(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 666 226**

(51) Int. CI.:

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **04.08.2008 PCT/KR2008/004514**

(87) Fecha y número de publicación internacional: **19.02.2009 WO09022803**

(96) Fecha de presentación y número de la solicitud europea: **04.08.2008 E 08793028 (5)**

(97) Fecha y número de publicación de la concesión europea: **28.03.2018 EP 2156593**

(54) Título: **Método para detectar un error de seguridad en un sistema de comunicaciones móviles y dispositivo de comunicaciones móviles**

(30) Prioridad:

10.08.2007 US 955040 P
23.07.2008 KR 20080071933

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.05.2018

(73) Titular/es:

LG ELECTRONICS INC. (100.0%)
20, YEOUIDO-DONG, YEONGDEUNGPO-GU
SEOUL 150-721, KR

(72) Inventor/es:

LEE, YOUNG-DAE;
CHUN, SUNG-DUCK;
PARK, SUNG-JUN y
YI, SEUNG-JUNE

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método para detectar un error de seguridad en un sistema de comunicaciones móviles y dispositivo de comunicaciones móviles

Campo técnico

La presente invención se refiere a un método y a un dispositivo para detectar un error de seguridad en un algoritmo de seguridad en uso para una capa de PDCP de un sistema LTE (Evolución a Largo Plazo).

Antecedentes de la técnica

La FIG. 1 es una estructura de red de un sistema LTE (Evolución a Largo Plazo), el sistema de comunicación móvil de la técnica relacionada. Para el sistema LTE, que ha evolucionado a partir del sistema UMTS existente, las estandarizaciones básicas están en curso en el 3GPP.

Una red LTE se puede dividir en una E-UTRAN (Red de Acceso de Radio Terrestre UMTS Evolucionada) y una CN (Red Central). Un E-UMTS incluye un terminal (o UE (Equipo de Usuario)), una estación base (eNB (NodoB Evolucionado) y una pasarela de acceso (aGW). La pasarela de acceso se puede dividir en una parte que maneja el procesamiento del tráfico de usuario y una parte que maneja el tráfico de control. En este caso, la parte de pasarela de acceso que procesa el tráfico de usuario y la parte de pasarela de acceso que procesa el tráfico de control pueden comunicarse una con otra usando una nueva interfaz. Pueden existir una o más celdas en un único eNB. Se puede usar una interfaz para transmitir tráfico de usuario o tráfico de control entre los eNB. La CN puede incluir la pasarela de acceso y un nodo o similar para el registro de usuario del UE. Se puede usar una interfaz para discriminar la E-UTRAN y la CN.

La FIG. 2 muestra una estructura ejemplar de un plano de control (plano C) de un protocolo de interfaz de radio entre el UE y la E-UTRAN en base a los estándares de red de acceso de radio del 3GPP. La FIG. 3 muestra una estructura ejemplar de un plano de usuario (plano U) del protocolo de interfaz de radio entre el UE y la E-UTRAN en base a los estándares de red de acceso de radio del 3GPP.

La estructura del protocolo de interfaz de radio entre el UE y la E-UTRAN se describirá ahora con referencia a las FIG. 2 y 3.

El protocolo de interfaz de radio tiene capas horizontales que comprenden una capa física, una capa de enlace de datos y una capa de red, y tiene planos verticales que comprenden un plano de usuario (plano U) para transmitir información de datos y un plano de control (plano C) para transmitir señales de control. Las capas de protocolo en las FIG. 2 y 3 se pueden categorizar como una primera capa (L1), una segunda capa (L2) y una tercera capa (L3) en base a las tres capas inferiores de un modelo de estándar de interconexión de sistemas abiertos (OSI) ampliamente conocido en el sistema de comunicación. Las capas de protocolo de radio existen como pares entre el UE y la E-UTRAN y manejan una transmisión de datos en una interfaz de radio.

Las capas del plano de control del protocolo de radio de la FIG. 2 y las del plano de usuario del protocolo de radio en la FIG. 3 se describirán ahora como sigue.

La capa física, la primera capa, proporciona un servicio de transferencia de información a una capa superior usando un canal físico. La capa física está conectada a una capa superior llamada capa de control de acceso al medio (MAC) a través de un canal de transporte. Los datos se transfieren entre la capa MAC y la capa física a través del canal de transporte. El canal de transporte se divide en un canal de transporte dedicado y un canal común según si se comparte o no un canal. Entre las diferentes capas físicas, esto es, entre una capa física de un lado de transmisión (emisor) y la de un lado de recepción (receptor), los datos se transfieren a través del canal físico.

La segunda capa incluye varias capas. Primero, una capa de control de acceso al medio (MAC) sirve para correlacionar varios canales lógicos con varios canales de transporte y realiza multiplexación de canal lógico correlacionando varios canales lógicos con un único canal de transporte. La capa de MAC está conectada a una capa superior llamada capa de control de enlace de radio (RLC) por un canal lógico. El canal lógico se divide en un canal de control que transmite información del plano de control y un canal de tráfico que transmite información del plano de usuario según un tipo de información transmitida.

Una capa de RLC (Control de Recursos de Radio), la segunda capa, segmenta o concatena los datos recibidos desde una capa superior para ajustar el tamaño de los datos para una capa inferior para transmitir adecuadamente los datos a una interfaz de radio. Además, con el fin de garantizar varias QoS requeridas por cada portador de radio RB, la capa de RLC proporciona tres modos de operación: un TM (Modo Transparente); un UM (Modo no Reconocido); y un AM (Modo Reconocido). En particular, la capa de RLC que opera en el AM (conocida como ‘capa de RLC de AM’, en lo sucesivo) realiza una función de retransmisión a través de una función de solicitud y repetición automática (ARQ) para una transmisión de datos fiable.

Una capa de protocolo de convergencia de datos por paquetes (PDCP) de la segunda capa realiza una función llamada compresión de cabecera que reduce el tamaño de una cabecera de un paquete IP, que es relativamente grande e incluye información de control innecesaria, con el fin de transmitir de manera eficiente el paquete IP tal como un IPv4 o IPv6 en una interfaz de radio que tiene un ancho de banda estrecho. La compresión de cabecera aumenta la eficiencia de transmisión en una interfaz de radio permitiendo que la parte de cabecera de los datos transmita solamente la información necesaria.

La capa de RRC situada en la parte más baja de la tercera capa se define solamente en el plano de control, y controla un canal lógico, un canal de transporte y un canal físico en relación con la configuración, la reconfiguración y la liberación de los portadores de radio (RB). Aquí, los RB se refieren a un camino lógico proporcionado por la primera y la segunda capas del protocolo de radio para la transmisión de datos entre el UE y la UTRAN. En general, la configuración del RB se refiere al proceso de estipulación de las características de una capa de protocolo de radio y un canal requerido para proporcionar un servicio de datos particular, y establecer los parámetros detallados y los métodos de operación respectivos.

En lo sucesivo, la capa de PDCP se describirá ahora en detalle. La capa de PDCP está conectada hacia arriba con la capa de RRC o con una aplicación de usuario, y está conectada hacia abajo con la capa de RLC. En la FIG. 4, el lado izquierdo muestra la estructura de funciones de la entidad de PDCP de transmisión y el lado derecho muestra la estructura de funciones de la entidad de PDCP de recepción. La estructura del lado de transmisión izquierdo muestra operaciones aplicadas a una SDU de PDCP cuando la capa de PDCP recibe la SDU de PDCP de una entidad superior, y la estructura del lado de recepción derecho muestra operaciones aplicadas a una PDU de PDCP cuando la capa de PDCP recibe la PDU de PDCP de una entidad inferior .

El PDCP se usa tanto para el plano de usuario como para el plano de control, y algunas funciones del PDCP se aplican selectivamente según un plano de usuario. Esto es, como se muestra en la FIG. 4, la función de compresión de cabecera se aplica solamente a los datos del plano de usuario, mientras que una función de protección de integridad se aplica solamente a los datos del plano de control.

