(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 715 273**

(51) Int. CI.:

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **22.10.2008 E 08018472 (4)**

(97) Fecha y número de publicación de la concesión europea: **12.12.2018 EP 2053828**

(54) Título: **Método y aparato de desencriptado para una capa de protocolo de convergencia de datos de paquete en un sistema de comunicación inalámbrico**

(30) Prioridad:

**22.10.2007 US 981518 P**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**03.06.2019**

(73) Titular/es:

**INNOVATIVE SONIC LIMITED (100.0%)**
**2nd Floor, The Axis, 26 Cybercity**
**Ebene 72201, MU**

(72) Inventor/es:

**KUO, RICHARD LEE-CHEE**

(74) Agente/Representante:

**CARVAJAL Y URQUIJO, Isabel**

**DESCRIPCIÓN**

Método y aparato de desencriptado para una capa de protocolo de convergencia de datos de paquete en un sistema de comunicación inalámbrico.

La presente invención se refiere a un método y un aparato para tratar el desencriptado de datos en un sistema de comunicaciones inalámbrico según las reivindicaciones 1 y 5.

El sistema de telecomunicaciones móviles de tercera generación (denominado sistema 3G) proporciona utilización de espectro de alta frecuencia, cobertura universal y transmisión de datos multimedia de alta calidad y a alta velocidad, y cumple también toda clase de requisitos de QoS simultáneamente, proporcionando servicios de transmisión diversos, flexibles y de dos vías y una mejor calidad de comunicación para reducir tasas de interrupción de transmisión. Sin embargo, debido a la demanda de alta velocidad y aplicaciones multimedia, se han desarrollado la tecnología de telecomunicaciones móviles de próxima generación y los protocolos de comunicación relacionados.

El sistema de comunicaciones inalámbrico de evolución a largo plazo (sistema LTE), un sistema de comunicaciones inalámbrico de alta velocidad avanzado establecido tras el sistema de telecomunicaciones móviles 3G, solamente soporta la transmisión conmutada por paquetes, y tiende a simplificar la estructura de sistema y reducir el retardo de trasmisión, para mejorar la tasa de transmisión.

En el sistema LTE, tras una conmutación de la llamada en curso, se permite que la capa de RLC (control de radioenlace) en un equipo de usuario (UE) entregue PDU (unidades de datos de protocolo) fuera de secuencia desde una estación de base de fuente hasta la capa de PDCP. La capa de PDCP (protocolo de convergencia de datos de paquete) es una capa superior de la capa de RLC, y se usa para descifrar las PDU, para evitar que se roben datos de usuario y determinada información de señalización. La entrega fuera de secuencia significa que se entregan paquetes a una capa superior que se ha quedado sin números de secuencia.

Generalmente, el desencriptado en el sistema de comunicación inalámbrico depende de un conjunto de parámetros de seguridad, que incluye una clave y otros parámetros o variables, tales como un valor de recuento, una identidad de portador y direcciones de paquetes. Un UE utiliza un algoritmo específico para descifrar los datos de texto cifrado según el conjunto de parámetros de seguridad, para generar los datos de texto plano.

El valor de recuento está compuesto por un HFN (número de hipertrama) de receptor y un SN (número de secuencia) incorporado en la cabecera de un paquete. El HFN es similar al número portante del SN. Cada vez que el SN devuelve su valor de representación máximo de vuelta a 0, el HFN se incrementa en uno. Por ejemplo, si SN se representa mediante 7 bits, que va desde 0 hasta 127, una vez que SN está por encima de 127, HFN se incrementa en 1, y SN se reinicia desde 0. Como resultado, según el SN, un emisor y un receptor pueden incrementar de manera oportuna el HFN, para conservar la sincronización del HFN y mantener el proceso de cifrado y descifrado. Además, antes de descifrar paquetes, la capa de PDCP compara el SN incorporado en una cabecera de un paquete con número de secuencia de receptor de PDCP previsto siguiente (Next_PDCP_RX_SN) mantenido en la capa de PDCP. Si el SN es menor que el Next_PDCP_RX_SN, significa que SN está por encima de 127, y ha de reiniciarse desde 0. Por tanto, el HFN de receptor (RX_HFN) se incrementa en 1, para conservar la sincronización con el emisor. La descripción anterior muestra que es necesario que la capa de PDCP mantenga un Next_PDCP_RX_SN y un RX_HFN para descifrar paquetes.

