(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 398 612**

(51) Int. CI.:

H04W 12/10 (2009.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.07.2006 E 09015157 (2)**

(97) Fecha y número de publicación de la concesión europea: **12.12.2012 EP 2157819**

(54) Título: **Método de modo de seguridad de estación móvil**

(30) Prioridad:

08.08.2005 US 199348

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.03.2013

(73) Titular/es:

MOTOROLA MOBILITY, LLC (100.0%)
600 North US Highway 45
Libertyville, IL 60048 , US

(72) Inventor/es:

ZHAO, HUI y
PUTCHA, PADMAJA

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Método de modo de seguridad de estación móvil.

Campo de la descripción

La presente descripción se refiere en general a comunicaciones de radiotelefonía y, en particular, a comprobación de integridad de mensajes de señalización en una estación móvil.

Antecedentes de la descripción

Según la Especificación Técnica 25.331 del Proyecto Partnership de Tercera Generación (3GPP), una variable INTEGRITY_PROTECTION_INFO indica el estado de protección de integridad en una estación móvil (MS) en la capa de control de recurso de radio (RRC). El estado de protección de integridad puede estar ya sea "no iniciado" o ya sea "iniciado". Si la variable INTEGRITY_PROTECTION_INFO tiene el valor "iniciado", cualquier mensaje de RRC recibido por la MS será comprobado en a un elemento de información (IE) "Integrity check info". Si el IE "Integrity check info" no está presente, la MS desechará el mensaje.

Según la Especificación Técnica 24.008 de 3GPP, la señalización de integridad protegida es obligatoria cuando una estación móvil está en modo conectada UMTS con una red. Existen algunas excepciones clave, sin embargo, en cuanto al requisito de que todos los mensajes de señalización de capa 3 estén protegidos en integridad. Por ejemplo, los mensajes de "petición de autenticación" del dominio conmutado de circuitos (CS) y de "petición de autenticación & cifrado" del dominio conmutado de paquetes (PS) no necesitan estar protegidos en integridad. De ese modo, estos tipos de mensajes pueden carecer del IE "Integrity check info".

Cuando las conexiones de dominio CS y de dominio PS entre una red y una estación móvil están siendo establecidas corrientemente, un mensaje de capa 3 no protegido en integridad del dominio puede ser recibido en la estación móvil después de otro mensaje del dominio que inicia la protección de integridad. El requisito de la Especificación Técnica 25.331 de 3GPP puede dar como resultado una MS que descarte el mensaje de capa 3 no protegido en integridad. La consecuencia de esta acción de descarte puede dar como resultado una incapacidad para completar una llamada. Por ejemplo, si un mensaje (y sus copias) de "petición de autenticación" de dominio CS es consecuentemente descartado por la MS, entonces no se puede completar la llamada y eventualmente decaerá.

En otras palabras, cuando un mensaje de capa 3 no protegido en integridad en un dominio es recibido por una MS después de que un comando inicie protección de integridad en otro dominio, la MS descarta el mensaje de capa 3 no protegido en integridad. Por otra parte, si el mismo mensaje de capa 3 no protegido en integridad en un dominio hubiera sido recibido por la MS con anterioridad a que el comando inicie protección de integridad en otro dominio, entonces la MS procesa apropiadamente el mensaje de capa 3 no protegido en integridad. Puesto que los mensajes de RRC (Estrato de Acceso) y los mensajes de capa 3 (Estrato de No Acceso) utilizan diferentes portadoras de radio y tienen diferentes prioridades, existe un riesgo real de que un mensaje no protegido en integridad para un dominio y un mensaje de iniciación de protección de integridad para otro dominio sean recibidos desordenados por una MS.

Existe una oportunidad de que una MS procese mensajes de capa 3 no protegidos en integridad y mensajes de iniciación de protección de integridad desordenados, para reducir el número de llamadas interrumpidas. Los diversos aspectos, características y ventajas de la descripción resultarán mucho más evidentes para quienes son expertos en la materia tras la consideración cuidadosa de los dibujos que siguen y de la descripción detallada que se acompaña.

El documento US 2003/236085 A1 divulga una disposición en la que un UE, en un sistema de 3GPP", puede procesar dos mensajes de RRC de forma independiente cada uno del otro, cada uno de los cuales puede contener un valor de INICIO para el mismo dominio. Para evitar pérdida de sincronización entre el UE y la UTRAN con respecto a estos valores de INICIO, en una primera realización un UE asegura que los valores de INICIO en los dos mensajes son idénticos si el primer mensaje no ha sido totalmente reconocido con anterioridad a la transmisión del segundo mensaje.

El documento US 2003/100291 A1 divulga una disposición que protege la seguridad de una comunicación entre una radio móvil y una red de acceso de radio (RAN). Se establece una conexión a través de la RAN para soportar una comunicación con la radio móvil.

Breve descripción de los dibujos

La Figura 1 muestra un sistema de 3GPP simplificado con una estación móvil y una red según una realización;

La Figura 2 muestra un diagrama de flujo de un método de modo de seguridad para la estación móvil mostrada en la Figuras 1 según una primera realización;

La Figura 3 muestra un primer ejemplo de diagrama de flujo de señal para un método de modo de seguridad en el sistema de 3GPP mostrado en la Figura 1 conforme a la primera realización;

La Figura 4 muestra un segundo ejemplo de diagrama de flujo de señal para un método de modo de seguridad en el sistema de 3GPP mostrado en la Figura 1 conforme a la primera realización;

La Figura 5 muestra un diagrama de flujo de un método de modo de seguridad para la estación móvil mostrada en la Figura 1 según una segunda realización;

La Figura 6 muestra un tercer ejemplo de diagrama de flujo de señal para un método de modo de seguridad en el sistema de 3GPP mostrado en la Figura 1 conforme a la segunda realización.

Descripción detallada

En ambos dominios conmutado de circuitos (CS) y conmutado de paquetes (PS), una red de núcleo puede iniciar un mensaje de señalización de capa 3 no protegido en integridad con anterioridad al inicio de un mensaje de control de recurso de radio (RRC) para el inicio de la protección de integridad. Cuando ambas red de núcleo CS y red de núcleo PS están normalmente estableciendo una conexión con una estación móvil (MS), un mensaje de señalización de capa 3 no protegido en integridad para un dominio puede llegar a una MS ya sea antes o ya sea después de un mensaje de iniciación de protección de integridad para otro dominio. Puesto que los mensajes de RRC (Estrato de Acceso) y los mensajes de capa 3 (Estrato de No Acceso) son enviados con diferentes prioridades sobre diferentes portadoras de radio, existe un riesgo real de que una MS reciba un mensaje de señalización de capa 3 no protegido en integridad para un dominio después de recibir un menaje de RRC (Estrato de Acceso) para el inicio de protección de integridad en otro dominio.