Se describirá ahora un procedimiento de procesamiento de datos realizado por la entidad de PDCP de transmisión en el lado izquierdo en la FIG. 4.

S1: La capa de PDCP asigna un número de secuencia a una SDU de PDCP recibida.

S2: Si un RB establecido es un RB de un plano de usuario, la capa de PDCP realiza una compresión de cabecera sobre la SDU de PDCP.

S3: Si el RB establecido es un RB del plano de control, la capa de PDCP realiza una operación de protección de integridad sobre la SDU de PDCP.

S4: La capa de PDCP realiza cifrado sobre los bloques de datos generados según los resultados del paso S2 o S3.

S5: La capa de PDCP configura una PDU de PDCP uniendo una cabecera adecuada a los bloques de datos cifrados, y entrega la PDU de PDCP configurada a la capa RLC.

Se describirá ahora un procedimiento de procesamiento de datos realizado por la entidad de PDCP de recepción en el lado derecho en la FIG. 4.

S6: La capa de PDCP elimina la cabecera de la PDU de PDCP recibida.

S7: La capa de PDCP realiza descifrado sobre la PDU de PDCP con la cabecera eliminada.

S8: Si el RB establecido es un RB del plano de usuario, la capa de PDCP realiza la descompresión de cabecera sobre la PDU de PDCP descifrada.

S9: Si el RB establecido es un RB del plano de control, la capa de PDCP realiza una operación de verificación de integridad sobre la PDU de PDCP descifrada.

S10: La capa de PDCP entrega bloques de datos, esto es, SDU de PDCP, que se han recibido a través del paso S8 o S9, a una capa superior. Si el RB establecido es un RB del plano de usuario, la capa de PDCP realiza reordenación según sea necesario, y entrega el mismo a una capa superior.

Se describirá ahora la compresión de cabecera realizada por la capa de PDCP. La compresión de cabecera está reduciendo el tamaño de una cabecera en base al hecho de que una cabecera IP de cada paquete IP que pertenece al mismo flujo de paquetes no se cambia en general. Los campos no cambiados se almacenan en forma de contexto en un compresor del lado de transmisión y en un descompresor del lado de recepción, y cuando se forma el contexto, solamente se transmiten los campos cambiados para reducir por ello la sobrecarga de la cabecera IP. En una etapa inicial de la compresión de cabecera, el compresor transmite un paquete de cabecera completo para formar un contexto con respecto a un flujo de paquetes correspondiente, así que no hay ganancia con la compresión

de cabecera. Pero, después de que el contexto se forma en el descompresor, el compresor puede transmitir solamente un paquete de cabecera comprimido, así que su ganancia se aumenta notablemente.

Una ROHC (Compresión Robusta de Cabecera), un esquema típico de compresión de cabecera usado en el sistema LTE, se usa para reducir la información de cabecera de un paquete en tiempo real, tal como un RTP (Protocolo de Transporte en Tiempo Real)/UDP (Protocolo de Diagrama de Usuario)/IP (Protocolo de Internet). Aquí, el paquete de RTP/UDP/IP se refiere a un paquete con cabeceras pertinentes que se han añadido a medida que los datos de una capa superior pasan a través de un RTP, un UDP y un IP. Incluye diversa información de cabecera requerida para que los datos se transfieran a un destino a través de Internet y se recuperen. En general, en cuanto el tamaño de cabecera del paquete de RTP/UDP/IP, el IPv4 (IP versión 4) tiene un tamaño de cabecera de 40 bytes y el IPv6 tiene un tamaño de cabecera de 60 bytes. Cuando las cabeceras se comprimen usando la ROHC, las cabeceras de 40 o 60 bytes se reducen a cabeceras de 1 a 3 bytes, obteniendo ganancias notables.

La FIG. 5 muestra un cambio en el tamaño de cabecera de un paquete formado según la ROHC. Específicamente, la FIG. 5 comparativamente muestra el cambio en el tamaño de cabecera del paquete de RTP/UDP/IP general y el cambio en el tamaño de cabecera con la ROHC aplicada. Cuando se transmite primero un flujo de paquetes, debido a que el contexto no está formado aún en el compresor del lado de transmisión y en el descompresor del lado de recepción, así se transmite una cabecera completa para formar el contexto. Cuando la cabecera completa se transmite en un grado, se forma un contexto y, de esta manera, se puede transmitir una cabecera comprimida. A este respecto, el contexto se puede dañar debido a una pérdida o similar de paquetes a mitad de camino, así que se requiere transmitir la cabecera completa en intervalos adecuados. En general, la cabecera completa incluye información adicional para formar el contexto, así que es ligeramente más grande que una cabecera normal.

Se describirá ahora la función de seguridad realizada por la capa de PDCP. Como se ha descrito anteriormente, la seguridad incluye dos funciones de cifrado y protección de integridad. En ambas de las funciones, se generan códigos que varían para cada paquete, con los cuales los datos originales se cifran o se comprueban para su integridad.

Los códigos que varían para cada paquete se generan usando un SN (Número de Secuencia) de PDCP añadido a una cabecera de cada PDU de PDCP, y uno de los factores de generación de código es CONTAR. El CONTAR tiene una longitud de 32 bits, de los cuales el bit menos significativo (LSB) incluye un SN de PDCP y los otros bits más significativos (MSB) restantes incluyen un HFN (Número de Hipertrama). La longitud del SN de PDCP es 5, 7 o 12 bits, esto es, diferente para cada RB, así que la longitud del HFN es diferente para cada caso como 27, 25 o 20 bits.

El cifrado se realiza de una forma como se muestra en la FIG. 6. El lado de transmisión genera datos cifrados cubriendo un código que se cambia para cada paquete, esto es, MÁSCARA, en datos originales. Aquí, la cobertura de la MÁSCARA, se refiere a realizar XOR sobre los datos originales y la MÁSCARA mediante bits. Cuando se reciben los datos cifrados de esta manera, el lado de recepción cubre la MÁSCARA de nuevo sobre los datos cifrados para descifrarlos. Aquí, la MÁSCARA tiene una longitud de 32 bits y se genera a partir de varios factores de entrada. En particular, con el fin de generar un valor diferente para cada paquete, se genera CONTAR usando un número de secuencia de PDCP diferente para cada PDU de PDCP, y el CONTAR generado se usa como uno de los factores de entrada de generación de MÁSCARA. Además de CONTAR, los factores de entrada de generación de MÁSCARA incluyen un ‘portador’, un valor de ID de un RB correspondiente, una ‘Dirección’ que tiene un valor hacia arriba o hacia abajo, una ‘CK (Clave de Cifrado)’ intercambiada por el terminal y la red en el establecimiento de un RB, o similar.

Además, la protección de integridad se realiza de una forma como se muestra en la FIG. 7. Al igual que el proceso de cifrado, en el proceso de protección de integridad, un código, esto es, ‘MAC-I (Integridad de Código de Autentificación de Mensajes)’, usando un ‘CONTAR’ que usa el SN de PDCP, un ‘Portador’, un valor de ID de un RB, una ‘Dirección’ que tiene un valor hacia arriba o hacia abajo, una ‘IK (Clave de Protección de Integridad)’ intercambiada por el terminal y la red en el establecimiento de un RB, o similares. Aquí, una diferencia del proceso de cifrado como se muestra en la FIG. 6 es que no se hace una operación XOR a la ‘MAC-I’ generada con datos originales sino que se une a una PDU de PDCP como se muestra en la FIG. 7. Cuando el lado de recepción recibe la PDU de PDCP unida a la MAC-I, genera una XMAC-I usando el mismo factor de entrada que el usado en el lado de transmisión y la compara con la MAC-I unida a la PDU de PDCP. Si los dos valores (esto es, XMAC-I y MAC-I unidas a la PDU de PDCP) son idénticos, se determina que los datos tienen integridad, mientras que si los dos valores son diferentes, se determina que los datos se han cambiado a mitad de camino.

