(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 752 727**

(51) Int. CI.:

H04W 12/04 (2009.01)
H04W 12/10 (2009.01)
H04L 29/06 (2006.01)
H04W 24/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **14.06.2010 PCT/EP2010/058294**

(87) Fecha y número de publicación internacional: **04.08.2011 WO11091865**

(96) Fecha de presentación y número de la solicitud europea: **14.06.2010 E 10727378 (1)**

(97) Fecha y número de publicación de la concesión europea: **07.08.2019 EP 2529565**

(54) Título: **Método y disposición para gestionar la reconfiguración de seguridad en un sistema de comunicación celular**

(30) Prioridad:

28.01.2010 US 298934 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.04.2020

(73) Titular/es:

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

(72) Inventor/es:

MCGANN, TOM

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

DESCRIPCIÓN

Método y disposición para gestionar la reconfiguración de seguridad en un sistema de comunicación celular

Campo técnico

La presente invención se refiere a sistemas de telecomunicación en general, y, específicamente, a la gestión de las reconfiguraciones de seguridad en tales sistemas.

Antecedentes

Para todos los sistemas de telecomunicaciones hay una variedad de procedimientos de reconfiguración presentes. Estos procedimientos se pueden dividir en dos grupos principales, en base a la naturaleza de los parámetros a reconfigurar, a saber, reconfiguraciones físicas y lógicas. Las reconfiguraciones físicas tienen que ver con las reconfiguraciones de naturaleza física, tales como la reconfiguración del portador de radio, la reconfiguración del canal de transporte, o la reconfiguración del canal físico. Las reconfiguraciones lógicas tienen que ver con reconfiguraciones no físicas, tales como, por ejemplo, la reconfiguración de parámetros de seguridad. Para un escenario típico de las especificaciones del 3GPP, estos dos tipos de reconfiguraciones se tratan de forma algo diferente y, en consecuencia, sufren problemas diferentes y por separado.

La presente descripción se centrará en reconfiguraciones lógicas, en particular en las reconfiguraciones de seguridad en relación con las especificaciones TS 25.331 V8.7.0 sección 8.1.12.4b [1] del 3GPP. Una de las áreas de mejora concierne al caso de llamadas interrumpidas debidas a un desajuste de las configuraciones de seguridad entre la red y un terminal de usuario, tal como un teléfono móvil, como consecuencia del procedimiento de reselección de célula durante la reconfiguración de seguridad.

Para los usuarios de 3G conectados en el llamado estado o modo de CELL_FACH que intentan configurar una llamada de voz con múltiples RAB, se produce la interrupción de la llamada si un procedimiento de reselección de célula de actualización de célula coincide con el procedimiento del modo de seguridad. Para mayor aclaración, el estado o modo de CELL_FACH es uno de los modos o estados, de funcionamiento, conectados de control de recursos de radio. Como tal, para un equipo de usuario en el estado de CELL_FACH se aplica lo siguiente.

- No se asigna al UE ningún canal físico dedicado.
- El UE monitoriza continuamente un FACH en el enlace descendente.
- Al UE se le asigna un canal de transporte común o compartido predeterminado en el enlace ascendente (por ejemplo, RACH) que pueda usar en cualquier momento de acuerdo con el procedimiento de acceso para ese canal de transporte.
- UTRAN conoce la posición del UE en el nivel de célula de acuerdo con la célula en la que el UE hizo la última actualización de la célula.

Cabe señalar que el procedimiento del modo de seguridad incluye negociación, de la que el esquema de protección del cifrado y de la integridad, las partes implicadas, por ejemplo, el equipo de usuario y el nodo de red van a usar para la comunicación. Un desajuste o una desalineación de la configuración de seguridad entre dos partes, como, por ejemplo, entre un terminal de usuario y una red, conducirá, en última instancia, a una llamada interrumpida, ya que las partes se ven incapaces de comunicarse entre sí.

Durante la movilidad del UE, dos de tales escenarios son posibles:

1) Reconfiguración de seguridad durante los procedimientos de actualización de célula, es decir, que la orden de modo de seguridad se recibe en un equipo de usuario (UE) desde una red justo después de haberse enviado un mensaje de actualización de célula desde el UE a la red.

2) Procedimiento de actualización de célula durante la reconfiguración de seguridad, es decir, que se envía un mensaje de actualización de célula desde el UE mientras el procedimiento del modo de seguridad aún está en curso.

La técnica anterior, representada por las especificaciones del 3GPP [1] [2] [3], describe cómo un equipo de usuario UE o móvil y una red deben manipular estos dos casos; sin embargo, hay margen de mejora para reducir adicionalmente el riesgo de que se interrumpan las llamadas como resultado de las limitaciones de la especificación del 3GPP.

En general, todos los problemas anteriormente mencionados están relacionados con la desalineación o el desajuste en los ajustes de seguridad (cifrado/integridad) cuando se aborta un procedimiento del modo de seguridad en curso, debido principalmente a la reselección de célula de actualización de célula. Si tanto el UE como el controlador de red

de radio (RNC) abortan la reconfiguración de seguridad, o si ninguno de los dos aborta, una solución de red podría manipular fácilmente este caso. Sin embargo, debido a las diferentes condiciones de la carrera que se producen entre la actualización de la célula y los procedimientos del modo de seguridad, el UE puede abortar la reconfiguración, pero no el RNC, y viceversa. El resultado es una desalineación de protección de integridad (y/o de cifrado) que da como resultado la interrupción de la llamada.

Con referencia a la figura 1, se describirá procedimientos conocidos del modo de seguridad desde el punto de vista del UE. Dentro de la extensión de tiempo designada "A", las especificaciones [1] del 3GPP aclaran que el UE abortará el procedimiento del modo de seguridad en curso si es necesario enviar una actualización de célula. Esta actualización de célula puede ser activada por cualquiera de los siguientes escenarios:

a) reselección para una nueva célula

b) reingreso al área de servicio

c) actualización periódica de célula

d) informar a la red de un fallo del UE ("fallo de canal físico" o "error irrecuperable de RLC")

Para la presente descripción, se explotará el caso de un equipo de usuario que aborta un procedimiento de reconfiguración de seguridad en curso debido a la reselección de una célula nueva.

Cuando se trata del periodo de tiempo designado anteriormente "B", las especificaciones del 3GPP son poco claras y están también limitadas con respecto al comportamiento de configuración de seguridad del UE. Si se envía un mensaje *Actualizacióndecélula* durante el procedimiento de seguridad, después de *Mododeseguridadcompletado,* pero antes de que se reciba el L2ACK, entonces, como se indicó anteriormente, el UE abortará el procedimiento de modo de seguridad [1] en curso con manipulación especial para el parámetro de integridad *COUNT-I.* Se proporciona alguna otra guía vaga mediante una afirmación dirigida al RNC [2], en la que se afirma que la red (NW) debe tener presente que el UE "puede" abortar el procedimiento de seguridad.

Abortar el procedimiento de seguridad en la UE en este punto, sin embargo, no es favorable, ya que el UE acaba de dar acuse de recibo al RNC (en el mensaje de “modo de seguridad completado“) de que la reconfiguración de seguridad se ha realizado incluso aunque la reconfiguración de seguridad no haya sido todavía totalmente aplicada en el UE hasta que se reciba el L2ACK para Mododeseguridadcompletado del RNC (es decir, es la limitación de área gris de la técnica anterior como se representa mediante [1]).

Si el UE aborta la reconfiguración de seguridad después de que el RNC haya recibido el “modo de seguridad completado”, la nueva reconfiguración de seguridad será aplicada por el RNC. Por consiguiente, hay un desajuste de seguridad, lo que lleva a la interrupción de la llamada (como lo evidencia el análisis de red en vivo). La llamada interrumpida se debe al hecho de que el UE y la red en este momento están usando diferentes configuraciones de seguridad y no son capaces de comunicarse.