Según la técnica anterior, tras una conmutación de la llamada en curso, un proceso de descifrado en la capa de PDCP del UE que opera en un modo no reconocido (UM) de la capa de RLC reestablece las variables de seguridad, concretamente un Next_PDCP_RX_SN y un RX_HFN, y luego descifra paquetes recibidos desde la estación de base de fuente. Es necesario reestablecer el Next_PDCP_RX_SN y el RX_HFN debido a un cambio de clave en la estación de base objetivo.

Sin embargo, estos paquetes se cifran mediante la estación de base de fuente antes de una conmutación de la llamada en curso que utiliza un valor de recuento generado por variables de seguridad que no están reestablecidas, al tiempo que el UE utiliza las variables de seguridad reestablecidas para descifrar paquetes durante una conmutación de la llamada en curso. En esta situación, el UE no puede descifrar paquetes recibidos desde la estación de base de fuente correctamente. Por ejemplo, un UE y una estación de base de fuente procesan un servicio de radiodifusión de medios por caudales (un servicio en UM). Al comienzo de la conmutación de la llamada en curso, los HFN en la estación de base de fuente y el UE (es decir TX_HFN y RX_HFN) son ambos “120” para generar un valor de recuento para cifrar y descifrar paquetes. Justo antes de la conmutación de la llamada en curso, partes de los paquetes se almacenan en la capa de RLC debido a que están fuera de secuencia. Tras la conmutación de la llamada en curso, estos paquetes fuera de secuencia se entregan a la capa de PDCP. Antes de que estos paquetes se descifren, el UE reestablece el Next_PDCP_RX_SN y el RX_HFN a “0” según un proceso de conmutación de la llamada en curso de la técnica anterior. Como resultado, cuando se descifran paquetes, el RX_HFN utilizado por el UE es diferente del TX_HFN utilizado por la estación de base de fuente para descifrar los paquetes. Por tanto, los paquetes no pueden descifrarse correctamente. En esta situación, aunque estos paquetes se descifran y se envían a una capa superior, datos descifrados incorrectos provocarán errores en imagen de radiodifusión de medios, y afectarán a la calidad de servicio.

El documento WO 2007/004051 A1 da a conocer que cuando se prepara un traspaso en la estación de base anterior, se intercambian sellos de tiempo que se usan para crear la clave de sesión con la estación de base objetivo. La estación de base anterior envía la red de acceso seleccionada y sellos de tiempo de equipo de usuario a la estación de base objetivo junto con señalización de transferencia de contexto. En este respecto, se da a conocer un enfoque novedoso, que utiliza un protocolo de transferencia de contexto entre estaciones de base.

El documento WO00/76194 A1 da a conocer una conmutación de la llamada en curso entre un sistema GSM y un sistema UMTS.

El documento US 2007/0242683 A1 da a conocer tratar un solo paquete de datos con dos porciones de paquete de datos diferentes basándose en dos operaciones diferentes.

Por tanto, en la técnica anterior, dado que las variables de seguridad reestablecidas son diferentes de las variables de seguridad utilizadas por la estación de base de fuente para cifrar paquetes, un equipo de usuario tras la conmutación de la llamada en curso se encontrará con una situación de falla de descifrado o paquetes de descrifrado en datos no válidos al descifrar los paquetes recibidos desde la estación de base de fuente.