Por algunas razones, la MÁSCARA o la MAC-I del lado de transmisión y del lado de recepción se pueden cambiar para causar un error en el cifrado o la protección de integridad. La razón principal para que la MÁSCARA o la MAC-I se cambien es debido a que un HFN, el MSB del CONTAR, se cambie. Esto ocurre cuando se pierden numerosas SDU de PDCP. La razón es debida a que el MSB del CONTAR es un HFN y el LSB del CONTAR es un SN y si el SN de PDCP alcanza un valor máximo, vuelve a cero (0) y se aumenta un HFN, el MSB. Esto es, si las SDU de PDCP se pierden tanto como para envolver un espacio de SN de PDCP, ocurre una desincronización de HFN. Por otra razón, puede haber un error que no se puede encontrar incluso con una inspección de CRC (Código de

Redundancia Cíclico) en una capa inferior, y en este caso, si el valor de SN de PDCP no está dentro de un intervalo válido, puede ocurrir una desincronización de HFN.

Cuando ocurre la desincronización de HFN, falla la seguridad. De esta manera, aunque el lado de recepción recibe datos, no pueden restaurar los datos originales, causando un problema de que el lado de recepción descarta continuamente los datos recibidos.

Con este problema surgiendo, se describirán por separado el RB del plano de usuario y el RB del plano de control.

Primero, en el caso del RB del plano de usuario, las PDU de PDCP recibidas se descifran y se someten a descompresión de cabecera. En este momento, si las PDU de PDCP se descifran con una MÁSCARA errónea, ocurre un error continuamente en el proceso de compresión de cabecera, así que el lado de recepción descarta continuamente las PDU de PDCP recibidas.

Segundo, en el caso del RB del plano de control, las PDU de PDCP recibidas se descifran y se someten a verificación de integridad. Si las PDU de PDCP se descifran con una MÁSCARA errónea o se comparan con una XMAC-I errónea, ocurren errores continuamente en el proceso de verificación de integridad, así que el lado de recepción descarta continuamente las PDU de PDCP recibidas.

Este problema surge debido a que no se proporciona actualmente una función de detección de desincronización de HFN. Como resultado, una vez que ocurre la desincronización de HFN, no se puede recuperar y las PDU recibidas desde entonces tienen un error y, de esta manera, se descartan continuamente.

La solicitud de patente coreana KR20030012048 es una técnica anterior adicional.

Esencia técnica de la presente invención

Por lo tanto, es un objeto de la presente invención permitir que una entidad de PDCP del lado de recepción determine si ocurre o no una desincronización de HFN, esto es, un fallo de seguridad, usando condiciones particulares, e informar un RRC para restablecer un RB o reiniciar una configuración de seguridad de un lado de transmisión o un lado de recepción usando un procedimiento de REINICIO de PDCP si ocurre la desincronización de HFN.

La invención se define por las reivindicaciones independientes.

Para lograr el objeto anterior, se proporciona un método para detectar un error de seguridad en un sistema de comunicación móvil, que incluye: (A) contar el número de paquetes erróneos entre uno o más paquetes recibidos; (B) comparar el número de paquetes erróneos contados con un valor de referencia; y (C) determinar un fallo de seguridad si el número de paquetes erróneos contados alcanza el valor de referencia.

El paso (A) puede incluir: recibir al menos un paquete transmitido desde un lado de transmisión; eliminar una cabecera del al menos un paquete recibido; descifrar en el al menos un paquete con la cabecera eliminada; determinar un error de un fallo de seguridad del al menos un paquete recibido realizando un proceso de descifrado de una cabecera comprimida o realizando un proceso de verificación de integridad del al menos un paquete descifrado; y aumentar un valor de recuento si hay un paquete determinado que tiene un error del fallo de seguridad.

El uno o más paquetes recibidos pueden ser datos de un plano de usuario o datos de un plano de control.

El método puede incluir además: (D) si el número de paquetes erróneos contados alcanza el valor de referencia para que se determine como el fallo de seguridad, realizar un proceso de recuperación de una configuración de seguridad.

El proceso de recuperación puede incluir la realización de un procedimiento de reinicio de una capa de PDCP.

El proceso de recuperación puede incluir la notificación a una capa de RRC.

La capa de RRC puede restablecer un RB (Portador de Radio), restablecer una conexión de RRC o reiniciar una configuración de seguridad con respecto a un RB particular.

El paso (A) se realiza en un proceso de descompresión de cabecera de una capa de PDCP (Protocolo de Convergencia de Datos por Paquetes) o en un proceso de verificación de integridad de la capa de PDCP.

El valor de referencia puede ser diferente según un RB.

Para lograr el objeto anterior, también se proporciona un método para detectar un error de seguridad en un sistema de comunicación móvil, que incluye: recibir al menos un paquete; realizar la verificación de integridad o la descompresión de cabecera en el al menos un paquete recibido; identificar un error en el al menos un paquete recibido mientras se realiza la verificación de integridad o la descompresión de cabecera; notificar el error

identificado a una capa de RRC, si se identifica que el al menos un paquete recibido tiene un error; y realizar un restablecimiento por la capa de RRC al recibir el error identificado.

El restablecimiento puede incluir al menos uno de restablecimiento de RB y restablecimiento de una capa de PDCP.

El restablecimiento puede ser un restablecimiento de una conexión de RRC.

La verificación de integridad puede usar la XMAC-I y la descompresión de cabecera puede usar el contexto.

El restablecimiento de la capa de PDCP puede ser un REINICIO de la capa de PDCP.

La presente invención proporciona el método para detectar eficazmente un fallo de seguridad como ocurre en la capa de PDCP de un lado de recepción, así que se puede evitar cualquier pérdida de datos adicional y un desperdicio resultante de recursos de radio.

Breve descripción de los dibujos

La FIG. 1 muestra una estructura de red de una Evolución a Largo Plazo (LTE), el sistema de comunicación móvil de la técnica relacionada;

La FIG. 2 muestra la arquitectura de un plano de control de un protocolo de interfaz de radio entre un terminal y una Red de Acceso de Radio Terrestre UMTS (UTRAN) Evolucionada basada en estándares de red de acceso de radio del 3GPP;

La FIG. 3 muestra la arquitectura de un plano de usuario del protocolo de interfaz de radio entre el terminal y la Red de Acceso de Radio Terrestre UMTS (UTRAN) Evolucionada basada en estándares de red de acceso de radio del 3GPP;

La FIG. 4 muestra una estructura de función de una capa de PDCP;

La FIG. 5 muestra un cambio en el tamaño de una cabecera de un paquete formado según una ROHC;

La FIG. 6 muestra un método de cifrado;

La FIG. 7 muestra un método de protección de integridad;

La FIG. 8 es un diagrama de bloques que muestra el proceso de determinación de un fallo de seguridad con respecto a un RB del plano de usuario según una realización de la presente invención; y

La FIG. 9 es un diagrama de bloques que muestra el proceso de determinación de un fallo de seguridad con respecto a un RB del plano de control según una realización de la presente invención.

Modo para llevar a cabo las realizaciones preferidas

La presente invención se aplica a un sistema de telecomunicaciones móviles y, más particularmente, a un Sistema de Telecomunicaciones Móviles Universal Evolucionado (E-UMTS) que ha evolucionado a partir de UMTS. No obstante, sin estar limitado al mismo, la presente invención también se puede aplicar a cualquier sistema de telecomunicaciones móviles y protocolos de comunicación a los que son aplicables las características técnicas de la presente invención.

La presente invención se puede modificar de forma variable y puede tener diversas realizaciones, unas particulares de las cuales se ilustrarán en los dibujos y se describirán en detalle. No obstante, se debería entender que la siguiente descripción ejemplar de la invención no se pretende que restrinja la invención a formas específicas de la presente invención, sino que más bien la presente invención se pretende que cubra todas las modificaciones, similitudes y alternativas que están incluidas en el espíritu y alcance de la presente invención.

Mientras que los términos “primero” y “segundo”, etc. se pueden usar para describir varios componentes, tales componentes no se deben limitar a los términos anteriores. Los términos anteriores se usan solamente para distinguir un componente de otro. Por ejemplo, un primer componente se puede referir como un segundo componente sin apartarse del alcance de los derechos de la presente invención, y del mismo modo un segundo componente se puede referir como un primer componente. El término “y/o” abarca tanto combinaciones de la pluralidad de elementos relacionados descritos como cualquier elemento de entre la pluralidad de elementos relacionados descritos.