La especificación XP040292878 3GPP-STANDARDS, 2500 WILSON BOULEVARD, SUITE 300, ARLINGTON, VIRGINIA 22201 EE.UU. divulga que la NW sabrá que el UE abortó una SMC debido a la falta de protección de integridad en el mensaje de actualización de célula.

Sumario

La presente invención se refiere a métodos y disposiciones para la gestión de la reconfiguración de seguridad mejorada en un sistema de comunicación celular. Es el objeto de la presente invención reducir el riesgo de llamadas interrumpidas debido a los procedimientos de actualización de célula.

En un método de gestión de reconfiguración de seguridad y de procedimientos de actualización de célula en un equipo de usuario en un sistema de comunicación celular se realiza el siguiente procedimiento. Un equipo de usuario recibe una solicitud de reconfiguración de seguridad desde un nodo, y, subsiguientemente, inicia y confirma la reconfiguración de seguridad solicitada en el nodo. En algún momento, antes de recibir el acuse de recibo del nodo, el equipo del usuario detecta una activación de actualización de célula y aborta la reconfiguración de seguridad ya confirmada en respuesta a la activación de actualización de célula detectada. Subsiguientemente, el equipo de usuario proporciona una indicación del estado de seguridad en respuesta a la reconfiguración de seguridad abortada, después, transmite conjuntamente, al nodo, un mensaje de actualización de célula y la indicación del estado de seguridad proporcionada, informando sobre la reconfiguración de seguridad anteriormente confirmada que se está abortando.

Mediante estas características, se evita un desajuste entre las configuraciones de seguridad entre un UE y un nodo en el sistema de comunicación celular. Como resultado, la tasa de interrupción de llamadas se reduce y la tasa de configuración de llamadas se puede mejorar.

De acuerdo con un aspecto adicional de la presente invención, una realización de un equipo de usuario en un sistema de comunicación celular incluye medios para detectar un evento de activación de actualización de célula, y medios para abortar cualquier procedimiento de reconfiguración de seguridad en curso en el equipo de usuario en respuesta al evento de activar la actualización de célula detectado. Además, el equipo de usuario incluye medios para proporcionar una indicación del estado de seguridad en respuesta a la reconfiguración de seguridad abortada, y medios para transmitir conjuntamente un mensaje de actualización de célula y la indicación del estado de seguridad proporcionada a un nodo.

De acuerdo con otro aspecto adicional más, una realización de un método de gestión de la reconfiguración de seguridad y los procedimientos de actualización de célula en un nodo en un sistema de comunicación celular de acuerdo con la presente invención incluye los pasos de transmitir una solicitud de reconfiguración de seguridad para un usuario de equipo, y de recibir una confirmación de reconfiguración de seguridad. El nodo reconoce y realiza la reconfiguración de seguridad confirmada. Subsiguientemente, el nodo recibe conjuntamente un mensaje de actualización de célula y una indicación del estado de seguridad que informa de que la reconfiguración de seguridad confirmada en el equipo del usuario está siendo abortada. Finalmente, el nodo gestiona la reconfiguración de seguridad solicitada en base a la indicación del estado de seguridad recibida.

De acuerdo con un aspecto adicional, una realización de un nodo en un sistema de comunicación celular incluye medios para transmitir una solicitud de reconfiguración de seguridad para un usuario de equipo, y medios para recibir una confirmación de reconfiguración de seguridad. Además, el nodo incluye medios para reconocer y realizar la reconfiguración de seguridad confirmada, y medios para recibir conjuntamente un mensaje de actualización de célula y una indicación del estado de seguridad que informa de que la reconfiguración de seguridad confirmada está siendo abortada en el equipo del usuario. Finalmente, el nodo incluye medios para gestionar la reconfiguración de seguridad solicitada en base a la indicación del estado de seguridad recibida.

La presente invención, además, coordina ventajosamente de actualización de célula y los procedimientos de reconfiguración de seguridad y supera las limitaciones de la especificación del 3GPP como ya se ha descrito.

Breve descripción de los dibujos

La invención, junto con objetos y ventajas adicionales de la misma, puede entenderse mejor por referencia a la siguiente descripción tomada junto con los dibujos que se acompañan, en los cuales:

la figura 1 es una ilustración esquemática de la señalización conocida durante un procedimiento de reconfiguración de seguridad en un equipo de usuario;

la figura 2 es una ilustración esquemática de la señalización conocida durante un procedimiento de reconfiguración de seguridad y de actualización de células;

la figura 3 es una ilustración esquemática de la señalización conocida durante un procedimiento de reconfiguración de seguridad y de actualización de la célula;

la figura 4 es una ilustración esquemática de una realización de un método de acuerdo con la presente invención;

la figura 5 es un diagrama de flujo esquemático de una realización de un método en un equipo de usuario de acuerdo con la presente invención;

la figura 6 es un diagrama de flujo esquemático de una realización adicional de un método en un equipo de usuario de acuerdo con la presente invención;

la figura 7 es un diagrama de flujo esquemático de una realización de un método en un nodo de red de acuerdo con la presente invención;

la figura 8 es una ilustración esquemática de una realización de un equipo de usuario de acuerdo con la presente invención;

la figura 9 es una ilustración esquemática de una realización de un nodo de red de acuerdo con la presente invención.

Abreviaturas

ACK Acuse de recibo

AM Modo de acuse de recibo

CU	Actualización de célula
CCCH	Canal de control común
CR	Solicitud de cambio
DCCG	Canal de control dedicado
FACH	Canal de acceso directo
IE	Elemento de información
KPI	Indicadores clave de rendimiento
L2	Capa 2
MP	Obligatoriamente presente
OP	Opcionalmente presente
NW	Red
RAB	Portador de acceso por radio
RIM	Búsqueda en movimiento (proveedor específico de UE)
RLC	Control de enlace de radio (protocolo L2)
RNC	Controlador de red de radio
SRB	Portador de señalización de radio
TM	Modo transparente
UM	Modo no reconocido
3GPP	Proyecto de asociación de 3ª generación

Descripción detallada

La presente descripción se describirá en el contexto de un sistema del 3GPP; sin embargo, es igualmente aplicable a sistemas similares con una estructura similar.

Con el fin de comprender completamente los beneficios de la presente invención, se proporciona a continuación una descripción más a fondo de las soluciones de la técnica anterior y sus potenciales inconvenientes.

Los dos principales escenarios de carrera mencionados anteriormente observados (durante una llamada de voz RAB múltiple desde un CELL-FACH) que conducen a los diversos síntomas de llamada interrumpida se describen adicionalmente a continuación y con referencia a la figura 2 y a la figura 3.

En el primer escenario de la carrera, con referencia a la figura 2, el mensaje de actualización de célula y la orden del modo de seguridad se cruzan o se encuentran en el aire. En consecuencia, el RNC recibe el mensaje actualizacióndecélula justo después de que se haya enviado la orden de modo de seguridad, mientras que el UE envía el mensaje actualizacióndecélula justo antes de que se reciba la orden de modo de seguridad, es decir, "Seguridad durante la CU" [3]. En la figura 2, el tiempo se representa en el eje vertical, aumentando desde arriba hacia abajo. Los diversos pasos de señalización del procedimiento en la figura 2 son los siguientes:

1- Mensaje de actualización de célula enviado desde el UE al RNC

2. Orden de modo de seguridad (solicitud de reconfiguración de seguridad) enviado desde el RNC al UE.

Como se ve claramente en la figura 2, las dos señales 1 y 2 se encuentran en el aire. En este caso, se hará saber al controlador de la red de radio de la actualización de la célula antes de recibir cualquier confirmación de la reconfiguración de seguridad solicitada.

En el segundo escenario de carrera, con referencia a la figura 3, el UE envía el mensaje Actualizacióndecélula antes

de recibir un acuse de recibo de L2 para el modo de seguridad completado, es decir, "CU durante la seguridad" [1]. En la figura 3, el tiempo se representa en el eje vertical, aumentando desde arriba hacia abajo.