Teniendo esto en cuenta, la presente invención tiene como objetivo proporcionar un método y un aparato para tratar el desencriptado de datos para una capa de protocolo de convergencia de datos de paquete (PDCP) de un equipo de usuario tras una conmutación de la llamada en curso en un sistema de comunicaciones inalámbrico, para descifrar correctamente paquetes recibidos desde una estación de base de fuente.

Esto se logra mediante las características de las reivindicaciones independientes. Las reivindicaciones dependientes están relacionadas con desarrollos y mejoras adicionales correspondientes.

Tal como se observará con mayor claridad a partir de la descripción detallada a continuación, un método reivindicado para tratar paquetes de datos cifrados por una estación de base de fuente antes de una conmutación de la llamada en curso en un sistema de comunicación inalámbrico, en el que el método se lleva a cabo en una capa de protocolo de convergencia de datos de paquete de un equipo de usuario, comprende recibir en un modo no reconocido los paquetes de datos desde la capa de RLC del equipo de usuario cuando el equipo de usuario realiza un procedimiento de conmutación de la llamada en curso. Según la invención, el método comprende además usar variables de seguridad correspondientes a la estación de base de fuente para descifrar los paquetes de datos recibidos y reestablecer las variables de seguridad después de usar variables de seguridad correspondientes a la estación de base de fuente para descifrar los paquetes de datos recibidos.

Las variables de seguridad comprenden un número de secuencia de receptor de PDCP previsto siguiente, conocido como Next_PDCP_RX_SN, y un número de hipertrama de receptor, conocido como RX_HFN.

**Breve descripción de los dibujos**

La figura 1 es un diagrama esquemático de un sistema de comunicación inalámbrico.

La figura 2 es un diagrama de bloques funcional de un dispositivo de comunicación inalámbrico.

La figura 3 es un diagrama esquemático de código de programa mostrado en la figura 2.

La figura 4 es un diagrama de flujo según una realización de la presente invención.

Remítase a la figura 1, que es un diagrama esquemático de un sistema 100 de comunicaciones inalámbrico. Se prefiere que el sistema 100 de comunicaciones inalámbrico sea un sistema LTE, y esté brevemente formado por un terminal de red y una pluralidad de equipos de usuario. En la figura 1, el terminal de red y los equipos de usuario (UE) se utilizan simplemente para ilustrar la estructura del sistema 100 de comunicaciones inalámbrico. En la práctica, el terminal de red puede incluir una pluralidad de estaciones de base, controladores de red de radio, y así sucesivamente, según demandas reales, y los UE pueden ser aparatos tales como teléfonos móviles, sistemas informáticos, etc.

Remítase a la figura 2, que es un diagrama de bloques funcional de un dispositivo 200 de comunicaciones, que puede utilizarse para implementar el equipo de usuario mostrado en la figura 1. Por motivos de brevedad, la figura 2 muestra solamente un dispositivo 202 de entrada, un dispositivo 204 de salida, un circuito 206 de control, una unidad 208 de procesamiento central (CPU), una memoria 210, un código 212 de programa y un transceptor 214 del dispositivo 200 de comunicaciones. En el dispositivo 200 de comunicaciones, el circuito 206 de control ejecuta el código 212 de programa en la memoria 210 a través de la CPU 208, controlando de ese modo una operación del dispositivo 200 de comunicaciones. El dispositivo 100 de comunicaciones puede recibir señales introducidas por un usuario a través del dispositivo 202 de entrada, tal como un teclado, y puede emitir imágenes y sonidos a través del dispositivo 204 de salida, tal como un monitor o unos altavoces. El transceptor 214 se usa para recibir y transmitir señales inalámbricas, entregando señales recibidas al circuito 206 de control, y emitiendo señales generadas por el circuito 206 de control de manera inalámbrica. Desde una perspectiva de un marco de protocolo de comunicaciones, el transceptor 214 puede verse como una porción de capa 1, y el circuito 206 de control puede utilizarse para

realizar funciones de capa 2 y capa 3.

