

SISTEMAS Y MÉTODOS PARA PREVENIR EL TRASPASO CAUSADO POR UN MENSAJE NO SEGURO DE UN NODO DE RED

CAMPO DE LA TÉCNICA

[0001] La presente divulgación se refiere en general a sistemas de comunicaciones inalámbricas y, más particularmente, a comunicaciones inalámbricas y operaciones relacionadas para manejar el traspaso relacionado con un mensaje recibido desde un nodo de red.

ANTECEDENTES

[0002] En LTE, la red podría traspasar un equipo de usuario (UE) de una celda a otra transmitiendo un mensaje *RRCCConnectionReconfiguration*, incluido un campo *mobilityControlInfo*. La **Figura 1** ilustra las comunicaciones y operaciones relacionadas realizadas por un UE y una Red de Acceso Terrestre Universal Evolucionada (EUTRAN) para una reconfiguración exitosa de la conexión del RRC. La condición de incluir *mobilityControlInfo* es que es obligatorio en caso de traspaso dentro de E-UTRA o hacia E-UTRA; de lo contrario, está ausente. El campo *mobilityControlInfo* y el elemento de información asociado (IE) contienen la información que el UE necesita para conectarse a la celda objetivo. El campo *mobilityControlInfo* solo puede incluirse en el mensaje *RRCCConnectionReconfiguration*.

[0003] En NR, los traspasos (reconfiguración con sincronización) se desencadenan por la transmisión desde la red al UE de un mensaje *NR RRCReconfiguration* que contiene *RadioBearerConfig* (configurando las capas de PDCP y SDAP) y *CellGroupConfig* (configurando las capas inferiores). *CellGroupConfig* contiene IE *SpCellConfig*, que a su vez contiene *reconfigurationWithSync*, que se utiliza durante el traspaso.

[0004] En la especificación de RRC, se definen las condiciones para que ciertos campos y los IE a incluirse en los mensajes de RRC. Definen, por

ejemplo, en qué condiciones debe incluirse un parámetro opcional; de lo contrario, un procedimiento previsto no tendría sentido.

[0005] Los procedimientos para *RRCReconfiguration* y Reconfiguración con sincronización se describen en NR 3GPP TS 38.331 (v15.3.0). Para un UE en RRC_IDLE, o durante un procedimiento de reserva de, p. ej., RRCResume, la red puede transmitir un mensaje RRCSetup al UE. La **Figura 2A** ilustra las comunicaciones y operaciones relacionadas realizadas por un UE y un nodo de red para una reconfiguración exitosa de la conexión del RRC. La **Figura 2B** ilustra las comunicaciones y operaciones relacionadas realizadas por un UE y un nodo de red para una conexión de RRC exitosa para el establecimiento de conexión de RRC. El mensaje RRCSetup se transmite sin protección en SRB0 y se describe en 3GPP TS 38.331 (v15.3.0).

SUMARIO

[0006] Los ejemplos descritos en la presente divulgación proporcionan técnicas para mejorar la seguridad del equipo de usuario, tal como, evitar que el equipo de usuario se traspase a una estación base malintencionada. Otras ventajas serán claramente aparentes para los experimentados en la técnica. Ciertos ejemplos pueden tener ninguna ventaja, algunas ventajas o todas las ventajas listadas.

[0007] Un sistema de una o más computadoras se puede configurar para realizar operaciones o acciones particulares en virtud de tener *software*, *firmware*, *hardware* o una combinación de ellos instalados en el sistema que en funcionamiento hace(n) que el sistema realice las acciones. Se pueden configurar uno o más programas informáticos para realizar operaciones o acciones particulares en virtud de la inclusión de instrucciones que, cuando se ejecutan mediante un aparato de procesamiento de datos, hacen que el aparato realice las acciones. Un aspecto general incluye un método por un

terminal para manejar mensajes desde nodos de red de un sistema de comunicaciones inalámbricas; el método incluye: recibir un mensaje desde un nodo de red. El método también incluye determinar que el mensaje contiene un campo *reconfigurationwithsync* y que la seguridad no está activada cuando se recibe el mensaje. El método también incluye responder a determinar, evitar la activación de una operación de traspaso. Otros ejemplos de este aspecto incluyen los correspondientes sistemas informáticos, aparatos y programas informáticos grabados en uno o más dispositivos de almacenamiento informáticos, cada uno configurado para realizar las acciones de los métodos.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0008] Los dibujos adjuntos, que se incluyen para proporcionar una comprensión adicional de la divulgación y se incorporan en una parte de esta solicitud, ilustran determinados ejemplos no limitantes de conceptos inventivos.

[0009] La **Figura 1** ilustra las comunicaciones y operaciones relacionadas realizadas por un UE y EUTRAN para una reconfiguración exitosa de la conexión del RRC.

