(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 530 961**

(51) Int. CI.:

H04L 1/16 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **16.09.2011 E 11799199 (2)**

(97) Fecha y número de publicación de la concesión europea: **17.12.2014 EP 2649740**

(54) Título: **Habilitación e inhabilitación de la protección de la integridad para portadores de radio de datos**

(30) Prioridad:

10.12.2010 US 421806 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.03.2015

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)
164 83 Stockholm, SE

(72) Inventor/es:

ÖSTERGAARD, JESSICA y
MILDH, GUNNAR

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Habilitación e inhabilitación de la protección de la integridad para portadores de radio de datos

Campo técnico

La tecnología versa sobre nodos receptores y remitentes de un sistema de comunicaciones inalámbricas y, en particular, sobre sistemas de comunicaciones inalámbricas con la capacidad de proteger la integridad de las transmisiones de datos en un portador de radio de datos entre los nodos receptor y remitente.

Antecedentes

La Figura 1 muestra un sistema de comunicaciones celulares con un nodo servidor 101 que sirve a un equipo de usuario (UE) 103 situado dentro del área geográfica de servicio del nodo servidor, denominada célula 105. Dependiendo del sistema, el nodo servidor 101 puede ser, por ejemplo, una estación base, un Nodo B, o un Nodo B evolucionado (eNodoB o eNB). En lo sucesivo, se denominará eNB al nodo servidor 101 en un ejemplo no limitante de un sistema de evolución a largo plazo (LTE). La comunicación es bidireccional entre el eNB 101 y el UE 103. Se dice que las comunicaciones del eNB 101 al UE 103 tienen lugar en una dirección de enlace descendente, mientras que se dice que las comunicaciones del UE 103 al eNB 101 tienen lugar en una dirección de enlace ascendente.

En un sistema de comunicaciones inalámbricas también pueden usarse nodos retransmisores. La Figura 2 ilustra un nodo retransmisor (RN) 204 con un área de servicio o célula 207, comunicándose el RN 204 con un eNB donador (DeNB) 202 con un área de servicio o célula 206, y uno o varios UE 203 situados dentro de la célula 207 del RN. Las transmisiones entre el UE 203 y el RN 204 se realizan por una interfaz de radio denotada Uu, que es la misma que para la comunicación regular del eNB al UE, de modo que, desde la perspectiva de un UE, el RN parece un eNB regular. Las transmisiones entre el RN 204 y el DeNB 202 se realizan por una interfaz de radio denotada Un, que reutiliza gran parte de la funcionalidad de la interfaz Uu. Esto quiere decir que el DeNB 202 gestiona el RN 204 como un UE, usando protocolos similares que cuando se comunica con un UE con algunas adiciones.

Para funcionar como un eNB en un sistema LTE, el RN 304 tiene una configuración S1 de interfaz hacia la red central con la entidad de gestión de la movilidad (MME) y/o la pasarela 308 de servicio (SGW), que está representada en el DeNB 302. El RN 304 también puede tener una configuración X2 de interfaz hacia otros eNB 301, en cuyo caso la interfaz X2 está representada en el DeNB 302. Se muestra la arquitectura en la Figura 3. Los eNB 301, los DeNB 302 y el RN 304 son todos parte de la red 300 de acceso de radio terrestre universal evolucionada (E-UTRAN), que es la red de radio del sistema LTE.

La descripción del elemento de trabajo de la versión 10 de 3GPP LTE para un retransmisor o RN incluye las siguientes características. En primer lugar, células 207 de control del RN (véase la ilustración en la **Figura 2**), cada una de las cuales parece a un UE una célula separada distinta de la célula 206 del DeNB. En segundo lugar, esas células controladas por un RN tienen sus propias ID de célula física, según se define en la versión 8 de LTE, y el RN transmite sus propios canales de sincronización y símbolos de referencia. En tercer lugar, el UE recibe directamente del RN información de planificación y respuesta a solicitudes de repetición automática híbrida (HARQ) y envía al RN su información del canal de control, tal como solicitudes de planificación (SR), índice de calidad del canal (CQI) y acuses de recibo (ACK). En cuarto lugar, preferiblemente no debería haber ningún impacto en el UE por la funcionalidad del RN, para que la célula 207 del RN pueda servir a los UE LTE preexistentes.

Es deseable dar soporte a la protección de la integridad de la señalización y/o los datos del RN entre el RN y el DeNB. Una opción es implementar esta protección de la integridad en la capa del protocolo de convergencia de paquetes de datos (PDCP) descrita en las especificaciones 3GPP como una funcionalidad específica a los retransmisores en la capa PDCP. En tal caso, la disposición y la configuración de la protección de la integridad serán realizadas por el protocolo RRC. La habilitación y la inhabilitación de la protección de la integridad PDCP —a veces denominadas también activación e inhabilitación de la protección de la integridad— pueden ser realizadas para cada portador de radio de datos (DRB), lo que quiere decir que no todos los DRB estarían necesariamente configurados para usar la protección de la integridad en un momento dado.

La protección de la integridad en PDCP puede usar un número de secuencia (SN) único como entrada al algoritmo de protección de la integridad para cada paquete que se proteja. Esto hace diferente al código de verificación de la integridad incluso para paquetes idénticos enviados en momentos diferentes por el mismo DRB, ya que tienen SN diferentes. Para evitar una sobrecarga innecesaria, puede no transmitirse con cada paquete el SN completo usado como entrada para la protección de la integridad, tal como un valor COUNT. En vez de ello, en cada paquete solo se transmite parte de los bits menos significativos de este valor de SN —normalmente 7 o 12 bits que se denominan SN de PDCP—. Entonces el transmisor y el receptor mantienen implícitamente un registro de los bits restantes del número de secuencia completo, es decir, los 25 o los 20 bits que se denominan contador de desbordamiento o número de hipertrama. Esto requiere que el receptor incremente el contador de desbordamiento cada vez que el SN de PDCP dé la vuelta; por ejemplo, que pase de un valor de contador 1111111 -> 0000000.

En la técnica anterior se propone dar soporte a la habilitación de la protección de la integridad en la configuración del DRB. Sin embargo, la propuesta solo permite la posibilidad de cambiar la protección de la integridad, es decir,

habilitar o inhabilitar la protección de la integridad, para un portador en curso en un traspaso. Se considera que cambiar la protección de la integridad de un DRB durante la operación normal es demasiado complejo, dado que es difícil coordinar el cambio de la protección de la integridad con el tráfico en curso en el DRB; por ejemplo, debido a las retransmisiones, lo que puede llevar a que algunos paquetes estén protegidos y otros no. Una inquietud es que esto pueda dificultar que el receptor sepa si se ha aplicado o no protección de la integridad a un paquete dado.

Así, según la propuesta, solo es posible habilitar o inhabilitar la protección de la integridad en la configuración inicial del DRB, en el traspaso o al abandonar el DRB y configurar un nuevo DRB para transportar el tráfico. El nuevo portador puede ser configurado con o sin protección de la integridad, dependiendo en qué se desee, independientemente de la configuración del DRB anterior. Sin embargo, el abandono de un portador y la configuración de uno nuevo es un procedimiento complejo que también induce una demora. Además, no hay soporte alguno para la entrega de datos sin pérdidas y libres de duplicados, dado que los paquetes relacionados con el DRB antiguo, que pueden haber sido transmitidos por el transmisor pero que de momento no han sido recibidos por el receptor, serán descartados por los protocolos de radio cuando se abandone el DRB antiguo.

Una posible solución al problema de la pérdida de paquetes cuando se abandona un DRB y se configura uno nuevo es desencadenar un traspaso dentro de la célula para habilitar o inhabilitar la protección de la integridad para un DRB en curso. Sin embargo, realizar un traspaso dentro de la célula solo para habilitar o inhabilitar la protección de la integridad de uno o más DRB causa una interrupción innecesaria de la transferencia de datos que introduce demoras, así como una carga innecesaria en el canal de acceso aleatorio, dado que un procedimiento de acceso aleatorio siempre forma parte de un traspaso. Además, un traspaso dentro de la célula es una solución innecesariamente compleja.