Un método de modo de seguridad de estación móvil recibe un mensaje de capa 3 ya sea en el dominio conmutado de paquetes (PS) o ya sea conmutado de circuitos (CS), determina si el mensaje de capa 3 está protegido en integridad, determina si la protección de integridad ha sido iniciada en ese dominio, y envía el mensaje de capa 3 a la capa de gestión de movilidad del propio dominio de la MS si el mensaje de capa 3 no está protegido en integridad y la protección de integridad no ha sido iniciada en ese dominio. Si la protección de integridad ha sido iniciada en ese dominio, entonces se descarta el mensaje de capa 3. Este método alberga una situación en la que una MS recibe un mensaje de capa 3 no protegido en integridad para un dominio después de recibir un mensaje de iniciación de protección de integridad en otro dominio.

La Figura 1 muestra un sistema 100 de 3GPP simplificado con una estación móvil 180 y una red 190 según una realización. En las realizaciones que se discuten, se muestra un sistema de comunicación inalámbrica de 3GPP; sin embargo, los principios divulgados pueden ser aplicados a otros tipos de sistemas de comunicación inalámbrica incluyendo las futuras versiones del sistema 3GPP. La estación móvil 180, mencionada a veces como dispositivo móvil o como equipo de usuario (UE), puede ser un radioteléfono, un ordenador transportable con conexión inalámbrica, un dispositivo de mensajería inalámbrica, u otro tipo de dispositivo de comunicación inalámbrica compatible con la red 190.

La red 190 incluye una red de núcleo 196 conmutada de circuitos (CS) así como una red de núcleo 198 conmutada de paquetes (PS). La red de núcleo 196 CS y la red de núcleo 198 PS operan independientemente cada una de la otra. Por ejemplo, la red de núcleo PS puede iniciar protección de integridad en un momento, y la red de núcleo CS puede iniciar protección de integridad en un momento posterior que no esté coordinado con la iniciación de protección de integridad de la red de núcleo PS. La red de núcleo 196 CS y la red de núcleo 198 PS están reunidas en un control de recurso de radio (RRC) y una entidad de control de enlace de radio (RLC) de Controlador de Red de Radio (RNC) dentro de la red 190 y de ese modo ambos mensajes PS y CS son transmitidos a través de un enlace 110 de comunicación inalámbrica hasta la estación móvil 180. La estación móvil 180 comunica con la red 190 a través del enlace 110 de comunicación inalámbrica también.

La Figura 2 muestra un diagrama de flujo 200 de un método de modo de seguridad para la estación móvil 180 mostrada en la Figura 1 conforme a una primera realización. En la etapa 210, la estación móvil 180 recibe un mensaje de transferencia directa de enlace descendente (DDT) de capa 3 conmutada de circuitos (CS) procedente de una red tal como la red 190 mostrada en la Figura 1. El mensaje DDT CS puede ser un mensaje de petición de autenticación, un mensaje de rechazo de autenticación, un mensaje de petición de identidad, un mensaje de aceptación de actualización de localización, un mensaje de rechazo de actualización de localización, un menaje de suspensión o uno de otros diversos tipos de mensajes de capa 3. En la etapa 220, la estación móvil 180 determina si la información de protección de integridad está presente en el mensaje DDT CS. Según la Especificación Técnica 25.331 de 3GPP, un elemento de información (IE) “Integrity check info” indica convenientemente si la información de comprobación de integridad está en el mensaje de capa 3. En esta realización, si el IE “Integrity check info” está presente, entonces existe información de protección de integridad presente en el mensaje DDT CS según la etapa 220. Si está presente la información de protección de integridad, la etapa 230 realiza protección de integridad de capa de RRC estándar sobre el mensaje DDT CS y el flujo termina en la etapa 290.

Si no está presente información de protección de integridad en el mensaje DDT CS, la etapa 240 determina si ha sido iniciado un procedimiento de modo de seguridad de protección de integridad por la red de núcleo CS. Si la estación móvil 180 ha recibido un mensaje de comando de modo de seguridad CS para iniciar la protección de integridad, entonces ha sido iniciado un procedimiento de modo de seguridad de protección de integridad por la red

de núcleo CS y la etapa 250 descarta el menaje DDT CS antes de que termine el flujo en la etapa 290. El hecho de descartar el mensaje DDT CS bajo estas condiciones cumple con los requisitos de la Especificación Técnica 25.331 de 3GPP. Alternativamente, si la variable INTEGRITY_PROTECTION_INFO fue modificada para que incluyera estados separados de iniciados y no iniciados para los dominios CS y PS, la etapa 240 podría ser determinada comprobando la variable de INTEGRITY_PROTECTION_INFO de la estación móvil.

Si la etapa 240 determina que un procedimiento de modo de seguridad de protección de integridad no ha sido iniciado por la red de núcleo CS (por ejemplo, solamente ha sido iniciado un modo de seguridad por la red de núcleo PS o que ninguna red de núcleo ha iniciado un modo de seguridad), la etapa 260 envía el mensaje DDT CS a la capa de gestión de movilidad (MM) conmutada de circuitos de la estación móvil 180 antes de que termine el flujo en la etapa 290. Puesto que la Especificación Técnica 24.008 de 3GPP proporciona flexibilidad para procesar un mensaje de capa 3 no protegido en integridad en un dominio particular cuando no ha sido iniciada la protección de integridad para ese dominio, el diagrama de flujo 200 impide que se interrumpa una llamada cuando un mensaje de señalización de capa 3 y un mensaje de iniciación de protección de integridad son recibidos de forma desordenada.