Con referencia a la figura 3, se describirá un problema típico resuelto por las realizaciones de la presente invención. Los diversos pasos de señalización del procedimiento en la figura 3 son los siguientes:

1. Orden de modo de seguridad

2. L2 ACK para (1)

3. Modo de seguridad completado

4. L2 ACK para (3)

5. Actualización de célula

En el instante de tiempo A, el UE selecciona una nueva célula, y aborta la reconfiguración de seguridad en curso, y tira de nuevo a la antigua reconfiguración de seguridad. En el instante de tiempo B, el RNC activa la nueva configuración de seguridad. En consecuencia, desde el instante de tiempo B, el UE y el RNC están funcionando con diferentes configuraciones de seguridad y son incapaces de mantener la llamada existente. En este caso, hay un desajuste de seguridad, ya que el UE está en la configuración de seguridad "antigua", mientras que el RNC está ahora en la configuración de seguridad "nueva" y, en de este modo, la situación conduce a la interrupción de la llamada.

Básicamente, la presente invención tiene por objeto permitir medios y disposiciones para evitar un desajuste en la configuración de seguridad entre un nodo de red y un equipo de usuario debido al segundo escenario de carrera anterior entre los procedimientos de actualización de célula y de reconfiguración de seguridad.

De acuerdo con una realización preferida de la presente invención, el UE está adaptado para incluir una indicación del estado de seguridad, como, por ejemplo, un elemento de información en el mensaje de actualización de célula enviado desde el UE al RNC. Este IE debe informar claramente al RNC de si un procedimiento de seguridad en curso en el UE ha sido abortado o no, y, así, el RNC puede decidir fácilmente si es necesario abortar también y revertir a las configuraciones antiguas de seguridad o no, o tomar otras medidas adecuadas.

Hoy, como se describió anteriormente, es posible que el UE aborte un procedimiento de reconfiguración de seguridad en curso justo antes de que finalice el procedimiento, con el fin de enviar una actualización de célula al RNC. Sin embargo, si el RNC ya ha completado este procedimiento de reconfiguración de seguridad en el momento de la recepción de esta actualización de célula, entonces, el RNC no tiene forma de saber con certeza que el procedimiento de seguridad anterior acaba de abortarse en el UE. Esto es actualmente una limitación en las especificaciones del 3GPP. La nueva indicación de estado propuesta, por ejemplo, el elemento de información IE, puede superar fácilmente la limitación del 3GPP.

Con referencia a la figura 4, se describirá un esquema de señalización de acuerdo con una realización de la presente invención. En comparación con el esquema de señalización de la figura 3, todos los pasos hasta el paso 4 son idénticos. Además, las acciones tomadas en los instantes de tiempo A y B son idénticas. Sin embargo, en el paso 5, el equipo del usuario proporciona una indicación del estado de seguridad en el mensaje de actualización de la célula. En esta realización, la indicación del estado de seguridad se proporciona como un elemento de información IE que se establece en *VERDADERO* si se ha abortado una reconfiguración de seguridad. En consecuencia, en el instante de tiempo C, el controlador de la red de radio recibe la indicación del estado de seguridad y se le informa de que el equipo del usuario ha abortado la reconfiguración de seguridad solicitada anteriormente. En esta realización, el controlador de red de radio procede a revertir a o tira de la configuración de seguridad anterior. De este modo, los dos nodos pueden comunicarse nuevamente utilizando la misma configuración de seguridad. Sin embargo, está implícito que el controlador de la red de radio puede tomar otras medidas o medidas adicionales al recibir la indicación del estado de seguridad.

Con referencia a la figura 5, se describirá una realización básica de un método para gestionar la reconfiguración de seguridad y los procedimientos de actualización de célula en un equipo de usuario en un sistema de comunicación celular de acuerdo con la presente invención. Inicialmente, un equipo de usuario detecta S30 un evento de activación de actualización de célula.

En respuesta al evento de activación de actualización de célula detectada, el equipo de usuario aborta S40 cualquier procedimiento de reconfiguración de seguridad en curso. Al abortar el procedimiento de reconfiguración de seguridad, el equipo del usuario revierte a o tira de una configuración de seguridad anterior, por ejemplo, de una ya existente. Subsecuentemente, el equipo del usuario proporciona S50 una indicación del estado de seguridad en respuesta a la reconfiguración de seguridad abortada. Finalmente, la indicación del estado de seguridad y un mensaje de actualización de célula se transmiten conjuntamente S60 a un nodo en el sistema de comunicación

celular, típicamente a un nodo de controlador de red de radio o a un nodo de control similar.

Básicamente, el mensaje de actualización de célula de la técnica anterior es modificado para incluir una indicación del estado de seguridad, como un elemento booleano de información que se establece en VERDADERO en caso de un procedimiento de reconfiguración de seguridad en curso que está siendo abortado en el equipo de usuario, y establecido en FALSO de lo contrario.

Con referencia a la figura 6, se describirá una realización detallada adicional de un método para gestionar la reconfiguración de seguridad y los procedimientos de actualización de célula en un equipo de usuario en un sistema de comunicación celular de acuerdo con la presente invención. Los pasos indicados en la realización anterior se denominan con los mismos números de referencia.

Inicialmente, el equipo de usuario recibe S10 una solicitud de reconfiguración de seguridad desde un nodo, por ejemplo, un controlador de red de radio. El equipo del usuario inicia y confirma S20 la reconfiguración de seguridad solicitada. En algún momento, antes de recibir el acuse de recibo del nodo, el equipo de usuario detecta S30 una activación de actualización de célula y, en consecuencia, se ve obligado a cambiar o volver a seleccionar la célula. En respuesta a la activación de actualización de célula detectada, el equipo del usuario aborta S40 la reconfiguración de seguridad ya confirmada. El equipo de usuario, entonces, proporciona S50 una indicación del estado de seguridad en respuesta a la reconfiguración de seguridad abortada. Finalmente, el equipo de usuario transmite conjuntamente S60, al nodo, un mensaje de actualización de célula y la indicación del estado de seguridad proporcionada informa de que la reconfiguración de seguridad confirmada está siendo abortada.

La indicación del estado de seguridad se establece preferentemente en un valor predeterminado en respuesta a una reconfiguración de seguridad abortada, de acuerdo con una realización particular de la invención se proporciona la indicación de estado como un elemento booleano de información. De acuerdo con una realización particular, la indicación del estado de seguridad se establece en VERDADERO sólo en el caso de una reconfiguración de seguridad abortada y de que se active un mensaje de actualización de célula para que se envíe durante una reconfiguración de seguridad en curso. De lo contrario, la indicación del estado de seguridad debe borrarse/establecerse en FALSO. La indicación del estado de seguridad no debe establecerse en el caso de que se haya abortado una reconfiguración de seguridad, pero no se envía un mensaje de actualización de célula hasta algún tiempo después del procedimiento de seguridad completado.

Con referencia a la figura 7, se describirá una realización básica de un método de gestión de reconfiguraciones de seguridad y procedimientos de actualización de célula en un nodo, como, por ejemplo, un controlador de red de radio, en un sistema de comunicación celular de acuerdo con la presente invención.

En algún punto en el tiempo, el nodo, como, por ejemplo, el controlador de red de radio, transmite S100 una solicitud de reconfiguración de seguridad a un equipo de usuario. Al recibir S200 una confirmación para la reconfiguración de seguridad, el nodo acusa el recibo S300 y realiza la reconfiguración de seguridad. Subsiguientemente, el controlador de red de radio recibe conjuntamente S400 un mensaje de actualización de célula y una indicación del estado de seguridad en el mensaje de actualización de célula, informando, la indicación, de que la reconfiguración de seguridad confirmada está siendo abortada. Finalmente, el controlador de red de radio gestiona su configuración de seguridad en base a la indicación del estado de seguridad recibida. Una posible acción sería revertir a una configuración de seguridad anterior en respuesta a la indicación de estado recibida. Otra posible acción sería volver a intentar la reconfiguración de seguridad abortada. Además, son posibles otras acciones, bajo la condición de que el controlador de red de radio reconozca la indicación del estado de seguridad incluida.