Otra manera posible de dar soporte a la habilitación o la inhabilitación de la protección de la integridad de un DRB durante la operación normal en la técnica anterior es incluir una indicación en la cabecera PDCP que indique si se aplica la protección de la integridad a un paquete dado. Sin embargo, esto introduce sobrecarga adicional en la cabecera PDCP y potencialmente podría ser objeto de uso indebido por parte de un “atacante” que pueda manipular un paquete que tenga protección de la integridad al cambiar la indicación de la cabecera PDCP diciendo que no está protegido.

El documento “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture (Release 9)”, BORRADOR 3GPP; 33401-950, PROYECTO DE ASOCIACIÓN DE 3ª GENERACIÓN (3GPP), da a conocer una reconfiguración de la protección de la integridad para portadores de radio en la configuración inicial o tras un traspaso.

Compendio

Por lo tanto, es un objeto abordar algunos de los problemas esbozados más arriba y permitir la reconfiguración de la protección de la integridad de un DRB distinta de la de la configuración inicial del DRB y el traspaso, sin perder ningún paquete ni añadir ninguna complejidad ni/o demoras. Este y otros objetos se logran mediante los métodos y los nodos remitentes y receptores según las reivindicaciones independientes, y mediante las realizaciones según las reivindicaciones dependientes.

Según una primera realización, se proporciona un método en un nodo remitente de un sistema de comunicaciones inalámbricas para dar soporte a la habilitación y la inhabilitación de la protección de la integridad de al menos un portador de radio de datos entre el nodo remitente y un nodo receptor. El método comprende, tras un restablecimiento de la conexión con éxito entre el nodo remitente y el nodo receptor, transmitir al nodo receptor un mensaje de reconfiguración de la conexión. El mensaje de reconfiguración de la conexión comprende un indicador que indica cuáles de los al menos un portador de radio de datos tendrán habilitada la protección de la integridad.

Según una segunda realización, se proporciona un método en un nodo receptor de un sistema de comunicaciones inalámbricas para habilitar e inhabilitar la protección de la integridad de al menos un portador de radio de datos entre un nodo remitente y el nodo receptor. El método comprende, tras un restablecimiento de la conexión con éxito entre el nodo remitente y el nodo receptor, recibir del nodo remitente un mensaje de reconfiguración de la conexión. El mensaje de reconfiguración de la conexión comprende un indicador que indica cuáles de los al menos un portador de radio de datos tendrán habilitada la protección de la integridad. El método comprende, además, habilitar la protección de la integridad de los paquetes en el al menos un portador de radio de datos indicado por el indicador, e inhabilitar la protección de la integridad de los paquetes en el resto de los al menos un portador de radio de datos.

Según una tercera realización, se proporciona un nodo remitente para un sistema de comunicaciones inalámbricas. El nodo remitente está configurado para dar soporte a la habilitación y la inhabilitación de la protección de la integridad de al menos un portador de radio de datos entre el nodo remitente y un nodo receptor. El nodo remitente comprende un transmisor configurado para transmitir al nodo receptor un mensaje de reconfiguración de la conexión tras un restablecimiento de la conexión con éxito entre el nodo remitente y el nodo receptor. El mensaje de reconfiguración de la conexión comprende un indicador que indica cuáles de los al menos un portador de radio de datos tendrán habilitada la protección de la integridad.

Según una cuarta realización, se proporciona un nodo receptor para un sistema de comunicaciones inalámbricas. El nodo receptor está configurado para habilitar e inhabilitar la protección de la integridad de al menos un portador de radio de datos entre un nodo remitente y el nodo receptor. El nodo receptor comprende un receptor configurado para recibir del nodo remitente un mensaje de reconfiguración de la conexión tras un restablecimiento de la conexión con éxito entre el nodo remitente y el nodo receptor. El mensaje de reconfiguración de la conexión comprende un indicador que indica cuáles de los al menos un portador de radio de datos tendrán habilitada la protección de la integridad. El nodo receptor también comprende una unidad de tratamiento configurada para habilitar la protección de la integridad de los paquetes en el al menos un portador de radio de datos indicado por el indicador, y para inhabilitar la protección de la integridad de los paquetes en el resto de los al menos un portador de radio de datos.

Una ventaja de las realizaciones es que posibilitan la habilitación y la inhabilitación de la protección de la integridad de un DRB en curso no solo en el traspaso, sino también en el restablecimiento de la conexión RRC.

En la siguiente descripción detallada se explicarán otros objetos, ventajas y características de las realizaciones cuando se la considera junto con los dibujos y las reivindicaciones adjuntos.

Breve descripción de los dibujos

La Figura 1 es una ilustración esquemática de un eNB y un UE en un sistema de comunicaciones inalámbricas.

La Figura 2 es una ilustración esquemática de un DeNB, un RN y un UE en un sistema de comunicaciones inalámbricas.

La Figura 3 es una ilustración esquemática de la arquitectura con un DeNB y un RN en un sistema de comunicaciones inalámbricas.

Las Figuras 4a-b son diagramas de señalización que ilustran el procedimiento de restablecimiento de la conexión RRC.

La Figura 5 es un diagrama de señalización que ilustra el procedimiento de reconfiguración de la conexión RRC.

La Figura 6 es un diagrama de flujo del método en el nodo remitente según algunas realizaciones.

La Figura 7 es un diagrama de flujo del método en el nodo receptor según algunas realizaciones.

Las Figuras 8a-b son diagramas de bloques que ilustran los nodos remitente y receptor según algunas realizaciones.

Descripción detallada

En lo que sigue se describirán diferentes aspectos con más detalle con referencias a ciertas realizaciones y a los dibujos adjuntos. Con fines de explicación y no de limitación se exponen detalles específicos, tales como escenarios y técnicas particulares, para proporcionar una comprensión cabal de las diferentes realizaciones. Sin embargo, también pueden existir otras realizaciones que se aparten de estos detalles específicos.

Se describen realizaciones en un contexto general no limitante en relación con una red LTE que emplea la protección de la integridad de un DRB entre un RN y un UE. Sin embargo, debería hacerse notar que las realizaciones también pueden ser aplicadas a otros tipos de redes de acceso de radio en las que se use la protección de la integridad de los DRB.

Aunque la tecnología siguiente se describe en el contexto de RN que se conectan con un DeNB, la tecnología también puede ser usada en otros escenarios cuando se usa la protección de la integridad; por ejemplo, para UE que se conectan con una estación base normal, tal como un eNB y un Nodo B.

Se aborda el problema de cómo permitir una reconfiguración de la protección de la integridad para un DRB en curso sin añadir complejidad ni demoras y sin perder ningún paquete de datos mediante una solución en la que un DeNB transmite un mensaje a un RN para una reconfiguración de la conexión inmediatamente después de un restablecimiento de la conexión con éxito entre el DeNB y el RN, y en el que el mensaje comprende un indicador que indica cuáles de los DRB tendrán habilitada la protección de la integridad. El RN puede entonces habilitar e inhabilitar la integridad de los DRB según el indicador cuando se reanuden después del restablecimiento.

Esta solución posibilita la habilitación o la inhabilitación de la protección de la integridad de los DRB en el restablecimiento de conexiones RRC sin introducir complejidad adicional relativa a la gestión de las transmisiones de datos en el DRB. Se suspenden todas las transmisiones de datos durante el periodo de restablecimiento del RRC, lo que quiere decir que el receptor puede determinar si un paquete fue enviado antes o después de la habilitación o la inhabilitación de la protección de la integridad. La tecnología también permite la entre de paquetes sin pérdidas durante la reconfiguración de la protección de la integridad, porque no se abandona el DRB.