[0010] La **Figura 2A** ilustra las comunicaciones y operaciones relacionadas realizadas por un UE y un nodo de red para una reconfiguración exitosa de la conexión del RRC.

[0011] La **Figura 2B** ilustra las comunicaciones y operaciones relacionadas realizadas por un UE y un nodo de red para una conexión de RRC exitosa para el establecimiento de conexión de RRC.

[0012] Las **figuras 3, 4, 5 y 6** son diagramas de flujo de operaciones que pueden ser realizadas por un terminal, tal como un UE, para manejar mensajes de nodos de red de un sistema de comunicaciones inalámbricas de conformidad con algunos ejemplos de la presente divulgación.

[0013] La **Figura 7** es un diagrama de bloque que ilustra un terminal que está configurado según algunos ejemplos.

[0014] La **Figura 8** es un diagrama de bloques que ilustra un nodo de red de un sistema de comunicación inalámbrica que está configurado de acuerdo con algunos ejemplos.

DESCRIPCIÓN DETALLADA

[0015] En la actualidad, las técnicas de traspaso presentan ciertos desafíos. Por ejemplo, los protocolos descritos anteriormente pueden permitir que una estación base falsa utilice mensajería de RRC para hacer que un UE realice el traspaso a la estación base falsa.

[0016] Los conceptos inventivos se describirán ahora de forma más completa de aquí en adelante tomando como referencia los dibujos adjuntos, en los que se muestran ejemplos de los conceptos inventivos. Sin embargo, los conceptos inventivos pueden representarse de muchas formas diferentes y no deben interpretarse que se limitan a los ejemplos que se exponen en el presente documento. Más bien, estos ejemplos se proporcionan de manera que esta divulgación sea completa y exhaustiva, y transmita plenamente el alcance de los actuales conceptos inventivos a los expertos en la técnica. Cabe señalar también que estos ejemplos no son mutuamente excluyentes. Se puede suponer tácitamente que los componentes de un ejemplo están presentes/se utilizan en otro ejemplo.

[0017] La siguiente descripción presenta varios ejemplos del objeto divulgado. Estos ejemplos se presentan como ejemplos de enseñanza y no deben interpretarse como una limitación del alcance del objeto divulgado. Por ejemplo, ciertos detalles de los ejemplos descritos pueden modificarse, omitirse o ampliarse sin apartarse del alcance del objeto descrito. El término "terminal" se utiliza de manera no limitante y, como se explica a continuación, puede

referirse a cualquier tipo de terminal de comunicación por radio. El término "terminal" en el presente documento puede reemplazarse de manera intercambiable con el término "terminal de radio", "terminal de comunicación por radio", "dispositivo de radio" o "equipo de usuario (UE)".

[0018] Como se explica más arriba, los protocolos descritos anteriormente pueden permitir que una estación base falsa utilice mensajería de RRC para hacer que un UE realice el traspaso a la estación base falsa. Más particularmente, la condición actual para *IE reconfigurationWithSync* establece que es obligatorio que esté presente en caso de cambio de *SpCell*, adición de *PSCell*, actualización de SI para *PSCell* y cambio de clave de seguridad; y de lo contrario, es opcional. Dado que el mensaje *RRCSetup* contiene *CellGroupConfig* (en *masterCellGroupConfig*), que incluye *spCellConfig*, incluir la condición para *reconfigurationWithSync* sería opcional.

[0019] Si un UE recibe un *RRCSetup* que contiene *reconfigurationWithSync*, las acciones del UE son, en el mejor de los casos, ambiguas. Algunos UE pueden intentar traspasar a otra celda y transmitir el mensaje *RRCSetupComplete* a esa celda recién indicada. Según las especificaciones de NR RRC, ese mensaje *RRCSetup* se envía en SRB0; por lo tanto, se envía desprotegido. En consecuencia, una estación base falsa puede intentar hacer eso cuando el UE intenta realizar el establecimiento de conexión inicial, o durante la reanudación de RRC, la estación base falsa podría obligar al UE a realizar el traspaso a la estación base falsa.

[0020] En consecuencia, los métodos y las operaciones se describen en el presente documento para que un UE maneje un mensaje de reconfiguración. Estos métodos y operaciones pueden incluir:

[0021] Paso 1 - Recepción de un mensaje no protegido (p. ej., en SRB0) que incluye un campo que solo se enviará en un mensaje protegido, tal como

un comando de traspaso (o un campo equivalente, p. ej., *mobilityControlInfo* o *reconfigurationWithSync*);

[0022] Paso 2 - Al ocurrir el evento descrito en el Paso 1, realizar un procedimiento de recuperación y proporcionar una indicación de falla a las capas superiores. El procedimiento de recuperación puede ser una transición a *RRC_IDLE* y la indicación puede ser un ‘fallo de conexión de RRC’;

[0023] Paso 3 - Registro de información sobre la detección asociada con el Paso 1 y el Paso 2. La información puede registrarse en la celda donde ocurre la falla e indicar al menos partes del mensaje que se enviaron sin protección; y

[0024] Paso 4 - informar la información registrada que se describe en el Paso 3. Eso se puede informar por solicitud de la red.