Con referencia a la figura 8, se describirá una realización general de un equipo de usuario de acuerdo con la presente invención. El equipo de usuario incluye una unidad 30 para detectar un evento de activación de actualización de célula, y una unidad 40 para abortar cualquier procedimiento de reconfiguración de seguridad en curso en el equipo de usuario en respuesta al evento de activación de actualización de célula detectado. Además, el equipo de usuario incluye una unidad 50 para proporcionar 50 una indicación del estado de seguridad en respuesta a la reconfiguración de seguridad abortada, y, finalmente, una unidad para transmitir conjuntamente 60 un mensaje de actualización de célula y la indicación del estado de seguridad proporcionada a un nodo en el sistema de comunicación.

De acuerdo con un modo de realización particular, también con referencia a la figura 8 (en particular las cajas con líneas de puntos), el equipo de usuario incluye adicionalmente una unidad 10 para recibir una solicitud de reconfiguración de seguridad de un nodo, y una unidad 20 para iniciar y confirmar la reconfiguración de seguridad solicitada;
Con referencia a la figura 9, se describirá una realización de un nodo de acuerdo con la presente invención. El nodo, por ejemplo un controlador de red de radio, incluye una unidad 100 para transmitir una solicitud de reconfiguración de seguridad a un equipo de usuario, y una unidad 200 para recibir una confirmación de reconfiguración de seguridad del equipo de usuario. Además, el nodo incluye una unidad 300 para reconocer y realizar la reconfiguración de seguridad confirmada, y una unidad 400 para recibir conjuntamente un mensaje de actualización de célula y una indicación del estado de seguridad informando sobre la reconfiguración de seguridad anteriormente

confirmada que se está abortando. Finalmente, el nodo incluye una unidad 500 para gestionar 500 la reconfiguración de seguridad solicitada anteriormente en base a la indicación del estado de seguridad recibida.

Se entiende que las partes funcionales de las formas de realización pueden implantarse como dentro de equipo físico informático (hardware), como, por ejemplo, procesadores, o como elementos de equipo lógico informático (software), como, por ejemplo, algoritmos ejecutables en un ordenador. También se entiende que algunas partes de la funcionalidad pueden proporcionarse fuera del equipo de usuario y/o del nodo y comunicarse al equipo de usuario y nodo utilizando otros medios de comunicación.

Las ventajas de la presente invención incluyen:

El principal beneficio del nuevo IE propuesto es superar las limitaciones del 3GPP y, de este modo, evitar innecesarias llamadas interrumpidas en la reconfiguración de seguridad en el CELL_FACH (por ejemplo, *típicamente,* en la configuración de llamada de voz del CELL_FACH), por consiguiente, KPI mejorados, y, de este modo, aumentar los ingresos y la satisfacción final del usuario.

Este nuevo *"Indicador de* estado de seguridad*"* IE asegura que no hay desajuste de seguridad entre el UE y el RNC, ya que el RNC también tira de la configuración de seguridad "antigua" si el actualizacióndecélula recibido desde el UE con IE = "VERDADERO", indicando que el UE ha abortado el procedimiento de seguridad debido a la reselección de célula de actualizacióndecélula. Como el RNC y el UE están utilizando las mismas claves de seguridad "antiguas" después de que el procedimiento de seguridad haya sido abortado, entonces, no debería producirse una interrupción *anormal de* llamadas.

En caso de cualesquiera escenarios *imprevistos*, este IE permitirá a la red considerar *otras* acciones correctivas alternativas en lugar de interrumpir la llamada como ocurre en la actualidad.

Referencias

1- Especificaciones [1] del 3GPP TS 25.331 V8.7.0 sección 8.1.12.4b, "Cell update procedure during security reconfiguration".

2- Especificaciones [2] del 3GPP TS 25.331 V8.7.0 sección 8.1.12.2.2, "Integrity protection configuration change".

3- Especificaciones [3] del 3GPP TS 25.331 V8.7.0 sección 8.3.1.9b, "Security reconfiguration during Cell update procedure".

REIVINDICACIONES

1. Un método para gestionar procedimientos de reconfiguración de seguridad y de actualización de célula en un equipo de usuario en un sistema de comunicación celular, comprendiendo el método:

detectar (S30) un evento de activación de actualización de célula, y

abortar (S40) cualquier procedimiento de reconfiguración de seguridad en curso en dicho equipo de usuario en respuesta a dicho evento de activación de actualización de célula detectado;

en el que el método está caracterizado por:

establecer (S50) una indicación del estado de seguridad a un valor predeterminado en respuesta a dicha reconfiguración de seguridad abortada y en respuesta a un mensaje de actualización de célula que se activa para que se envíe durante un procedimiento de reconfiguración de seguridad en curso, en el que la indicación del estado de seguridad es un elemento booleano de información, y

transmitir conjuntamente (S60) un mensaje de actualización de célula y dicha indicación del estado de seguridad a un nodo, en el que la indicación del estado de seguridad informa sobre el procedimiento de reconfiguración de seguridad que se aborta en el equipo de usuario.

2. Método de acuerdo con la reivindicación 1, caracterizado por:

antes de detectar (S30) el evento de activación de actualización de célula, recibir (S10) una solicitud de reconfiguración de seguridad de un nodo, e

iniciar y confirmar (S20) dicha reconfiguración de seguridad solicitada;

en el que el método está caracterizado adicionalmente porque la indicación del estado de seguridad informa sobre dicha reconfiguración de seguridad confirmada que se está abortando.

3. Método de acuerdo con la reivindicación 1 o 2, caracterizado porque dicho paso de transmitir conjuntamente dicho mensaje de actualización de célula y dicha indicación del estado de seguridad proporcionada comprende transmitir dicho mensaje de actualización de célula y dicha indicación del estado de seguridad proporcionada en un mismo mensaje de actualización de célula.

4. Método de acuerdo con la reivindicación 3, caracterizado porque dicha indicación del estado de seguridad se proporciona como un elemento booleano de información en dicho mensaje de actualización de célula.

5. Un equipo de usuario en un sistema de comunicación celular que comprende:

medios para detectar (30) un evento de activación de actualización de célula;

medios para abortar (40) cualquier procedimiento de reconfiguración de seguridad en curso en dicho equipo de usuario en respuesta a dicho evento de activación de actualización de célula detectado;

caracterizado por medios para establecer (50) una indicación del estado de seguridad a un valor predeterminado en respuesta a dicha reconfiguración de seguridad abortada y en respuesta a un mensaje de actualización de célula que se activa para ser enviado durante un procedimiento de reconfiguración de seguridad en curso en el que la indicación del estado de seguridad es un elemento booleano de información, y

medios para transmitir conjuntamente (60) un mensaje de actualización de célula y dicha indicación del estado de seguridad a un nodo, en el que la indicación del estado de seguridad informa sobre el procedimiento de reconfiguración de seguridad que se aborta en el equipo de usuario.

6. Equipo de usuario de acuerdo con la reivindicación 5, caracterizado por:

medios para recibir (10) una solicitud de reconfiguración de seguridad de un nodo; y

medios para iniciar y confirmar (20) dicha reconfiguración de seguridad solicitada.