Así, la protección de la integridad de un DRB puede cambiarse en el restablecimiento de la conexión RRC, lo que quiere decir que la protección de la integridad de un DRB puede ser cambiado en momentos distintos que en la

configuración del DRB y el traspaso. El restablecimiento de la conexión RRC puede ocurrir, por ejemplo, cuando el RN sufre un fallo del radioenlace que puede ser debido a diversos problemas en el radioenlace. Además, el restablecimiento de la conexión RRC puede ocurrir cuando el RN pierde la sincronización del contador de desbordamiento, cuando el RN no logra verificar la integridad de los paquetes entrantes o cuando el RN no logra implementar una reconfiguración de la conexión RRC. En lo sucesivo se describen tres escenarios ejemplares no limitantes en los que puede ser beneficioso habilitar o inhabilitar la protección de la integridad en uno o más DRB, que también incluyen la señalización durante el restablecimiento. Se describen estos tres escenarios para ilustrar la tecnología y algunas ventajas de ella.

Escenario 1: En este escenario se supone que se aplica la protección de la integridad para un DRB, pero que el RN y el DeNB pierden la sincronización de sus contadores de desbordamiento, por ejemplo, debido a demasiadas pérdidas de paquetes. Por lo tanto, fallará la protección de la integridad de los paquetes en el DRB. Potencialmente, este fallo puede provocar que el RN realice un restablecimiento de la conexión RRC. En el momento del restablecimiento, puede resultar deseable que el DeNB pueda desactivar la protección de la integridad de este DRB para evitar intentos ulteriores de restablecimiento procedente del RN. Al evitar los intentos de restablecimiento procedente del RN, se da control al DeNB para que resuelve el caso de error en el que se pierde la sincronización del contador de desbordamiento.

Escenario 2: En este escenario se supone que un “atacante” está intentando manipular los paquetes en el enlace entre el RN y el DeNB. El RN puede detectar que algunos paquetes están modificados, por ejemplo, detectando un salto en el SN, o que se usen valores improbables para algunos campos del protocolo. Esto puede desencadenar un restablecimiento de la conexión RRC. En consecuencia del restablecimiento, el DeNB puede habilitar la protección de la integridad de algunos DRB para una mayor seguridad contra el ataque.

Escenario 3: En este escenario se supone que ocurre un restablecimiento hacia una célula del DeNB con diferente soporte de la protección de la integridad de DRB de la que tenía la anterior célula del DeNB. Por ejemplo, si un RN con todos sus DRB configurados con protección de la integridad experimenta un fallo de radioenlace en una célula 1 del DeNB, el RN puede intentar restablecer su conexión RRC contra una célula 2 del DeNB. Esta célula 2 del DeNB puede no soportar la protección de integridad del DRB en absoluto, o puede no tener la capacidad de tratamiento para soportar la protección de la integridad en todos los DRB del RN. Sin la posibilidad de inhabilitar la protección de la integridad en el restablecimiento, la célula 2 del DeNB debe entonces rechazar el intento de restablecimiento de RRC o rechazar los DRB que no pueda gestionar. En cambio, al permitir la reconfiguración de la protección de la integridad, este problema puede solucionarse aceptable el intento de restablecimiento y todos los DRB, e inhabilitando la protección de la integridad en los DRB cuando no pueda dársele soporte. En otra situación, la célula 2 del DeNB puede soportar únicamente los DBR con integridad protegida de un RN, y puede entonces aceptar únicamente la solicitud de restablecimiento del RRC si puede configurar la protección de la integridad en los DRB.

Restablecimiento del RRC con cambio de la protección de la integridad: Durante el procedimiento de restablecimiento de la conexión RRC en E-UTRAN, se suspenden todos los DRB. Para reanudar los DRB, se lleva a cabo una reconfiguración de la conexión RRC. El DeNB transmite una indicación para cada DRB en el primer mensaje de reconfiguración del RRC de la conexión después del restablecimiento de la conexión RRC. La indicación indica si debería aplicarse para ese DRB la protección de la integridad efectuada en la transmisión y la verificación de la integridad en la recepción. Cuando el RN recibe una indicación de que debería aplicarse la protección/verificación de la integridad para un DRB dado, el RN aplica la protección/verificación de la integridad para todos los paquetes subsiguientes en este DRB. Se aplica la protección/verificación de la integridad o bien hasta que se abandone el DRB o hasta que el RN reciba indicaciones ulteriores de que deba dejar de efectuar la protección/verificación de la integridad; por ejemplo, en el traspaso o en un restablecimiento ulterior de la conexión RRC. La indicación de la protección de la integridad puede ser, por ejemplo, del mismo tipo que la correspondiente indicación enviada para cambiar la protección de la integridad en un traspaso.

En las Figuras 4a y 4b se muestra una ilustración del procedimiento de restablecimiento de la conexión RRC en E-UTRAN. La Figura 4a ilustra un restablecimiento de la conexión RRC con éxito, y la Figura 4b ilustra un restablecimiento de la conexión RRC sin éxito. En las Figuras 4a y 4b, en S41, el UE 403 transmite a la E-UTRAN 401 un mensaje de solicitud de restablecimiento de la conexión RRC (RRCConnectionReestablishmentRequest). En la Figura 4a, la E-UTRAN devuelve un mensaje de restablecimiento de la conexión RRC (RRCConnectionReestablishment) en S42, y el UE responde con un mensaje de restablecimiento de la conexión RRC completo (RRCConnectionReestablishmentComplete) en S43. Así, el restablecimiento de la conexión tiene éxito. Si la E-UTRAN tiene que rechazar el restablecimiento, se devuelve un mensaje de rechazo del restablecimiento de la conexión RRC (RRCConnectionReestablishmentReject) en S44 al UE tras recibir la solicitud en S41, según se ilustra en la Figura 4b. Las Figuras 4a y 4b muestran la interacción entre el UE 403 y la E-UTRAN 401. Sin embargo, en el caso descrito más arriba con un DeNB y un RN, las Figuras 4a y 4b pueden ser interpretadas como una ilustración de la señalización entre un RN y su DeNB durante un procedimiento de restablecimiento de la conexión RRC. Así, el UE 403 puede ser sustituido por el RN, y la E-UTRAN 401 por el DeNB.

Una solicitud de restablecimiento de la conexión RRC solo tiene éxito si la célula (marcada E-UTRAN en las figuras) está preparada para él, lo que significa que tenga un contexto válido de UE para el UE que intenta restablecer su conexión RRC. Esto quiere decir que la célula conoce la configuración del DRB del UE que intenta efectuar un

restablecimiento del RRC. Tras la finalización con éxito del procedimiento de restablecimiento de la conexión RRC, se suspenden todos los DRB. Para reanudar los DRB, se envía una reconfiguración de la conexión RRC, según se ilustra en la Figura 5. El procedimiento de reconfiguración de la conexión se inicia cuando la E-UTRAN 501 envía un mensaje de reconfiguración de la conexión RRC (RRCConnectionReconfiguration) en S51 al UE 503. El UE contesta con un mensaje de reconfiguración de la conexión RRC completa (RRCConnectionReconfigurationComplete) en S52. La Figura 5 muestra la interacción entre el UE 503 y la E-UTRAN 501. Sin embargo, en el caso de un RN que se conecta con un DeNB, la Figura 5 puede ser interpretada como una ilustración de la señalización entre el RN y el DeNB durante la reconfiguración de la conexión RRC. Así, el UE 503 puede ser sustituido por el RN, y la E-UTRAN 501 por el DeNB. Hay también un caso de fallo de la reconfiguración de la conexión RRC, no ilustrado aquí, que es aplicable si el UE o el RN son incapaces de atenerse a la configuración.

Según una realización, se incluye la indicación de la protección de la integridad para cada DRB, dentro del mensaje de reconfiguración de la conexión RRC (*RRCConnectionReconfiguation*) en S51. Sin embargo, pueden contemplarse otros mensajes de reconfiguración de la conexión, siempre que sea un mensaje de reconfiguración que se produzca tras un restablecimiento de la conexión con el propósito de reanudar los DRB tras una suspensión debida al restablecimiento. La indicación de la protección de la integridad permite habilitar la protección de la integridad para el DRB si estaba inhabilitada previamente; inhabilitar la protección de la integridad para el DRB si estaba habilitada previamente; y mantener la protección de la integridad habilitada o inhabilitada, como antes del restablecimiento y la reconfiguración. El procedimiento para cambiar la protección de la integridad en el restablecimiento puede ser el mismo para todos los escenarios descritos anteriormente.