La Figura 3 muestra un primer ejemplo de diagrama 300 de flujo de señal para un método de modo de seguridad en el sistema 100 de 3GPP mostrado en la Figura 1 según la primera realización. En este primer ejemplo, un mensaje 370 de petición de autenticación CS no protegido en integridad es iniciado por una red de núcleo 396 CS con anterioridad a que el mensaje 350 de iniciación de protección de integridad sea iniciado por una red de núcleo PS, pero el mensaje 370 no protegido en integridad se recibe en la estación móvil 380 después de que haya sido recibido el mensaje 350 de iniciación de protección de integridad en la estación móvil 380. En este ejemplo, en el que una estación móvil 380 está iniciando una llamada, en vez de descartar el mensaje 370 de petición de autenticación CS no protegido en integridad, la estación móvil 380 pasa el mensaje 370 a su capa 386 de gestión de movilidad (MM) de dominio conmutado de circuitos.

Este primer ejemplo de diagrama 300 de flujo de señal muestra cuatro capas en una estación móvil 380: una capa 382 de control de enlace de radio (RLC), una capa 384 de control de recurso de radio (RRC), una capa 386 de gestión de movilidad (MM) de dominio conmutado de circuitos, y una capa 388 de gestión de movilidad de GPRS (GMM) de dominio conmutado de paquetes. Las capas 382, 384 de RLC y RRC se consideran capas “inferiores”, mientras que las capas 386, 388 de MM y GMM se consideran capas “superiores”. La capa 386 de MM utilizada en el dominio CS es análoga a la capa 388 de GMM del dominio PS; ambas son capas de gestión de movilidad.

También se han mostrado cuatro capas de una red 390 en el primer ejemplo de diagrama 300 de flujo de señal. La red 390 tiene una capa 392 de control de enlace de radio (RLC) y una capa 394 de control de recurso de radio (RRC) que son contrapartidas de las capas 382, 384 de RLC y RRC de la estación móvil 380. La red 390 posee también una red de núcleo 396 CS y una red de núcleo 398 PS, las cuales han sido mostradas en la Figura 1 como red de núcleo 196 CS y red de núcleo 198 PS. Según se ha expuesto con anterioridad, la red de núcleo 396 CS y la red de núcleo 398 PS operan independientemente cada una de la otra.

Una vez que se ha establecido una conexión de RRC entre la estación móvil 380 y la red 390 usando varios mensajes 310, se genera un mensaje 320 de actualización de localización CS por parte de la capa 386 de MM conmutada de circuitos, y se pasa a la capa 384 de RRC, es reempaquetado para la capa 382 de RLC, y se transmite desde la capa de RLC de la estación móvil 380 como mensaje 325. El mensaje 325 es recibido en la capa 392 de RLC de la red, convertido y enviado a la capa 394 de RRC, la cual reenvía el mensaje a la red de núcleo 396 CS para su procesamiento. En el lado de conmutación de paquetes, se genera un mensaje 330 de petición de unión en la capa 388 de GMM conmutada de paquetes, es reempaquetado en la capa 384 de RRC, y transmitido desde la estación móvil 380 a través de la capa 382 de RLC como mensaje 335. La capa 392 de RLC de la red 390 recibe el mensaje 335 y lo convierte para la capa 394 de RRC, la cual lo procesa a continuación y lo reenvía a la red de núcleo 398 PS. El mensaje 320 de actualización de localización CS y el mensaje 330 de petición de unión PS, no están coordinados entre sí y pueden ocurrir en cualquier secuencia de tiempo.

En respuesta al mensaje 320 de actualización de localización CS, la red 390 envía un mensaje 370 de petición de autenticación CS no protegido en integridad seguido de un comando de modo de seguridad CS (no representado) para iniciar la protección de integridad. La petición de autenticación se genera por medio de la red de núcleo 396 CS como mensaje 371, y es empaquetado por la capa 394 de RRC como mensaje 373. Dependiendo del tamaño y de la prioridad del mensaje 373, puede transcurrir algo de tiempo después de que la capa 392 de RLC de la red 390 transmita un mensaje 375 no protegido en integridad que contenga el mensaje 370 de petición de autenticación CS. Mientras tanto, en respuesta al mensaje 330 de petición de unión, la red de núcleo 398 PS ha iniciado un mensaje 340 de petición de autenticación & cifrado, seguido por un comando 350 de modo de seguridad para el inicio de protección de integridad. La estación móvil 380 inicia protección de integridad y prepara un mensaje 360 de modo de seguridad completado para la capa 382 de RLC cuando se han completado los procedimientos de modo de seguridad en la estación móvil 380. Mientras tanto, la capa 388 de GMM conmutada de paquetes es también avisada de que se ha completado el modo de seguridad PS, utilizando el mensaje 369 procedente de la capa 384 de RRC.

De ese modo, cuando un mensaje 375 no protegido en integridad, que porta un mensaje 370 de petición de autenticación de dominio conmutado de circuitos procedente de la red 390, llega a la estación móvil 380, la estación

móvil 380 está en modo de seguridad para el dominio PS. Usando el diagrama de flujo 200 mostrado en la Figura 2, la estación móvil 380 determina que el mensaje 375 no contiene información de protección de integridad, que la protección de integridad no ha sido iniciada en el dominio CS, y de ese modo reenvía la petición de autenticación CS a la capa 386 de MM conmutada de circuitos. Generalmente hablando, el mensaje 370 de petición de autenticación podría ir seguido de un mensaje de comando de modo de seguridad conmutado de circuitos para el inicio de la protección de integridad.

Sin el diagrama de flujo 200 mostrado en la Figura 2, el mensaje 375 de petición de autenticación de dominio CS habría sido descartado por la estación móvil 380 debido a que el mensaje 375 no contenía información de protección de integridad y se habría iniciado un modo de seguridad. Al descartarse este mensaje 375 (y sus copias), se habría obtenido como resultado eventualmente una llamada interrumpida.

La Figura 4 muestra un segundo ejemplo de diagrama 400 de flujo de señal para un método de modo de seguridad en el sistema 100 de 3GPP mostrado en la Figura 1 según la primera realización. En este segundo ejemplo, en el que una estación móvil 480 está siendo preparada para recibir una llamada entrante, se inicia un mensaje 470 de petición de autenticación CS no protegido en integridad por parte de una red de núcleo 496 CS con anterioridad a que se inicie el mensaje 450 de iniciación de protección de integridad PS, pero el mensaje 470 no protegido en integridad es recibido en la estación móvil 480 después de que el mensaje 450 de iniciación de protección de integridad ha sido recibido en la estación móvil 480. En este ejemplo, en vez de descartar el mensaje 470 de petición de autenticación CS no protegido en integridad, la estación móvil 480 pasa el mensaje 470 a su capa 486 de gestión de movilidad conmutada de circuitos.