Remítase a continuación a la figura 3. La figura 3 es un diagrama del código 212 de programa mostrado en la figura 2. El código 212 de programa incluye una capa 300 de aplicación, una capa 302 3 y una capa 306 2, y está acoplado a una capa 310 1. La capa 302 3 comprende una capa 304 de PDCP. La capa 306 2 se utiliza para realizar control de enlace. La capa 310 1 se utiliza para realizar conexiones físicas. En enlace descendente, la capa 304 de PDCP recibe una PDU (unidad de datos de protocolo) desde la capa 306 2, y realiza procesos, tales como retirada de cabecera, descompresión de cabecera, desencriptado, etc., para entregar los datos de plano de usuario descifrados a una capa superior (tal como la capa 300 de aplicación).

Para el descifrado de la capa de PDCP tras la conmutación de la llamada en curso, el código 212 de programa según la realización de la presente invención proporciona un código 320 de programa de desencriptado para descifrar paquetes recibidos desde una estación de base de fuente. Remítase a la figura 4, que es un diagrama esquemático de un proceso 40 según una realización de la presente invención. El proceso 40 se utiliza en la capa de PDCP de un equipo de usuario, y se usa para descifrar datos de plano de usuario tras una conmutación de la llamada en curso. El proceso 40 puede codificarse al código 320 de programa de desencriptado, e incluye las siguientes etapas:

Etapa 400: Inicio.

Etapa 402: Usar variables de seguridad correspondientes a una estación de base de fuente para descifrar paquetes recibidos desde la estación de base de fuente cuando el equipo de usuario realiza un procedimiento de conmutación de la llamada en curso desde la estación de base de fuente a una estación de base objetivo.

Etapa 404: Reestablecer las variables de seguridad.

Etapa 406: Reestablecer protocolo de compresión y descompresión de cabecera.

Etapa 408: Fin

Según el proceso 40, la realización de la presente invención usa variables de seguridad correspondientes a la estación de base de fuente para descifrar paquetes recibidos desde la estación de base de fuente, reestablece las variables de seguridad, y luego reestablece el protocolo de compresión y descompresión de cabecera, para completar el procedimiento de conmutación de la llamada en curso de la capa de PDCP.

Preferiblemente, las variables de seguridad incluyen un número de secuencia de receptor de PDCP previsto siguiente (Next_PDCP_RX_SN) y un número de hipertrama de receptor (RX_HFN).

Dicho de otro modo, el UE utiliza variables de seguridad correspondientes a una estación de base de fuente para descifrar paquetes recibidos desde la estación de base de fuente, para evitar que las variables de seguridad reestablecidas no puedan descifrar paquetes recibidos desde la estación de base de fuente correctamente, o descifrar paquetes en datos no válidos puesto que el equipo de usuario lleva a cabo una conmutación de la llamada en curso y reestablece variables de seguridad a “0” antes de descifrar los paquetes recibidos desde la estación de base de fuente.

En el proceso 40, las variables de seguridad correspondientes a la estación de base de fuente significan variables de seguridad no modificadas cuando un equipo de usuario lleva a cabo un procedimiento de conmutación de la llamada en curso. Preferiblemente, un equipo de usuario usa variables de seguridad para descifrar paquetes recibidos desde la estación de base de fuente antes de que se reestablezcan las variables de seguridad debido a un procedimiento de conmutación de la llamada en curso.

Tal como puede observarse, cuando un equipo de usuario lleva a cabo a procedimiento de conmutación de la llamada en curso desde una estación de base de fuente hasta una estación de base objetivo, la capa de PDCP del equipo de usuario usa variables de seguridad correspondientes a la estación de base de fuente para descifrar paquetes recibidos desde la estación de base de fuente, para hacer que los paquetes se descifren correctamente, de modo que aumenta la validez de los paquetes descifrados en el sistema de comunicación inalámbrico.