La Figura 6 es un diagrama de flujo de un método en el nodo remitente de un sistema de comunicaciones inalámbricas para dar soporte a la habilitación y la inhabilitación de la protección de la integridad de uno o más DRB entre el nodo remitente y un nodo receptor. En algunas realizaciones, el nodo remitente puede ser una estación base de radio, y el nodo receptor puede ser un RN o un UE.

El método comprende, tras un restablecimiento de la conexión con éxito entre el nodo remitente y el nodo receptor:

– 610: Transmitir un mensaje de reconfiguración de la conexión al nodo receptor. El mensaje de reconfiguración de la conexión comprende un indicador que indica cuáles de los DRB tendrán habilitada la protección de la integridad.

En una realización, el mensaje transmitido de reconfiguración de la conexión es un mensaje de reconfiguración de la conexión RRC tras un restablecimiento de la conexión RRC. Sin embargo, en realizaciones alternativas pueden contemplarse otros mensajes para reconfigurar la conexión. En una realización, la protección de la integridad comprende:

- Añadir una suma de comprobación de protección de la integridad a un paquete transmitido.
- Verificar una suma de comprobación de protección de la integridad en un paquete recibido.
- Descartar el paquete recibido cuando falla la verificación de la suma de comprobación de protección de la integridad.

La verificación de la suma de comprobación de protección de la integridad comprende calcular un código de autenticación para la integridad basado en algunos parámetros de entrada y compararlo con la suma de comprobación recibida en el paquete. Si se corresponden entre sí, la verificación tiene éxito.

La Figura 7 es un diagrama de flujo de un método en un nodo receptor de un sistema de comunicaciones inalámbricas para habilitar e inhabilitar la protección de la integridad de uno o más DRB entre un nodo remitente y el nodo receptor. En algunas realizaciones, el nodo remitente puede ser una estación base de radio, y el nodo receptor puede ser un RN o un UE. El método comprende, tras un restablecimiento de la conexión con éxito entre el nodo remitente y el nodo receptor:

– 710: Recibir del nodo remitente un mensaje de reconfiguración de la conexión. Este mensaje de reconfiguración de la conexión comprende un indicador que indica cuáles de los DRB tendrán habilitada la protección de la integridad.

– 720: Habilitar la protección de la integridad de los paquetes en los DRB indicados por el indicador. Así, los paquetes transmitidos en los DRB indicados tendrán ahora protegida su integridad, con independencia de que tuvieran o no protegida su integridad antes del restablecimiento de la conexión.

– 730: Inhabilitar la protección de la integridad de los paquetes en el resto de los DRB. No se usará protección de la integridad alguna en los DRB para los que no se indicó que tuvieran habilitada la protección de la integridad, con independencia de que tuvieran o no protegida su integridad antes del restablecimiento de la conexión.

En una realización, el mensaje recibido de reconfiguración de la conexión es un mensaje de reconfiguración de la conexión RRC tras un restablecimiento de la conexión RRC. Sin embargo, en realizaciones alternativas pueden

contemplarse otros mensajes para reconfigurar la conexión. En una realización, la protección de la integridad comprende:

- Añadir una suma de comprobación de protección de la integridad a un paquete transmitido.
- Verificar una suma de comprobación de protección de la integridad en un paquete recibido.
- Descartar el paquete recibido cuando falla la verificación de la suma de comprobación de protección de la integridad.

En el diagrama de bloques de la Figura 8a se ilustran esquemáticamente un nodo remitente 800 y un nodo receptor 850 para un sistema de comunicaciones inalámbricas según algunas realizaciones. En algunas realizaciones, el nodo receptor puede ser un RN o un UE. En cualquiera de los dos casos, el nodo remitente puede ser una estación base de radio. El nodo remitente 800 está configurado para dar soporte a la habilitación y la inhabilitación de la protección de la integridad fe uno o más DRB entre el nodo remitente y el nodo receptor 850. El nodo remitente comprende un transmisor 801 configurado para transmitir al nodo receptor un mensaje de reconfiguración de la conexión tras un restablecimiento de la conexión con éxito entre el nodo remitente y el nodo receptor. El mensaje de reconfiguración de la conexión comprende un indicador que indica cuáles de los DRB tendrán habilitada la protección de la integridad. En la Figura 8a, el transmisor 801 está conectado a una antena 803 por medio de un puerto de antena. Sin embargo, puede haber más de una antena y/o más de un puerto de antena.

En una realización, el mensaje transmitido de reconfiguración de la conexión es un mensaje de reconfiguración de la conexión RRC tras un restablecimiento de la conexión RRC. En una realización, la protección de la integridad comprende:

- Añadir una suma de comprobación de protección de la integridad a un paquete transmitido.
- Verificar una suma de comprobación de protección de la integridad en un paquete recibido.
- Descartar el paquete recibido cuando falla la verificación de la suma de comprobación de protección de la integridad.

El nodo receptor 850 ilustrado en la Figura 8a está configurado para habilitar e inhabilitar la protección de la integridad de uno o más DRB entre el nodo remitente 800 y el nodo receptor. El nodo receptor comprende un receptor 851 configurado para recibir un mensaje de reconfiguración de la conexión del nodo remitente tras un restablecimiento de la conexión con éxito entre el nodo remitente y el nodo receptor. El mensaje de reconfiguración de la conexión comprende un indicador que indica cuáles de los DRB tendrán habilitada la protección de la integridad. El receptor 851 está conectado a una antena 853 por medio de un puerto de antena. Sin embargo, puede haber más de una antena y/o más de un puerto de antena.

El nodo receptor también comprende una unidad 852 de tratamiento configurada para habilitar la protección de la integridad de los paquetes en los DRB indicados por el indicador, y para inhabilitar la protección de la integridad de los paquetes en el resto de los DRB. En una realización, el mensaje recibido de reconfiguración de la conexión es un mensaje de reconfiguración de la conexión RRC tras un restablecimiento de la conexión de RRC. En una realización, la protección de la integridad comprende:

- Añadir una suma de comprobación de protección de la integridad a un paquete transmitido.
- Verificar una suma de comprobación de protección de la integridad en un paquete recibido.
- Descartar el paquete recibido cuando falla la verificación de la suma de comprobación de protección de la integridad.

Las unidades descritas anteriormente con referencia a la Figura 8a pueden ser unidades lógicas, unidades físicas separadas o una mezcla de unidades tanto lógicas como físicas.

La Figura 8b ilustra esquemáticamente una realización del nodo receptor 850, que es una manera alternativa de dar a conocer la realización ilustrada en la Figura 8a. El nodo receptor 850 comprende un receptor 851 conectado a una antena 853 por medio de un puerto de antena, tal como ya se ha descrito más arriba con referencia a la Figura 8a. El nodo receptor 850 también comprende una unidad central 855 de procesamiento (CPU), que puede ser una sola unidad o varias unidades. Además, el nodo receptor 850 comprende al menos un producto 856 de programa informático en forma de memoria no volátil, por ejemplo, una EEPROM (memoria de solo lectura programable y borrable eléctricamente), una memoria flash o una unidad de disco. El producto 856 de programa informático comprende un programa informático 857, que comprende un medio de código que, cuando se ejecuta en el nodo receptor 850 hace que la CPU 855 del nodo receptor 850 lleve a cabo las etapas del procedimiento descrito anteriormente en relación con la Figura 7.

De ahí que, en la realización descrita, el medio de código del programa informático 857 del nodo receptor 850 comprenda un módulo 857a para habilitar la protección de la integridad de los paquetes en el DRB indicado por el

indicador recibido en el mensaje de reconfiguración de la conexión, y un módulo 857b para inhabilitar la protección de la integridad en el resto de los DRB. Así, el medio de código puede ser implementado como código de programa informático estructurado en módulos de programa informático. Los módulos 857a y 857b esencialmente llevan a cabo las etapas 720 y 730 del flujo de la Figura 7 para emular el nodo receptor 850 descrito en la Figura 8a. En otras palabras, cuando los módulos 857a y 857b son ejecutados en la CPU 855, corresponden a la unidad 852 de tratamiento de la Figura 8a.