Este segundo ejemplo de diagrama 400 de flujo de señal muestra cuatro capas de una estación móvil 480: una capa 482 de control de enlace de radio (RLC), una capa 484 de control de recurso de radio (RRC), una capa 486 de gestión de movilidad (MM) de dominio conmutado de circuitos y una capa 488 de gestión de movilidad de GPRS (GMM) de dominio conmutado de paquetes. También se han mostrado cuatro capas de red 490 en el diagrama 400 de flujo de señal del segundo ejemplo. La red 490 tiene una capa 492 de control de enlace de radio (RLC) y una capa 494 de control de recurso de radio (RRC) que son contrapartida de las capas 482, 484 de RLC y de RRC de la estación móvil 480. La red 490 tiene también una red de núcleo 496 CS y una red de núcleo 498 PS, las cuales se han mostrado en la Figura 1 como red de núcleo 196 CS y red de núcleo 198 PS. Según se ha expuesto anteriormente, la red de núcleo 496 CS y la red de núcleo 498 PS operan independientemente cada una de la otra.

Inicialmente, la red de núcleo 496 CS envía un mensaje 401 de radiobúsqueda a través de la capa 494 de RRC a la capa 492 de RLC, la cual lo transmite como mensaje 405. La capa 482 de RLC de la estación móvil 480 convierte el mensaje 405 recibido y lo pasa a la capa 484 de RRC. A continuación, los mensajes establecen una conexión 410 de RRC entre la estación móvil 480 y la red 490.

La estación móvil 480 proporciona a continuación un mensaje 420 de respuesta de radiobúsqueda CS desde la capa 486 de MM hasta la capa 484 de RRC, el cual es convertido en un mensaje para la capa 482 de RLC y transmitido a la red 490. El mensaje de respuesta de radiobúsqueda CS recibido es convertido por la capa 492 de RLC y enviado a la capa 494 de RRC, y finalmente alcanza la red de núcleo 496 CS. Mientras tanto, la capa 488 de GMM de la estación móvil 480 prepara un mensaje 430 de petición de servicio PS para servicio de UMTS solamente. El mensaje inicial procedente de la capa 488 de GMM es convertido en la capa 484 de RRC y transmitido desde la capa 482 de RLC. Cuando la capa 492 de RLC de la red 490 recibe el mensaje 430, lo pasa a la capa 494 de RRC, la cual pasa a su vez una forma del mensaje a la red de núcleo 498 PS.

Aunque el mensaje 420 de respuesta de radiobúsqueda CS y el mensaje 430 de petición de servicio PS no están coordinados cada uno en relación con el otro, se activa un mensaje 470 de petición de autenticación CS posterior seguido de un comando de modo de seguridad CS (no mostrado) con la recepción del mensaje 420 de respuesta de radiobúsqueda CS en la red 490. Después de que el mensaje 420 de respuesta de radiobúsqueda CS ha sido procesado por la red de núcleo 496 CS, la red de núcleo 496 CS responde con un mensaje 470 de petición de autenticación CS. Este mensaje se inicia como mensaje 471 desde la red de núcleo 496 CS, es convertido en un mensaje 473 por la capa 494 de RRC, y puede llevar un tiempo que la capa 492 de RLC lo transmita como un mensaje 475.

Mientras tanto, la red de núcleo 498 PS ha respondido al mensaje 430 de petición de servicio PS con un mensaje 440 de petición de autenticación & cifrado PS seguido de un menaje 450 de comando de modo de seguridad PS para iniciar protección de integridad. Cuando la estación móvil 480 recibe el mensaje 450 de iniciación de protección de integridad, lo pasa a la capa 484 de RRC. La capa de RRC inicia protección de integridad y avisa a la red 490 utilizando un mensaje 460 de modo de seguridad PS completado. La capa 484 de RRC utiliza también un mensaje 469 para avisar a la capa 488 de GMM conmutada de paquetes acerca de cuándo se ha completado el modo de seguridad.

La estación móvil 480 recibe entonces el mensaje 470 de petición de autenticación CS a través del mensaje 475 después de que se ha completado el modo de seguridad PS. Usando el diagrama de flujo 200 mostrado en la Figura 2, la estación móvil 480 determina que el mensaje 475 no contiene información de protección de integridad, que la protección de integridad no ha sido iniciada en el dominio CS, y de ese modo envía la petición 470 de autenticación

a la capa 486 de MM conmutada de circuitos. Generalmente hablando, el mensaje 470 de petición de autenticación podría ir seguido de un mensaje de comando de modo de seguridad conmutado de circuitos para iniciar la protección de integridad.

Sin el diagrama de flujo 200 mostrado en la Figura 2, el mensaje 475 de petición de autenticación CS podría haber sido descartado por la estación móvil 480 debido a que el mensaje 475 no contenía información de protección de integridad y se había iniciado un modo de seguridad. El desecho de este mensaje 475 podría haber impedido que la llamada entrante telefoneara a la estación móvil 480.

Los conceptos mostrados en la Figura 2 pueden ser reproducidos para el dominio PS. La Figura 5 muestra un diagrama de flujo 500 de un método de modo de seguridad para la estación móvil 180 mostrada en la Figura 1 conforme a una segunda realización. En la etapa 510, la estación móvil 180 recibe mensaje de transferencia directa de enlace descendente (DDT) de capa 3 conmutada de paquetes (PS) procedente de una red tal como la red 190 mostrada en la Figura 1. El mensaje DDT PS podría ser un mensaje de petición de autenticación & cifrado, un mensaje de rechazo de autenticación & cifrado, un menaje de petición de identidad, un mensaje de aceptación de actualización de área de enrutamiento, un mensaje de rechazo de actualización de área de enrutamiento, un mensaje de rechazo de servicio, o uno de otros diversos tipos de mensajes de capa 3. En la etapa 520, la estación móvil 180 determina si se encuentra presente información de protección de integridad en el mensaje DDT PS. Según la Especificación Técnica 25.331 de 3GPP, un elemento de información (IE) “Integrity check info” registra convenientemente si la información de protección de integridad está en el mensaje de capa 3. En esta realización, si el IE “integrity check info” está presente, entonces existe información de protección de integridad en el mensaje DDT PS de acuerdo con la etapa 520. Si la información de protección de integridad está presente, la etapa 530 realiza protección de integridad de capa de RRC estándar sobre el mensaje DDT PS y el flujo termina en la etapa 590.