Cuando se menciona que un componente está “conectado” a o “accediendo” a otro componente, esto puede significar que está conectado directamente a o accediendo al otro componente, pero ha de ser entendido que puede existir otro componente entre medias. Por otra parte, cuando se menciona que un componente está “conectado directamente” a o “accediendo directamente” a otro componente, ha de ser entendido que no hay otros componentes entre medias.

Los términos usados en la presente solicitud se usan meramente para describir realizaciones particulares, y no se pretende que limiten la presente invención. Una expresión usada en singular abarca la expresión del plural, a menos que tenga un significado claramente diferente en el contexto. En la presente solicitud, ha de ser entendido que los términos tales como “que incluye” o “que tiene”, etc., se pretende que indiquen la existencia de las características, números, operaciones, acciones, componentes, partes o combinaciones de los mismos descritos en la especificación, y no se pretende que excluyan la posibilidad de que puedan existir o se puedan añadir una o más de otras características, números, operaciones, acciones, componentes, partes, o combinaciones de los mismos.

A menos que se defina de otro modo, todos los términos usados en la presente memoria, incluyendo términos técnicos o científicos, tienen los mismos significados que los entendidos generalmente por aquéllos con conocimientos ordinarios en el campo de la técnica a la que pertenece la presente invención. Tales términos como los definidos en un diccionario usado de manera general han de ser interpretados que tienen los significados iguales a los significados contextuales en el campo de técnica pertinente, y no han de ser interpretados que tienen significados ideales o excesivamente formales a menos que se defina claramente en la presente solicitud.

Las realizaciones de la presente invención se describirán a continuación en detalle con referencia a los dibujos anexos, donde esos componentes se representan con el mismo número de referencia que son iguales o están en correspondencia, con independencia del número de figura, y se omiten explicaciones redundantes.

Los términos en uso en la presente invención se describirán como sigue.

Un fallo de seguridad se refiere a un fenómeno en que una MÁSCARA (en el caso del plano U) o una MAC-I (en el caso del plano C) de un lado de transmisión o de un lado de recepción se cambian para causar un error en el cifrado o la protección de integridad, dando como resultado una desincronización de HFN.

Una configuración de seguridad se refiere a cifrado o protección de integridad, y el cifrado en la presente memoria se realiza sobre un paquete (datos) del plano de usuario y la protección de integridad se realiza sobre un paquete (datos) del plano de control.

La presente invención se basa en tal reconocimiento de que, actualmente, una capa de PDCP no proporciona una función para detectar una desincronización de HFN. De esta manera, la presente invención aborda el problema de que una vez que ocurre una desincronización de HFN, no se puede recuperar, así que todas las PDU recibidas por un lado de recepción tienen un error y, de esta manera, el lado de recepción descarta continuamente las PDU recibidas.

Un concepto básico de la presente invención es que 1) se definen las condiciones para determinar un fallo de seguridad, 2) una entidad de PDCP del lado de recepción determina si ha ocurrido o no una desincronización de HFN, esto es, un fallo de seguridad, usando las condiciones particulares (es decir, las condiciones para determinar el fallo de seguridad), 3) si se determina que ha ocurrido un fallo de seguridad, la entidad de PDCP del lado de recepción informa a una capa de RRC para restablecer un RB o realizar un procedimiento de REINICIO de PDCP, 4) para reiniciar por ello una configuración de seguridad del lado de transmisión y del lado de recepción.

Las condiciones determinantes del fallo de seguridad según la presente invención se describirán ahora en detalle.

Las condiciones determinantes del fallo de seguridad difieren según si un RB correspondiente pertenece al plano de usuario o al plano de control.

Primero, se describirán ahora las condiciones determinantes del fallo de seguridad en el caso del RB del plano U.

El lado de recepción realiza descompresión de cabecera sobre los datos descifrados. Si el descifrado no se realiza adecuadamente, ocurre un error de CRC durante la descompresión de cabecera, que da como resultado el fallo de la descompresión de cabecera. De esta manera, el número de paquetes fallidos para la descompresión de cabecera funciona como una base para la desincronización de HFN. Esto es, el PDCP cuenta el número de paquetes erróneos durante la descompresión de cabecera con respecto al RB del plano U, y si el número de paquetes erróneos es mayor que un valor de referencia (o valor umbral), la capa de PDCP determina que hay un problema de seguridad y realiza un proceso de recuperación del fallo de seguridad. Con este fin, la entidad de PDCP del lado de recepción usa una variable (o contador) para contar el número de paquetes de error de CRC durante la descompresión de cabecera, y aumenta el valor de la variable siempre que ocurre un error en un paquete. A partir de entonces, cuando la variable alcanza un valor de referencia predeterminado (valor umbral), el PDCP determina que hay un problema en la configuración de seguridad. Mientras tanto, el valor de referencia se puede notificar a la capa de RRC del lado de transmisión (es decir, la capa de RRC de UE) por la capa de RRC del lado de recepción (esto es, capa de RRC de eNB) en el establecimiento de RB, y luego a la entidad de PDCP del lado de transmisión (esto es, entidad de PDCP de UE) por la capa de RRC del lado de transmisión (capa de RRC de UE). El valor de referencia se puede determinar previamente como un valor particular y tener un valor diferente según un RB. El valor de la variable (o contador) para contar los paquetes erróneos se puede aumentar siempre que ocurren errores en los paquetes (por ejemplo, si los errores ocurren discontinuamente), o se puede aumentar solamente cuando ocurren errores en los paquetes continuamente.

La FIG. 8 es un diagrama de bloques que muestra el proceso de determinación de un fallo de seguridad por la entidad de PDCP del lado de recepción con respecto al RB del plano de usuario según una realización de la presente invención. El proceso de determinación de un fallo de seguridad en el caso del RB del plano U se describirá ahora en detalle.

S20: La entidad de PDCP del lado de recepción recibe las PDU de PDCP de la PDU1~PDU20 desde una capa inferior, esto es, el RLC.

S21: La entidad de PDCP del lado de recepción elimina una cabecera de las PDU recibidas y las entrega a una unidad de descifrado.

S22: La unidad de descifrado de la entidad de PDCP del lado de recepción realiza el descifrado sobre las PDU con cabeceras eliminadas. Si ocurre un fallo de seguridad en una PDU1, esto es, si ocurre una desincronización de HFN, la PDU1 y todas las otras PDU posteriores (esto es, la PDU2~PDU20) no se descifran adecuadamente.

S23: No obstante, la entidad de PDCP del lado de recepción no reconoce el hecho de que los paquetes (esto es, la PDU1~PDU20) no se han descifrado adecuadamente, y los entrega a una unidad de descompresión de cabecera.

S24: La unidad de descompresión de cabecera realiza la descompresión de cabecera sobre los paquetes recibidos, pero todos ellos tienen un error. El error identificado se puede determinar en base a los valores de CRC de las cabeceras.

S25: La entidad de PDCP del lado de recepción cuenta el número de paquetes en los que ha ocurrido un error durante la descompresión de cabecera. Si el número de paquetes erróneos contados alcanza (esto es, que es mayor que) un valor de referencia predefinido (es decir, un valor umbral que puede ser, por ejemplo, 20), la entidad de PDCP del lado de recepción determina que hay un error en la configuración de seguridad.

