plazo (LTE) o sistema LTE-Avanzado (LTE-A).

Compendio

La invención se define en las reivindicaciones.

Con el método de verificación de integridad, el terminal y el equipo del lado de la red proporcionado por las realizaciones de la presente descripción, habiendo recibido los datos del plano de usuario transmitidos por el equipo del lado de la red, el terminal realiza una verificación de integridad en los datos del plano de usuario recibidos del equipo del lado de la red basado en la información de configuración de verificación de integridad del plano de usuario, para determinar si los datos del plano de usuario están alterados, mejorando así la seguridad de los datos del plano de usuario.

Breve descripción de los dibujos

Para describir más claramente las soluciones técnicas de la presente descripción o de la técnica relacionada, a continuación se describen brevemente los dibujos adjuntos necesarios para describir las realizaciones o la técnica relacionada. Aparentemente, los dibujos que acompañan a la siguiente descripción muestran solo algunas realizaciones de la presente descripción, y una persona con experiencia ordinaria en la técnica puede derivar otros dibujos de estos dibujos adjuntos sin esfuerzos creativos.

La Fig. 1 es una vista esquemática de una arquitectura de sistema para un método de verificación de integridad proporcionado por la presente descripción;

La Fig. 2 es una vista esquemática de una arquitectura de sistema para un método de verificación de integridad proporcionado por la presente descripción;

La Fig. 3 es un diagrama de flujo esquemático de un método de verificación de integridad proporcionado por una realización de la presente descripción;

La Fig. 4 es un diagrama de flujo esquemático de un método de verificación de integridad proporcionado por una realización de la presente descripción;

La Fig. 5 es un diagrama de flujo de un método de verificación de integridad proporcionado por una realización de la presente descripción;

La Fig. 6 es un diagrama de flujo de un método de verificación de integridad proporcionado por una realización de la presente descripción;

La Fig. 7 es un diagrama de flujo de un método de verificación de integridad proporcionado por una realización de la presente descripción;

La Fig. 8 es un diagrama estructural esquemático de un terminal proporcionado por una realización de la presente descripción;

La Fig. 9 es un diagrama estructural esquemático de un terminal proporcionado por una realización de la presente descripción;

La Fig. 10 es un diagrama estructural esquemático del equipo del lado de la red proporcionado por una realización de la presente descripción;

La Fig. 11 es un diagrama estructural esquemático del equipo del lado de la red proporcionado por una realización de la presente descripción;

La Fig. 12 es un diagrama estructural esquemático de un terminal proporcionado por otra realización de la presente descripción;

La Fig. 13 es un diagrama estructural esquemático del equipo del lado de la red proporcionado por otra realización de la presente descripción.

Descripción detallada

Para que el objetivo, las soluciones técnicas y las ventajas de la presente descripción sean más claros, las soluciones técnicas en las realizaciones de esta descripción se describen clara y completamente junto con los dibujos en las realizaciones de esta descripción. Aparentemente, las realizaciones descritas son simplemente una parte en lugar de todas las realizaciones de esta descripción. Todas las demás realizaciones obtenidas por un experto en la materia basándose en las realizaciones de esta descripción sin ningún esfuerzo creativo se encuentran dentro del alcance de protección de esta descripción.

Los términos "comprenden", "incluyen", "tienen" y cualquier variación de los mismos en la especificación y las reivindicaciones de la presente descripción pretenden cubrir un significado de inclusión no exclusivo, de modo que un proceso, un método, un sistema, un producto, o un dispositivo que incluye una serie de pasos o unidades no solo incluye los pasos o unidades enumerados expresamente, sino que también puede incluir otros pasos o unidades no enumerados expresamente o incluir pasos o unidades inherentes al proceso, el método, el producto o el dispositivo.

La Fig. 1 es una primera vista esquemática de una arquitectura de sistema para un método de verificación de integridad proporcionado por la presente descripción. Como se muestra en la Fig. 1, la arquitectura del sistema proporcionada por esta realización incluye un equipo del lado de la red y un terminal.

El equipo del lado de la red puede ser una estación transceptora base (BTS) en un sistema global de comunicación móvil (GSM) o un sistema de acceso múltiple por división de código (CDMA), o un NodoB (NB) en un sistema de acceso múltiple por división de código de banda ancha (WCDMA), o un Nodo B evolucionado (eNB o eNodoB) en un sistema LTE, o una estación base en un nuevo sistema técnico de acceso de radio (Nueva RAT o NR), o una estación repetidora o punto de acceso, o una estación base en un futura red 5G, o similar, y no se limita en este documento.

El terminal puede ser un terminal inalámbrico o un terminal con cable. Un terminal inalámbrico puede referirse a un dispositivo utilizado para proporcionar voz y/u otro servicio de conectividad de datos a un usuario, un dispositivo de mano con una función de conexión inalámbrica u otro dispositivo de procesamiento conectado a un módem inalámbrico. Un terminal inalámbrico puede comunicarse con una o más redes centrales a través de una red de acceso por radio (RAN). El terminal inalámbrico puede ser un terminal móvil, como un teléfono móvil (también llamado teléfono celular) o un ordenador equipado con un terminal móvil, como un dispositivo móvil portátil, de bolsillo, de mano, integrado en un ordenador o montado en un vehículo, que intercambia voz y/o datos con la red de acceso por radio. Por ejemplo, puede ser un teléfono de servicio de comunicación personal (PCS), un teléfono inalámbrico, un teléfono de protocolo de inicio de sesión (SIP), una estación de bucle local inalámbrico (WLL), un asistente digital personal (PDA) o similar. Un terminal inalámbrico también puede denominarse sistema, unidad de abonado, estación de abonado, estación móvil, móvil, estación remota, terminal remoto, terminal de acceso, terminal de usuario, agente de usuario o un dispositivo de usuario o equipo de usuario, y no se limita en este documento.

La Fig. 2 es una segunda vista esquemática de una arquitectura de sistema para un método de verificación de integridad proporcionado por la presente descripción. La arquitectura del sistema que se muestra en la Fig. 1 es un sistema de comunicación de conectividad única. La arquitectura del sistema en la Fig. 2 es un sistema de comunicación de conectividad múltiple sobre la base de la realización mostrada en la Fig. 1. El sistema de comunicación de

conectividad múltiple puede ser, por ejemplo, un sistema de comunicación de conectividad dual (DC).

El sistema de comunicación de conectividad dual se refiere a un sistema en el que el terminal tiene acceso tanto al primer equipo del lado de la red como al segundo equipo del lado de la red. En esta realización, el primer equipo del lado de la red puede ser uno de los equipos del lado de la red descritos en la realización de la Fig. 1, y el segundo equipo del lado de la red puede ser uno de los equipos del lado de la red descritos en la realización de la Fig. 1. En una posible implementación, como se muestra en la Fig. 2, el sistema de comunicaciones de doble conectividad incluye equipos del lado de la red en una red LTE y equipos del lado de la red en una red NR. Uno de los sistemas, por ejemplo, el equipo del lado de la red en la red LTE en esta realización, actúa como un nodo maestro (MN), y el otro sistema, por ejemplo, el equipo del lado de la red en la red NR en esta realización, actúa como un nodo secundario (SN). En el sistema de conectividad dual, hay dos grupos de celdas, a saber, un grupo de celdas maestras (MCG) y un grupo de celdas secundarias (SCG). El grupo de celdas maestras puede incluir una celda primaria (PCell) y una o más celdas secundarias (SCell). El grupo de celdas secundarias puede incluir una celda secundaria primaria (PSCell) y una o más SCells. El nodo maestro corresponde a la celda primaria y la celda secundaria, y el nodo secundario corresponde a la celda secundaria primaria y la celda secundaria. Para una implementación específica del terminal, consulte la descripción de la realización que se muestra en la Fig. 1, y no se volverá a describir aquí en esta realización.

Aunque se ha presentado una arquitectura de sistema posible en la realización descrita anteriormente, la arquitectura de sistema específica no está particularmente limitada en esta realización, y en esta realización se puede aplicar cualquier arquitectura de sistema que incluya un terminal y un equipo del lado de la red.

En un futuro sistema de comunicaciones móviles de 5ª generación (5G), para admitir diversos servicios, como banda ancha móvil mejorada (eMBB) y comunicación de baja latencia ultraconfiable (URLLC), la mera consideración de la seguridad de los datos del plano de control no puede satisfacer la demanda de seguridad, y también se debe tener en cuenta la seguridad de los datos del plano de usuario. Como tal, la presente descripción proporciona un método de verificación de integridad de los datos del plano de usuario, para garantizar la seguridad de los datos del plano de usuario. Se realizará una descripción detallada del método proporcionado por la presente descripción con referencia a realizaciones específicas.

La Fig. 3 es un diagrama de flujo esquemático de un método de verificación de integridad proporcionado por una realización de la presente descripción. Este ejemplo está implementado por un terminal. Como se muestra en la Fig. 3, el método incluye los siguientes pasos.

S301: recibir, por parte del terminal, datos del plano de usuario transmitidos por el equipo del lado de la red.

Al iniciarse, el terminal selecciona una celda adecuada de una red móvil terrestre pública (PLMN) seleccionada para registrarse. Después de registrarse en una determinada celda, el terminal puede recibir un mensaje del sistema y un mensaje de difusión de celda. Cuando el terminal necesita realizar una comunicación de servicio, establece una conexión de control de recursos de radio (RRC) con el equipo del lado de la red. Después del establecimiento de la conexión de RRC, el terminal puede intercambiar datos del plano de usuario con el equipo del lado de la red.

En esta realización, se presenta un posible proceso de establecimiento de conexión de RRC. Este proceso de establecimiento de conexión de RRC se implementa a través de una portadora de radio (RB). La RB incluye una portadora de radio de señalización (SRB) y una portadora de radio de datos (DRB). La SRB es un canal de transmisión para los mensajes de señalización del sistema, y la DRB es el canal de transmisión para los datos del plano de usuario. La SRB incluye SRB0, SRB1 y SRB2, la SRB0 está configurada para transmitir mensajes de RRC, la SRB1 está configurada para transmitir mensajes de RRC y algunos mensajes de estrato sin acceso (NAS), y la SRB2 está configurada para transmitir algunos mensajes de NAS.

Hablando de una manera popular y fácil de entender, la conexión de RRC se refiere a la SRB1 establecida entre el terminal y el equipo del lado de la red, ya que no es necesario establecer la SRB0. El terminal puede adquirir la configuración y los recursos de la SRB0 en un estado inactivo. Un proceso de inicio de servicio en el sistema es el siguiente: la señalización se transmite sobre la SRB0 para establecer la SRB1, una vez que se establece la SRB1, el terminal entra en un estado de conexión de RRC; luego la señalización se transmite por la SRB1 para establecer el SRB2 para la transmisión de señalización NAS; y la señalización se transmite por el SRB1 para establecer la DRB para la transmisión de datos del plano de usuario. Puede verse que después de establecer la DRB entre el terminal y el equipo del lado de la red, el terminal recibe datos del plano de usuario transmitidos por el equipo del lado de la red sobre la DRB establecida.

S302: realizar, por parte del terminal, una verificación de integridad en los datos del plano de usuario en base a la información de configuración de verificación de integridad del plano de usuario.

Habiendo recibido los datos del plano de usuario, el terminal realiza la verificación de integridad en los datos del plano de usuario en base a la información de configuración de verificación de integridad del plano de usuario de una manera dirigida y específica. La información de configuración de verificación de integridad del plano de usuario puede ser acordada de antemano por el terminal y el equipo del lado de la red, o configurada para el terminal por el equipo del lado de la red. La información de configuración de verificación de integridad del plano de usuario puede indicar al terminal que realice la verificación de integridad en todos o algunos de los datos del plano de usuario recibidos. La

información de configuración de verificación de integridad del plano de usuario puede incluir además información de indicación configurada para indicar un algoritmo de verificación de integridad correspondiente a la verificación de integridad realizada por el terminal en los datos del plano de usuario, etc. La información de indicación puede denominarse cuarta información de indicación en este documento, para distinguirse de la información de indicación primera, segunda y tercera en las realizaciones siguientes.