Si no está presente la información de protección de integridad en el mensaje DDT PS, la etapa 540 determina si ha sido iniciado un modo de seguridad de protección de integridad por parte de la red de núcleo PS. Si la estación móvil 180 ha recibido un mensaje de comando de modo de seguridad PS para iniciar protección de integridad, entonces ha sido iniciado un modo de seguridad de protección de integridad por la red de núcleo PS y la etapa 550 descarta el mensaje DDT PS con anterioridad a que el flujo termine en la etapa 590. Descartar el mensaje DDT PS bajo estas condiciones cumple con los requisitos de la Especificación Técnica 25.331 de 3GPP. Alternativamente, si se modificó la variable INTEGRITY_PROTECTION_INFO para que incluyera estados separados de iniciados y no iniciados para los dominios CS y PS, la etapa 540 podría ser determinada comprobando la variable de INTEGRITY_PROTECTION_INFO de la estación móvil.

Si la etapa 540 determina que no ha sido iniciado un modo de seguridad de protección de integridad por la red de núcleo PS (por ejemplo, solamente ha sido iniciado un modo de seguridad por la red de núcleo CS o ninguna red de núcleo ha iniciado un modo de seguridad), la etapa 560 envía el mensaje DDT PS a la capa de GMM conmutada de paquetes de la estación móvil 180 antes de que termine el flujo en la etapa 590. Puesto que la Especificación Técnica 24.008 de 3GPP proporciona flexibilidad para procesar un mensaje de capa 3 no protegido en integridad en un dominio particular cuando no ha sido iniciada protección de integridad para ese dominio, el diagrama de flujo 500 impide que una llamada se interrumpa cuando un mensaje de señalización de capa 3 y un mensaje de iniciación de protección de integridad son recibidos desordenados.

La Figura 6 muestra un tercer ejemplo de diagrama 600 de flujo de señal para un método de modo de seguridad en un sistema de 3GPP mostrado en la Figura 1 conforme a la segunda realización. En este tercer ejemplo, un mensaje 670 de petición de autenticación & cifrado PS no protegido en integridad es iniciado por una red de núcleo 698 PS con anterioridad a que se inicie un mensaje 650 de iniciación de protección de integridad, pero el mensaje 670 no protegido en integridad es recibido en la estación móvil 680 después de que el mensaje 650 de iniciación de protección de integridad ha sido recibido en la estación móvil 680. En este ejemplo, cuando una estación móvil 680 está iniciando una llamada, en vez de descartar el mensaje 670 de petición de autenticación & cifrado PS no protegido en integridad, la estación móvil 680 pasa el mensaje 670 a su capa de gestión de movilidad de dominio conmutada de paquetes, la capa 688 de GMM.

Este diagrama 600 de flujo de señal del tercer ejemplo muestra cuatro capas de una estación móvil 680: una capa 682 de control de enlace de radio (RLC), una capa 684 de control de recurso de radio (RRC), una capa 686 de gestión de movilidad (MM) de dominio conmutado de circuitos, y una capa 688 de gestión de movilidad de GPRS (GMM) de dominio conmutado de paquetes. También ha sido mostrada una red 690 en el diagrama 600 de flujo de señal del tercer ejemplo. La red 690 tiene una capa 692 de control de enlace de radio (RLC) y una capa 694 de control de recurso de radio (RRC) que son contrapartidas de las capas 682, 684 de RLC y de RRC de la estación móvil 680. La red 690 tiene también una red de núcleo 696 CS y una red de núcleo 698 PS, las cuales se han mostrado en la Figura 1 como red de núcleo 196 CS y red de núcleo 198 PS. Según se ha expuesto anteriormente, la red de núcleo 696 CS y la red de núcleo 698 PS operan independientemente cada una de la otra.

Después de que se ha establecido una conexión de RRC entre la estación móvil 680 y la red 690 utilizando varios mensajes 610, se genera un mensaje 620 de actualización de localización CS por parte de la capa 686 de MM que se pasa a la capa 684 de RRC para su reempaquetamiento, y es transmitido desde la capa 682 de RLC de la estación móvil 680. El mensaje 620 es recibido en la capa 692 de RLC de la red, convertido y enviado a la capa 694 de RRC, la cual reenvía el mensaje a la red de núcleo 696 CS para su procesamiento. En el dominio de

conmutación de paquetes, se genera un mensaje 630 de petición de unión en la capa 688 de GMM, que es reempaquetado en la capa 684 de RRC, y transmitido desde la estación móvil 680 a través de la capa 682 de RLC. La capa 692 de RLC de la red 690 recibe el mensaje 630, lo convierte para la capa 694 de RRC, la cual lo reenvía a la red de núcleo 698 PS. El mensaje 620 de actualización de localización CS y el mensaje 630 de petición de unión PS no están coordinados entre sí, y pueden ocurrir en cualquier secuencia de tiempo. En respuesta al mensaje 630 de petición de unión PS, la red 690 envía un mensaje 670 de petición de autenticación & cifrado PS. La petición de autenticación & cifrado se genera mediante la red de núcleo 698 PS como mensaje 671, y es empaquetado por la capa 694 de RRC como mensaje 673. Dependiendo del tamaño y de la prioridad del mensaje 673, puede transcurrir algún tiempo antes de que la capa de RLC de la red 690 transmita un mensaje 675 no protegido en integridad que contenga el mensaje 670 de petición de autenticación & cifrado PS.

Mientras tanto, en respuesta al mensaje 620 de actualización de localización CS, la red de núcleo 696 CS ha enviado un mensaje 640 de petición de autenticación CS seguido de un mensaje 650 de comando de modo de seguridad CS que direcciona el inicio de protección de integridad. Cuando el mensaje 650 de comando de modo de seguridad CS es recibido por la estación móvil 680 en la capa 682 de RLC y se pasa a la capa 684 de RRC, la estación móvil 680 inicia la protección de integridad. Cuando los procedimientos de modo de seguridad se han completado en la estación móvil 680, se envía un mensaje 660 de modo de seguridad completado a la red 690. Mientras tanto, se avisa también a la capa 686 de MM de dominio conmutado de circuitos de que el modo de seguridad CS ha sido completado, utilizando el mensaje 669 desde la capa 684 de RRC.