Esto es, en la realización que se muestra en la FIG. 8, primero, cuando la entidad de PDCP del lado de recepción realiza la descompresión de cabecera sobre el paquete recibido, determina un error basado en un valor de CRC de la cabecera. Segundo, la entidad de PDCP del lado de recepción cuenta el número de paquetes erróneos. Tercero, si el número de paquetes erróneos alcanza el valor de referencia, la entidad de PDCP del lado de recepción determina que ha ocurrido un fallo de seguridad. Al determinar el fallo de seguridad, la entidad de PDCP del lado de recepción realiza rápidamente un proceso de recuperación del fallo de seguridad con el fin de evitar una posible pérdida de datos adicional y un desperdicio de recursos de radio. El proceso de recuperación se puede realizar de manera que, por ejemplo, la capa de RRC del lado de recepción informe al terminal acerca del error del fallo de seguridad, de modo que el terminal pueda cortar su conexión con la red y establezca una conexión de RRC de nuevo desde el principio. Alternativamente, la capa de RRC puede restablecer un RB o poner en marcha de nuevo una configuración de seguridad con respecto a un RB particular entre el terminal (UE) y la red.

Primero, las condiciones para determinar un fallo de seguridad en el caso del RB del plano C se describirán como sigue.

En el caso del RB del plano C, no se realiza la descompresión de cabecera y, en su lugar, se realiza la verificación de integridad. De esta manera, el fallo de seguridad se debería determinar en base a una base diferente de la del RB del plano U. Al realizar la verificación de integridad, se compara un valor de MAC-I incluido en una PDU y un valor de XMAC-I generado por la entidad de PDCP del lado de recepción en sí misma. Si los dos valores son diferentes, se determina que la verificación de integridad falla y se descartan los paquetes recibidos por la entidad de PDCP del lado de recepción. De esta manera, en la presente invención, con respecto al RB del plano C, si los paquetes en más de un cierto número tienen un error al realizar la verificación de integridad, se determina como un fallo de seguridad, y se realiza un proceso de recuperación del fallo de seguridad. Con este fin, al realizar la verificación de integridad, la entidad de PDCP del lado de recepción cuenta el número de errores, esto es, el número de casos donde el valor de MAC-I incluido en la PDU y la XMAC-I generada por la entidad de PDCP del lado de recepción en sí misma son diferentes. En otras palabras, la entidad de PDCP del lado de recepción usa una variable (contador) para contar el número de paquetes correspondientes que tienen diferentes valores (el valor de MAC-I incluido en las PDU y el valor de XMAC-I generado por la entidad de PDCP del lado de recepción en sí misma). Es decir, siempre que ocurren errores en los paquetes, la entidad de PDCP del lado de recepción aumenta el valor de la variable, y cuando la variable alcanza un valor de referencia predeterminado (valor umbral), la entidad de PDCP del lado de recepción determina que hay un problema en la configuración de seguridad. Mientras tanto, el valor de referencia se puede notificar a la capa de RRC del lado de transmisión (esto es, la capa de RRC del UE) por la capa de RRC del lado de recepción (esto es, la capa de RRC de eNB) en el establecimiento de RB, y luego a la entidad de PDCP del lado de transmisión (esto es, la entidad de PDCP del UE) por la capa de RRC del lado de transmisión (capa de RRC del UE). El valor de referencia se puede determinar previamente como un valor particular y tiene un valor diferente según un RB. El valor de la variable (o contador) para contar los paquetes erróneos se puede aumentar siempre que ocurren errores en los paquetes (por ejemplo, si los errores ocurren discontinuamente), o se pueden aumentar solamente cuando ocurren errores en los paquetes continuamente.

La FIG. 9 es un diagrama de bloques que muestra el proceso de determinación de un fallo de seguridad por la entidad de PDCP del lado de recepción con respecto al RB del plano de control según una realización de la presente

invención. El proceso de determinación de un fallo de seguridad con respecto al RB del plano C se describirá ahora en detalle.

S30: La entidad de PDCP del lado de recepción recibe las PDU de PDCP de la PDU1~PDU20 desde una capa inferior, esto es, la capa de RLC.

S31: La entidad de PDCP del lado de recepción elimina las cabeceras de las PDU recibidas y las entrega a la unidad de descifrado.

S32: La entidad de PDCP del lado de recepción realiza el descifrado sobre las PDU con cabeceras eliminadas. Si ocurre un fallo de seguridad en una PDU1, esto es, si ocurre una desincronización de HFN, la PDU1 y todas las demás PDU posteriores (esto es, la PDU2~PDU20) no se descifran adecuadamente.

S33: No obstante, la entidad de PDCP del lado de recepción no reconoce el hecho de que los paquetes (esto es, la PDU1~PDU20) no se han descifrado adecuadamente, y los entrega a una unidad de verificación de integridad.

S34: La unidad de verificación de integridad realiza la verificación de integridad sobre los paquetes recibidos (esto es, la PDU1~PDU20), pero todos ellos tienen un error. El error identificado se puede determinar comparando el valor de MAC-I incluido en las PDU y el valor de XMAC-I generado por la entidad de PDCP del lado de recepción en sí misma.

S35: La entidad de PDCP del lado de recepción cuenta el número de paquetes a los que ha ocurrido un error durante la verificación de integridad. Si el número de paquetes erróneos contados alcanza un valor de referencia predefinido (que puede ser, por ejemplo, 20), la entidad de PDCP del lado de recepción determina que hay un error en la configuración de seguridad.

La realización en la FIG. 9 muestra el caso donde ocurre el error durante el proceso de descifrado. Pero, en realidad, un error puede ocurrir durante el proceso de verificación de integridad. En este caso, el procedimiento de procesamiento de seguimiento es el mismo que se ha descrito anteriormente. Por ejemplo, si el descifrado se realiza con éxito sobre todos los paquetes, pero una PDU 1 tiene un error debido a un parámetro de verificación de integridad erróneo, todos los paquetes posteriores tendrían un error. De esta manera, en cualquier caso, el número de paquetes erróneos se cuenta en la verificación de integridad para determinar si ha ocurrido o no un fallo de seguridad.

Cuando la entidad de PDCP del lado de recepción determina un fallo de seguridad, la entidad de PDCP del lado de recepción realiza rápidamente un proceso de recuperación del fallo de seguridad con el fin de evitar una posible pérdida de datos adicional y un desperdicio de recursos de radio. El proceso de recuperación se puede realizar de manera que, por ejemplo, la capa de RRC del lado de recepción informe al terminal acerca del error del fallo de seguridad, de modo que el terminal pueda cortar su conexión a la red y establezca una conexión de RRC de nuevo desde el principio. Alternativamente, la capa de RRC puede restablecer un RB o poner en marcha de nuevo una configuración de seguridad con respecto a un RB particular entre el terminal (UE) y la red.

El método descrito hasta ahora se puede implementar por software, hardware o su combinación. Por ejemplo, el método según la presente invención se puede almacenar en un medio de almacenamiento (por ejemplo, una memoria interna de un terminal móvil, una memoria rápida, un disco duro o similar), y se puede implementar mediante códigos o lenguajes de comando en un programa de software que se puede ejecutar por un procesador (por ejemplo, un microprocesador interno de un terminal móvil).

La invención que se describe de esta manera, será obvio que la misma se puede variar de muchas maneras. Tales variaciones no han de ser consideradas como un alejamiento del alcance de la invención, y todas de tales modificaciones que serían obvias para un experto en la técnica se pretende que estén incluidas dentro del alcance de las siguientes reivindicaciones.

REIVINDICACIONES

1. Un método de realización de un procedimiento de restablecimiento en un sistema de comunicación móvil, comprendiendo el método:

recibir, por una entidad de protocolo de convergencia de datos por paquetes “PDCP”, al menos una unidad de datos de PDCP;

realizar, por la entidad de PDCP, una comprobación de integridad sobre la al menos una unidad de datos de PDCP;

indicar, por la entidad de PDCP, un fallo de comprobación de integridad a una entidad de control de recursos de radio “RRC” si la comprobación de integridad falla con respecto a la al menos una unidad de datos de PDCP; y

realizar, por la entidad de RRC, un procedimiento de restablecimiento tras la indicación de fallo de comprobación de integridad de la entidad de PDCP,

en donde la al menos una unidad de datos de PDCP es para un plano de control.

2. El método de la reivindicación 1, en donde el procedimiento de restablecimiento comprende al menos uno de restablecimiento de un portador de radio “RB” o restablecimiento de una conexión de RRC.