El algoritmo de verificación de integridad puede ser, por ejemplo, un algoritmo de estándar de cifrado avanzado (AES), un algoritmo SNOW 3G, un algoritmo ZUC o similar, y el algoritmo específico no está particularmente limitado aquí en esta realización.

Como apreciarán los expertos en la materia, se pueden incluir varios parámetros e información relacionados con la verificación de integridad en la información de configuración de verificación de integridad del plano de usuario.

Un proceso ejemplar de verificación de integridad realizado en los datos del plano de usuario por el terminal puede ser el siguiente. El terminal usa los parámetros transportados en los datos del plano de usuario y los parámetros conocidos mantenidos por el terminal para generar información de verificación de integridad usando un algoritmo de protección de integridad y compara la información de verificación de integridad con la información de verificación de integridad conocida. Si los dos son consistentes entre sí, entonces la verificación tiene éxito y se determina que los datos no están alterados. Si los dos no son coherentes entre sí, la verificación falla, es decir, los datos del plano de usuario se encuentran alterados y se determina que la verificación de integridad de los datos ha fallado y los datos no se pueden utilizar. Como apreciarán los expertos en la técnica, un proceso de verificación de integridad se presenta aquí solo como un ejemplo, y también se pueden aplicar otras formas de procesos de verificación de integridad en las realizaciones de la presente descripción.

En algunas realizaciones opcionales, la operación de verificación de integridad realizada en los datos del plano de usuario por el terminal se implementa en la capa del protocolo de convergencia de datos en paquetes (PDCP) del terminal.

Según el método de verificación de integridad proporcionado por una realización de la presente descripción, después de recibir los datos del plano de usuario transmitidos por el equipo del lado de la red, el terminal realiza la verificación de integridad en los datos del plano de usuario recibidos del equipo del lado de la red en base a la información de configuración de verificación de integridad del plano de usuario, y luego determina si los datos del plano de usuario han sido alterados, mejorando así la seguridad de los datos del plano de usuario.

La Fig. 4 es un diagrama de flujo esquemático de un método de verificación de integridad proporcionado por una realización de la presente descripción. Este ejemplo se implementa mediante un equipo del lado de la red, que puede ser el equipo del lado de la red como se muestra en la Fig. 1 o cualquiera de los equipos del lado de la red en el sistema de conectividad múltiple como se muestra en la Fig. 2. En correspondencia con la Fig. 3, esta realización es implementada por el equipo del lado de la red. Como se muestra en la Fig. 4, este método incluye los siguientes pasos.

S401: transmitir, por el equipo del lado de la red, información de configuración de verificación de integridad de datos del plano de usuario a un terminal. La información de configuración de verificación de integridad de datos del plano de usuario está configurada para indicar al terminal que realice una verificación de integridad en los datos del plano de usuario recibidos del equipo del lado de la red.

S402: transmitir, por el equipo del lado de la red, los datos del plano de usuario al terminal.

En correspondencia con la realización que se muestra en la figura 3, en la que el equipo del lado de la red configura la información de configuración de verificación de integridad de datos del plano de usuario para el terminal, el equipo del lado de la red puede transmitir primero la información de configuración de verificación de integridad de datos del plano de usuario al terminal antes de transmitir los datos del plano de usuario al terminal. En algunas realizaciones opcionales, la información de configuración de verificación de integridad del plano de usuario puede ser información recién agregada, o campos de extensión agregados al mensaje de RRC durante el establecimiento de RRC, o información transportada en el mensaje de reconfiguración durante la reconfiguración de RRC. En esta realización, el proceso específico de transmisión de la información de configuración de verificación de integridad del plano de usuario al terminal por parte del equipo del lado de la red no está particularmente limitado. Una vez establecida la DRB entre el equipo del lado de la red y el terminal, el equipo del lado de la red transmite los datos del plano de usuario al terminal a través de la DRB, y el terminal realiza la verificación de integridad de los datos del plano de usuario.

Según el método de verificación de integridad proporcionado por esta realización, el equipo del lado de la red transmite la información de configuración de verificación de integridad de datos del plano de usuario al terminal, para instruir al terminal para que realice la verificación de integridad en los datos del plano de usuario recibidos del equipo de lado de la red. Después de que el equipo del lado de la red transmite los datos del plano de usuario al terminal, el equipo del lado de la red realiza la verificación de integridad en los datos del plano de usuario utilizando la información de configuración de verificación de integridad del plano de usuario. Por medio de la verificación de integridad, el terminal puede determinar si los datos del plano de usuario han sido alterados, mejorando así la seguridad de los datos del plano de usuario.

A continuación se realizará una descripción detallada del método de verificación de integridad proporcionado por la

presente descripción con referencia a una realización específica.

En un ejemplo específico, sobre la base de las realizaciones mostradas en la Fig. 3 y la Fig. 4, la información de configuración de verificación de integridad del plano de usuario incluye primera información de indicación configurada para indicar una DRB correspondiente a la verificación de integridad. Un proceso de implementación específico de un método correspondiente de verificación de integridad puede ser como se muestra en la Fig. 5.

La Fig. 5 es un diagrama de flujo de un método de verificación de integridad proporcionado por una realización de la presente descripción. Como se muestra en la Fig. 5, el método incluye: S501, recibir, por parte del terminal, los datos del plano de usuario transmitidos por el equipo del lado de la red; S502, realizar, por parte del terminal, la verificación de integridad en los datos del plano de usuario transportados en la DRB indicada por la primera información de indicación, y la primera información de indicación está configurada para indicar una DRB correspondiente a la verificación de integridad.

En concreto, solo existe un tipo de DRB y el protocolo establece que cada terminal puede utilizar hasta 8 DRB para transmitir diferentes servicios. El terminal puede realizar la verificación de integridad en todas las DRB o en algunas de ellas. Específicamente, la primera información de indicación indica un identificador de la DRB en la que se va a realizar la verificación de integridad. El identificador de la DRB puede ser, por ejemplo, un valor de la DRB, un número de secuencia de la DRB, etc. El identificador de la DRB no está particularmente limitado en esta realización. Específicamente, el identificador de la DRB en la que se va a realizar la verificación de integridad puede indicarse según la importancia de los datos del plano de usuario transportados en la DRB.

El terminal puede realizar la verificación de integridad en los datos del plano de usuario transportados en la DRB indicada por la primera información de indicación. Es decir, el terminal puede realizar la verificación de integridad en los datos del plano de usuario transportados en una DRB específica a propósito. De esta forma, se mejora la eficiencia de verificación de integridad del terminal, mientras que se reduce la demanda de capacidad del terminal y también se reduce el consumo de energía del terminal.

En algunas realizaciones opcionales, sobre la base de esta realización, el terminal puede determinar si la verificación de integridad de datos ha fallado según un primer criterio de determinación de si los datos del plano de usuario fallan la verificación de integridad. El primer criterio de determinación de si los datos del plano de usuario fallan en la verificación de integridad puede configurarse en la información de configuración de verificación de integridad del plano de usuario, acordada de antemano por el terminal y el equipo del lado de la red, transmitida al terminal por el equipo del lado de la red, o configurado por el propio terminal. El modo de configuración del primer criterio de determinación en cuanto al fallo de la verificación de integridad no está particularmente limitado en esta realización.

Específicamente, el primer criterio de determinación en cuanto al fallo de la verificación de integridad incluye: si al menos una de las DRB indicadas por la primera información de indicación falla la verificación de integridad, los datos del plano de usuario fallan la verificación de integridad.

Durante una implementación específica, si el terminal determina que los datos del plano de usuario transportados en al menos una de las DRB indicadas por la primera información de indicación fallan la verificación de integridad, entonces el terminal determina que los datos del plano de usuario fallan la verificación de integridad. Puede verse desde arriba, los identificadores de múltiples DRB pueden indicarse en la primera información de indicación, y los datos del plano de usuario se transmiten entre el equipo del lado de la red y el terminal a través de múltiples DRB. El terminal puede determinar que los datos del plano de usuario fallan en la verificación de integridad cuando se determina que una o más de las DRB o todas las DRB indicadas fallan en la verificación de integridad.

Que el terminal determine que los datos del plano de usuario transportados en la DRB fallan en la verificación de integridad tiene las siguientes implementaciones posibles.

En una posible implementación, si al menos uno de los paquetes de datos transportados por la DRB falla la verificación de integridad, entonces los datos del plano de usuario transportados por la DRB fallan la verificación de integridad.

Específicamente, se pueden transportar múltiples paquetes de datos en la DRB. Cuando uno o más paquetes de datos transportados en la DRB fallan en la verificación de integridad, el terminal determina que la DRB falla en la verificación de integridad. El número de paquetes de datos que fallan en la verificación de integridad se puede acordar de antemano o establecerlo el propio terminal.

En otra implementación posible, si la relación entre el número de paquetes de datos transportados en la DRB que fallan la verificación de integridad y el número de paquetes de datos recibidos transportados en la DRB excede un umbral preestablecido, entonces se determina que los datos del plano de usuario transportados en la DRB fallan la verificación de integridad.

Específicamente, el terminal realiza la verificación de integridad consecutivamente en los paquetes de datos recibidos transportados en la DRB, cuenta los paquetes de datos que fallan la verificación de integridad y cuenta los paquetes de datos recibidos transportados en la DRB. Cuando la relación entre el número N de paquetes de datos que fallan en la verificación de integridad y el número M de paquetes de datos recibidos transportados en la DRB supera el umbral

preestablecido, es decir, la relación N/M supera el umbral preestablecido, entonces se determina que los datos del plano de usuario transportados en la DRB fallan en la verificación de integridad.

En otra implementación posible más, si el número de paquetes de datos transportados en la DRB que fallan en la verificación de integridad excede un número preestablecido, entonces se determina que los datos del plano de usuario transportados en la DRB fallan en la verificación de integridad.

Específicamente, el terminal realiza la verificación de integridad consecutivamente en los paquetes de datos recibidos transportados en la DRB, y cuenta los paquetes de datos que fallan en la verificación de integridad. Cuando el número de paquetes de datos que fallan en la verificación de integridad excede el umbral preestablecido, entonces el terminal determina que los datos del plano de usuario transportados en la DRB fallan en la verificación de integridad.

En otra implementación posible, si el número de paquetes de datos transportados en la DRB que fallan en la verificación de integridad excede un número preestablecido en una duración preestablecida, entonces se determina que los datos del plano de usuario transportados en la DRB fallan en la verificación de integridad.

Específicamente, en la duración preestablecida, se cuentan los paquetes de datos que fallan en la verificación de integridad. Si el número de paquetes de datos transportados en la DRB que fallan en la verificación de integridad excede el número preestablecido, entonces el terminal determina que los datos del plano de usuario transportados en la DRB fallan en la verificación de integridad.

En otra implementación posible, si el número de paquetes de datos consecutivos transportados en la DRB que fallan en la verificación de integridad excede un número preestablecido, entonces se determina que los datos del plano de usuario transportados en la DRB fallan en la verificación de integridad.

Específicamente, se cuentan los paquetes de datos consecutivos que fallan la verificación de integridad. Si el número contado excede el número preestablecido, entonces el terminal determina que los datos del plano de usuario transportados en la DRB fallan en la verificación de integridad.

En otro ejemplo específico, sobre la base de las realizaciones que se muestran en la Fig. 3 y la Fig. 4, la información de configuración de verificación de integridad del plano de usuario incluye una segunda información de indicación configurada para indicar al terminal que realice la verificación de integridad en todos los datos recibidos del plano de usuario. El proceso de implementación específico del método correspondiente de verificación de integridad puede ser como se muestra en la Fig. 6.

La Fig. 6 es un diagrama de flujo de un método de verificación de integridad proporcionado por una realización de la presente descripción. Como se muestra en la Fig. 6, el método incluye: S601, recibir, por parte del terminal, los datos del plano de usuario transmitidos por el equipo del lado de la red; y S602, realizar, por parte del terminal, la verificación de integridad de todos los datos del plano de usuario recibidos por el terminal en base a la segunda información de indicación. La segunda información de indicación está configurada para dar instrucciones al terminal para que realice la verificación de integridad en todos los datos del plano de usuario recibidos.