De ese modo, cuando el mensaje 675 no protegido en integridad que porta un mensaje 670 de petición de autenticación & cifrado procedente de la red 690, llega a la estación móvil 680, la estación móvil 680 está en modo de seguridad para el dominio CS. Utilizando el diagrama de flujo 500 mostrado en la Figura 5, la estación móvil 680 determina que el mensaje 675 no contiene información de protección de integridad, que la protección de integridad no ha sido iniciada en el dominio PS, y así reenvía el mensaje 670 de petición de autenticación & cifrado de PS a la capa 688 de GMM. Generalmente hablando, el mensaje 670 de petición de autenticación & cifrado podría ir seguido por un mensaje de comando de modo de seguridad conmutado de paquetes para el inicio de la protección de integridad.

Sin el diagrama de flujo 500 mostrado en la Figura 5, el mensaje 675 de petición de autenticación & cifrado de dominio conmutado de paquetes habría sido descartado por la estación móvil 680 debido a que el mensaje 675 no contenía información de protección de integridad y habría sido iniciado un modo de seguridad. Descartar este mensaje 675 (y sus copias) habría dado como resultado eventualmente una llamada interrumpida.

De ese modo, un método de modo de seguridad cumple con las especificaciones técnicas de 3GPP y distingue aún más entre modos de seguridad en dominios diferentes. Si un dispositivo móvil recibe un mensaje sin protección de integridad en un dominio, y se determina que no se ha iniciado un modo de seguridad para ese dominio, entonces el mensaje puede ser procesado por el dispositivo móvil. Diferenciando entre modos de seguridad en dominios diferentes, se pueden reducir las llamadas interrumpidas, especialmente para situaciones en que los mensajes de capa 3 en un dominio son recibidos después de mensajes de iniciación de protección de integridad procedentes de otro dominio, lo que es muy posible cuando se están estableciendo concurrentemente conexiones PS y CS.

Aunque esta descripción incluye lo que se ha considerado que actualmente son realizaciones preferidas y mejores modos de la invención descrita de una manera que establece posesión de la misma por los inventores y que permite a los expertos en la materia hacer uso de la invención, se comprenderá y se apreciará que existen muchos equivalentes respecto a las realizaciones preferidas descritas en la presente memoria, y que las modificaciones y variaciones pueden hacerse sin apartarse del alcance de la invención, las cuales no están limitadas por las realizaciones preferidas sino por las reivindicaciones anexas, incluyendo las correcciones realizadas durante la tramitación de la presente solicitud y de todos los equivalentes de las reivindicaciones según han sido redactadas.

Se comprende además que el uso de términos de relación tales como primero y segundo, y similares, se utilizan únicamente para distinguir una entidad, artículo o acción de otra sin que necesariamente se requiera, o implique, ninguna relación real u orden entre tales entidades, artículos o acciones. Gran parte de la funcionalidad inventiva y muchos de los principios inventivos son mejor implementados con, o en, programas o instrucciones de software. Se espera que cualquier experto en la materia, a pesar de un esfuerzo posiblemente significativo y de muchas opciones de diseño motivadas, por ejemplo, por tiempo disponible, tecnología actual y consideraciones económicas, cuando está guiado por los conceptos y principios descritos en la presente memoria, sea fácilmente capaz de generar tales instrucciones y programas de software con experimentación mínima. Por lo tanto, la discusión adicional de ese software, si la hay, será limitada en interés de la brevedad y de la minimización de cualquier riesgo de oscurecer los principios y los conceptos conforme a la presente invención.

REIVINDICACIONES

1.- Un método de modo de seguridad que comprende establecer (610) una conexión de control de recurso de radio entre una estación móvil y una red, recibir (650) un mensaje de iniciación de modo de seguridad para un primer dominio desde la red en la estación móvil, y completar (660) la iniciación de modo de seguridad por medio de la estacón móvil, estando el método caracterizado por:

recibir (675), en la estación móvil, un mensaje de capa 3 para un segundo dominio desde la red, y

reenviar el mensaje de capa 3 a una capa de gestión de movilidad de la estación móvil para el segundo dominio.

2.- Un método de modo de seguridad según la reivindicación 1, en donde el primer dominio es conmutado de circuitos (196) y el segundo dominio es conmutado de paquetes (198).

3.- Un método de modo de seguridad según la reivindicación 1, en donde el primer dominio es conmutado de paquetes (198) y el segundo dominio es conmutado de circuitos (196).

4.- Un método de modo de seguridad según la reivindicación 1, en donde el mensaje de capa 3 es una petición de autenticación (670).

5.- Un método de modo de seguridad según la reivindicación 4, en donde el mensaje de capa 3 es una petición de autenticación para un dominio (470) conmutado de circuitos.

6.- Un método de modo de seguridad según la reivindicación 4, en donde la petición de autenticación es una petición de autenticación & cifrado para un dominio (670) conmutado de paquetes.

7.- Un método de modo de seguridad según la reivindicación 1, que comprende además:

recibir, en la estación móvil, un mensaje de capa 3 para el primer dominio desde la red, con anterioridad a recibir un mensaje de iniciación de modo de seguridad para un primer dominio desde la red.

8.- Un método de modo de seguridad según la reivindicación 1, que comprende además:

recibir, en la estación móvil, un mensaje de iniciación de modo de seguridad para el segundo dominio desde la red.