[0025] En otro ejemplo, el procedimiento para *reconfigurationWithSync* se amplía para comprobar si se recibió cuando la seguridad no está activada. Si el UE recibe la *reconfigurationWithSync_unprotected*, realiza una acción que va a *RRC_IDLE* y posiblemente informa del fallo al UE cuando se conecta a la red.

[0026] En otro ejemplo, se agregan condiciones a los campos que se enviarán solo en mensaje seguro, tal como *reconfigurationWithSync*. En el caso de *RRCSetup*, se puede definir que el campo no se incluirá en el mensaje de modo que,, al incluirlo, el UE ignore el campo o realice acciones de recuperación, tal como realizar una recuperación de NAS.

[0027] Las realizaciones descritas en el presente documento proporcionan ventajas, que incluyen evitar o prevenir que una estación base falsa provoque el traspaso de un UE que intenta establecer una conexión de RRC a la estación base falsa. La red puede ser informada del ataque (si se informa) y luego puede tomar las acciones apropiadas.

[0028] En términos más generales, estos ejemplos pueden incluir definir acciones de UE particulares que se tomarán en respuesta a recibir en un mensaje no protegido un campo (o equivalente, p. ej., elemento de información) que se enviará protegido según las condiciones de las especificaciones. Por lo tanto, el comportamiento del UE puede ser predecible y, debido a los procedimientos de recuperación definidos, existe un riesgo reducido de ataques, ya que el UE intentará volver a la red real y/o volver a autenticarse en caso de que la falla se origine debido a una estación base falsa.

[0029] Varios ejemplos también pueden definir operaciones para registrar y comunicar información asociada con la falla, cuando ocurre, para que la red real tenga la oportunidad de detectar que podría haber una estación base falsa en una ubicación particular actuando en un momento particular. De este modo, la red real puede iniciar acciones correctivas en respuesta a la notificación.

[0030] En algunos ejemplos, cuando el UE transmite una *RRCSetupRequest*, *RRCResumeRequest* o *RRCResumeRequest1*, este mensaje se enviará no protegido en SRB0 (es decir, no cifrado o con protección de integridad, aunque los mensajes de solicitud de reanudación contengan un token de seguridad utilizado para la autenticación). La red respondería entonces con el mensaje *RRCSetup*, que contiene *RadioBearerConfig* y *CellGroupConfig*, que se utiliza para configurar SRB1. Sin embargo, dado que la seguridad aún no se ha activado, el mensaje *RRCSetup* también se envía sin protección. Después de la recepción del mensaje *RRCSetup*, la red transmite *SecurityModeCommand* (SMC), que contiene la configuración requerida para activar la seguridad (es decir, una indicación de qué algoritmos de seguridad usar). El SMC también se envía sin cifrar, pero tiene protección de integridad. Sin embargo, dado que es opcional incluir la

condición para el IE *reconfigurationWithSync* en el IE *CellGroupConfig*, el UE realizaría los procedimientos especificados para la Reconfiguración con sincronización. Esto significa que el UE se puede sincronizar con la celda indicada en *reconfigurationWithSync* y luego completaría el procedimiento de establecimiento de conexión hacia esa celda. Si el nodo objetivo luego transmitiera el SMC, incluidos los algoritmos nulos, el UE activaría la seguridad sin proteger realmente los mensajes (ya que los algoritmos nulos no agregan ninguna protección).

[0031] La **Figura 3** es un diagrama de flujo de operaciones que pueden ser realizadas por un terminal, tal como un UE, para manejar mensajes de nodos de red de un sistema de comunicaciones inalámbricas de conformidad con algunos ejemplos de la presente divulgación.

[0032] Con referencia a la Figura 3, las operaciones reciben 300 un mensaje de un nodo de red y determinan 302 si el mensaje tiene protección de seguridad y contiene un campo que debería enviarse en un mensaje con protección de seguridad. En respuesta a cuando la determinación es que el mensaje tiene protección de seguridad, las operaciones desencadenan 304 una operación de traspaso a una celda objetivo utilizando el campo. Por el contrario, en respuesta a cuando la determinación es que el mensaje no tiene seguridad protegida y el campo debe enviarse en un mensaje con seguridad protegida, las operaciones evitan 306 la activación de la operación de traspaso.