Aunque el medio de código en la realización dada a conocer anteriormente en relación con la Figura 8b está implementado como módulo de programa informático, en realizaciones alternativas puede implementarse, al menos parcialmente, como circuitos de soporte físico.

Aunque la anterior descripción contiene muchos detalles específicos, no debería interpretarse que sean limitantes, sino que meramente proporcionan ilustraciones de algunas realizaciones actualmente preferentes. La tecnología abarca plenamente otras realizaciones que pueden resultar evidentes para los expertos en la técnica. La referencia a un elemento en singular no se pretende que signifique “uno y solo uno”, a no ser que así se afirme explícitamente, sino, más bien “uno o más”. Se pretende que todos los equivalentes estructurales y funcionales de los elementos de las realizaciones anteriormente descritas que son conocidos a las personas con un dominio normal de la técnica estén abarcados por la presente solicitud. Además, no es preciso que un dispositivo o un método aborden cada uno de los problemas y todos ellos cuya solución se busca por medio de la tecnología descrita para que estén abarcados por la misma.

La descripción presenta detalles específicos, tales como realizaciones particulares, con fines de explicación y no de limitación. Sin embargo, un experto en la técnica apreciará que pueden emplearse otras realizaciones aparte de estos detalles específicos. En algunos casos, se omiten descripciones detalladas de métodos, interfaces, circuitos y dispositivos bien conocidos para no ofuscar la descripción con detalles innecesarios. En las figuras se muestran bloques individuales correspondientes a diversos nodos. Los expertos en la técnica apreciarán que las funciones de esos bloques pueden ser implementadas usando circuitos individuales de soporte físico y/o programas y datos de soporte lógico, junto con un microprocesador digital adecuadamente programado o un ordenador de uso general. Los nodos que se comunican usando la interfaz aérea también tienen una circuitería adecuada de comunicaciones por radio. Se reconocerá que diversas acciones pueden ser realizadas por circuitos especializados (por ejemplo, puertas lógicas analógicas y/o discretas interconectadas para llevar a cabo una función especializada), por uno o más procesadores programados con un conjunto adecuado de instrucciones, o por una combinación de ambos. En la presente memoria se usa la expresión “circuitería configurada para llevar a cabo una o más acciones descritas” para referirse a cualquier realización tal (es decir, uno o más circuitos especializados y/o uno o más procesadores programados). Además, también puede considerarse que la tecnología esté implementada enteramente dentro de cualquier forma de memoria legible por ordenador, tal como una memoria de estado sólido, un disco magnético o un disco óptico que contengan un conjunto apropiado de instrucciones informáticas que hagan que un procesador lleve a cabo las técnicas descritas en la presente memoria.

REIVINDICACIONES

1. Un método en un nodo remitente (800) de un sistema de comunicaciones inalámbricas para dar soporte a la habilitación y la inhabilitación de la protección de la integridad de al menos un portador de radio de datos entre el nodo remitente y un nodo receptor (850), comprendiendo el método, tras un restablecimiento de la conexión con éxito entre el nodo remitente y el nodo receptor:

– transmitir (610) al nodo receptor (850) un mensaje de reconfiguración de la conexión, **caracterizado porque** el mensaje de reconfiguración de la conexión comprende un indicador que indica cuáles de los al menos un portador de radio de datos tendrán habilitada la protección de la integridad.

2. El método según la reivindicación 1 en el que el mensaje transmitido de reconfiguración de la conexión es un mensaje de reconfiguración de la conexión de control de recursos de radio, RRC, tras un restablecimiento de la conexión de RRC.

3. El método según cualquiera de las reivindicaciones precedentes en el que la protección de la integridad comprende:

– añadir una suma de comprobación de protección de la integridad a un paquete transmitido,

– verificar una suma de comprobación de protección de la integridad en un paquete recibido, y

– descartar el paquete recibido cuando falla la verificación de la suma de comprobación de protección de la integridad.

4. El método según cualquiera de las reivindicaciones precedentes, en el que el nodo receptor es un nodo retransmisor.

5. El método según cualquiera de las reivindicaciones 1-3 en el que el nodo receptor es un equipo de usuario.

6. El método según cualquiera de las reivindicaciones precedentes en el que el nodo remitente es una estación base de radio.

7. Un método en un nodo receptor (850) de un sistema de comunicaciones inalámbricas para habilitar e inhabilitar la protección de la integridad de al menos un portador de radio de datos entre un nodo remitente (800) y el nodo receptor, comprendiendo el método, tras un restablecimiento de la conexión con éxito entre el nodo remitente y el nodo receptor:

– recibir (710) del nodo remitente un mensaje de reconfiguración de la conexión, **caracterizado porque** el mensaje de reconfiguración de la conexión comprende un indicador que indica cuáles de los al menos un portador de radio de datos tendrán habilitada la protección de la integridad,

– habilitar (720) la protección de la integridad de los paquetes en el al menos un portador de radio de datos indicado por el indicador, e

– inhabilitar (730) la protección de la integridad de los paquetes en el resto de los al menos un portador de radio de datos.

8. El método según la reivindicación 7 en el que el mensaje recibido de reconfiguración de la conexión es un mensaje de reconfiguración de la conexión de control de recursos de radio, RRC, tras un restablecimiento de la conexión de RRC.

9. El método según cualquiera de las reivindicaciones 7-8 en el que la protección de la integridad comprende:

– añadir una suma de comprobación de protección de la integridad a un paquete transmitido,

– verificar una suma de comprobación de protección de la integridad en un paquete recibido, y

– descartar el paquete recibido cuando falla la verificación de la suma de comprobación de protección de la integridad.

10. El método según cualquiera de las reivindicaciones 7-9 en el que el nodo receptor es un nodo retransmisor.

11. El método según cualquiera de las reivindicaciones 7-9 en el que el nodo receptor es un equipo de usuario.

12. El método según cualquiera de las reivindicaciones 7-11 en el que el nodo remitente es una estación base de radio.

13. Un nodo remitente (800) para un sistema de comunicaciones inalámbricas, configurado para dar soporte a la habilitación y la inhabilitación de la protección de la integridad de al menos un portador de radio de datos entre el

nodo remitente y un nodo receptor (850), comprendiendo el nodo remitente un transmisor (801) configurado para transmitir al nodo receptor un mensaje de reconfiguración de la conexión tras un restablecimiento de la conexión con éxito entre el nodo remitente y el nodo receptor, **caracterizado porque** el mensaje de reconfiguración de la conexión comprende un indicador que indica cuáles de los al menos un portador de radio de datos tendrán habilitada la protección de la integridad.

14. El nodo remitente según la reivindicación 13 en el que el mensaje transmitido de reconfiguración de la conexión es un mensaje de reconfiguración de la conexión de control de recursos de radio, RRC, tras un restablecimiento de la conexión de RRC.

15. El nodo remitente según cualquiera de las reivindicaciones 13-14 en el que la protección de la integridad comprende:

- añadir una suma de comprobación de protección de la integridad a un paquete transmitido,
- verificar una suma de comprobación de protección de la integridad en un paquete recibido, y
- descartar el paquete recibido cuando falla la verificación de la suma de comprobación de protección de la integridad.

16. El nodo remitente según cualquiera de las reivindicaciones 13-15 en el que el nodo remitente es una estación base de radio.

17. Un nodo receptor (850) para un sistema de comunicaciones inalámbricas, configurado para habilitar e inhabilitar la protección de la integridad de al menos un portador de radio de datos entre un nodo remitente (800) y el nodo receptor, comprendiendo el nodo receptor:

- un receptor (851) configurado para recibir del nodo remitente un mensaje de reconfiguración de la conexión tras un restablecimiento de la conexión con éxito entre el nodo remitente y el nodo receptor, **caracterizado porque** el mensaje de reconfiguración de la conexión comprende un indicador que indica cuáles de los al menos un portador de radio de datos tendrán habilitada la protección de la integridad, y
- una unidad (852) de tratamiento configurada para habilitar la protección de la integridad de los paquetes en el al menos un portador de radio de datos indicado por el indicador, y para inhabilitar la protección de la integridad de los paquetes en el resto de los al menos un portador de radio de datos.