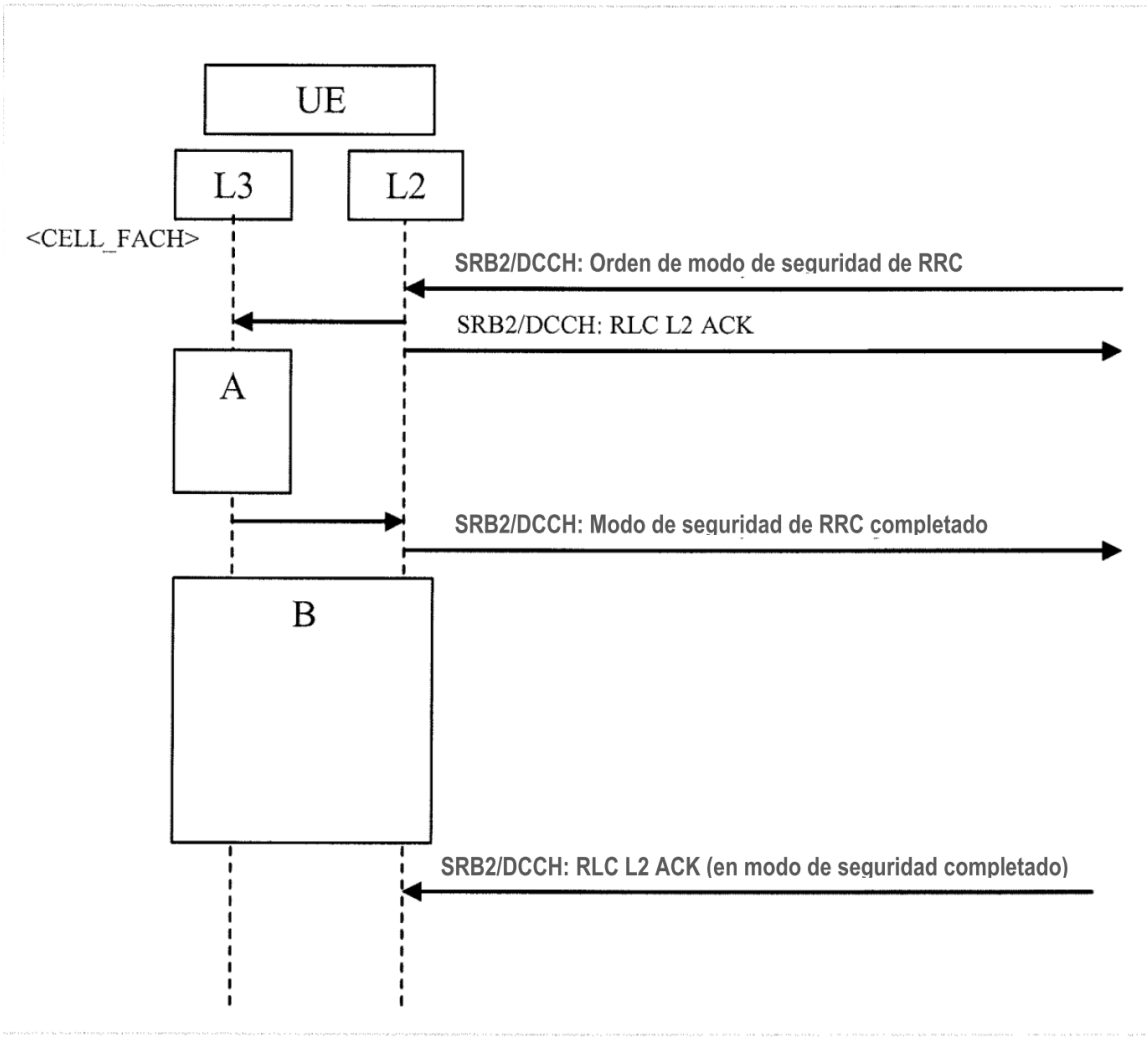
UE
L3
L2
<CELL_FACH>
SRB2/DCCH: Orden de modo de seguridad de RRC
SRB2/DCCH: RLC L2 ACK
A
SRB2/DCCH: Modo de seguridad de RRC completado
B
SRB2/DCCH: RLC L2 ACK (en modo de seguridad completado)