[0033] En un ejemplo adicional, el paso de determinar 302 si el mensaje tiene seguridad protegida y contiene un campo que debería enviarse en un mensaje con seguridad protegida, incluye determinar si el mensaje contiene un comando de traspaso que tiene seguridad protegida. El paso de responder cuando la determinación es que el mensaje tiene seguridad protegida, activando 304 una operación de traspaso a una celda objetivo usando el

campo, incluye activar la operación de traspaso a la celda objetivo usando información en el comando de traspaso. El paso de respuesta a cuando la determinación es que el mensaje no tiene protección de seguridad y el campo debe enviarse en un mensaje con protección de seguridad, evitando 306 la activación de la operación de traspaso, incluye evitar la activación de la operación de traspaso usando la información en el comando de traspaso.

[0034] El comando de traspaso puede recibirse 300 en un campo de *mobilityControlInfo* del mensaje. El paso de determinar 302 si el mensaje tiene protección de seguridad y contiene un campo que debería enviarse en un mensaje con seguridad protegida, puede incluir determinar si el campo *mobilityControlInfo* del mensaje tiene protección de seguridad.

[0035] El comando de traspaso puede recibirse 300 en un campo de *reconfigurationWithSync* del mensaje. El paso de determinar 302 si el mensaje tiene protección de seguridad y contiene un campo que debería enviarse en un mensaje con seguridad protegida, puede incluir determinar si el campo *reconfigurationWithSync* del mensaje tiene protección de seguridad.

[0036] Algunos ejemplos adicionales están dirigidos a operaciones de traspaso que pueden realizarse en E-UTRA o en E-UTRA, u otro sistema de comunicaciones inalámbricas. El paso de determinar 302 si el mensaje tiene protección de seguridad y contiene un campo que debería enviarse en un mensaje con seguridad protegida, puede incluir determinar si el mensaje es un mensaje *RRConnectionReconfiguration* que tiene protección de seguridad y contiene un campo *mobilityControlInfo*. El paso de responder cuando la determinación es que el mensaje tiene protección de seguridad, activando 304 una operación de traspaso a una celda objetivo usando el campo, puede incluir activar la operación de traspaso a la celda objetivo usando información en el campo *mobilityControlInfo*. El paso de respuesta a que, cuando se determina

que el mensaje no tiene protección de seguridad y que el campo debe enviarse en un mensaje con protección de seguridad, se impide la activación de operación de traspaso, puede incluir evitar la activación de la operación de traspaso con la información en el campo *mobilityControlInfo*.

[0037] Algunos ejemplos adicionales están dirigidos a operaciones de traspaso que pueden realizarse en un sistema de comunicaciones inalámbricas de NR. El paso de determinar 302 si el mensaje tiene protección de seguridad y contiene un campo que debería enviarse en un mensaje con seguridad protegida, puede incluir determinar si el mensaje es un mensaje *RRCReconfiguration* que tiene protección de seguridad y contiene *RadioBearerConfig* y *CellGroupConfig*. El paso de responder cuando la determinación es que el mensaje tiene protección de seguridad, activando 304 una operación de traspaso a una celda objetivo usando el campo, puede incluir activar la operación de traspaso a la celda objetivo usando *RadioBearerConfig* y *CellGroupConfig*. El paso de respuesta a cuando la determinación es que el mensaje no tiene protección de seguridad y el campo debe enviarse en un mensaje con protección de seguridad, evitando la activación de la operación de traspaso usando *RadioBearerConfig* y *CellGroupConfig*.

[0038] El paso de determinar si el mensaje es un mensaje *RRCReconfiguration* que tiene seguridad protegida y contiene un *RadioBearerConfig* y *CellGroupConfig*, puede incluir determinar si el mensaje comprende un campo *reconfigurationWithSync* que tiene seguridad protegida.

[0039] En algunos ejemplos adicionales, cuando la determinación es que el mensaje tiene seguridad protegida, el paso de activar 304 la operación de traspaso a la celda objetivo utiliza un campo *reconfigurationWithSync* contenido en el mensaje. Responder a cuando la determinación es que el mensaje no tiene protección de seguridad y el campo debe enviarse en un mensaje con

protección de seguridad, el paso de evitar 306 la activación de la operación de traspaso evita el uso del campo *reconfigurationWithSync* contenido en el mensaje para una operación de traspaso.

[0040] El paso de activar 304 la operación de traspaso a la celda objetivo usando el campo *reconfigurationWithSync* contenido en el mensaje, puede incluir realizar una operación de sincronización al enlace descendente de una celda objetivo indicada por el campo *reconfigurationWithSync*, y realizar un procedimiento de establecimiento de conexión hacia la celda objetivo.

[0041] El paso de determinar 302 si el mensaje tiene seguridad protegida incluye determinar si el mensaje tiene protección de cifrado y/o si el mensaje tiene protección de integridad.