Además, los paquetes se transmiten en UM durante una conmutación de la llamada en curso, y los paquetes recibidos desde la estación de base de fuente pueden ser unos datos de plano de usuario.

Obsérvese que la figura 4 es un diagrama de flujo según una realización a modo de ejemplo de la presente invención, y los expertos en la técnica pueden realizar alteraciones y modificaciones de manera acorde. Por ejemplo, el equipo de usuario usa variables de seguridad correspondientes a la estación de base de fuente para descifrar paquetes recibidos desde la estación de base de fuente, ejecuta la etapa 406 en primer lugar, y luego ejecuta la etapa 404. El punto principal es que el equipo de usuario variables de seguridad no reestablecidas para descifrar paquetes.

En la técnica anterior, la capa de PDCP descifra los paquetes recibidos desde la estación de base de fuente con variables de seguridad reestablecidas. Dado que las variables de seguridad reestablecidas difieren de las variables de seguridad utilizadas para el cifrado de estación de base de fuente, los paquetes se descifrarán incorrectamente. En comparación con la realización de la presente invención, con el fin de descifrar correctamente, el equipo de usuario mantiene variables de seguridad en la capa de PDCP para descifrar los paquetes recibidos desde la estación de base de fuente, y luego reestablece variables de seguridad tras completar el desencriptado. En esta situación, el usuario utiliza variables de seguridad correspondientes a la estación de base de fuente para descifrar los paquetes recibidos desde la estación de base de fuente, descifrando correctamente de ese modo los paquetes, para aumentar la validez de los paquetes descifrados en el sistema de comunicación inalámbrico.

En conclusión, la realización de la presente invención utiliza las variables de seguridad correspondientes a la estación de base de fuente para descifrar los paquetes recibidos desde la estación de base de fuente, y luego reestablece las variables de seguridad para el procesamiento en la estación de base de base objetivo. Por tanto, el equipo de usuario puede descifrar correctamente paquetes, y generar datos útiles y válidos.

**REIVINDICACIONES**

1. Método para tratar paquetes de datos cifrados mediante una estación de base de fuente antes de una conmutación de la llamada en curso en un sistema de comunicación inalámbrico, el método se lleva a cabo en un protocolo de convergencia de datos de paquete, denominado a continuación en el presente documento capa de PDCP de un equipo de usuario, en el que el método comprende:

recibir en un modo no reconocido paquetes de datos fuera de secuencia almacenados en la capa de RLC del equipo de usuario tras un procedimiento (402) de conmutación de la llamada en curso

caracterizado por las etapas de:

usar variables de seguridad correspondientes a la estación de base de fuente para descrifrar los paquetes (402) de datos fuera de secuencia; y

reestablecer las variables de seguridad tras terminar de descifrar todos los paquetes de datos fuera de secuencia almacenados en la capa (404) de RLC;

en el que las variables de seguridad comprenden un número de secuencia de receptor de PDCP previsto siguiente, conocido como Next_PDCP_RX_SN, y un número de hipertrama de receptor, conocido como RX_HFN.

2. Método según la reivindicación 1, caracterizado porque los paquetes recibidos desde la estación de base de fuente se utilizan para transmisión de datos de plano de usuario.

3. Método según una de las reivindicaciones anteriores, caracterizado porque los paquetes de datos se reciben mediante la capa de RLC del equipo de usuario desde la estación de base de fuente antes de que se inicie el procedimiento de conmutación de la llamada en curso.

4. Método según una de las reivindicaciones anteriores, caracterizado porque reestablecer las variables de seguridad significa establecer las variables de seguridad a cero.