18. El nodo receptor según la reivindicación 17 en el que el mensaje recibido de reconfiguración de la conexión es un mensaje de reconfiguración de la conexión de control de recursos de radio, RRC, tras un restablecimiento de la conexión de RRC.

19. El nodo receptor según cualquiera de las reivindicaciones 17-18 en el que la protección de la integridad comprende:

- añadir una suma de comprobación de protección de la integridad a un paquete transmitido,
- verificar una suma de comprobación de protección de la integridad en un paquete recibido, y
- descartar el paquete recibido cuando falla la verificación de la suma de comprobación de protección de la integridad.

20. El nodo receptor según cualquiera de las reivindicaciones 17-19 en el que el nodo receptor es un nodo retransmisor.

21. El nodo receptor según cualquiera de las reivindicaciones 17-19 en el que el nodo receptor es un equipo de usuario.

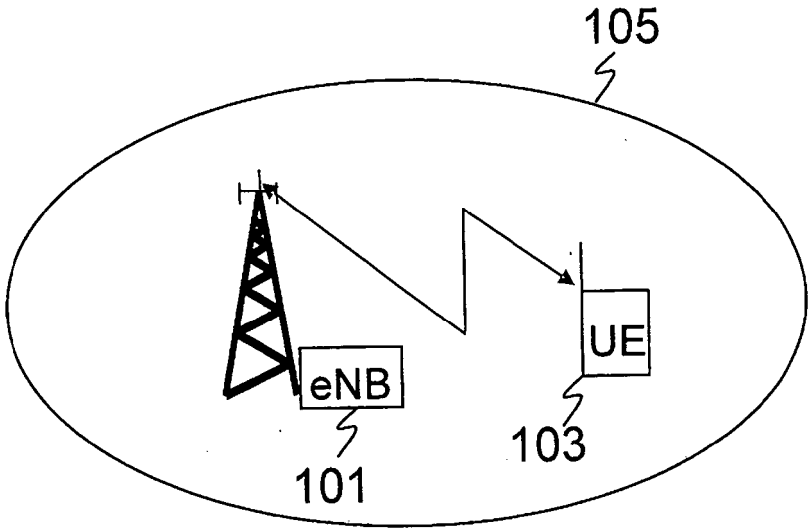

Fig. 1

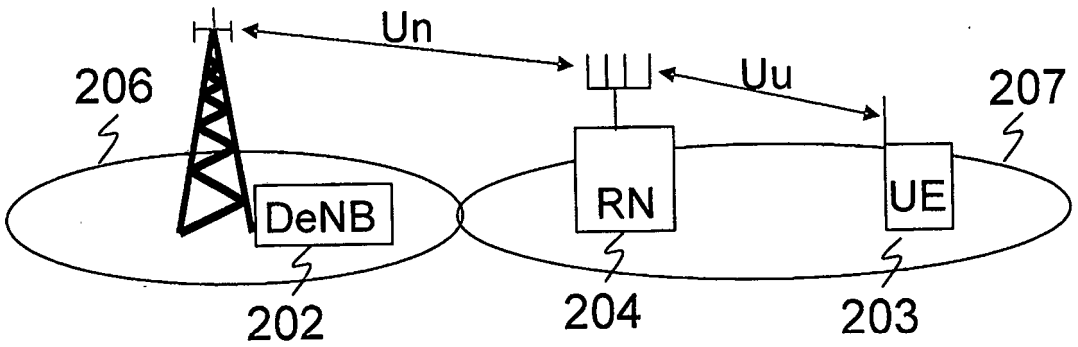

Fig. 2

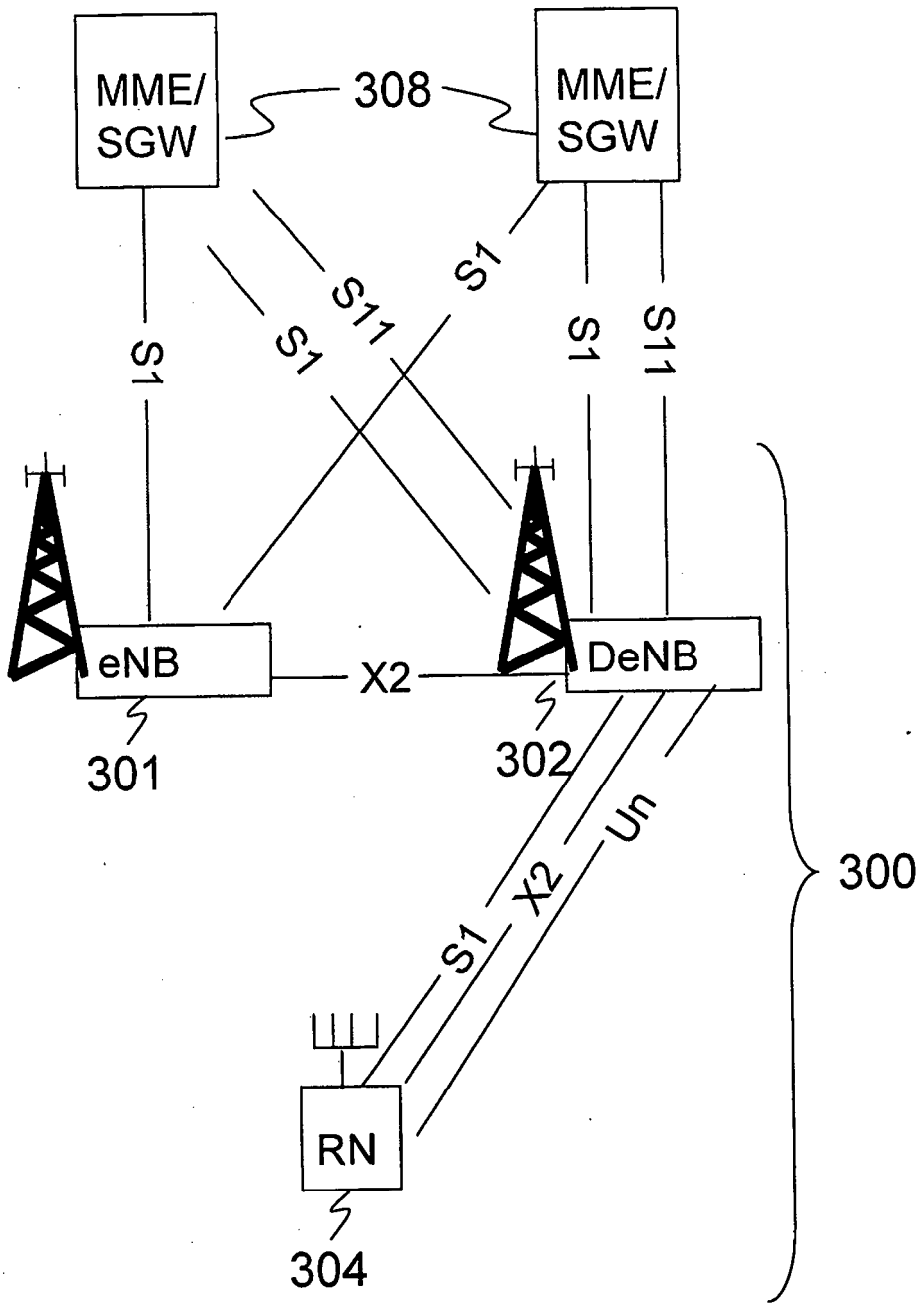
MME/
SGW
308
MME/
SGW
S1
S11
S1
S1
S11
S1
eNB
X2
DeNB
301
302
Un
X2
S1
300
RN
304