Específicamente, el terminal puede ser instruido a nivel de terminal. Es decir, el terminal realiza la verificación de integridad en todos los datos del plano de usuario, independientemente de a qué DRB pertenezca el paquete de datos en los datos del plano de usuario.

En esta realización, la información de configuración de integridad del plano de usuario puede incluir además un segundo criterio de determinación de si los datos del plano de usuario fallan en la verificación de integridad. En algunas realizaciones opcionales, sobre la base de esta realización, el terminal puede determinar si la verificación de integridad de datos ha fallado basándose en el segundo criterio de determinación de si los datos del plano de usuario fallan en la verificación de integridad. El segundo criterio de determinación de si los datos del plano de usuario fallan en la verificación de integridad puede configurarse en la información de configuración de verificación de integridad del plano de usuario, acordada de antemano por el terminal y el equipo del lado de la red, transmitida al terminal por el equipo del lado de la red, o configurado por el propio terminal. En esta realización, el modo de configuración del segundo criterio de determinación en cuanto al fallo de la verificación de integridad no está particularmente limitado.

Específicamente, el segundo criterio de determinación en cuanto al fallo en la verificación de integridad incluye: si al menos uno de los paquetes de datos del plano de usuario falla la verificación de integridad, entonces los datos del plano de usuario fallan la verificación de integridad; o si una proporción del número de paquetes de datos del plano de usuario que fallan la verificación de integridad al número de paquetes de datos recibidos excede un umbral preestablecido, entonces los datos del plano de usuario fallan la verificación de integridad; o si el número de paquetes de datos de los datos del plano de usuario que fallan la verificación de integridad excede un número preestablecido, entonces los datos del plano de usuario fallan la verificación de integridad; o si el número de paquetes de datos de los datos del plano de usuario que fallan la verificación de integridad excede un número preestablecido en una duración predeterminada, entonces los datos del plano de usuario fallan la verificación de integridad; o si el número de paquetes de datos consecutivos de los datos del plano de usuario que fallan la verificación de integridad excede un número preestablecido, entonces los datos del plano de usuario fallan la verificación de integridad.

En esta realización, el terminal realiza la verificación de integridad de todos los datos del plano de usuario recibidos. Para el proceso de implementación específico del recuento de los paquetes de datos o el número de paquetes de datos, consulte la realización que se muestra en la Fig. 5. En esta realización se omite una descripción repetida.

En la realización descrita anteriormente, el paquete de datos incluye una unidad de datos de protocolo (PDU) y/o una unidad de datos de servicio (SDU) de una capa de protocolo de convergencia de datos de paquetes (PDCP), una capa de control de enlace de radio (RLC) y/o una capa de control de acceso al medio (MAC).

Se puede ver desde arriba, la determinación de los datos del plano de usuario falla, la verificación de integridad se puede implementar en varios modos. En un proceso de implementación específico, el modo puede configurarse de manera flexible según la importancia de los datos del plano de usuario o la capacidad del terminal.

Sobre la base de la realización descrita anteriormente, la presente descripción especifica además las operaciones posteriores del terminal después del fallo de la verificación de integridad, como se muestra específicamente en la Fig. 7. La Fig. 7 es un diagrama de flujo de un método de verificación de integridad proporcionado por una realización de la presente descripción. Como se muestra en la Fig. 7, el método incluye: S701, recibir, por parte del terminal, datos del plano de usuario transmitidos por el equipo del lado de la red; S702, realizar, por parte del terminal, la verificación de integridad en los datos del plano de usuario en base a la información de configuración de verificación de integridad del plano de usuario; S703, determinar, por parte del terminal, si los datos del plano de usuario fallan en la verificación de integridad, si es así, el proceso continúa hasta S704, de lo contrario, el proceso continúa hasta S705; S704, realizar, por parte del terminal, un proceso de procesamiento de fallos de verificación de integridad; y S705, adquirir, por parte del terminal, los datos del plano de usuario.

Para procesos de implementación específicos de S701 a S703, consulte la realización descrita anteriormente. En esta realización se omite una descripción repetida.

El proceso de fallo de verificación de integridad puede ser acordado de antemano por el terminal y el equipo del lado de la red, establecido por el propio terminal o configurado para el terminal por el equipo del lado de la red.

En esta realización, el proceso de verificación de integridad realizado por el terminal puede tener dos implementaciones posibles.

En una posible implementación, cuando el terminal determina que los datos del plano de usuario fallan en la verificación de integridad, el terminal realiza el proceso de fallo en la verificación de integridad. Es decir, el terminal realiza el proceso de fallo de verificación de integridad una vez que falla la verificación de integridad.

En otra posible implementación, antes de que el terminal realice la verificación de integridad, el equipo del lado de la red transmite un mensaje de activación del procesamiento de fallos al terminal. El mensaje de activación del procesamiento de fallos está configurado para indicar al terminal que inicie el proceso de procesamiento de fallos de la verificación de integridad al fallar la verificación de integridad.

Es decir, si el terminal no ha recibido el mensaje de activación del procesamiento de fallos, después de que el terminal determina que los datos del plano de usuario fallan en la verificación de integridad, el terminal no realizará el proceso de procesamiento de fallos de verificación de integridad subsiguiente. Si el terminal ha recibido el mensaje de activación del procesamiento de fallos, después de que el terminal determina que los datos del plano de usuario fallan en la verificación de integridad, el terminal realizará el proceso de procesamiento de fallos de verificación de integridad subsiguiente.

En algunas realizaciones opcionales, si los datos del plano de usuario fallan en la verificación de integridad, el terminal realiza al menos uno de los siguientes pasos: transmitir, mediante la capa PDCP del terminal, un mensaje de notificación de fallo de verificación de integridad a la capa de RRC del terminal; descartar, por parte del terminal, los datos del plano de usuario; transmitir, por el terminal, el mensaje de notificación de fallo de verificación de integridad al equipo del lado de la red; liberar, por parte del terminal, la conexión de RRC con el equipo del lado de la red; activar, por parte del terminal, un mecanismo de fallo de enlace de radio (RLF); liberar, por parte del terminal, una configuración DRB del equipo del lado de la red.

Como apreciarán los expertos en la materia, el proceso de procesamiento de fallos en la verificación de integridad incluye al menos uno de los pasos descritos anteriormente.

Durante un proceso de implementación específico, la capa PDCP del terminal realiza la verificación de integridad en los datos del plano de usuario. Cuando los datos del plano de usuario fallan en la verificación de integridad, la capa PDCP del terminal transmite un mensaje de notificación de fallo de verificación de integridad a la capa de RRC y descarta los datos del plano de usuario.

El terminal también puede transmitir un mensaje de notificación de fallo de verificación de integridad al equipo del lado de la red. En algunas realizaciones opcionales, el mensaje de fallo de verificación de integridad implicado en esta realización puede llevar un identificador de la DRB que falla la verificación de integridad. Durante un proceso de reconfiguración de RRC, el equipo del lado de la red puede reconfigurar la DRB para el terminal en función del identificador de la DRB que falla la verificación de integridad.

El terminal también puede liberar la conexión de RRC con el equipo del lado de la red y transmitir un mensaje de notificación de que el terminal ha liberado la conexión de RRC con el equipo del lado de la red. Durante un proceso de procesamiento posterior, el terminal también puede restablecer la conexión de RRC con el equipo del lado de la red.

El terminal también puede activar un mecanismo de fallo de enlace de radio (RLF). Después de activar el mecanismo de RLF, el terminal restablece el RRC dentro de un período de tiempo específico. Si el restablecimiento fallo dentro del período de tiempo especificado, el terminal puede iniciar posteriormente una solicitud de establecimiento de RRC.

El terminal también puede liberar la configuración de la DRB del equipo del lado de la red. Como apreciarán los expertos en la materia, el equipo del lado de la red configura una DRB disponible para el terminal para la transmisión de datos del plano de usuario. Al fallar la verificación de integridad, el terminal puede liberar la configuración de la DRB configurada por el equipo del lado de la red para el terminal.

Durante un proceso de implementación específico, el proceso de fallo de verificación de integridad puede seleccionarse de manera flexible según diferentes arquitecturas de sistemas y diferentes escenarios.

A continuación, se describirá en detalle el método de verificación de integridad proporcionado por una realización de la presente descripción con respecto a diferentes escenarios.

En un posible escenario de aplicación como se muestra en la Fig. 2, es decir, un escenario de conectividad múltiple, la información de configuración de verificación de integridad del plano de usuario incluye además una tercera información de indicación configurada para instruir al terminal para que realice la verificación de integridad en los datos recibidos del plano de usuario transmitidos. por otro equipo del lado de la red.

Por ejemplo, el equipo del lado de la red en LTE transmite la información de configuración de verificación de integridad del plano de usuario al terminal. En algunas realizaciones opcionales, la información de configuración de verificación de integridad del plano de usuario incluye primera información de indicación o segunda información de indicación descrita anteriormente. En esta realización, la información de configuración de verificación de integridad del plano de usuario incluye además una tercera información de indicación. Es decir, el equipo del lado de la red en LTE también instruye al terminal para que realice una verificación de integridad en los datos recibidos del plano de usuario transmitidos por el equipo del lado de la red en la nueva red de acceso por radio. El proceso de verificación de integridad realizado por el terminal en los datos del plano de usuario de la nueva red de acceso por radio es el mismo que el proceso de verificación de integridad realizado por el terminal en los datos del plano de usuario de la LTE.

En este proceso, el equipo del lado de la red (el equipo del lado de la red en la red LTE) transmite un mensaje de notificación de configuración finalizada al otro equipo del lado de la red (el equipo del lado de la red en la nueva red de acceso por radio). El mensaje de notificación de configuración finalizada está configurado para notificar al otro equipo del lado de la red que la información de configuración de verificación de integridad del plano de usuario transmitida al terminal por el equipo del lado de la red es aplicable al otro equipo del lado de la red. En este punto, el otro equipo del lado de la red no tiene que transmitir la información de configuración de verificación de integridad del plano de usuario al terminal.

Para otro posible escenario de aplicación, continúe consultando la Fig. 2. El terminal opera en un sistema de conectividad dual (DC) y el equipo del lado de la red en esta realización es un nodo secundario (SN) en el sistema de DC. Si los datos del plano de usuario fallan en la verificación de integridad, el terminal transmite información de fallo de verificación de integridad al nodo maestro (MN) en el sistema de DC.

Específicamente, después de que el terminal determina que los datos del plano de usuario fallan en la verificación de integridad, el terminal puede transmitir información de fallo de verificación de integridad al equipo del lado de la red y/u otro equipo del lado de la red. En caso de que el terminal transmita la información de fallo de verificación de integridad a otro equipo del lado de la red que no sea el equipo del lado de la red que transmitió los datos del plano de usuario al terminal, la información de fallo de la verificación de integridad incluye el identificador del equipo del lado de la red.

Por ejemplo, en caso de que el equipo del lado de la red en la nueva red de acceso por radio actúe como el nodo secundario y el equipo del lado de la red en la red LTE actúe como el nodo maestro, si el nodo secundario (SN) transmitió los datos del plano de usuario al terminal y los datos del plano de usuario fallaron la verificación de integridad realizada por el terminal, entonces el terminal puede transmitir la información de fallo de la verificación de integridad de los datos del plano de usuario con el identificador del nodo secundario (SN) al nodo maestro en lugar de transmitir el información de fallo de verificación de integridad al nodo secundario. En este punto, el nodo maestro puede desconectarse del nodo secundario (SN) y restablecer una conexión con un nuevo nodo secundario (SN).

Otro escenario posible puede ser un sistema de conectividad múltiple como se muestra en la Fig. 2, o un escenario de agregación de portadoras (CA). En CA, se agregan dos o más portadoras de componentes (CC) para formar un grupo de portadoras a fin de admitir un mayor ancho de banda de transmisión. La portadora correspondiente a la celda primaria (Pcell) se denomina portadora de componentes primarios (PCC) o portadora primaria; y la portadora correspondiente a la celda secundaria (Scell) se denomina portadora de componente secundarios (SCC) o portadora secundaria. Esta realización presenta ilustrativamente un escenario que incluye una celda primaria, una celda secundaria primaria y una celda secundaria. Para otros escenarios que incluyen una celda primaria y/o una celda

secundaria primaria y una celda secundaria, esta realización también es aplicable.