5. Dispositivo (100) de comunicaciones para tratar correctamente un desencriptado de datos en un protocolo de convergencia de datos de paquete, denominado a continuación en el presente documento capa de PDCP, tras una conmutación de la llamada en curso en un sistema de comunicaciones inalámbrico, comprendiendo el dispositivo (100) de comunicaciones:

un circuito (106) de control para realizar funciones del dispositivo (100) de comunicaciones;

un procesador (108) instalado en el circuito (106) de control, para ejecutar un código (112) de programa para controlar el circuito (106) de control; y

una memoria (110) instalada en el circuito (106) de control y acoplada al procesador (108) para almacenar el código (112) de programa;

caracterizado porque el dispositivo de comunicaciones constituye un aparato que a su vez es capaz de llevar a cabo el método según una de las reivindicaciones anteriores.

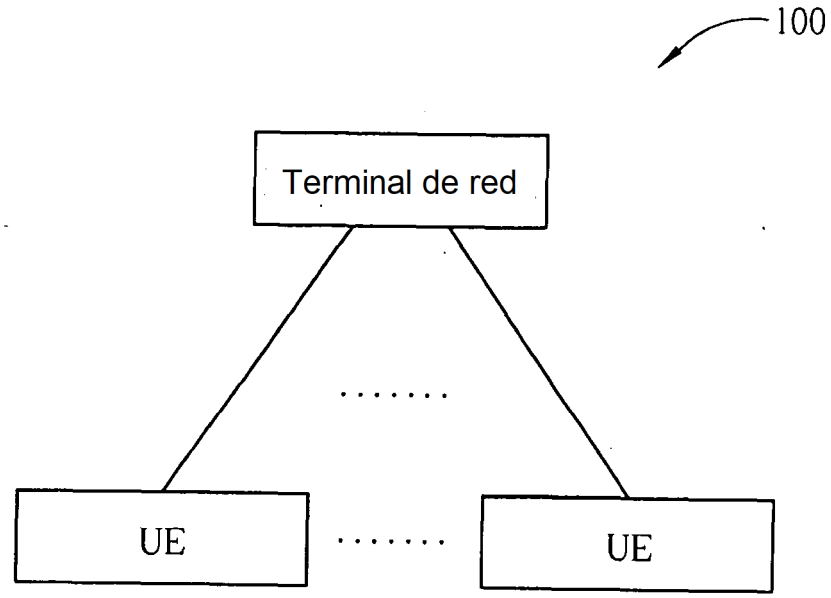


FIG. 1

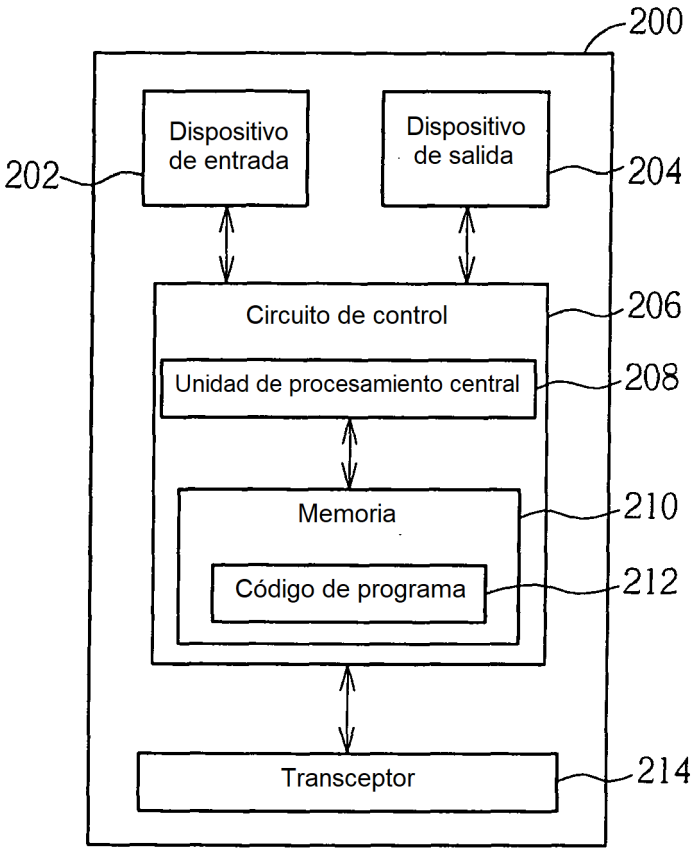
200
Dispositivo de entrada
202
Dispositivo de salida
204
Circuito de control
206
Unidad de procesamiento central
208
Memoria
210
Código de programa
212
Transceptor
214