[0042] En el presente ejemplo, el UE va a *RRC_IDLE* cuando recibe un mensaje *reconfigurationWithSync* desprotegido. Los procedimientos de reconfiguración con sincronización pueden extenderse para describir el comportamiento del UE en caso de que el UE reciba *reconfigurationWithSync* (o un campo equivalente que indique un traspaso y/o adición de SCG) en un mensaje desprotegido. Por ejemplo, cuando el UE entra en el procedimiento de Reconfiguración con sincronización, comprueba si se ha activado la seguridad. Si la seguridad no está activada, el UE realiza las acciones al ir a *RRC_IDLE* y notifica a la capa superior como se muestra a continuación. Las operaciones correspondientes según este ejemplo pueden incluir lo siguiente, que puede ser una modificación de 3GPP TS 38.331 (v15.3.0):

5.3.5.5.2 Reconfiguración con sincronización

El UE realizará las siguientes acciones para ejecutar una reconfiguración con sincronización.

1> si la seguridad no está activada, realizar las acciones al ir a RRC IDLE como se especifica en 5.3.11 con la causa de liberación 'otro' con la cual finaliza el procedimiento;

1> detener el temporizador T310 para la SpCell correspondiente, si está en ejecución;

1> iniciar el temporizador T304 para la SpCell correspondiente con el valor del temporizador establecido en *t304*, como se incluye en *reconfigurationWithSync*;

2> si se incluye *frequencyInfoDL*:

2> considere que el SpCell objetivo es uno en la frecuencia de SSB indicada por *frequencyInfoDL* con una identidad de celda física indicada por *physCellId*;

1> si no:

2> considerar que la SpCell objetivo es una en la frecuencia de SSB de la SpCell fuente con una identidad de celda física indicada por *physCellId*;

1> iniciar la sincronización con el DL del SpCell objetivo;

1> aplicar la configuración BCCH especificada definida en 9.1.1.1;

1> adquirir el *MIB*, que está programado como se especifica en 3GPP TS 38.213 [13];

1> realizar las acciones especificadas en la sección 5.2.2.4.1;

NOTA: El UE debe realizar la reconfiguración con sincronización tan pronto como sea posible después de la recepción del mensaje de RRC que desencadena la reconfiguración con sincronización, que podría ser antes de confirmar la recepción exitosa (HARQ y ARQ) de este mensaje.

1> restablecer la entidad MAC de este grupo de celdas;

1> considerar que las SCell(s) de este grupo de celdas, si están configuradas, están desactivadas;

1> aplicar el valor de *newUE-Identity* como el C-RNTI para este grupo de celdas;

Nota del editor: Verifique que esto no configure algunos parámetros comunes que luego se descarten debido a, p. ej., liberación de SCell o debido a liberación de LCH.

1> configurar las capas inferiores de conformidad con el *spCellConfigCommon* recibido;

1> configurar las capas inferiores de conformidad con los campos adicionales, no tratados anteriormente, si se incluyen en la *reconfigurationWithSync* recibida.

[0043] La **Figura 4** es un diagrama de flujo de las operaciones correspondientes que pueden ser realizadas por un terminal, tal como un UE, para manejar mensajes de nodos de red de un sistema de comunicaciones inalámbricas de conformidad con el ejemplo anterior de la presente divulgación.

[0044] Con referencia a la Figura 4, las operaciones incluyen responder cuando la determinación es que el mensaje no tiene seguridad protegida y el campo debe enviarse en un mensaje con seguridad protegida, realizando 400 un procedimiento de recuperación y/o indicando una falla a las capas superiores.

[0045] El procedimiento de recuperación puede incluir la transición 402 del terminal a *RRC_IDLE*. El fallo indicado a las capas superiores puede incluir una indicación de fallo de conexión de RRC.

[0046] El paso de responder cuando la determinación es que el mensaje no tiene protección de seguridad y el campo debe enviarse en un mensaje con protección de seguridad, realizando 400 un procedimiento de recuperación y/o indicando una falla en las capas superiores, puede incluir responder cuando se

determina que un campo de *reconfigurationWithSync* del mensaje se recibe sin protección de seguridad, haciendo la transición 402 del terminal a *RRC_IDLE*.

[0047] Las operaciones pueden incluir responder cuando la determinación es que el mensaje no tiene protección de seguridad y el campo debe enviarse en un mensaje con protección de seguridad, y registrar 406 información según, al menos, parte del contenido del mensaje que se recibió sin protección de seguridad. Las operaciones pueden incluir además informar 408 la información registrada a un nodo de red.