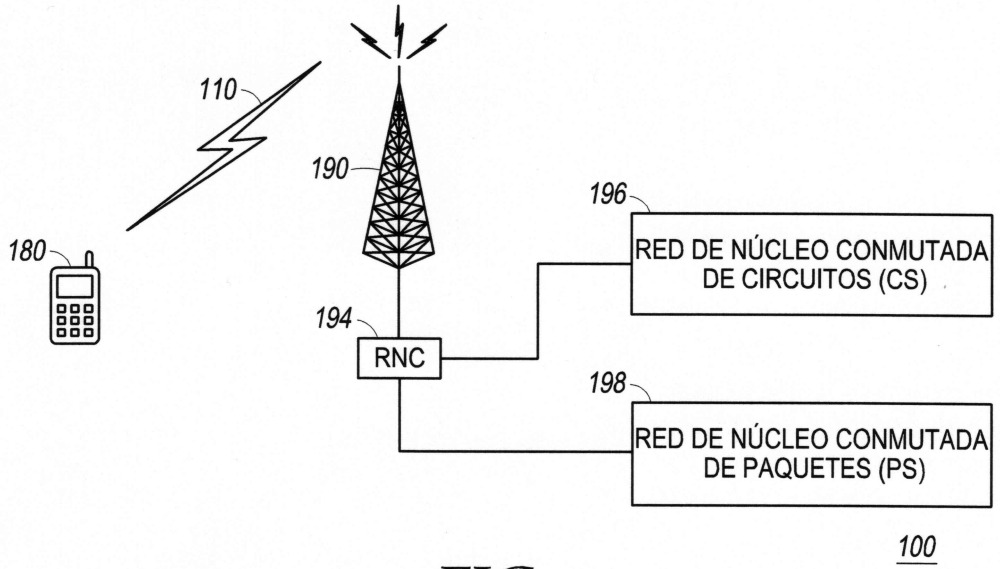
110
190
196
RED DE NÚCLEO CONMUTADA DE CIRCUITOS (CS)
180
194
RNC
198
RED DE NÚCLEO CONMUTADA DE PAQUETES (PS)
100

FIG. 1

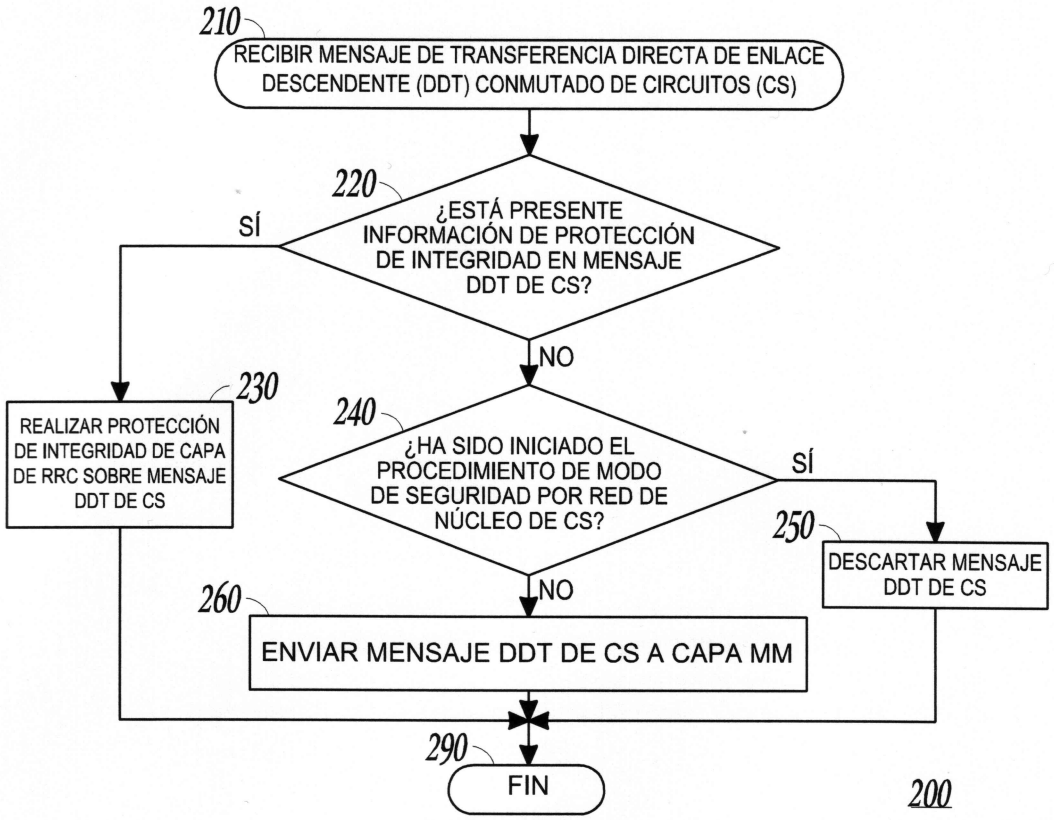
210
RECIBIR MENSAJE DE TRANSFERENCIA DIRECTA DE ENLACE DESCENDENTE (DDT) CONMUTADO DE CIRCUITOS (CS)
220
¿ESTÁ PRESENTE INFORMACIÓN DE PROTECCIÓN DE INTEGRIDAD EN MENSAJE DDT DE CS?
SÍ
NO
230
REALIZAR PROTECCIÓN DE INTEGRIDAD DE CAPA DE RRC SOBRE MENSAJE DDT DE CS
240
¿HA SIDO INICIADO EL PROCEDIMIENTO DE MODO DE SEGURIDAD POR RED DE NÚCLEO DE CS?
SÍ
250
DESCARTAR MENSAJE DDT DE CS
NO
260
ENVIAR MENSAJE DDT DE CS A CAPA MM
290
FIN
200