FIG. 2

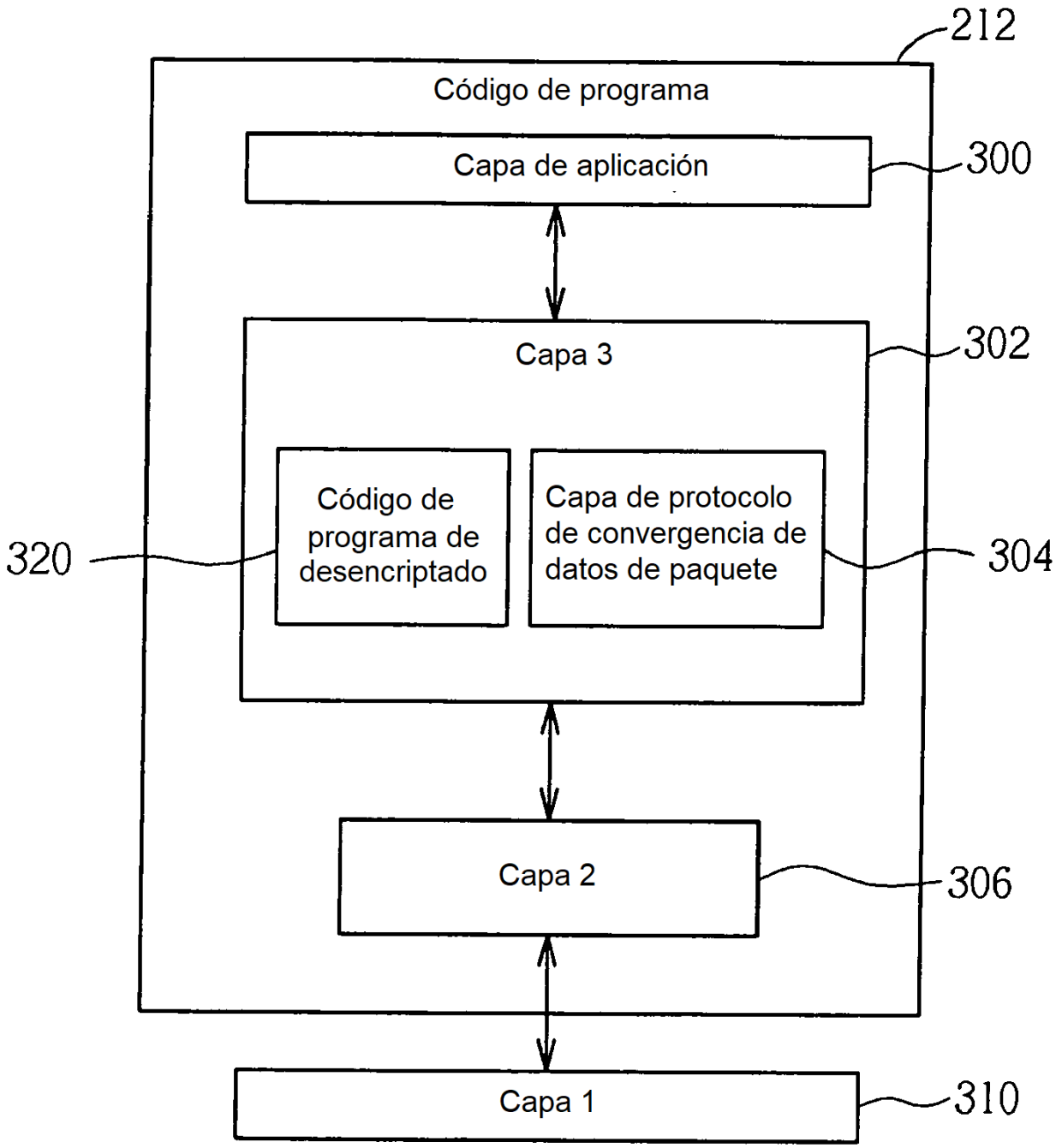
212
Código de programa
Capa de aplicación
300
Capa 3
302
Código de programa de desencriptado
Capa de protocolo de convergencia de datos de paquete
320
304
Capa 2
306
Capa 1
310