Fig. 3

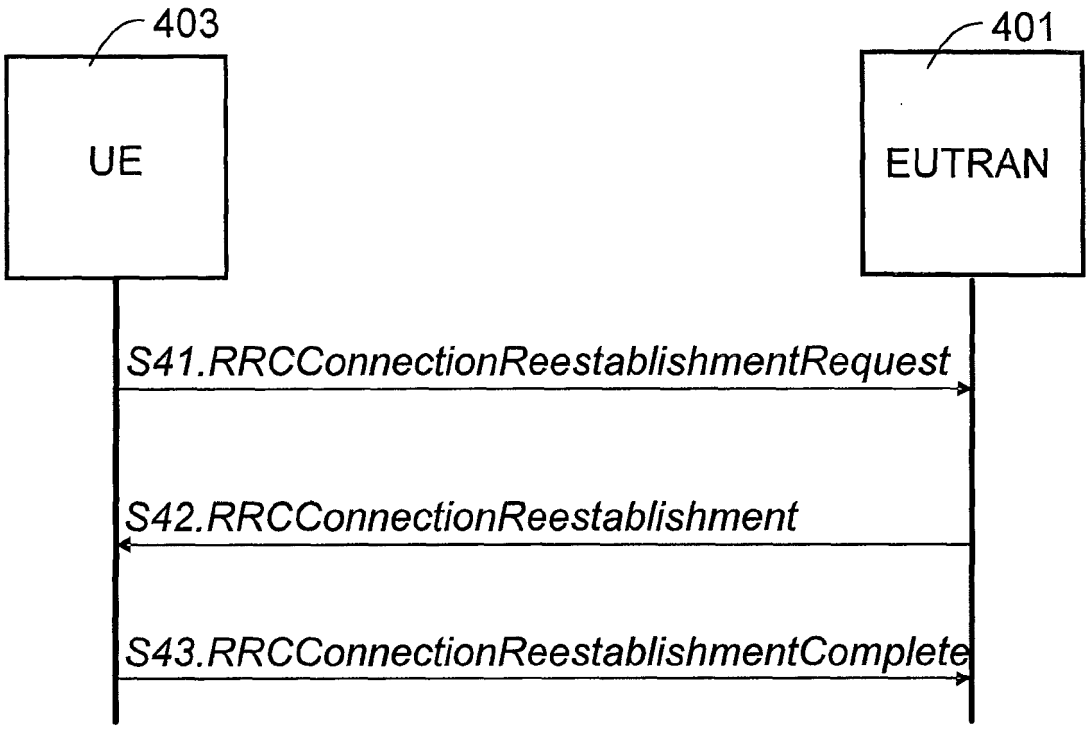
403
401
UE
EUTRAN
S41.RRCConnectionReestablishmentRequest
S42.RRCConnectionReestablishment
S43.RRCConnectionReestablishmentComplete

Fig. 4a

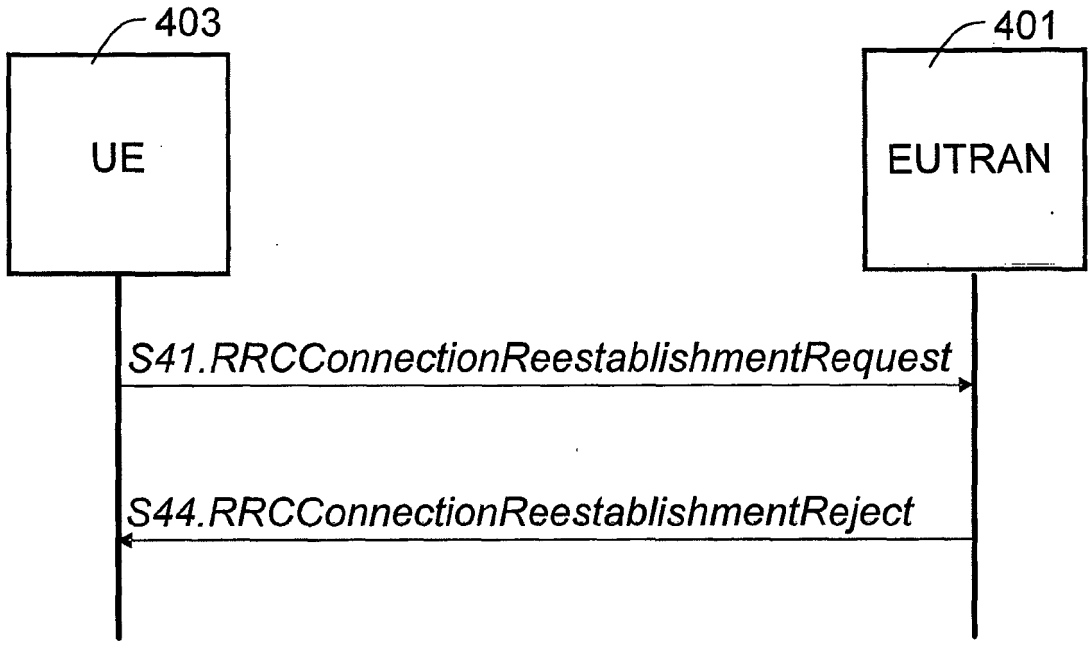
403
401
UE
EUTRAN
S41.RRCConnectionReestablishmentRequest
S44.RRCConnectionReestablishmentReject

Fig. 4b

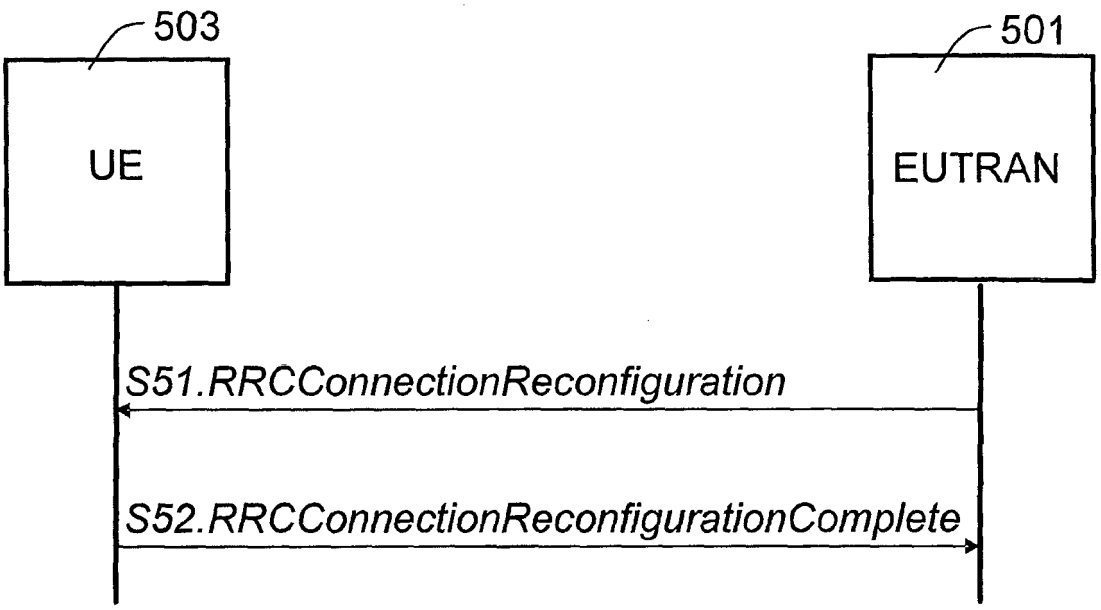

Fig. 5

Transmitir un mensaje de reconfiguración de la conexión tras un restablecimiento de la conexión con éxito, comprendiendo el mensaje un indicador que indica cuáles de los portadores de radio de datos tendrán habilitada la protección de la integridad — 610