Cuando el terminal opera en una celda primaria en un sistema de conectividad dual (DC) o un sistema de agregación de portadoras (CA), si los datos del plano de usuario falla la verificación de integridad, entonces la capa PDCP del terminal transmite un mensaje de notificación de fallo de verificación de integridad a la capa de RRC, el terminal descarta los datos del plano de usuario; el terminal libera la conexión de RRC con el equipo del lado de la red o activa el mecanismo de fallo del enlace de radio (RLF).

Cuando el terminal opera en una celda secundaria en un sistema de conectividad dual (DC) o un sistema de agregación de portadoras (CA), si los datos del plano de usuario fallan la verificación de integridad, entonces el terminal libera la configuración de portadora de radio de datos (DRB) del secundario. o todas las celdas secundarias, o deja de utilizar la DRB de la celda secundaria o de todas las celdas secundarias.

Como apreciarán los expertos en la materia, la celda principal es responsable del RRC entre el equipo del lado de la red y el terminal, mientras que la celda secundaria está configurada para proporcionar recursos de radio adicionales, sin comunicación de RRC entre la celda secundaria y el terminal. Por lo tanto, cuando el terminal está ubicado en la celda secundaria descrita anteriormente, si falla la verificación de integridad realizada por el terminal, es posible que el terminal no realice el proceso de liberar la conexión de RRC con el equipo del lado de la red y activar el mecanismo de RLF como se describe anteriormente.

Cuando el terminal está realizando el proceso de transmisión del mensaje de notificación de fallo de verificación de integridad al equipo del lado de la red, y después de que el terminal transmite el mensaje de notificación de fallo de verificación de integridad al equipo del lado de la red, el equipo del lado de la red transmite información de reconfiguración de RRC al terminal. El mensaje de reconfiguración de RRC incluye nueva información de configuración de verificación de integridad de datos de plano de usuario, y el mensaje de reconfiguración de RRC también puede incluir otra información de configuración. No existe ninguna limitación particular en esta realización a este respecto.

Como apreciarán los expertos en la materia, los escenarios descritos anteriormente son meramente ejemplares y, durante un proceso de implementación específico, se pueden realizar varias combinaciones o derivaciones a partir de estos escenarios para obtener otros escenarios de aplicación. Tales combinaciones o derivaciones no se enumerarán en esta realización.

La Fig. 8 es un diagrama estructural esquemático de un terminal proporcionado por una realización de la presente descripción. Como se muestra en la Fig. 8, un terminal 80 incluye un módulo 801 de recepción de datos y un módulo 802 de verificación de integridad. El módulo 801 de recepción de datos está configurado para recibir datos del plano de usuario transmitidos por el equipo del lado de la red y el módulo 802 de verificación de integridad está configurado para realizar una verificación de integridad en los datos del plano de usuario en función de la información de configuración de verificación de integridad del plano de usuario.

En algunas realizaciones opcionales, los datos del plano de usuario se transportan en la portadora de radio de datos (DRB). La información de configuración de verificación de integridad del plano de usuario incluye primera información de indicación configurada para indicar una DRB correspondiente a la verificación de integridad. El módulo de verificación de integridad está específicamente configurado para realizar una verificación de integridad en los datos del plano de usuario transportados en la DRB indicados por la primera información de indicación.

En algunas realizaciones opcionales, el módulo 802 de verificación de integridad está específicamente configurado para: si los datos del plano de usuario transportados en al menos una de las DRB indicadas por la primera información de indicación fallan en la verificación de integridad, entonces determinar que los datos del plano de usuario fallan en la verificación de integridad.

En algunas realizaciones opcionales, el módulo 802 de verificación de integridad está específicamente configurado para: si al menos uno de los paquetes de datos transportados en la DRB falla la verificación de integridad, determinar que los datos del plano de usuario transportados en la DRB fallan la verificación de integridad; o si la relación entre el número de paquetes de datos transportados en la DRB que fallan la verificación de integridad y la cantidad de paquetes de datos recibidos transportados en la DRB excede un umbral preestablecido, determinar que los datos del plano de usuario transportados en la DRB fallan la verificación de integridad; o si el número de paquetes de datos transportados en la DRB que fallan la verificación de integridad excede un número preestablecido, determinar que los datos del plano de usuario transportados en la DRB fallan la verificación de integridad; o si el número de paquetes de datos transportados en la DRB que fallan la verificación de integridad excede un número preestablecido en una duración preestablecida, determinar que los datos del plano de usuario transportados en la DRB fallan la verificación de integridad; o si el número de paquetes de datos consecutivos transportados en la DRB que fallan en la verificación de integridad excede un número preestablecido, determinar que los datos del plano de usuario transportados en la DRB fallan en la verificación de integridad.

En algunas realizaciones opcionales, la información de configuración de verificación de integridad del plano de usuario incluye una segunda información de indicación configurada para indicar al terminal que realice la verificación de integridad en todos los datos del plano de usuario recibidos. El módulo 802 de verificación de integridad está específicamente configurado para realizar la verificación de integridad en todos los datos del plano de usuario recibidos

por el terminal en base a la segunda información de indicación.

En algunas realizaciones opcionales, el módulo 802 de verificación de integridad está configurado específicamente para: si al menos uno de los paquetes de datos del plano de usuario falla la verificación de integridad, determinar que los datos del plano de usuario fallan la verificación de integridad; o si una relación entre el número de paquetes de datos del plano de usuario que fallan la verificación de integridad y el número de paquetes de datos recibidos excede un umbral preestablecido, determinar que los datos del plano de usuario fallan la verificación de integridad; o si el número de paquetes de datos de los datos del plano de usuario que fallan la verificación de integridad excede un número preestablecido, determinar que los datos del plano de usuario fallan la verificación de integridad; o si el número de paquetes de datos de los datos del plano de usuario que fallan la verificación de integridad excede un número preestablecido en una duración predeterminada, determinar que los datos del plano de usuario fallan la verificación de integridad; o si el número de paquetes de datos consecutivos de los datos del plano de usuario que fallan en la verificación de integridad excede un número preestablecido, determinar que los datos del plano de usuario fallan en la verificación de integridad.

En algunas realizaciones opcionales, el paquete de datos incluye una unidad de datos de protocolo (PDU) y/o una unidad de datos de servicio (SDU) de una capa de protocolo de convergencia de datos de paquetes (PDCP), una capa de control de enlace de radio (RLC) y/o una capa de control de acceso al medio (MAC).

En algunas realizaciones opcionales, la información de configuración de verificación de integridad del plano de usuario incluye además un criterio de determinación sobre si los datos del plano de usuario fallan en la verificación de integridad.

El terminal según esta realización puede realizar el método mostrado en la realización descrita anteriormente y tiene principios de implementación y efectos técnicos similares y no se describirá de nuevo aquí en esta realización.

La Fig. 9 es un diagrama estructural esquemático de un terminal proporcionado por una realización de la presente descripción. Sobre la base de la realización que se muestra en la Fig. 8, el terminal en esta realización incluye además: un módulo 803 de ejecución de procesos, un módulo 804 de recepción de mensajes de activación, un módulo 805 de recepción de información de configuración y un módulo 806 de transmisión de información de fallos. En algunas realizaciones opcionales, el módulo 803 de ejecución de procesos está configurado para ejecutar al menos uno de los siguientes pasos si los datos del plano de usuario fallan en la verificación de integridad: transmitir un mensaje de notificación de fallo de verificación de integridad a la capa de control de recursos de radio (RRC); descartar los datos del plano de usuario; transmitir el mensaje de notificación de fallo de verificación de integridad al equipo del lado de la red; liberar la conexión de RRC con el equipo del lado de la red; activar un mecanismo de fallo de enlace de radio (RLF); liberar la configuración de DRB del equipo del lado de la red.

En algunas realizaciones opcionales, los datos del plano de usuario se transportan en la portadora de radio de datos (DRB) y el mensaje de notificación de fallo de verificación de integridad incluye el identificador de la DRB que falla la verificación de integridad.

En algunas realizaciones opcionales, el módulo 804 de recepción de mensajes de activación está configurado para: antes de que el módulo de verificación de integridad realice la verificación de integridad en los datos del plano de usuario en función de la información de configuración de verificación de integridad del plano de usuario, recibir el mensaje de activación de procesamiento de fallos transmitido por el equipo del lado de la red.

En algunas realizaciones opcionales, el módulo 805 de recepción de información de configuración está configurado para: antes de que el módulo de verificación de integridad realice la verificación de integridad en los datos del plano de usuario basándose en la información de configuración de verificación de integridad del plano de usuario, recibir la configuración de verificación de integridad de los datos del plano de usuario información transmitida por el equipo del lado de la red.

En algunas realizaciones opcionales, el terminal opera en una celda primaria en un sistema de conectividad dual (DC) o un sistema de agregación de portadoras (CA), y el módulo 802 de verificación de integridad está configurado además para: si los datos del plano de usuario fallan en la verificación de integridad, transmitir un mensaje de notificación de fallo de verificación de integridad a la capa de RRC, descartar los datos del plano de usuario; liberar la conexión de RRC con el equipo del lado de la red o activar el mecanismo de fallo del enlace de radio (RLF).

En algunas realizaciones opcionales, el terminal opera en una celda secundaria en un sistema de conectividad dual (DC) o un sistema de agregación de portadoras (CA), y el módulo 802 de verificación de integridad está configurado además para: si los datos del plano de usuario fallan en la verificación de integridad, liberar la configuración de la portadora de radio de datos (DRB) de la celda secundaria o de todas las celdas secundarias, o dejar de usar la DRB de la celda secundaria o de todas las celdas secundarias.

En algunas realizaciones opcionales, el terminal opera en un sistema de doble conectividad (DC) y el equipo del lado de la red actúa como el nodo secundario (SN) en el sistema de DC. El módulo 806 de transmisión de información de fallos está configurado para: si los datos del plano de usuario fallan en la verificación de integridad, transmitir información de fallos en la verificación de integridad al nodo maestro (MN) en el sistema de DC.

En algunas realizaciones opcionales, la información de fallo de verificación de integridad incluye el identificador del equipo del lado de la red.

En algunas realizaciones opcionales, el terminal opera en un sistema de conectividad dual (DC), y la información de configuración de verificación de integridad de datos del plano de usuario incluye además una tercera información de indicación configurada para instruir al terminal para que realice la verificación de integridad en los datos del plano de usuario recibidos transmitidos por otro equipo del lado de la red.

En algunas realizaciones opcionales, la información de configuración de verificación de integridad del plano de usuario incluye además una cuarta información de indicación configurada para indicar el algoritmo de verificación de integridad correspondiente a la verificación de integridad realizada en los datos del plano de usuario por el terminal.

El terminal proporcionado por esta realización puede realizar el método mostrado en la realización descrita anteriormente y tiene principios de implementación y efectos técnicos similares y no se describirá de nuevo aquí en esta realización.

La Fig. 10 es un diagrama estructural esquemático del equipo del lado de la red proporcionado por una realización de la presente descripción. Como se muestra en la Fig. 10, el equipo 100 del lado de la red incluye un módulo 1001 de transmisión de información de configuración y un módulo 1002 de transmisión de datos.

El módulo 1001 de transmisión de información de configuración está configurado para transmitir información de configuración de verificación de integridad de datos de plano de usuario al terminal. La información de configuración de verificación de integridad de datos del plano de usuario está configurada para indicar al terminal que realice la verificación de integridad en los datos del plano de usuario recibidos del equipo del lado de la red. El módulo 1002 de transmisión de datos está configurado para transmitir los datos del plano de usuario al terminal.

Los datos del plano de usuario se transportan en la portadora de radio de datos (DRB). La información de configuración de verificación de integridad del plano de usuario incluye primera información de indicación configurada para indicar una DRB correspondiente a la verificación de integridad.