Fig. 1

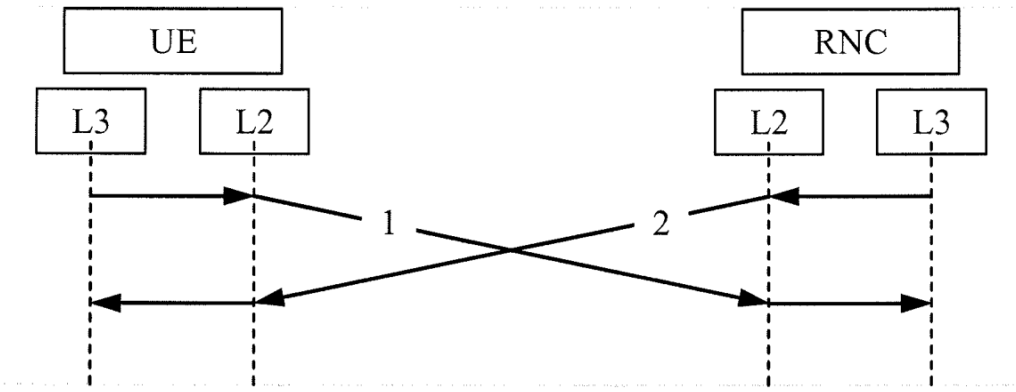

Fig. 2

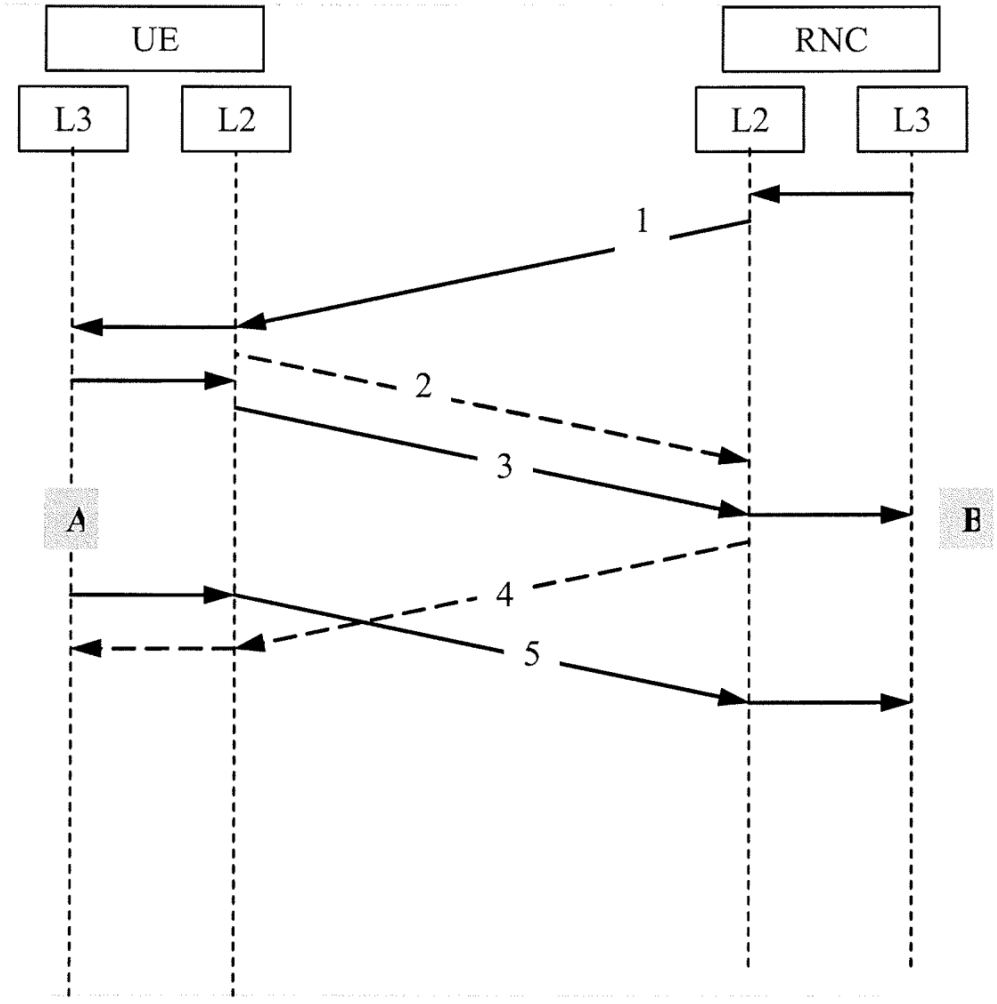

Fig. 3

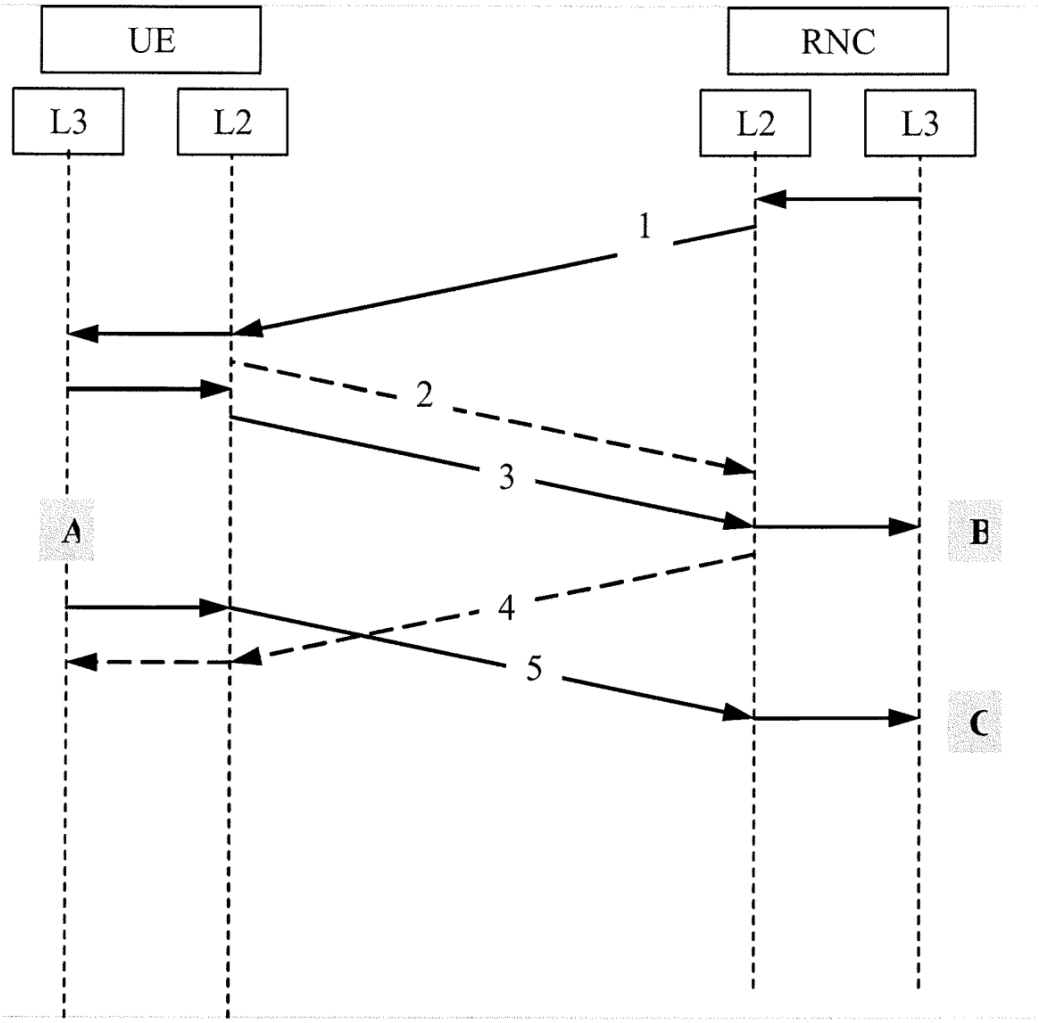

Fig. 4

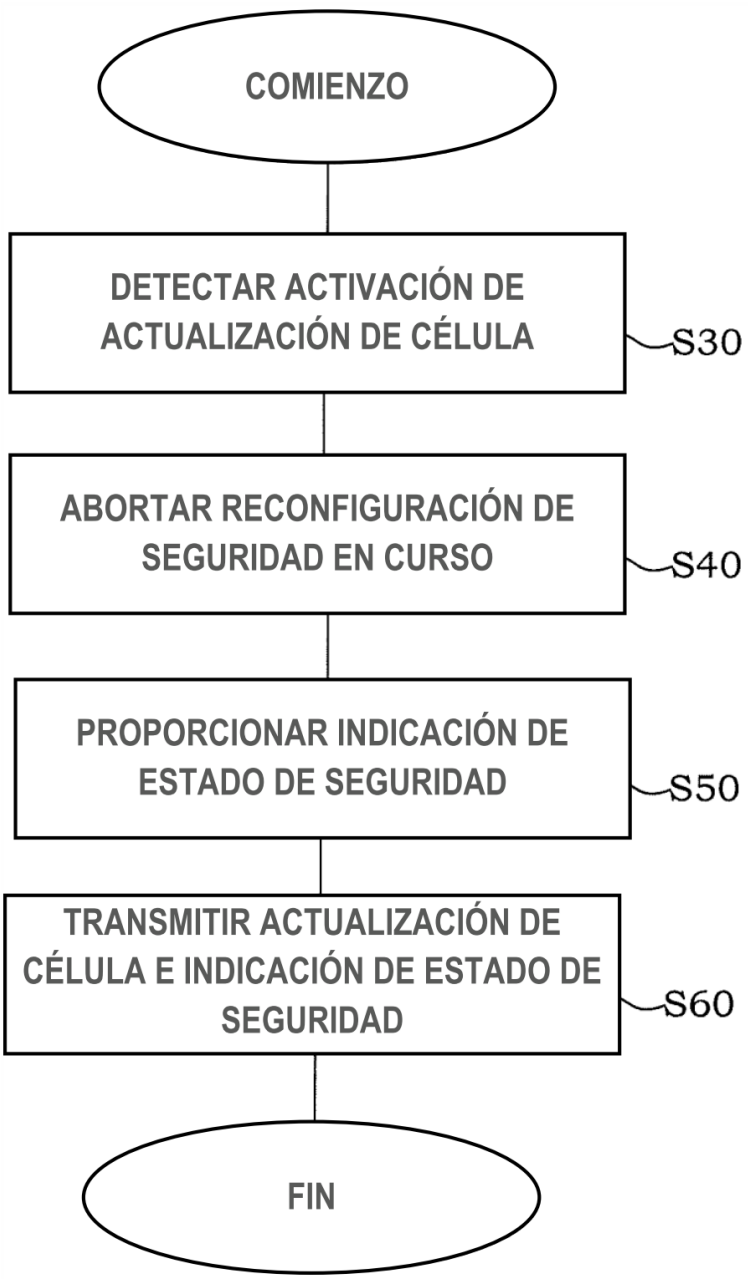
COMIENZO
DETECTAR ACTIVACIÓN DE ACTUALIZACIÓN DE CÉLULA
S30
ABORTAR RECONFIGURACIÓN DE SEGURIDAD EN CURSO
S40
PROPORCIONAR INDICACIÓN DE ESTADO DE SEGURIDAD
S50
TRANSMITIR ACTUALIZACIÓN DE CÉLULA E INDICACIÓN DE ESTADO DE SEGURIDAD
S60
FIN