3. El método de la reivindicación 1, en donde realizar la comprobación de integridad sobre la unidad de datos de PDCP comprende:

contar un número de unidades de datos de PDCP con integridad fallida entre la al menos una unidad de datos recibida;

comparar el número de unidades de datos de PDCP con integridad fallida contadas con un valor de referencia; y

determinar el fallo de comprobación de integridad si el número de unidades de datos de PDCP con integridad fallida contado alcanza el valor de referencia.

4. El método de la reivindicación 1, que comprende además descifrar, por la entidad de PDCP, la al menos una unidad de datos recibida.

5. El método de la reivindicación 7, que comprende además eliminar, por la entidad de PDCP, al menos una cabecera de PDCP de la al menos una unidad de datos de PDCP recibida.

6. El método de la reivindicación 3, en donde las unidades de datos de PDCP con integridad fallida están en un orden consecutivo.

7. El método según la reivindicación 3, en donde el fallo de comprobación de integridad se identifica si un valor de integridad de código de autenticación de mensaje “MAC-I” de la al menos una unidad de datos recibida es diferente de un valor de integridad de código de autenticación de mensaje esperado “XMAC-I” generado por la entidad de PDCP.

8. Un aparato en un sistema de comunicación móvil, comprendiendo el aparato:

una entidad de protocolo de convergencia de datos por paquetes “PDCP” configurada para

recibir al menos una unidad de datos de PDCP,

realizar una comprobación de integridad sobre la al menos una unidad de datos de PDCP, e

indicar un fallo de comprobación de integridad a una entidad superior si la comprobación de integridad falla con respecto a la al menos una unidad de datos de PDCP; y

una entidad de control de recursos de radio “RRC” que es la entidad superior, configurada para realizar un procedimiento de restablecimiento tras la indicación de fallo de comprobación de integridad de la entidad de PDCP,

en donde la al menos una unidad de datos de PDCP es para un plano de control.

9. El aparato de la reivindicación 8, en donde el procedimiento de restablecimiento comprende al menos uno de restablecimiento de un portador de radio “RB” o restablecimiento de una conexión de RRC.

10. El aparato de la reivindicación 8, en donde la comprobación de integridad comprende:

contar un número de unidades de datos de PDCP con integridad fallida entre la al menos una unidad de datos de PDCP,

comparar el número de unidades de datos de PDCP con integridad fallida contado con un valor de referencia, e

identificar el fallo de comprobación de integridad si el número de unidades de datos de PDCP con integridad fallida contado alcanza el valor de referencia.

11. El aparato de la reivindicación 10, en donde las unidades de datos de PDCP con integridad fallida están en un orden consecutivo.

12. El aparato según la reivindicación 10, en donde el fallo de comprobación de integridad se identifica si un valor de integridad de código de autenticación de mensaje “MAC-I” de la al menos una unidad de datos de PDCP es diferente de un valor de integridad de código de autenticación de mensaje esperado “XMAC-I” generado por la entidad de PDCP.

13. El aparato de la reivindicación 8, en donde la entidad de PDCP está configurada además para descifrar la al menos una unidad de datos de PDCP.

14. El aparato de la reivindicación 13, en donde la entidad de PDCP está configurada además para eliminar al menos una cabecera de PDCP de la al menos una unidad de datos de PDCP.