En algunas realizaciones opcionales, la información de configuración de verificación de integridad del plano de usuario incluye además un primer criterio de determinación de si los datos del plano de usuario fallan en la verificación de integridad. El primer criterio de determinación de si los datos del plano de usuario fallan en la verificación de integridad incluye: si los datos del plano de usuario transportados en al menos una de las DRB indicadas por la primera información de indicación fallan la verificación de integridad, entonces los datos del plano de usuario fallan la verificación de integridad.

En algunas realizaciones opcionales, que los datos del plano de usuario transportados en la DRB falla la verificación de integridad incluye: si al menos uno de los paquetes de datos transportados en la DRB falla la verificación de integridad, entonces los datos del plano de usuario transportados en la DRB fallan la verificación de integridad; o si la relación entre el número de paquetes de datos transportados en la DRB que fallan la verificación de integridad y el número de paquetes de datos recibidos transportados en la DRB excede un umbral preestablecido, entonces los datos del plano de usuario transportados en la DRB fallan la verificación de integridad; o si el número de paquetes de datos transportados en la DRB que fallan la verificación de integridad excede un número preestablecido, entonces los datos del plano de usuario transportados en la DRB fallan la verificación de integridad; o si el número de paquetes de datos transportados en la DRB que fallan la verificación de integridad excede un número preestablecido en una duración preestablecida, entonces los datos del plano de usuario transportados en la DRB fallan la verificación de integridad; o si el número de paquetes de datos consecutivos transportados en la DRB que fallan en la verificación de integridad excede un número preestablecido, entonces los datos del plano de usuario transportados en la DRB fallan en la verificación de integridad.

En algunas realizaciones opcionales, la información de configuración de verificación de integridad del plano de usuario incluye una segunda información de indicación configurada para indicar al terminal que realice la verificación de integridad en todos los datos del plano de usuario recibidos.

En algunas realizaciones opcionales, la información de configuración de verificación de integridad del plano de usuario incluye además un segundo criterio de determinación sobre si los datos del plano de usuario fallan en la verificación de integridad. El segundo criterio de determinación de si los datos del plano de usuario fallan la verificación de integridad incluye: si al menos uno de los paquetes de datos del plano de usuario falla la verificación de integridad, entonces los datos del plano de usuario fallan la verificación de integridad; o si una relación entre el número de paquetes de datos del plano de usuario que fallan la verificación de integridad y el número de paquetes de datos recibidos excede un umbral preestablecido, entonces los datos del plano de usuario fallan la verificación de integridad; o si el número de paquetes de datos de los datos del plano de usuario que fallan la verificación de integridad excede un número preestablecido, entonces los datos del plano de usuario fallan la verificación de integridad; o si el número de paquetes de datos de los datos del plano de usuario que fallan la verificación de integridad excede un número preestablecido en una duración predeterminada, entonces los datos del plano de usuario fallan la verificación de integridad; o si el número de paquetes de datos consecutivos de los datos del plano de usuario que fallan la verificación de integridad excede un número preestablecido, entonces los datos del plano de usuario fallan la verificación de integridad.

En algunas realizaciones opcionales, el paquete de datos incluye una unidad de datos de protocolo (PDU) y/o una unidad de datos de servicio (SDU) de una capa de protocolo de convergencia de datos de paquetes (PDCP), una capa de control de enlace de radio (RLC) y/o una capa de control de acceso al medio (MAC).

El equipo del lado de la red proporcionado por esta realización puede realizar el método mostrado en la realización descrita anteriormente y tiene principios de implementación y efectos técnicos similares y no se describirá de nuevo aquí en esta realización.

La Fig. 11 es un diagrama estructural esquemático del equipo del lado de la red proporcionado por una realización de la presente descripción. Como se muestra en la Fig. 11, sobre la base de la realización que se muestra en la Fig. 10, el equipo del lado de la red en esta realización incluye además un módulo 1003 de transmisión de mensajes de activación y un módulo 1004 de recepción de información de fallos. El módulo 1003 de transmisión de mensajes de activación es configurado para transmitir un mensaje de activación de procesamiento de fallos al terminal.

En algunas realizaciones opcionales, el equipo del lado de la red opera en un sistema de conectividad dual (DC) y el equipo del lado de la red actúa como el nodo maestro (MN) en el sistema de DC. El módulo 1004 de recepción de información de fallos está configurado para recibir la información de fallos de verificación de integridad transmitida por el terminal. La información de fallo de verificación de integridad incluye el identificador del nodo secundario correspondiente al fallo de la verificación de integridad en el sistema DC.

En algunas realizaciones opcionales, el equipo del lado de la red opera en un sistema de conectividad dual (DC) y la información de configuración de verificación de integridad del plano de usuario incluye además información de tercera indicación configurada para indicar al terminal que realice la verificación de integridad en los datos recibidos del plano de usuario transmitidos. por otro equipo del lado de la red.

En algunas realizaciones opcionales, la información de configuración de verificación de integridad del plano de usuario incluye además una cuarta información de indicación configurada para indicar el algoritmo de verificación de integridad correspondiente a la verificación de integridad realizada en los datos del plano de usuario por el terminal.

El equipo del lado de la red proporcionado por esta realización puede realizar el método mostrado en la realización descrita anteriormente y tiene principios de implementación y efectos técnicos similares y no se describirá de nuevo aquí en esta realización.

La Fig. 12 es un diagrama estructural esquemático de un terminal proporcionado por otra realización de la presente descripción. Como se muestra en la Fig. 12, un terminal 1200 como se muestra en la Fig. 12 incluye: al menos un procesador 1201, un almacenamiento 1202, al menos una interfaz 1204 de red y una interfaz 1203 de usuario. Varios componentes en el terminal 1200 están acoplados a entre sí a través de un sistema 1205 de bus. Se aprecia que el sistema 1205 de bus está configurado para permitir la comunicación de conexión entre estos componentes. Además de un bus de datos, el sistema 1205 de bus también incluye un bus de alimentación, un bus de control y un bus de señal de estado. Sin embargo, en aras de la claridad, todos los buses se indican colectivamente como el sistema 1205 de bus en la Fig. 11.

La interfaz 1203 de usuario puede incluir una pantalla, un teclado o un dispositivo de clic como un ratón, una bola de seguimiento, un panel táctil o una pantalla táctil y similares.

Se aprecia que el almacenamiento 1202 en las realizaciones de la presente descripción puede ser un almacenamiento volátil o un almacenamiento no volátil, o puede incluir tanto un almacenamiento volátil como un almacenamiento no volátil. El almacenamiento no volátil puede ser una memoria de sólo lectura (ROM), una ROM programable (PROM), una PROM borrable (EPROM), una EPROM eléctrica (EEPROM) o una memoria flash. El almacenamiento volátil puede ser una memoria de acceso aleatorio (RAM) que actúa como caché externo. A modo de ejemplo y sin limitación, se pueden usar muchas formas de RAM, como una RAM estática (SRAM), una RAM dinámica (DRAM), una DRAM síncrona (SDRAM), una SDRAM de doble velocidad de datos (DDRSDRAM), una RAM mejorada SDRAM (ESDRAM), una DRAM de enlace sincronizado (SLDRAM) y una RAM rambus directa (DRRAM). El almacenamiento 1202 en el sistema y método descritos en las realizaciones de la presente descripción pretende incluir, sin limitarse a, estos y otros tipos adecuados de almacenamiento.

En algunas realizaciones, el almacenamiento 1202 almacena los siguientes elementos, módulos ejecutables o estructuras de datos, o los subconjuntos de los mismos, o los conjuntos de extensión de los mismos: un sistema operativo 12021 y una aplicación 12022.

El sistema operativo 12021 incluye varios programas de sistema, como un programa de capa de marco, un programa de capa de biblioteca central o un programa de capa de controlador y similares, y está configurado para implementar varios servicios básicos y manejar tareas basadas en hardware. La aplicación 12022 incluye varias aplicaciones, como un reproductor multimedia, un navegador y similares, y está configurada para implementar varios servicios de aplicaciones. Los programas para implementar el método de las realizaciones de la presente descripción pueden incluirse en la aplicación 12022.

En una realización de la presente descripción, llamando a programas o instrucciones almacenados en el

almacenamiento 1202, específicamente programas o instrucciones almacenados en la aplicación 12022, el procesador 1201 está configurado para realizar la verificación de integridad en los datos del plano de usuario transmitidos por el equipo del lado de la red basado en la información de configuración de verificación de integridad del plano de usuario después de que la interfaz 1204 de red recibe los datos del plano de usuario.

El método descrito en las realizaciones de la presente descripción descrita anteriormente puede ser aplicado o implementado por el procesador 1201. El procesador 1201 puede ser un chip de circuito integrado con capacidades de procesamiento de señales. Durante la implementación, se pueden lograr varios pasos del método descrito anteriormente en forma de hardware mediante circuitos lógicos integrados en el procesador 1201, o en forma de software mediante instrucciones. El procesador 1201 puede ser un procesador de propósito general, un procesador de señal digital (DSP), un circuito integrado de aplicación específica (ASIC), una matriz de puertas programables en campo (FPGA) u otros dispositivos lógicos programables, puertas discretas o dispositivos lógicos de transistores, o componentes de hardware discretos. Los métodos, pasos y diagramas de bloques lógicos descritos en las formas de realización de la presente descripción pueden implementarse o realizarse. El procesador de propósito general puede ser un microprocesador o el procesador puede ser cualquier procesador convencional o similar. Los pasos del método descrito en relación con las realizaciones de la presente descripción pueden incorporarse directamente en forma de hardware mediante el procesador de codificación o implementarse mediante la combinación de hardware en el procesador de codificación y el módulo de software. El módulo de software puede residir en un medio de almacenamiento bien conocido en la técnica, como una memoria de acceso aleatorio, una memoria flash, una memoria de solo lectura, una memoria de solo lectura programable o una memoria programable borrable eléctricamente, o un registro. El medio de almacenamiento reside en el almacenamiento 1202 y el procesador 1201 lee la información en el almacenamiento 1202 y completa los pasos del método descrito anteriormente en combinación con el hardware del procesador 1201.

Se aprecia que las realizaciones descritas en la presente descripción pueden implementarse en hardware, software, firmware, middleware, microcódigo o una combinación de los mismos. Para la implementación de hardware, la unidad de procesamiento puede implementarse en uno o más circuitos integrados específicos de la aplicación (ASIC), un procesador de señal digital (DSP), un dispositivo DSP (DSPD), un dispositivo lógico programable (PLD), una puerta programable en campo matriz (FPGA), un procesador de propósito general, un controlador, un microcontrolador, un microprocesador, otras unidades electrónicas para realizar las funciones descritas en la presente descripción, o combinaciones de los mismos.

Para la implementación de software, las técnicas descritas en las realizaciones de la presente descripción pueden implementarse mediante módulos (por ejemplo, procesos, funciones, etc.) que realizan las funciones descritas en las realizaciones de la presente descripción. Los códigos de software pueden almacenarse en un almacenamiento y ser ejecutados por un procesador. El almacenamiento puede implementarse interna o externamente al procesador.

Específicamente, el procesador 1201 puede llamar a programas o instrucciones almacenados en el almacenamiento 1202 para ejecutar el método realizado por el terminal en la realización del método descrita anteriormente. Los principios de implementación y los efectos técnicos son similares y no se volverán a describir aquí en esta realización.

La Fig. 13 es un diagrama estructural esquemático del equipo del lado de la red proporcionado por otra realización de la presente descripción. Como se muestra en la Fig. 13, el equipo 1300 del lado de la red incluye una antena 1301, una unidad 1302 de radiofrecuencia y una unidad 1303 de banda base. La antena 1301 está conectada a la unidad 1302 de radiofrecuencia. En la dirección del enlace ascendente, la unidad 1302 de radiofrecuencia recibe información a través de la antena 1301 y transmite la información recibida a la unidad 1303 de banda base para su procesamiento. En la dirección del enlace descendente, la unidad 1303 de banda base procesa la información a transmitir y la transmite a la unidad 1302 de radiofrecuencia. La unidad 1302 de radiofrecuencia procesa la información recibida y la transmite a través de la antena 1301.