[0048] En otro ejemplo, el UE ignora el *IE reconfigurationWithSync* si se recibe desprotegido. Por ejemplo, el UE puede considerar el *IE reconfigurationWithSync* si la seguridad ha sido activada. Si la seguridad no está activada, el UE ignora ese IE. Las operaciones correspondientes según este ejemplo pueden incluir lo siguiente, que puede ser una modificación de 3GPP TS 38.331 (v15.3.0):

5.3.5.5 Configuración del grupo de celdas

5.3.5.5.1 General

La red configura el UE con el Grupo de Celdas Principal (MCG) y cero o un Grupo de Celdas Secundario (SCG). Para EN-DC, el MCG se configura como se especifica en TS 36.331 [10]. La red proporciona los parámetros de configuración para un grupo de celdas en el IE *CellGroupConfig*.

El UE realiza las siguientes acciones basándose en un IE *CellGroupConfig* recibido:

1> si *CellGroupConfig* contiene *spCellConfig* con *reconfigurationWithSync* y se ha activado la seguridad:

2> realizar la reconfiguración con sincronización según 5.3.5.5.2;

2> reanudar todos los portadores de radio suspendidos y reanudar la transmisión de SCG para todos los portadores de radio, si están suspendidos;

- 1> si *CellGroupConfig* contiene *rlc-BearerToReleaseList*:
- 2> realizar la liberación del portador de RLC como se especifica en 5.3.5.5.3;
- 1> si *CellGroupConfig* contiene *rlc-BearerToAddModList*:
- 2> realizar la adición/modificación del portador de RLC como se especifica en 5.3.5.5.4;
- 1> si *CellGroupConfig* contiene *mac-CellGroupConfig*:
- 2> configurar la entidad MAC de este grupo de celdas como se especifica en 5.3.5.5.5;
- 1> si *CellGroupConfig* contiene *sCellToReleaseList*:
- 2> realizar la liberación de SCell como se especifica en 5.3.5.5.8;
- 1> si *CellGroupConfig* contiene *spCellConfig*:
- 2> configurar *SpCell* como se especifica en 5.3.5.5.7;
- 1> si *CellGroupConfig* contiene *sCellToAddModList*:
- 2> realizar la adición/modificación de SCell como se especifica en 5.3.5.5.9.

[0049] La **Figura 5** es un diagrama de flujo de las operaciones correspondientes que pueden ser realizadas por un terminal, tal como un UE, para manejar mensajes de nodos de red de un sistema de comunicaciones inalámbricas de conformidad con el ejemplo anterior de la presente divulgación.

[0050] Con referencia a la Figura 5, las operaciones incluyen responder cuando se determina 302 que un campo *reconfigurationWithSync* del mensaje se recibe sin protección de seguridad, evitando 500 el uso del contenido del campo *reconfigurationWithSync* para cualquier operación de reconfiguración de celdas por parte del terminal.

[0051] En otro ejemplo, el UE ignora el mensaje *RRCSetup* completo si incluye *reconfigurationWithSync*. Los procedimientos para la recepción del

mensaje *RRCSetup* pueden modificarse de modo que si el mensaje incluye *reconfigurationWithSync*, el UE debería ignorar el mensaje completo. En un subejemplo, el UE también almacena información sobre el mensaje incorrecto y lo informa a la red en un informe de falla cuando luego vuelve a RRC_CONNECTED. La información que se registra e informa puede comprender campos, partes del mensaje o el mensaje completo. Cuando se informa a la red real, la red real puede inspeccionar lo que ha sucedido. Eso puede incluir información adicional relacionada con la ubicación (p. ej., posicionamiento, identificador(es) de celda, etc.), tiempo, mediciones de radio, etc. También se puede incluir la medición de celda vecina. Las operaciones correspondientes según este ejemplo pueden incluir lo siguiente, que puede ser una modificación de 3GPP TS 38.331 (v15.3.0):

5.3.3.4 Recepción del *RRCSetup* por el UE

El UE realizará las siguientes acciones al recibir el *RRCSetup*:

1> si el masterCellGroup incluido en el mensaje *RRCSetup* contiene *reconfigurationWithSync* en *SpCellConfig*:

2> configurar *failureType* en *setupSecurityFailure*

2> finaliza el procedimiento;

1> si el *RRCSetup* se recibe en respuesta a una *RRCReestablishmentRequest*; o

1> si el *RRCSetup* se recibe en respuesta a una *RRCResumeRequest* o *RRCResumeRequest1*:

2> descartar el contexto de UE AS almacenado, *fullI-RNTI* y *shortI-RNTI*;

2> indicar a las capas superiores la reserva de la conexión de RRC;

1> realizar el procedimiento de configuración del grupo de celdas de conformidad con el *masterCellGroup* recibido y como se especifica en 5.3.5.5;

1> realizar el procedimiento de configuración del portador de radio de conformidad con el *radioBearerConfig* recibido y como se especifica en 5.3.5.6;

1> si está almacenada, descartar la información de prioridad de reelección de celda provista por las *cellReselectionPriorities* o heredada de otro RAT;

1> detener el temporizador T300, T301 o T319 si está en ejecución;

Nota del editor: FFS Si es necesario definir las acciones de UE relacionadas con los temporizadores de control de acceso (equivalentes a T302, T303, T305, T306, T308 en LTE). Por ejemplo, informar a las capas superiores si un temporizador determinado no está en ejecución.