Fig. 6

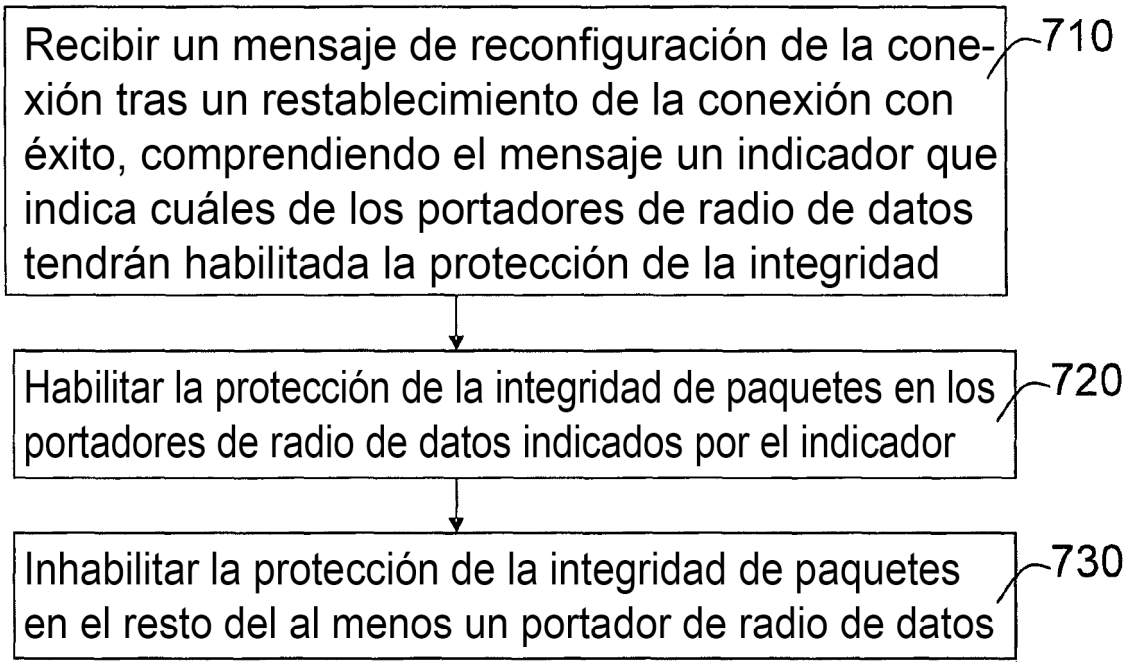
Recibir un mensaje de reconfiguración de la conexión tras un restablecimiento de la conexión con éxito, comprendiendo el mensaje un indicador que indica cuáles de los portadores de radio de datos tendrán habilitada la protección de la integridad
710
Habilitar la protección de la integridad de paquetes en los portadores de radio de datos indicados por el indicador
720
Inhabilitar la protección de la integridad de paquetes en el resto del al menos un portador de radio de datos
730

Fig. 7

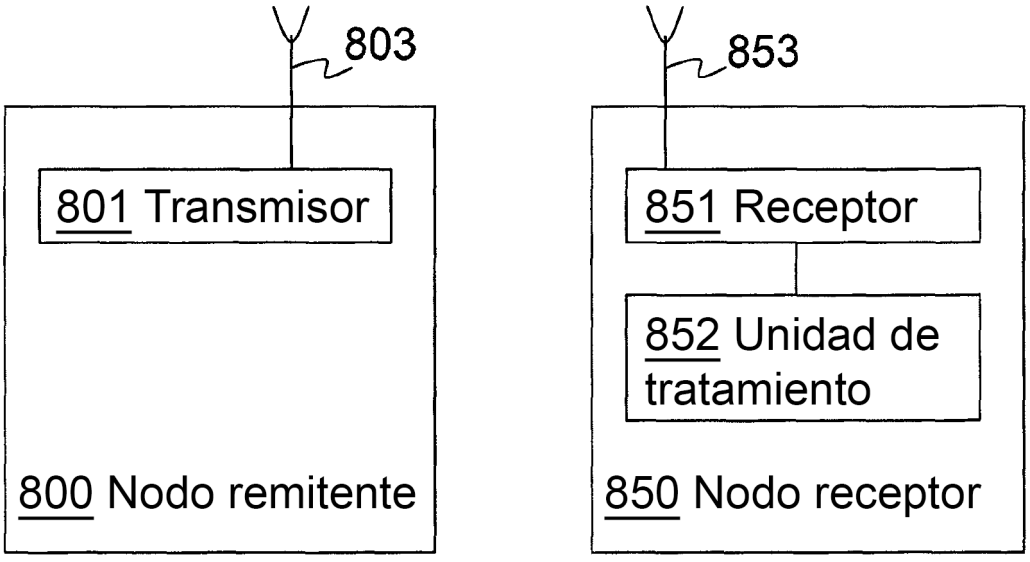
803
801 Transmisor
800 Nodo remitente
853
851 Receptor
852 Unidad de tratamiento
850 Nodo receptor

Fig. 8a

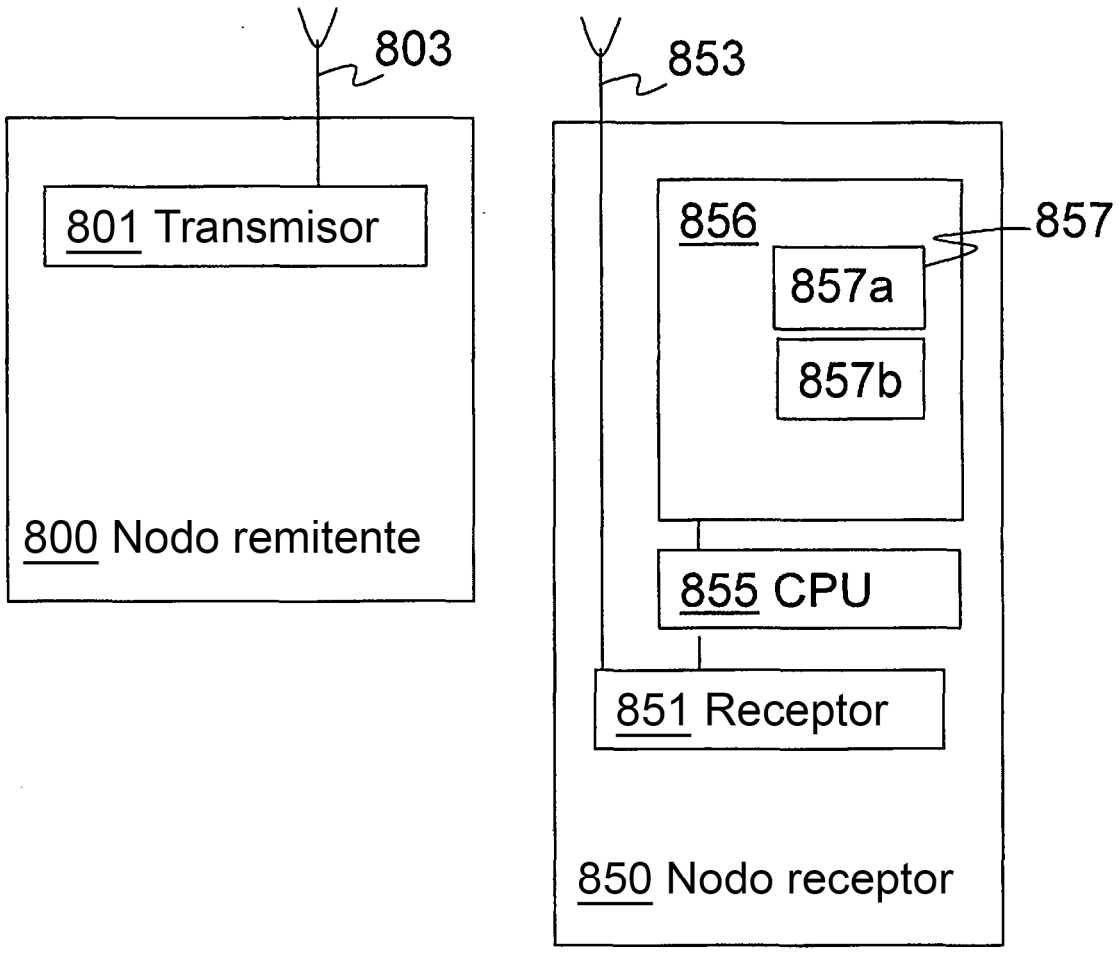
803
801 Transmisor
800 Nodo remitente
853
856
857
857a
857b
855 CPU
851 Receptor
850 Nodo receptor

Fig. 8b