La unidad de procesamiento de banda de frecuencia puede residir en la unidad 1303 de banda base. El método ejecutado por el equipo del lado de la red en la realización anterior puede implementarse en la unidad 1303 de banda base. La unidad 1303 de banda base incluye un procesador 13031 y un almacenamiento 13032.

La unidad 1303 de banda base puede, por ejemplo, incluir al menos una placa de procesamiento de banda base que tenga múltiples chips dispuestos en ella, como se muestra en la Fig. 12. Uno de los chips es, por ejemplo, el procesador 13031 que está conectado al almacenamiento 13032 para llamar el programa en el almacenamiento 13032 para ejecutar las operaciones del equipo del lado de la red que se muestra en la realización del método anterior.

La unidad 1303 de banda base puede incluir además una interfaz 13033 de red configurada para intercambiar información con la unidad 1302 de radiofrecuencia. La interfaz es, por ejemplo, una interfaz de radio pública común (CPRI).

El procesador en este documento puede ser un procesador o referirse a múltiples elementos de procesamiento de forma colectiva. Por ejemplo, el procesador puede ser una CPU, o puede ser un ASIC, o uno o más circuitos integrados configurados para implementar el método realizado por el equipo del lado de la red, como uno o más DSP, o una o más FPGA. El elemento de almacenamiento puede ser un almacenamiento o puede referirse a múltiples elementos de almacenamiento de forma colectiva.

El almacenamiento 13032 puede ser un almacenamiento volátil o un almacenamiento no volátil, o puede incluir tanto

un almacenamiento volátil como un almacenamiento no volátil. El almacenamiento no volátil puede ser una ROM, una PROM, una EPROM, una EEPROM o una memoria flash. El almacenamiento volátil puede ser una memoria RAM y se usa como caché externo. A modo de ejemplo y sin ninguna limitación, se pueden utilizar varias formas de RAM, como una SRAM, una DRAM, una SDRAM, una DDRSDRAM, una ESDRAM, una SLDRAM y una DRRAM. El almacenamiento 13032 descrito en las realizaciones de la presente descripción pretende incluir, sin limitación, estos y otros tipos de almacenamiento adecuados.

Específicamente, el procesador 13031 puede llamar a programas almacenados en el almacenamiento 13032 para ejecutar el método realizado por el equipo del lado de la red en la realización descrita anteriormente. Los principios de implementación y los efectos técnicos son similares y no se volverán a describir aquí en esta realización.

Una persona con experiencia ordinaria en la técnica puede darse cuenta de que las unidades y los pasos del algoritmo de los ejemplos descritos en relación con las realizaciones descritas en la presente descripción pueden implementarse en hardware electrónico, o una combinación de software informático y hardware electrónico. La implementación de estas funciones en hardware o software depende de las aplicaciones específicas y las restricciones de diseño de la solución técnica. Los artesanos expertos pueden usar diferentes métodos para implementar la función descrita para cada aplicación en particular, pero dicha implementación no debe considerarse como una desviación del alcance de esta descripción.

Los expertos en la materia pueden comprender claramente que, en aras de la comodidad y la concisión de la descripción, para los procesos operativos específicos de los sistemas, aparatos y unidades descritos anteriormente, se puede hacer referencia a los procesos correspondientes en las realizaciones del método descritos anteriormente y se omite una descripción repetida.

En las realizaciones proporcionadas por la presente descripción, se aprecia que los aparatos y métodos descritos pueden implementarse de otras formas. Por ejemplo, las realizaciones del aparato descritas anteriormente son solo ejemplares. Por ejemplo, las unidades se dividen simplemente en términos de sus funciones lógicas. Sin embargo, en la implementación real, puede haber otros métodos de división. Por ejemplo, se pueden combinar o integrar varias unidades o componentes en otro sistema, o se pueden ignorar o no implementar algunas características. Además, los acoplamientos mutuos o los acoplamientos directos o las conexiones de comunicación mostrados o comentados pueden implementarse a través de algunas interfaces. Los acoplamientos indirectos o conexiones de comunicación entre los dispositivos o unidades pueden implementarse en formas eléctricas, mecánicas o de otro tipo.

La unidad descrita como partes separadas puede estar separada físicamente o no, y las partes que se muestran como una unidad pueden ser o no una unidad física, es decir, pueden estar ubicadas en un lugar o pueden estar distribuidas en múltiples unidades de red. Algunas o todas estas unidades pueden seleccionarse según las necesidades reales para lograr el propósito de la solución de la realización.

Además, varias unidades funcionales en las realizaciones de la presente descripción pueden integrarse en una unidad de procesamiento, o cada una de las unidades puede existir sola físicamente. Alternativamente, dos o más unidades funcionales pueden integrarse en una unidad.

Si las funciones se implementan en forma de una unidad funcional de software y se venden o utilizan como un producto independiente, las funciones pueden almacenarse en un medio de almacenamiento legible por ordenador. Basándose en tal entendimiento, las soluciones técnicas de esta descripción esencialmente, o la parte que contribuye al estado de la técnica, o una parte de las soluciones técnicas pueden implementarse en forma de un producto de software. El producto de software se almacena en un medio de almacenamiento e incluye varias instrucciones para dar instrucciones a un dispositivo informático (que puede ser un ordenador personal, un servidor o un equipo de red) para realizar todos o parte de los pasos de los métodos descritos en las realizaciones de la descripción. El medio de almacenamiento anterior incluye cualquier medio que pueda almacenar código de programa, como una unidad flash de bus serie universal (USB), un disco duro extraíble, una ROM, una RAM, un disco magnético o un disco óptico.

Lo mencionado anteriormente son simplemente implementaciones específicas de la presente descripción, pero el alcance de la descripción no se limita de ningún modo a las mismas. Cualquier modificación o sustitución que se les ocurriría fácilmente a los expertos en la materia, sin apartarse del alcance técnico descrito en la descripción, debería estar incluida en el alcance de la presente descripción. Por lo tanto, el alcance de la presente descripción se determinará por el alcance de las reivindicaciones.

Como apreciará un experto en la materia, todos o algunos de los pasos para implementar las diversas realizaciones de métodos descritos anteriormente pueden ejecutarse mediante hardware asociado con instrucciones de programa. El programa antes mencionado puede almacenarse en un medio de almacenamiento legible por ordenador. El programa, cuando se ejecuta, realiza los pasos de las realizaciones del método descritas anteriormente; y el medio de almacenamiento antes mencionado incluye varios medios que pueden almacenar códigos de programa, tales como una ROM, una RAM, un disco magnético o un disco óptico.

Finalmente, cabe señalar que las realizaciones anteriores solo se utilizan para ilustrar la solución técnica de las realizaciones de la presente descripción, y de ninguna manera constituyen ninguna limitación de la presente descripción; aunque se proporciona una descripción detallada de la presente descripción con referencia a las

realizaciones anteriores, debe tenerse en cuenta que las modificaciones a la solución técnica establecida en las realizaciones o los reemplazos equivalentes de una parte o la totalidad de las características técnicas pueden ser realizados por alguien con experiencia ordinaria en la técnica, y estas modificaciones o reemplazos no harán que las esencias de las soluciones técnicas correspondientes se aparten del alcance de las soluciones técnicas de las realizaciones de la presente descripción.

REIVINDICACIONES

1. Un método de verificación de integridad, que comprende:

recibir (S301), por un terminal, datos del plano de usuario transmitidos por un equipo del lado de la red;

realizar (S302), por parte del terminal, la verificación de integridad en los datos del plano de usuario en base a la información de configuración de verificación de integridad de los datos del plano de usuario;

caracterizado por que el terminal opera en un sistema de conectividad dual, DC, y el equipo del lado de la red actúa como un nodo secundario, SN, en el sistema de DC;

los datos del plano de usuario se transportan en una portadora de radio de datos, DRB, y la información de configuración de verificación de integridad del plano de usuario comprende una primera información de indicación configurada para indicar una DRB correspondiente a la verificación de integridad;

la realización (S302), por parte del terminal, de la verificación de integridad en los datos del plano de usuario en base a la información de configuración de verificación de integridad de los datos del plano de usuario comprende:

en caso de que al menos uno de los paquetes de datos transportados en la DRB indicados por la primera información de indicación falle la verificación de integridad, determinar, por parte del terminal, que los datos del plano de usuario transportados en la DRB fallan la verificación de integridad; o

en caso de que la relación entre el número de paquetes de datos transportados en la DRB indicada por la primera información de indicación que fallan la verificación de integridad y el número de paquetes de datos recibidos transportados en la DRB exceda un umbral preestablecido, determinar, por parte del terminal, que los datos del plano de usuario transportados en la DRB fallan en la verificación de integridad; o

en caso de que el número de paquetes de datos transportados en la DRB indicados por la primera información de indicación que fallan la verificación de integridad exceda un número preestablecido, determinar, por parte del terminal, que los datos del plano de usuario transportados en la DRB fallan la verificación de integridad; o

en caso de que el número de paquetes de datos transportados en la DRB indicados por la primera información de indicación que fallan en la verificación de integridad exceda un número preestablecido en una duración preestablecida, determinar, por parte del terminal, que los datos del plano de usuario transportados en la DRB fallan en la integridad cheque; o

en caso de que el número de paquetes de datos consecutivos transportados en la DRB indicados por la primera información de indicación que fallan la verificación de integridad supere un número preestablecido, determinar, por parte del terminal, que los datos del plano de usuario transportados en la DRB fallan la verificación de integridad;

y,

antes de realizar (S302), por parte del terminal, la verificación de integridad en los datos del plano de usuario en base a la información de configuración de verificación de integridad de los datos del plano de usuario, el método comprende además:

recibir, por parte del terminal, la información de configuración de verificación de integridad de datos del plano de usuario transmitida por el equipo del lado de la red;

y,

después de realizar (S302), por parte del terminal, la verificación de integridad en los datos del plano de usuario en base a la información de configuración de verificación de integridad de los datos del plano de usuario, el método comprende además:

en caso de que los datos del plano de usuario fallen en la verificación de integridad, transmitir, por parte del terminal, información de fallo de verificación de integridad a un nodo maestro, MN, en el sistema de DC.

2. El método según la reivindicación 1, en el que la información de configuración de verificación de integridad de datos del plano de usuario comprende además una tercera información de indicación;

la tercera información de indicación está configurada para dar instrucciones al terminal para que realice la verificación de integridad en los datos recibidos del plano de usuario transmitidos por otro equipo del lado de la red.

3. El método según la reivindicación 1 ó 2, en el que la información de configuración de verificación de integridad de datos del plano de usuario comprende además una cuarta información de indicación;

la cuarta información de indicación está configurada para indicar un algoritmo de verificación de integridad correspondiente a la verificación de integridad realizada en los datos del plano de usuario por el terminal.

4. Un método de verificación de integridad, que comprende:

transmitir (S401), mediante un equipo del lado de la red, información de configuración de verificación de integridad de datos del plano de usuario a un terminal, donde la información de configuración de verificación de integridad de datos del plano de usuario está configurada para instruir al terminal para que realice la verificación de integridad en los datos del plano de usuario recibidos del equipo del lado de la red;

transmitir (S402), por el equipo del lado de la red, los datos del plano de usuario al terminal;

caracterizado por que el equipo del lado de la red opera en un sistema de conectividad dual, DC, y el equipo del lado de la red actúa como un nodo secundario, SN, en el sistema de DC;

los datos del plano de usuario se transportan en una portadora de radio de datos, DRB, la información de configuración de verificación de integridad del plano de usuario comprende una primera información de indicación configurada para indicar una DRB correspondiente a la verificación de integridad;

la información de configuración de verificación de integridad del plano de usuario comprende además un primer criterio de determinación de si los datos del plano de usuario fallan en la verificación de integridad;

el primer criterio de determinación de si los datos del plano de usuario fallan en la verificación de integridad comprende:

en caso de que al menos uno de los paquetes de datos transportados en la DRB indicados por la primera información de indicación falle la verificación de integridad, los datos del plano de usuario transportados en la DRB fallan la verificación de integridad; o

en caso de que la relación entre el número de paquetes de datos transportados en la DRB indicada por la primera información de indicación que falla la verificación de integridad y el número de paquetes de datos recibidos transportados en la DRB exceda un umbral preestablecido, los datos del plano de usuario transportados en la DRB fallan la verificación de integridad; o

en caso de que el número de paquetes de datos transportados en la DRB indicados por la primera información de indicación que fallan la verificación de integridad exceda un número preestablecido, los datos del plano de usuario transportados en la DRB fallan la verificación de integridad; o

en caso de que el número de paquetes de datos transportados en la DRB indicados por la primera información indicación que fallan la verificación de integridad exceda un número preestablecido en una duración preestablecida, los datos del plano de usuario transportados en la DRB fallan la verificación de integridad; o

en caso de que el número de paquetes de datos consecutivos transportados en la DRB indicados por la primera información de indicación que falla la verificación de integridad exceda un número preestablecido, los datos del plano de usuario transportados en la DRB fallan la verificación de integridad.