Fig. 5

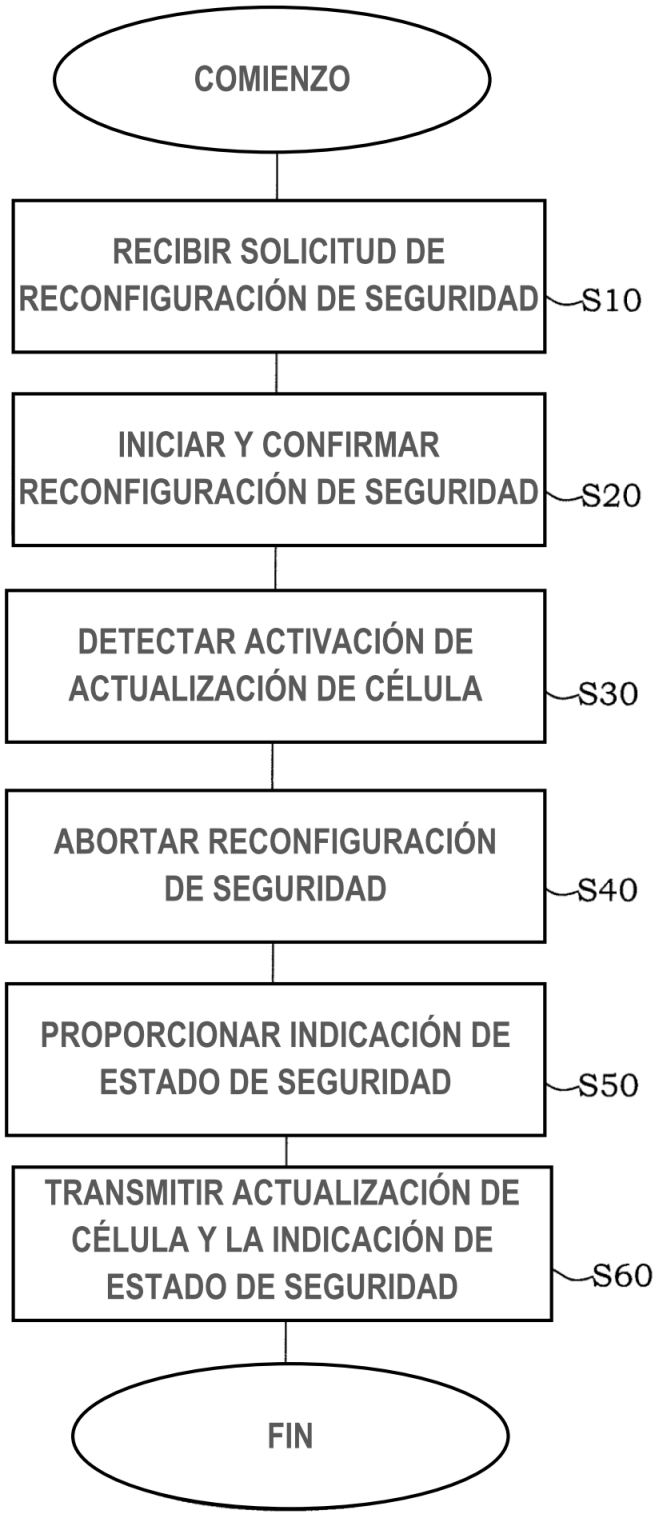
COMIENZO
RECIBIR SOLICITUD DE RECONFIGURACIÓN DE SEGURIDAD
S10
INICIAR Y CONFIRMAR RECONFIGURACIÓN DE SEGURIDAD
S20
DETECTAR ACTIVACIÓN DE ACTUALIZACIÓN DE CÉLULA
S30
ABORTAR RECONFIGURACIÓN DE SEGURIDAD
S40
PROPORCIONAR INDICACIÓN DE ESTADO DE SEGURIDAD
S50
TRANSMITIR ACTUALIZACIÓN DE CÉLULA Y LA INDICACIÓN DE ESTADO DE SEGURIDAD
S60
FIN

Fig. 6

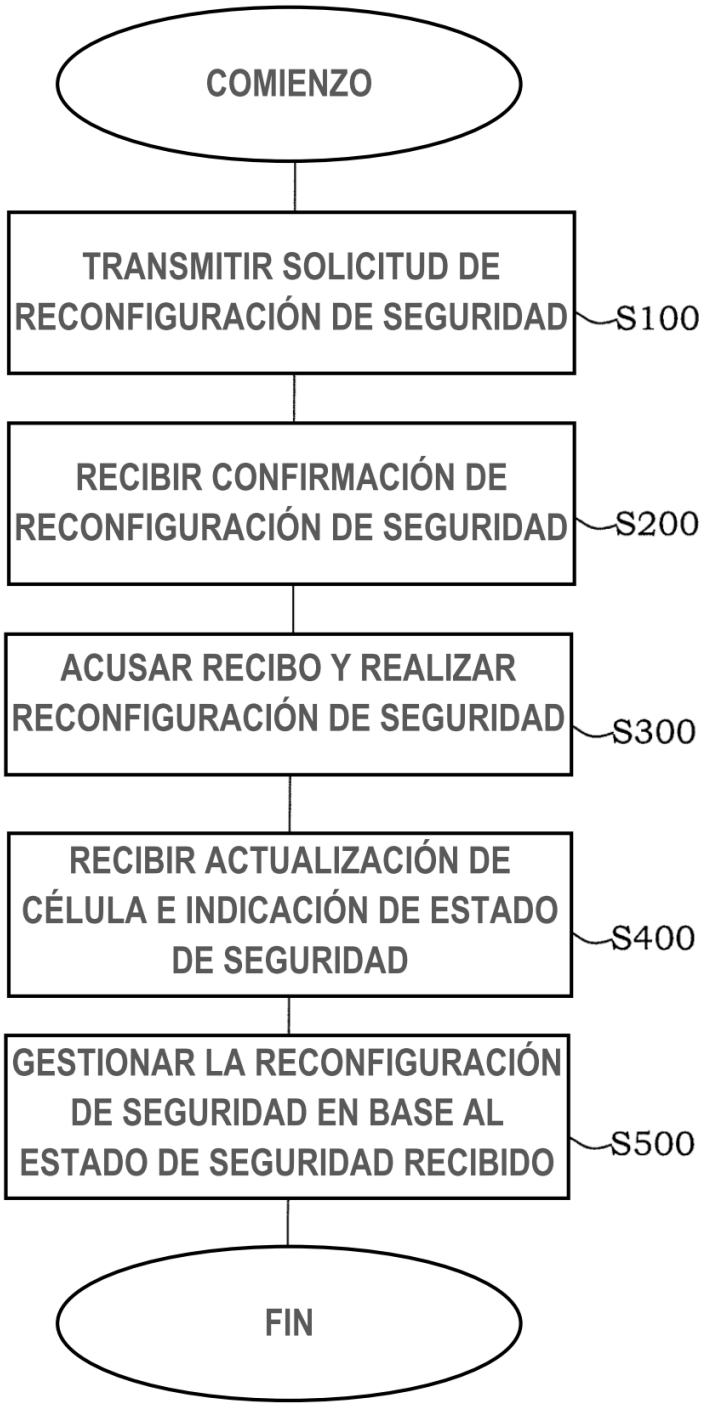
COMIENZO
TRANSMITIR SOLICITUD DE RECONFIGURACIÓN DE SEGURIDAD
S100
RECIBIR CONFIRMACIÓN DE RECONFIGURACIÓN DE SEGURIDAD
S200
ACUSAR RECIBO Y REALIZAR RECONFIGURACIÓN DE SEGURIDAD
S300
RECIBIR ACTUALIZACIÓN DE CÉLULA E INDICACIÓN DE ESTADO DE SEGURIDAD
S400
GESTIONAR LA RECONFIGURACIÓN DE SEGURIDAD EN BASE AL ESTADO DE SEGURIDAD RECIBIDO
S500
FIN