FIG. 1

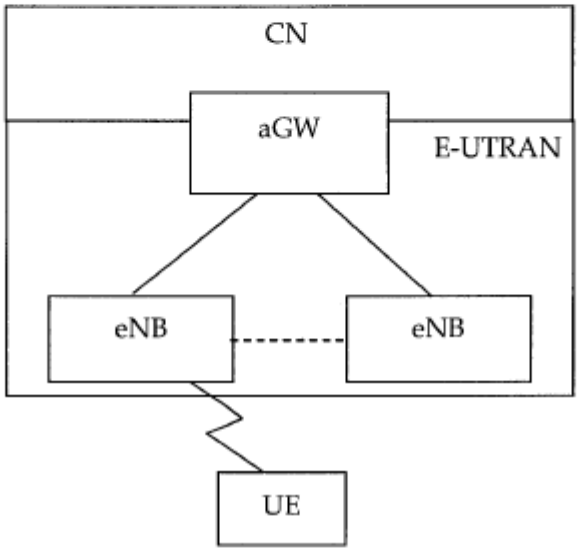


FIG. 2

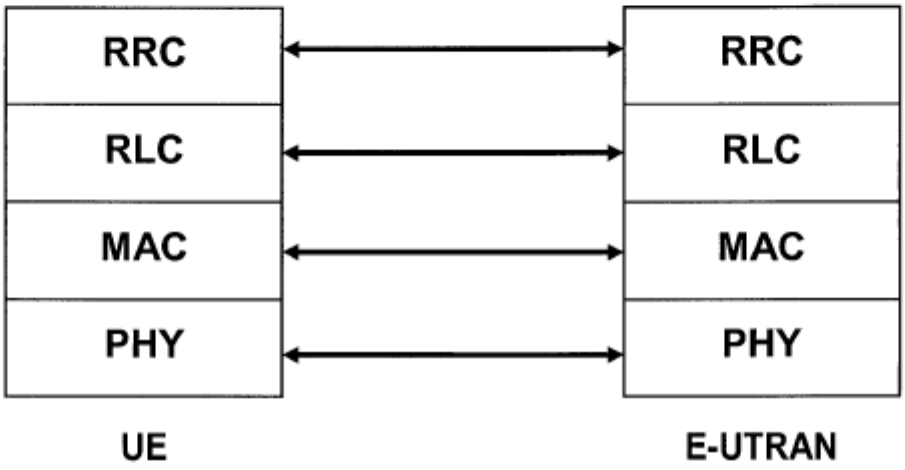


FIG. 3

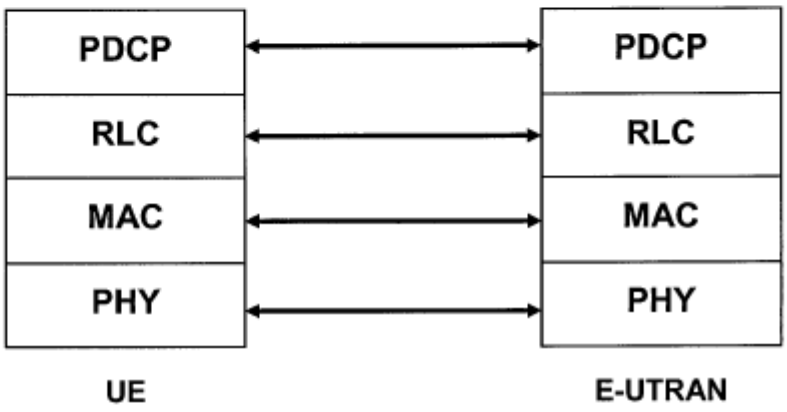


FIG. 4

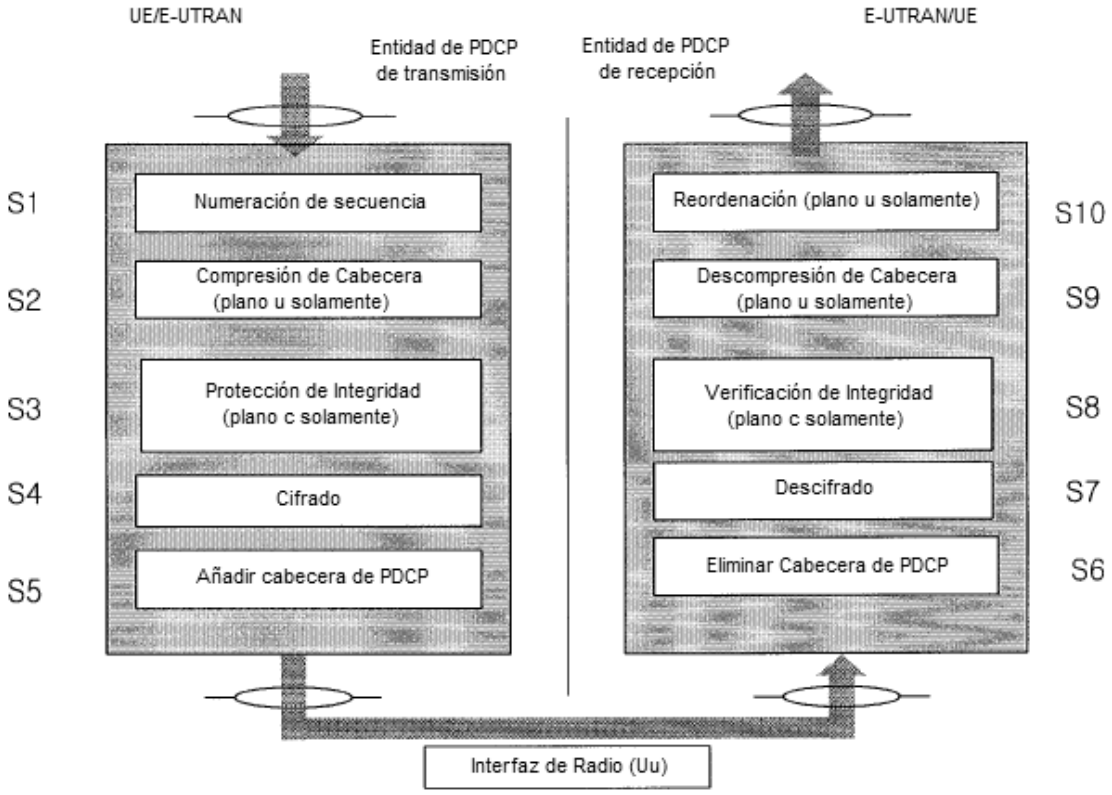

UE/E-UTRAN
E-UTRAN/UE
Entidad de PDCP de transmisión
Entidad de PDCP de recepción
S1
Numeración de secuencia
S2
Compresión de Cabecera (plano u solamente)
S3
Protección de Integridad (plano c solamente)
S4
Cifrado
S5
Añadir cabecera de PDCP
S10
Reordenación (plano u solamente)
S9
Descompresión de Cabecera (plano u solamente)
S8
Verificación de Integridad (plano c solamente)
S7
Descifrado
S6
Eliminar Cabecera de PDCP
Interfaz de Radio (Uu)

FIG. 5

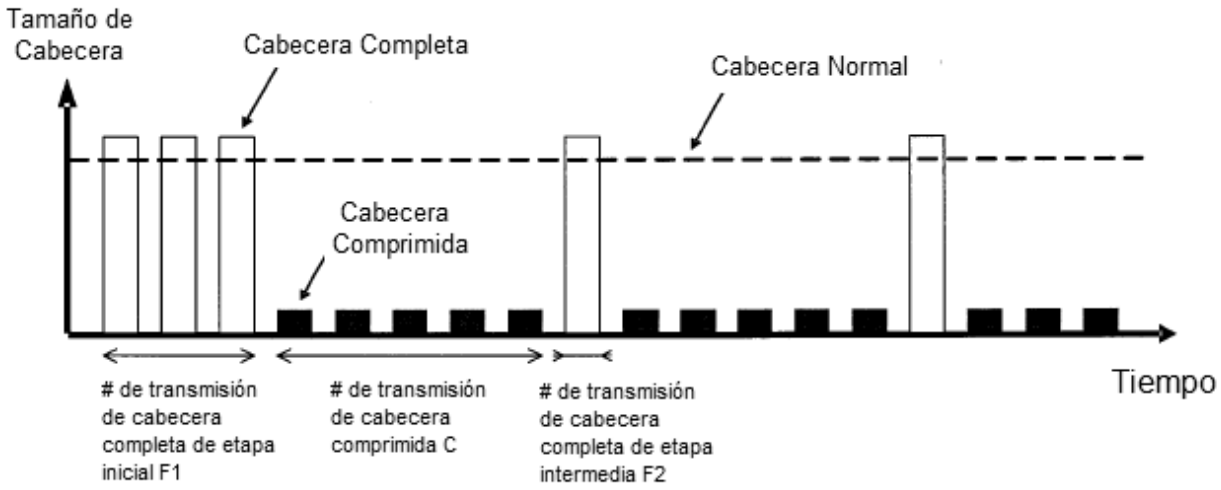

Tamaño de Cabecera
Cabecera Completa
Cabecera Normal
Cabecera Comprimida
Tiempo
de transmisión de cabecera completa de etapa inicial F1
de transmisión de cabecera comprimida C
de transmisión de cabecera completa de etapa intermedia F2

FIG. 6

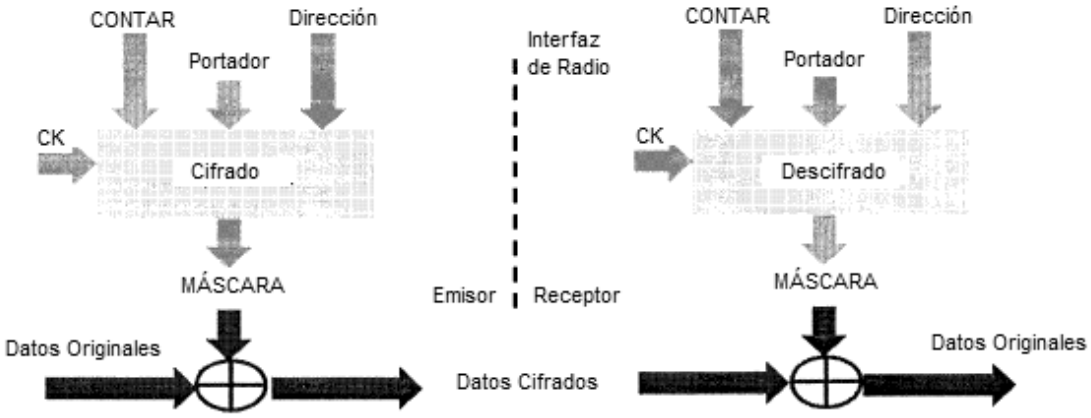

CONTAR
Dirección
Portador
CK
Cifrado
MÁSCARA
Datos Originales
Interfaz de Radio
Emisor
Receptor
Datos Cifrados
CONTAR
Dirección
Portador
CK
Descifrado
MÁSCARA
Datos Originales

FIG. 7

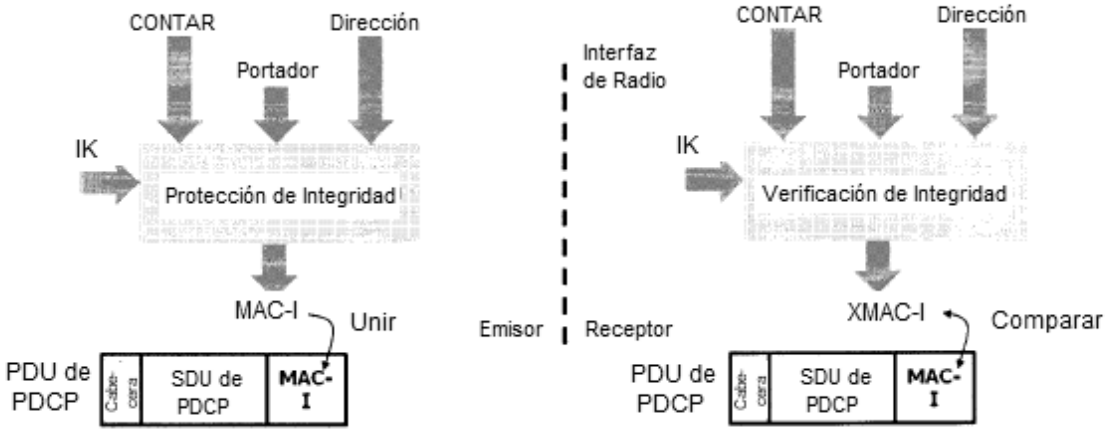

CONTAR
Dirección
Portador
IK
Protección de Integridad
MAC-I
Unir
PDU de PDCP
Cabe-cera
SDU de PDCP
MAC-I
Interfaz de Radio
Emisor
Receptor
CONTAR
Dirección
Portador
IK
Verificación de Integridad
XMAC-I
Comparar
PDU de PDCP
Cabe-cera
SDU de PDCP
MAC-I