1> detener el temporizador T320, si está en ejecución;

1> si el *RRCSetup* se recibe en respuesta a una *RRCResumeRequest* o *RRCSetupRequest*:

2> entrar en RRC_CONNECTED;

2> detener el procedimiento de reelección de celda;

1> considerar que la celda actual sea PCell;

1> configurar el contenido del mensaje *RRCSetupComplete* de la siguiente manera:

2> si las capas superiores proporcionan un *5G-S-TMSI*:

3> si el *RRCSetup* se recibe en respuesta a una *RRCSetupRequest*:

4> establecer el *ng-5G-S-TMSI-Value* en *ng-5G-S-TMSI-Part2*;

3> si no:

4> establecer el *ng-5G-S-TMSI-Value* en *ng-5G-S-TMSI*;

2> establecer la *selectedPLMN-Identity* en la PLMN seleccionada por las capas superiores (TS 24.501 [23]) de la(s) PLMN incluida(s) en la *plmn-IdentityList* en *SIB1*;

2> si *masterCellGroup* contiene *reportUplinkTxDirectCurrent*:

- 3> incluir el *uplinkTxDirectCurrentList*;
- 2> si las capas superiores proporcionan el 'AMF registrado':
- 3> incluir y configurar el *registeredAMF* de la siguiente manera:
- 4> si la identidad de PLMN de 'AMF registrado' es diferente de la PLMN seleccionada por las capas superiores:

- 5> incluir *plmnIdentity* en el *registeredAMF* y establecerlo en el valor de la identidad PLMN en el 'AMF registrado' recibido de las capas superiores;

- 4> establecer el *amf-Identifier* al valor recibido de las capas superiores;

- 3> incluir y establecer el *guami-Type* en el valor proporcionado por las capas superiores;

Nota del editor: FFS Confirmar si el *guami-Type* está incluido y configurado en la condición mencionada anteriormente.

- 2> si las capas superiores proporcionan uno o más S-NSSAI (ver TS 23.003 [20]):

- 3> incluir la *s-nssai-List* y establecer el contenido en los valores proporcionados por las capas superiores;

- 2> establecer el *dedicatedNAS-Message* para incluir la información recibida de las capas superiores;

- 1> enviar el mensaje *RRCSetupComplete* a las capas inferiores para su transmisión, tras lo cual el procedimiento finaliza

[0052] La **Figura 6** es un diagrama de flujo de las operaciones correspondientes que pueden ser realizadas por un terminal, tal como un UE, para manejar mensajes de nodos de red de un sistema de comunicaciones inalámbricas de conformidad con el ejemplo anterior de la presente divulgación.

[0053] Con referencia a la Figura 6, las operaciones incluyen responder cuando se determina que un campo *reconfigurationWithSync* de un mensaje

RRCSetup se recibe sin protección de seguridad, evitando 600 el uso de cualquier contenido del mensaje RRCSetup para cualquier operación de reconfiguración de celdas por parte del terminal.

[0054] Las operaciones pueden incluir además responder cuando se determina 302 que un campo de *reconfigurationWithSync* de un mensaje RRCSetup se recibe sin protección de seguridad, evitando 600 el uso de cualquier contenido del mensaje RRCSetup para cualquier operación de reconfiguración de celda por parte del terminal y la información de registro según, al menos, parte del contenido del mensaje RRCSetup, y comunicando 602 la información registrada en un informe de falla a un nodo de red.

[0055] En otro ejemplo de la presente divulgación, la condición de *reconfigurationWithSync* se modifica para no permitir que se incluya en RRCSetup, o cualquier mensaje desprotegido, o en un mensaje transmitido cuando la seguridad no está activada. Entonces dependería de la implementación del UE cómo tratar la *reconfigurationWithSync*, p. ej.:

- Usar las configuraciones
- Ignorar el IE (*reconfigurationWithSync*),
- Ignorar el mensaje completo (RRCSetup)

[0056] A continuación, se muestran diferentes subejemplos del cambio propuesto.