Fig. 7

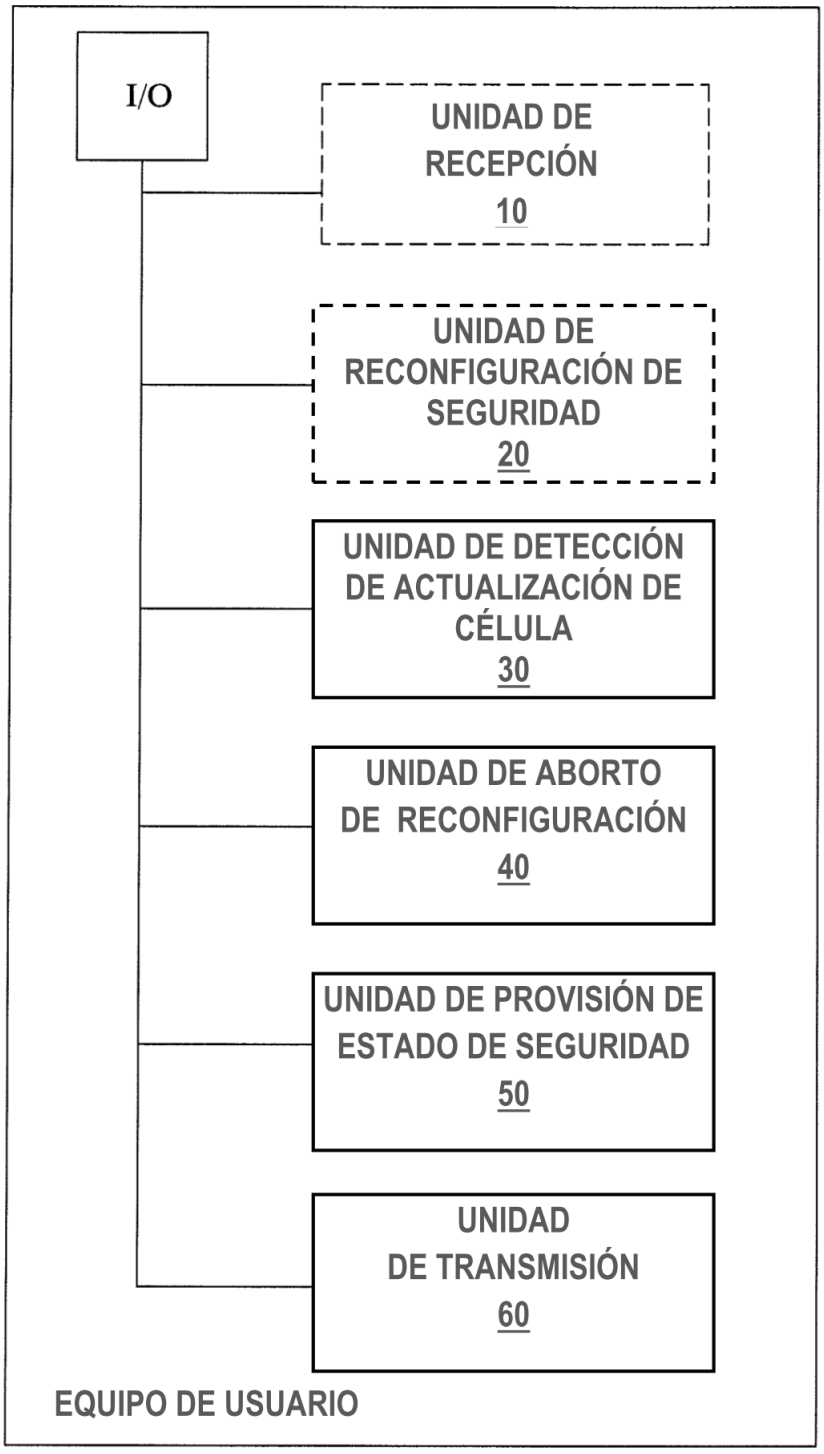
I/O
UNIDAD DE RECEPCIÓN
10
UNIDAD DE RECONFIGURACIÓN DE SEGURIDAD
20
UNIDAD DE DETECCIÓN DE ACTUALIZACIÓN DE CÉLULA
30
UNIDAD DE ABORTO DE RECONFIGURACIÓN
40
UNIDAD DE PROVISIÓN DE ESTADO DE SEGURIDAD
50
UNIDAD DE TRANSMISIÓN
60
EQUIPO DE USUARIO

Fig. 8

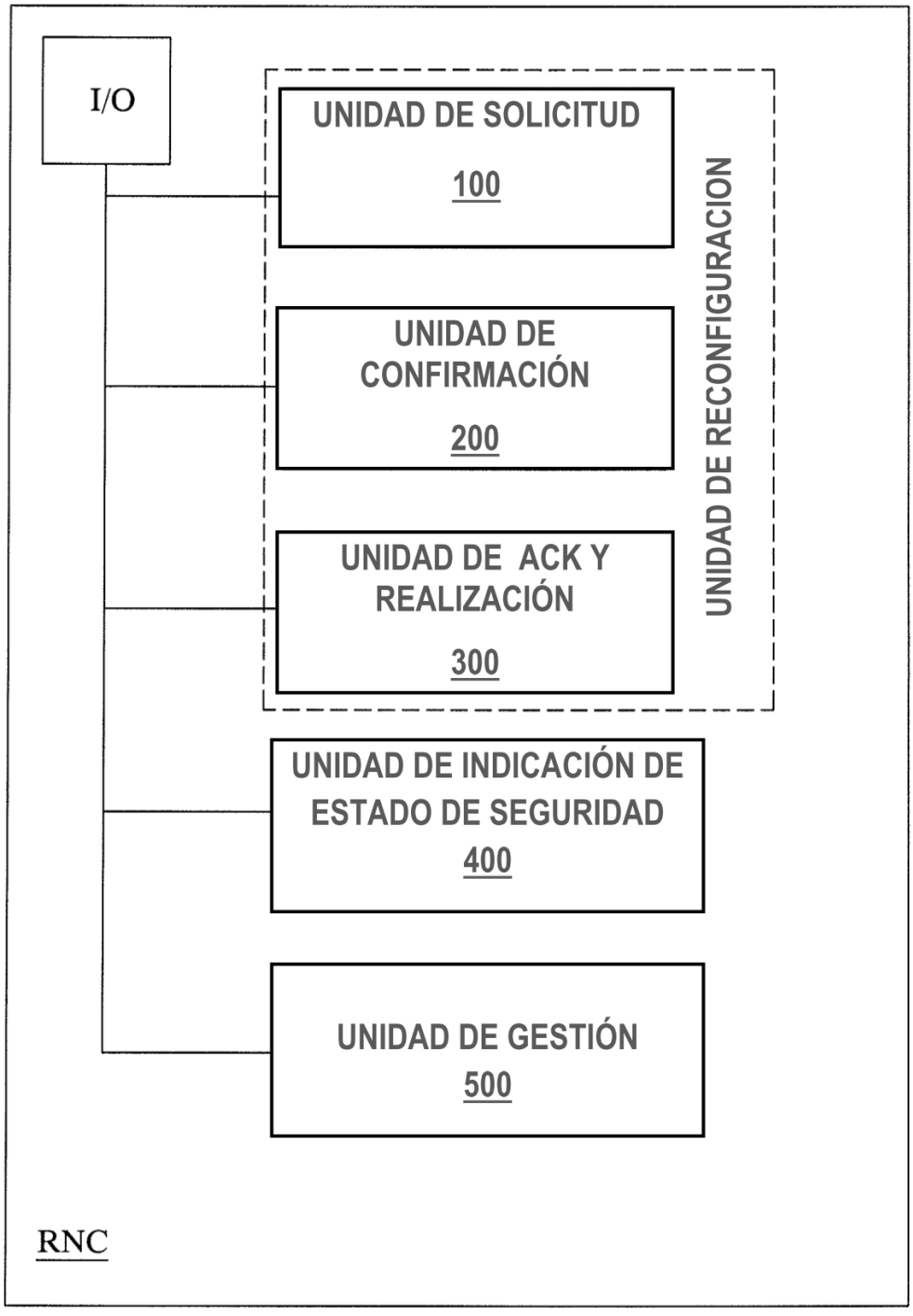
I/O
UNIDAD DE SOLICITUD
100
UNIDAD DE CONFIRMACIÓN
200
UNIDAD DE ACK Y REALIZACIÓN
300
UNIDAD DE RECONFIGURACION
UNIDAD DE INDICACIÓN DE ESTADO DE SEGURIDAD
400
UNIDAD DE GESTIÓN
500
RNC

Fig. 9