FIG. 3

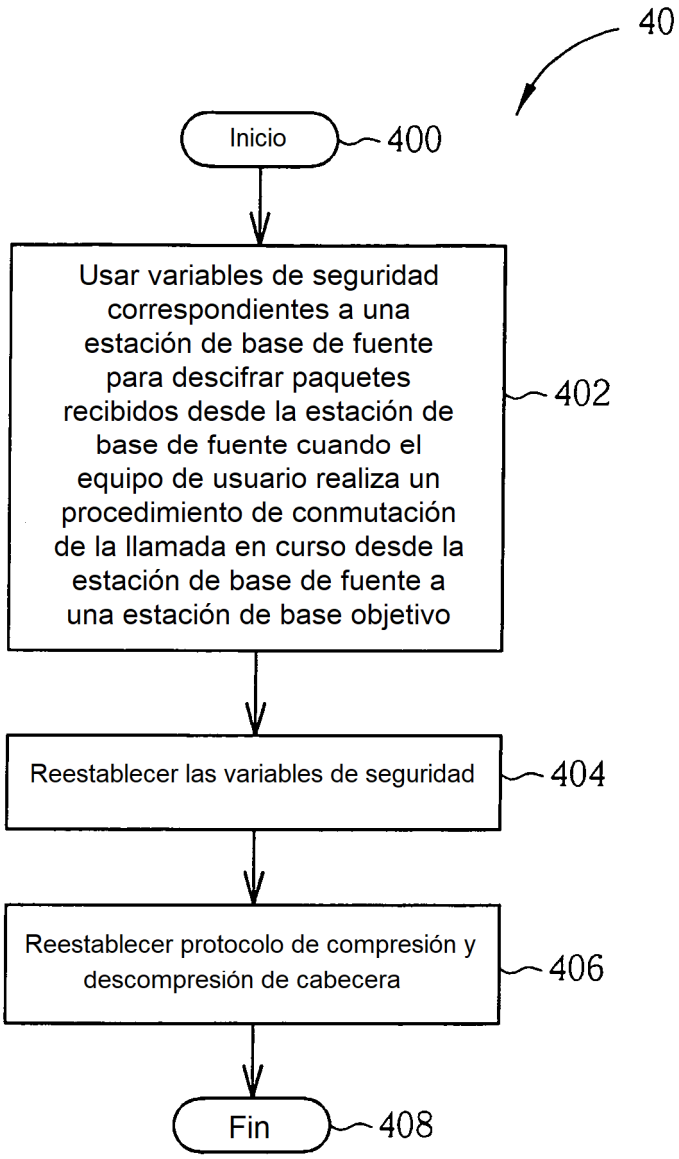
40
Inicio
400
Usar variables de seguridad correspondientes a una estación de base de fuente para descifrar paquetes recibidos desde la estación de base de fuente cuando el equipo de usuario realiza un procedimiento de conmutación de la llamada en curso desde la estación de base de fuente a una estación de base objetivo
402
Reestablecer las variables de seguridad
404
Reestablecer protocolo de compresión y descompresión de cabecera
406
Fin
408

FIG. 4