5. Un terminal (80), que comprende:

un módulo (801) de recepción de datos, configurado para recibir datos del plano de usuario transmitidos por el equipo (100) del lado de la red;

un módulo (802) de verificación de integridad, configurado para realizar una verificación de integridad en los datos del plano de usuario en base a la información de configuración de verificación de integridad de los datos del plano de usuario;

caracterizado por que el terminal (80) opera en un sistema de doble conectividad, DC, y el equipo (100) del lado de la red actúa como un nodo secundario, SN, en el sistema de DC;

los datos del plano de usuario se transportan en una portadora de radio de datos, DRB, y la información de configuración de verificación de integridad del plano de usuario comprende una primera información de indicación configurada para indicar una DRB correspondiente a la verificación de integridad;

el módulo (802) de verificación de integridad está configurado específicamente para:

en caso de que al menos uno de los paquetes de datos transportados en la DRB indicados por la primera información de indicación falle la verificación de integridad, determinar que los datos del plano de usuario transportados en la DRB fallen la verificación de integridad; o

en caso de que una proporción de la cantidad de paquetes de datos transportados en la DRB indicados por la primera información de indicación que falla la verificación de integridad a la cantidad de paquetes de datos recibidos transportados en la DRB exceda un umbral preestablecido, determinar que los datos del plano de usuario transportados en la DRB fallan la verificación de integridad; o

en caso de que el número de paquetes de datos transportados en la DRB indicados por la primera información de

indicación que fallan la verificación de integridad exceda un número preestablecido, determinar que los datos del plano de usuario transportados en la DRB fallan la verificación de integridad; o

en caso de que el número de paquetes de datos transportados en la DRB indicados por la primera información de indicación que fallan la verificación de integridad exceda un número preestablecido en una duración preestablecida, determinar que los datos del plano de usuario transportados en la DRB fallan la verificación de integridad; o

en caso de que el número de paquetes de datos consecutivos transportados en la DRB indicados por la primera información de indicación que fallan la verificación de integridad exceda un número preestablecido, determinar que los datos del plano de usuario transportados en la DRB fallan la verificación de integridad;

y,

el terminal (80) comprende además un módulo (805) de recepción de información de configuración, configurado para, antes de realizar, mediante el módulo (802) de verificación de integridad, la verificación de integridad en los datos del plano de usuario en función de la configuración de verificación de integridad de datos del plano de usuario información, recibir la información de configuración de verificación de integridad de datos del plano de usuario transmitida por el equipo (100) del lado de la red

y,

el terminal (80) comprende además un módulo (806) de transmisión de información de fallos configurado para: en caso de que los datos del plano de usuario fallen la verificación de integridad, transmitir información de fallo de verificación de integridad a un nodo maestro, MN, en el sistema DC.

6. El terminal (80) según la reivindicación 5, en el que la información de configuración de verificación de integridad de datos del plano de usuario comprende además una tercera información de indicación;

la tercera información de indicación está configurada para instruir al terminal (80) para que realice la verificación de integridad en los datos recibidos del plano de usuario transmitidos por otro equipo (100) del lado de la red.

7. El terminal (80) según la reivindicación 5 ó 6, en el que la información de configuración de verificación de integridad de datos del plano de usuario comprende además una cuarta información de indicación;

la cuarta información de indicación está configurada para indicar un algoritmo de verificación de integridad correspondiente a la verificación de integridad realizada en los datos del plano de usuario por el terminal (80).

8. Equipo (100) del lado de la red, que comprende:

un módulo (1001) de transmisión de información de configuración, configurado para transmitir información de configuración de verificación de integridad de datos del plano de usuario a un terminal (80), en el que la información de configuración de verificación de integridad de datos del plano de usuario está configurada para instruir al terminal (80) para realizar una verificación de integridad de los datos del plano de usuario recibidos desde el equipo (100) del lado de la red;

un módulo (1002) de transmisión de datos, configurado para transmitir los datos del plano de usuario al terminal (80);

caracterizado por que el equipo (100) del lado de la red opera en un sistema de conectividad dual, DC, y el equipo (100) del lado de la red actúa como un nodo secundario, SN, en el sistema de DC;

los datos del plano de usuario se transportan en una portadora de radio de datos, DRB, la información de configuración de verificación de integridad del plano de usuario comprende una primera información de indicación configurada para indicar una DRB correspondiente a la verificación de integridad;

la información de configuración de verificación de integridad del plano de usuario comprende además un primer criterio de determinación de si los datos del plano de usuario fallan en la verificación de integridad;

el primer criterio de determinación de si los datos del plano de usuario fallan en la verificación de integridad comprende:

en caso de que al menos uno de los paquetes de datos transportados en la DRB indicados por la primera información de indicación falle la verificación de integridad, los datos del plano de usuario transportados en la DRB fallan la verificación de integridad; o

en caso de que la relación entre el número de paquetes de datos transportados en la DRB indicada por la primera información de indicación que falla la verificación de integridad y el número de paquetes de datos recibidos transportados en la DRB exceda un umbral preestablecido, los datos del plano de usuario transportados en la DRB fallan la verificación de integridad; o

en caso de que el número de paquetes de datos transportados en la DRB indicados por la primera información de indicación que fallan la verificación de integridad exceda un número preestablecido, los datos del plano de usuario

transportados en la DRB fallan la verificación de integridad; o

en caso de que el número de paquetes de datos transportados en la DRB indicados por la primera información de indicación que fallan la verificación de integridad exceda un número preestablecido en una duración preestablecida, los datos del plano de usuario transportados en la DRB fallan la verificación de integridad; o

en caso de que el número de paquetes de datos consecutivos transportados en la DRB indicados por la primera información de indicación que falla la verificación de integridad exceda un número preestablecido, los datos del plano de usuario transportados en la DRB fallan la verificación de integridad.

Fig. 1

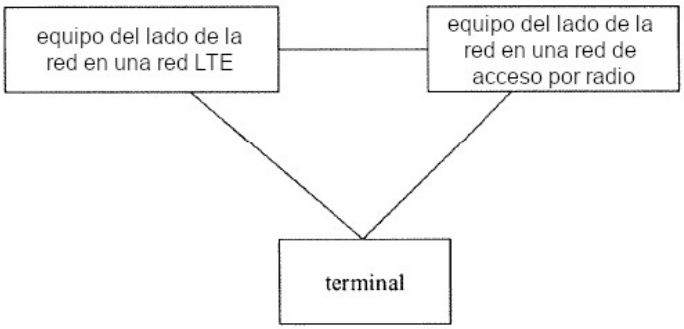

Fig. 2

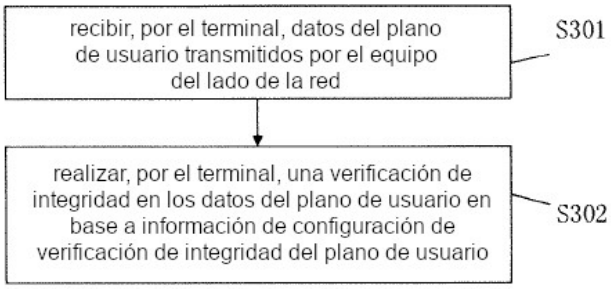

Fig. 3

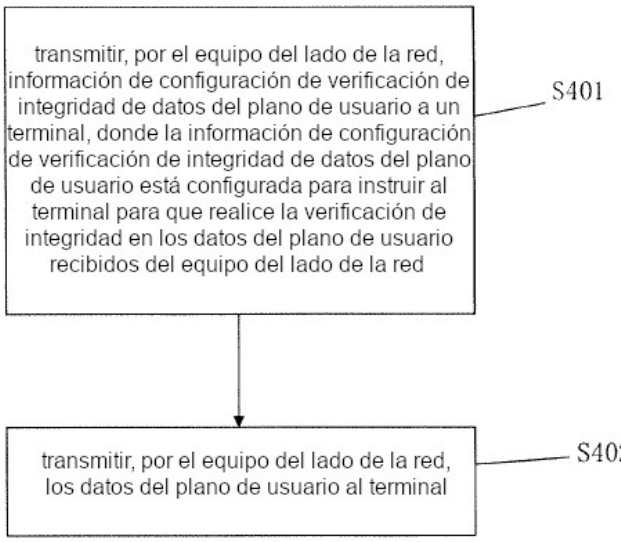

Fig. 4

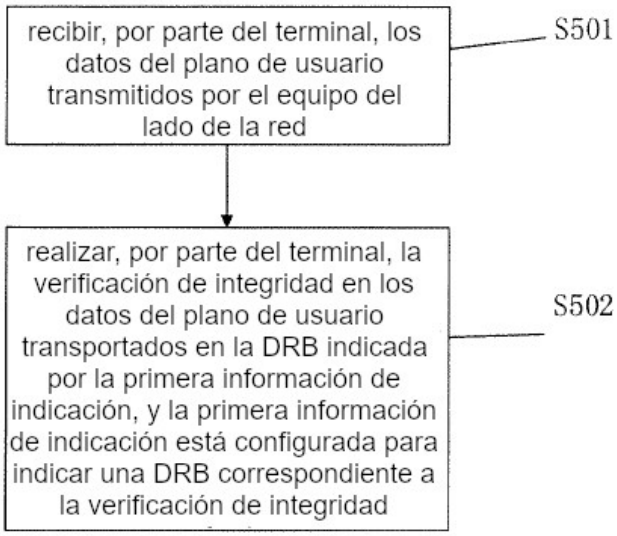
recibir, por parte del terminal, los datos del plano de usuario transmitidos por el equipo del lado de la red
S501
realizar, por parte del terminal, la verificación de integridad en los datos del plano de usuario transportados en la DRB indicada por la primera información de indicación, y la primera información de indicación está configurada para indicar una DRB correspondiente a la verificación de integridad
S502

Fig. 5

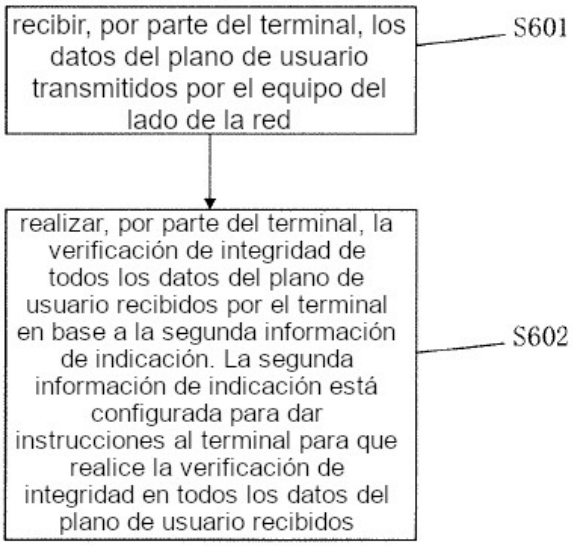
recibir, por parte del terminal, los datos del plano de usuario transmitidos por el equipo del lado de la red
S601
realizar, por parte del terminal, la verificación de integridad de todos los datos del plano de usuario recibidos por el terminal en base a la segunda información de indicación. La segunda información de indicación está configurada para dar instrucciones al terminal para que realice la verificación de integridad en todos los datos del plano de usuario recibidos
S602