FIG. 8

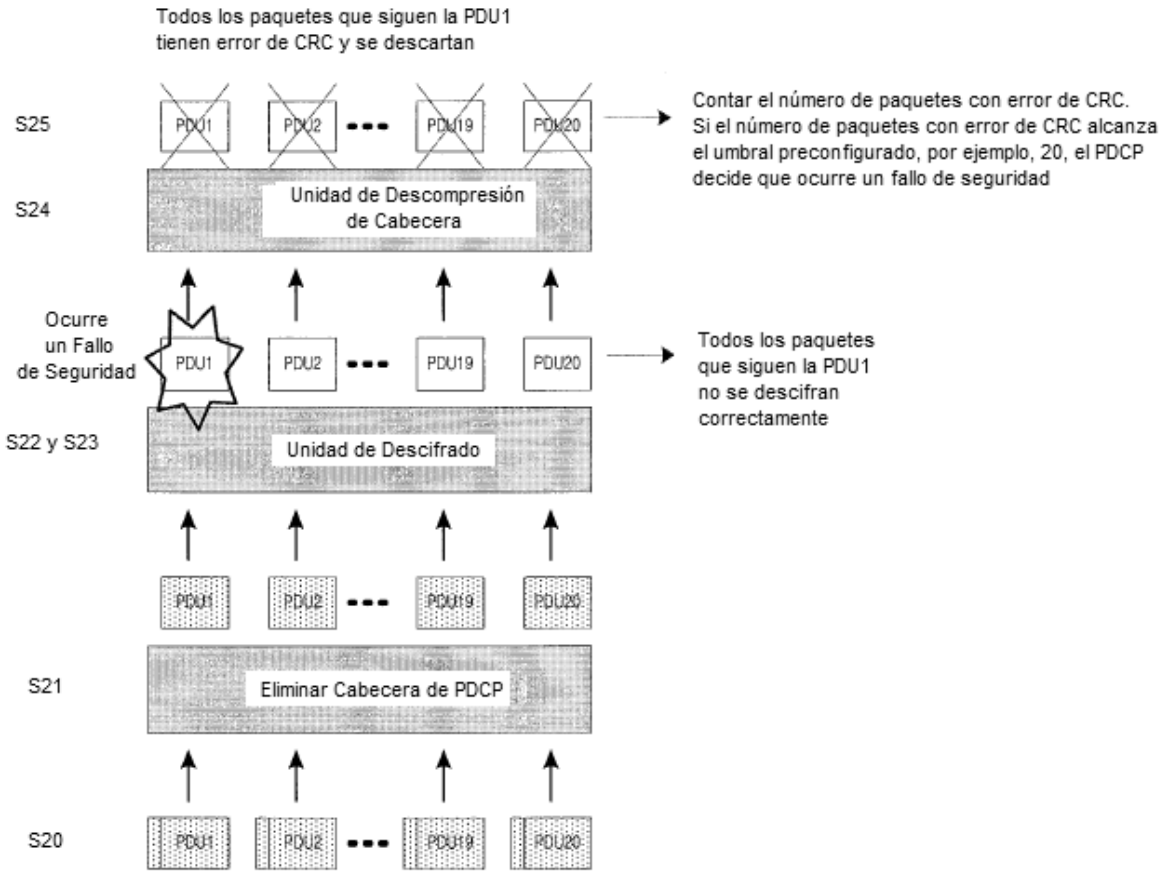
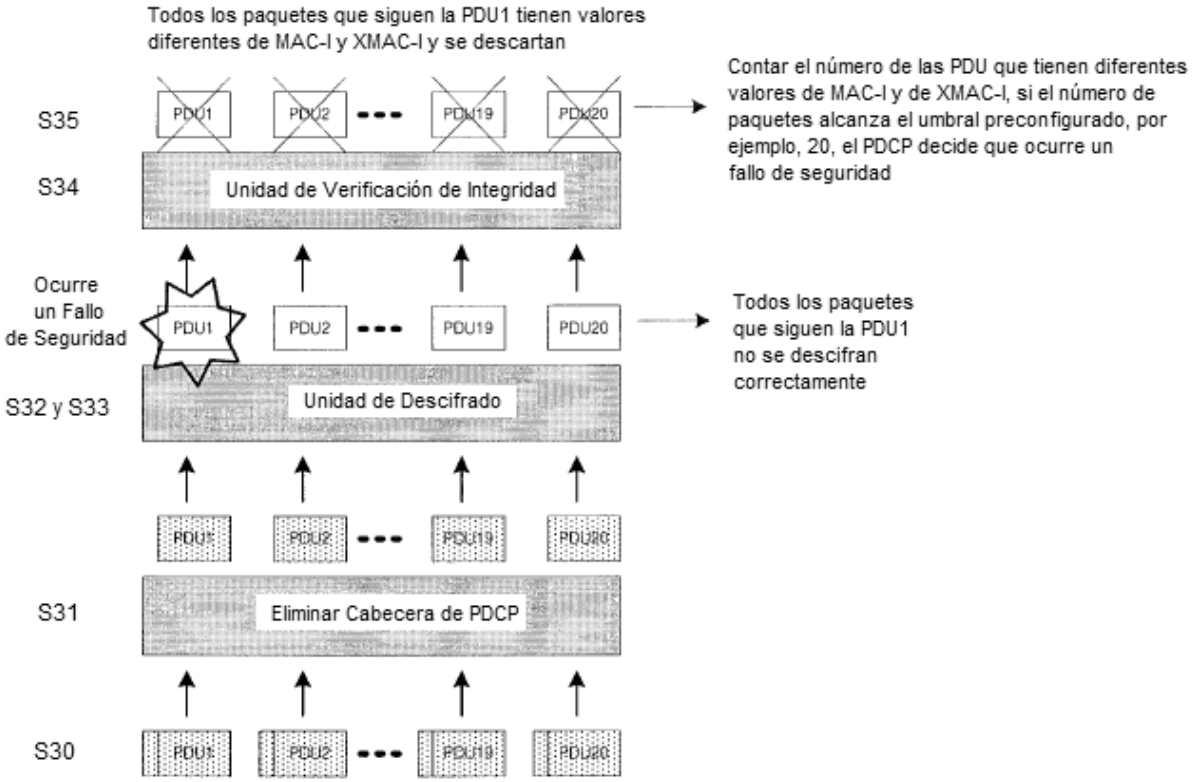

Todos los paquetes que siguen la PDU1
tienen error de CRC y se descartan
S25
PDU1
PDU2
PDU19
PDU20
Contar el número de paquetes con error de CRC.
Si el número de paquetes con error de CRC alcanza
el umbral preconfigurado, por ejemplo, 20, el PDCP
decide que ocurre un fallo de seguridad
S24
Unidad de Descompresión
de Cabecera
Ocurre
un Fallo
de Seguridad
PDU1
PDU2
PDU19
PDU20
Todos los paquetes
que siguen la PDU1
no se descifran
correctamente
S22 y S23
Unidad de Descifrado
PDU1
PDU2
PDU19
PDU20
S21
Eliminar Cabecera de PDCP
S20
PDU1
PDU2
PDU19
PDU20

FIG. 9


Todos los paquetes que siguen la PDU1 tienen valores diferentes de MAC-I y XMAC-I y se descartan
Contar el número de las PDU que tienen diferentes valores de MAC-I y de XMAC-I, si el número de paquetes alcanza el umbral preconfigurado, por ejemplo, 20, el PDCP decide que ocurre un fallo de seguridad
S35
S34
Unidad de Verificación de Integridad
Ocurre un Fallo de Seguridad
Todos los paquetes que siguen la PDU1 no se descifran correctamente
S32 y S33
Unidad de Descifrado
S31
Eliminar Cabecera de PDCP
S30
PDU1
PDU2
PDU19
PDU20