Subrealización

Presencia condicional	Explicación
<i>ReconfWithSync</i>	El campo es obligatorio en caso de cambio de SpCell, adición de PSCell, actualización de SI para PSCell y cambio de clave de seguridad; de lo contrario, es opcional. need M. <u>Este campo no está presente en el mensaje RRCSetup.</u>

Subrealización

Presencia condicional	Explicación
<i>ReconfWithSync</i>	El campo está presente obligatoriamente en caso de cambio de SpCell, adición de PSCell, actualización de SI para PSCell y cambio de clave de seguridad; de lo contrario, está presente opcionalmente, necesita M. <u>Este campo solo se puede incluir si la seguridad está activada.</u>

Subrealización

Presencia condicional	Explicación
<i>ReconfWithSync</i>	El campo está presente obligatoriamente en caso de cambio de SpCell, adición de PSCell, actualización de SI para PSCell y cambio de clave de seguridad; de lo contrario, está presente opcionalmente, necesita M. <u>Este campo no puede incluirse en un mensaje desprotegido.</u>

[0057] Las operaciones correspondientes que puede realizar un terminal, tal como un UE, pueden incluir uno cualquiera o más de los siguientes ejemplos.

[0058] En un ejemplo, el paso de determinar 302 si el mensaje tiene protección de seguridad y contiene un campo que debe enviarse en un mensaje con protección de seguridad, incluye cuando se recibe un mensaje RRCSetup, determinar que el mensaje RRCSetup no tiene protección de seguridad y contiene un campo que debe enviarse en un mensaje con protección de seguridad siempre que el mensaje RRCSetup contenga un campo *reconfigurationWithSync*.

[0059] En otro ejemplo, el paso de determinar 302 si el mensaje tiene protección de seguridad y contiene un campo que debería enviarse en un mensaje con seguridad protegida, incluye cuando se recibe un mensaje RRCSetup que tiene activada la protección de seguridad, determinando que un campo *reconfigurationWithSync* del mensaje RRCSetup tiene protección de seguridad.

[0060] En otro ejemplo, el paso de determinar 302 si el mensaje tiene protección de seguridad y contiene un campo que debe enviarse en un mensaje con protección de seguridad, incluye cuando se recibe un mensaje

RRCSetup que no tiene protección de seguridad activada, determinando que el mensaje RRCSetup contiene un campo que debe enviarse en un mensaje con protección de seguridad siempre que el mensaje RRCSetup sin protección de seguridad activa contenga un campo *reconfigurationWithSync*.

[0061] Por lo tanto, varios ejemplos de la presente divulgación pueden funcionar para evitar o prevenir que el funcionamiento de estaciones base falsas incluya *reconfigurationWithSync* en el mensaje de RRCSetup desprotegido para provocar el traspaso del UE al mismo. Estos ejemplos pueden modificar las operaciones del UE que desencadenan el retorno a RRC_IDLE si el UE recibe este IE, o pueden modificar las operaciones para hacer que el UE ignore todo el mensaje.

[0062] La **Figura 7** es un diagrama de bloque que ilustra un terminal 700 que está configurado según algunos ejemplos. El terminal 700 puede incluir, a mero título enunciativo, un terminal inalámbrico, un dispositivo de comunicación inalámbrico, un terminal de comunicación inalámbrico, un nodo terminal, un UE, un dispositivo de comunicación, etc. El terminal 700 incluye un transceptor de RF 730 que comprende uno o más amplificadores de potencia que transmiten y reciben a través de una o más antenas 740 para proporcionar comunicaciones de radio de enlace ascendente y enlace descendente con un nodo de red de radio (p. ej., una estación base, eNB, gNB, etc.) de un sistema de comunicación inalámbrica. El terminal 700 incluye además un circuito procesador 710 (también denominado procesador) acoplado al transceptor de RF 730 y un circuito de memoria 720 (también denominado memoria). La memoria 720 almacena un programa legible por computadora que cuando es ejecutado por el procesador 710 hace que el procesador 710 realice operaciones según los ejemplos que se describen en el presente documento.

[0063] La **Figura 8** es un diagrama de bloques que ilustra un nodo de red 800 (p. ej., una estación base, eNB, gNB, etc.) de un sistema de comunicación inalámbrica que está configurado de acuerdo con algunos ejemplos. El nodo de red 800 incluye un circuito procesador 810 (también denominado procesador), un circuito de memoria 820 (también denominado memoria) y una interfaz de red 850 (p. ej., interfaz de red cableada y/o interfaz de red inalámbrica) configurada para comunicarse con otros nodos de la red. El nodo de red 800 puede configurarse como un nodo de red de radio que contiene un transceptor de RF 830 con uno o más amplificadores de potencia que transmiten y reciben a través de una o más antenas 840 que pueden ser parte del nodo de red 800 o pueden estar conectados comunicativamente, pero geográficamente separados del nodo de red 800. La memoria 820 almacena un programa legible por computadora que cuando es ejecutado por el procesador 810 hace que el procesador 810 realice operaciones según los ejemplos que se describen en el presente documento.