Fig. 6

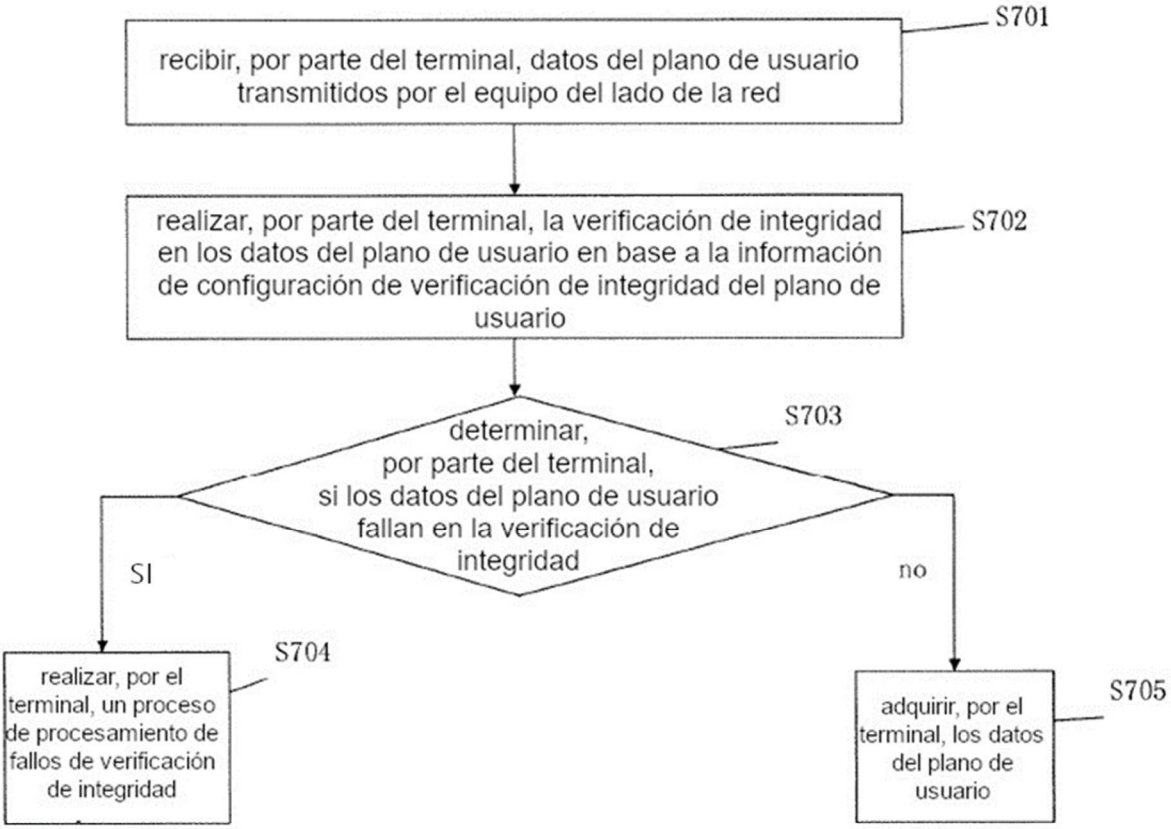
S701
recibir, por parte del terminal, datos del plano de usuario transmitidos por el equipo del lado de la red
S702
realizar, por parte del terminal, la verificación de integridad en los datos del plano de usuario en base a la información de configuración de verificación de integridad del plano de usuario
S703
determinar, por parte del terminal, si los datos del plano de usuario fallan en la verificación de integridad
SI
no
S704
realizar, por el terminal, un proceso de procesamiento de fallos de verificación de integridad
S705
adquirir, por el terminal, los datos del plano de usuario

Fig. 7

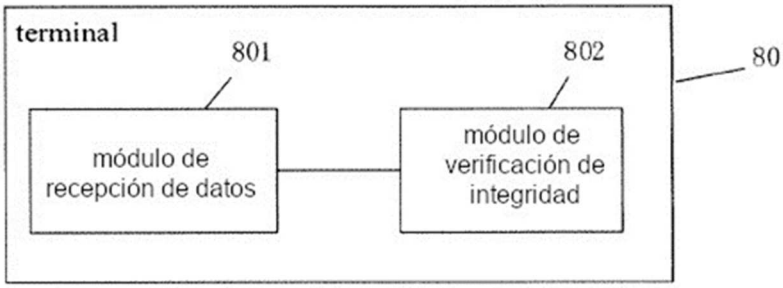
terminal
801
802
80
módulo de recepción de datos
módulo de verificación de integridad

Fig. 8

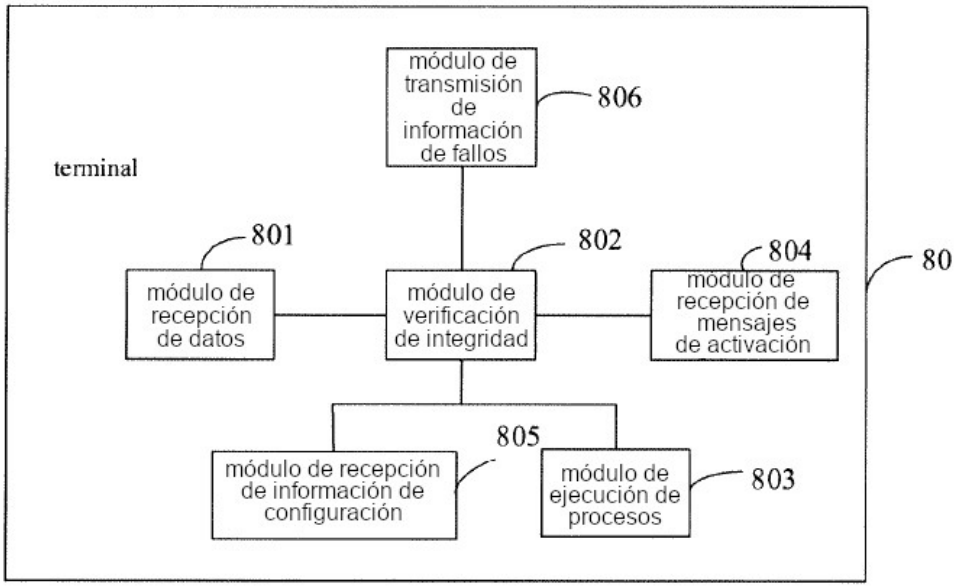

Fig. 9

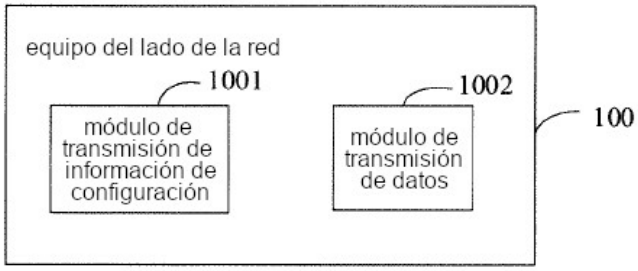

Fig. 10

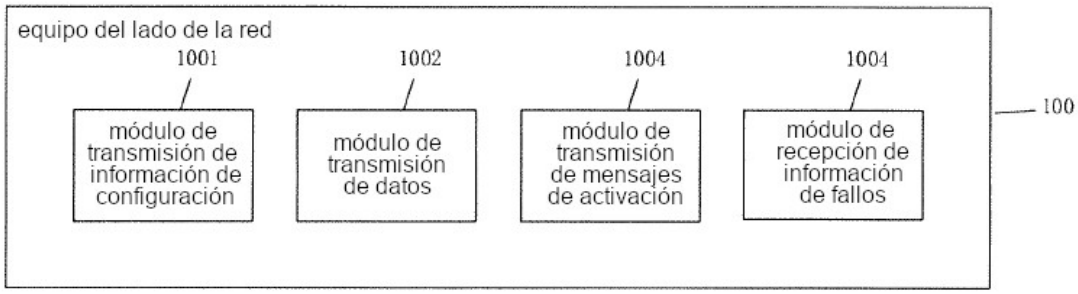

Fig. 11

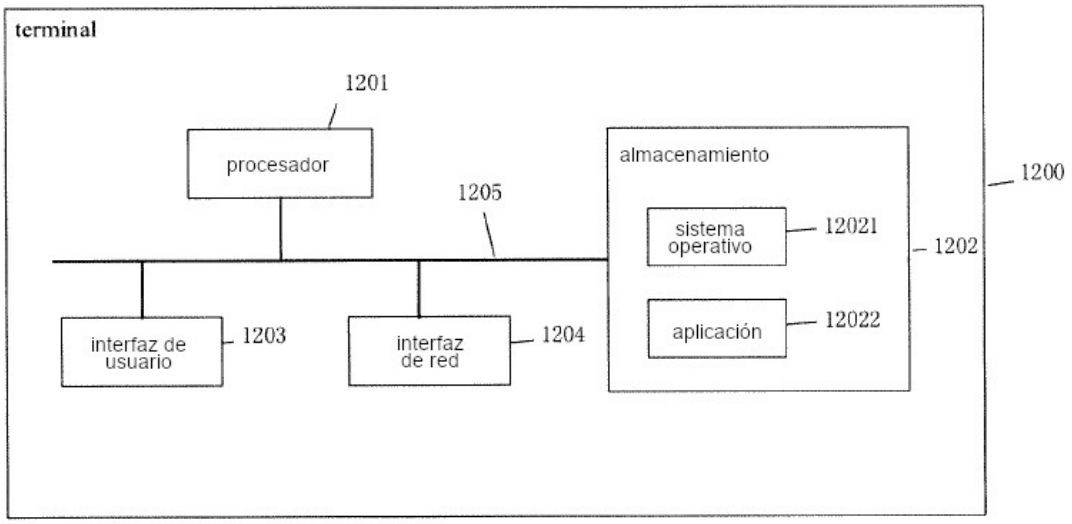
terminal
1201
procesador
1205
almacenamiento
sistema operativo
12021
1202
1200
aplicación
12022
interfaz de usuario
1203
interfaz de red
1204

Fig. 12

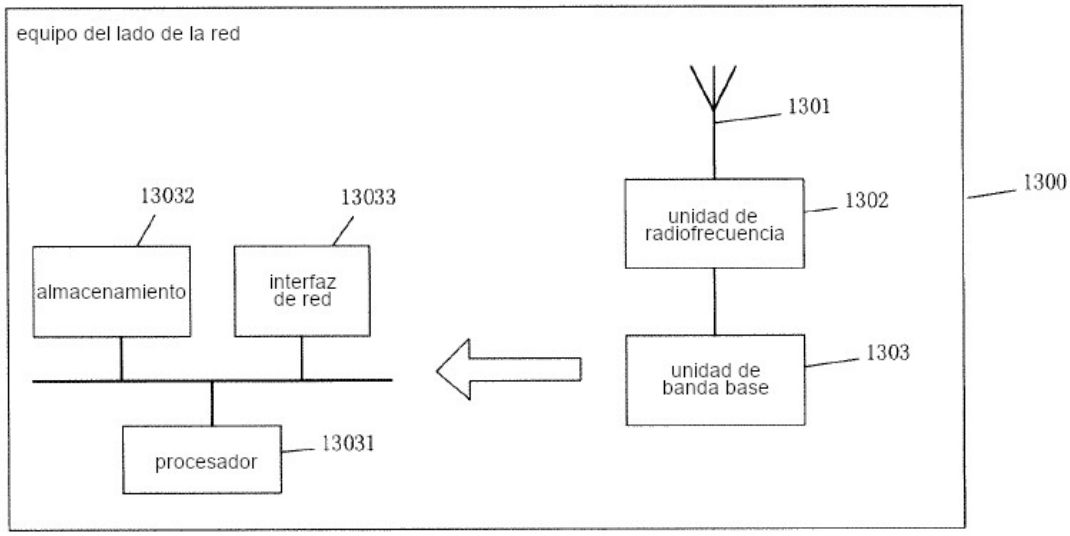
equipo del lado de la red
1301
13032
13033
unidad de radiofrecuencia
1302
1300
almacenamiento
interfaz de red
unidad de banda base
1303
procesador
13031

Fig. 13