FIG. 2

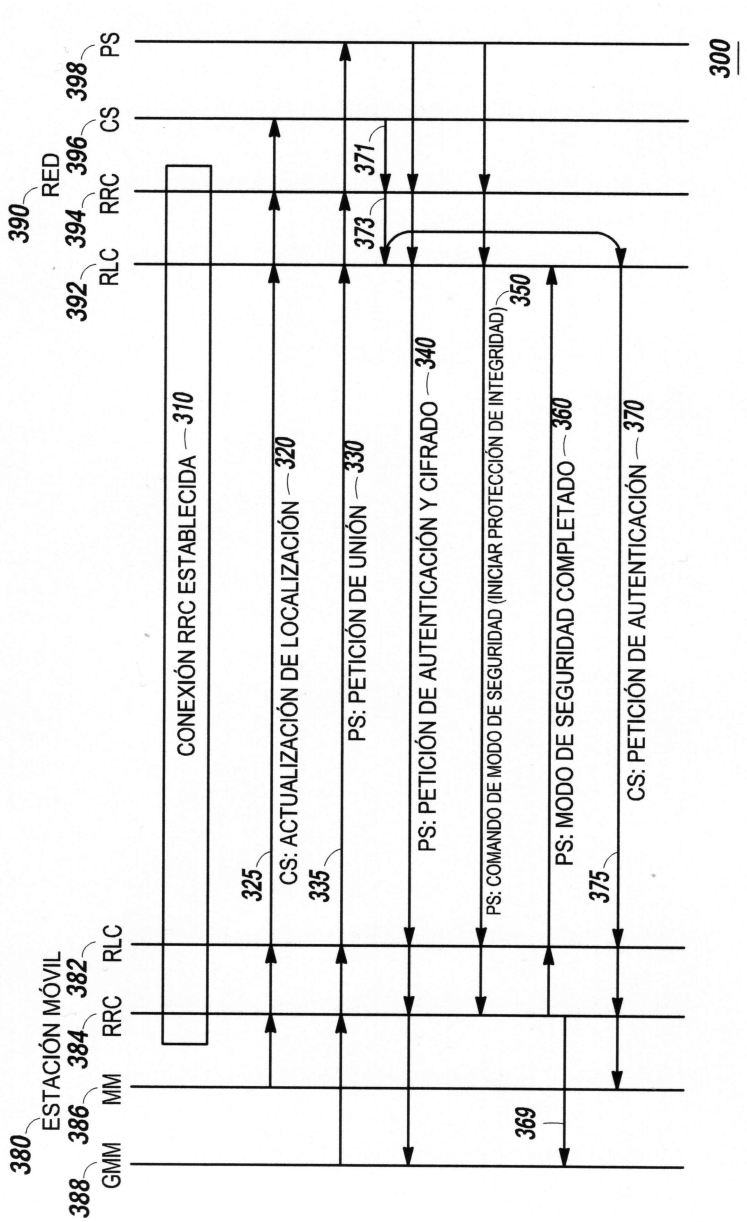
300
380 ESTACIÓN MÓVIL
388 GMM
386 MM
384 RRC
382 RLC
390 RED
398 PS
396 CS
394 RRC
392 RLC
CONEXIÓN RRC ESTABLECIDA 310
325
CS: ACTUALIZACIÓN DE LOCALIZACIÓN 320
335
PS: PETICIÓN DE UNIÓN 330
371
373
PS: PETICIÓN DE AUTENTICACIÓN Y CIFRADO 340
PS: COMANDO DE MODO DE SEGURIDAD (INICIAR PROTECCIÓN DE INTEGRIDAD) 350
PS: MODO DE SEGURIDAD COMPLETADO 360
369
375
CS: PETICIÓN DE AUTENTICACIÓN 370

FIG. 3

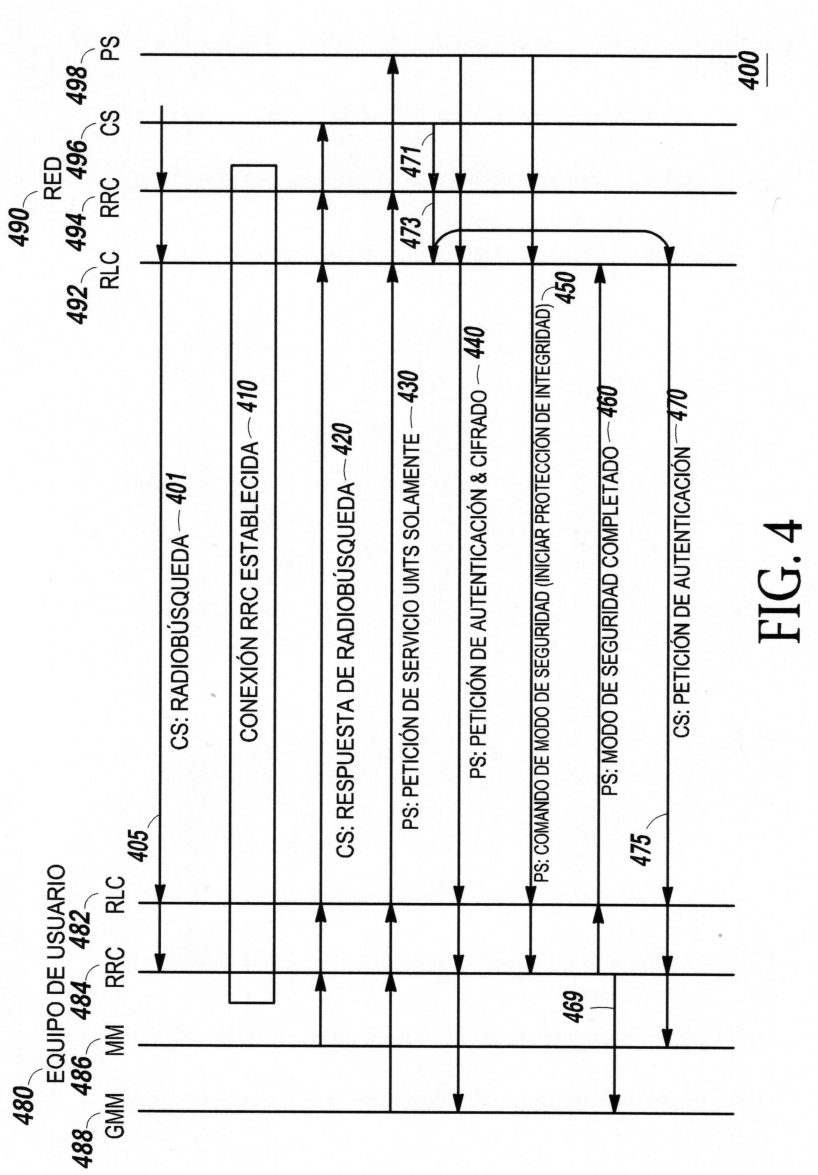
400
EQUIPO DE USUARIO
480
GMM
488
MM
486
RRC
484
RLC
482
RED
490
RLC
492
RRC
494
CS
496
PS
498
405
CS: RADIOBÚSQUEDA 401
CONEXIÓN RRC ESTABLECIDA 410
CS: RESPUESTA DE RADIOBÚSQUEDA 420
PS: PETICIÓN DE SERVICIO UMTS SOLAMENTE 430
PS: PETICIÓN DE AUTENTICACIÓN & CIFRADO 440
PS: COMANDO DE MODO DE SEGURIDAD (INICIAR PROTECCIÓN DE INTEGRIDAD) 450
PS: MODO DE SEGURIDAD COMPLETADO 460
CS: PETICIÓN DE AUTENTICACIÓN 470
471
473
469
475

FIG. 4

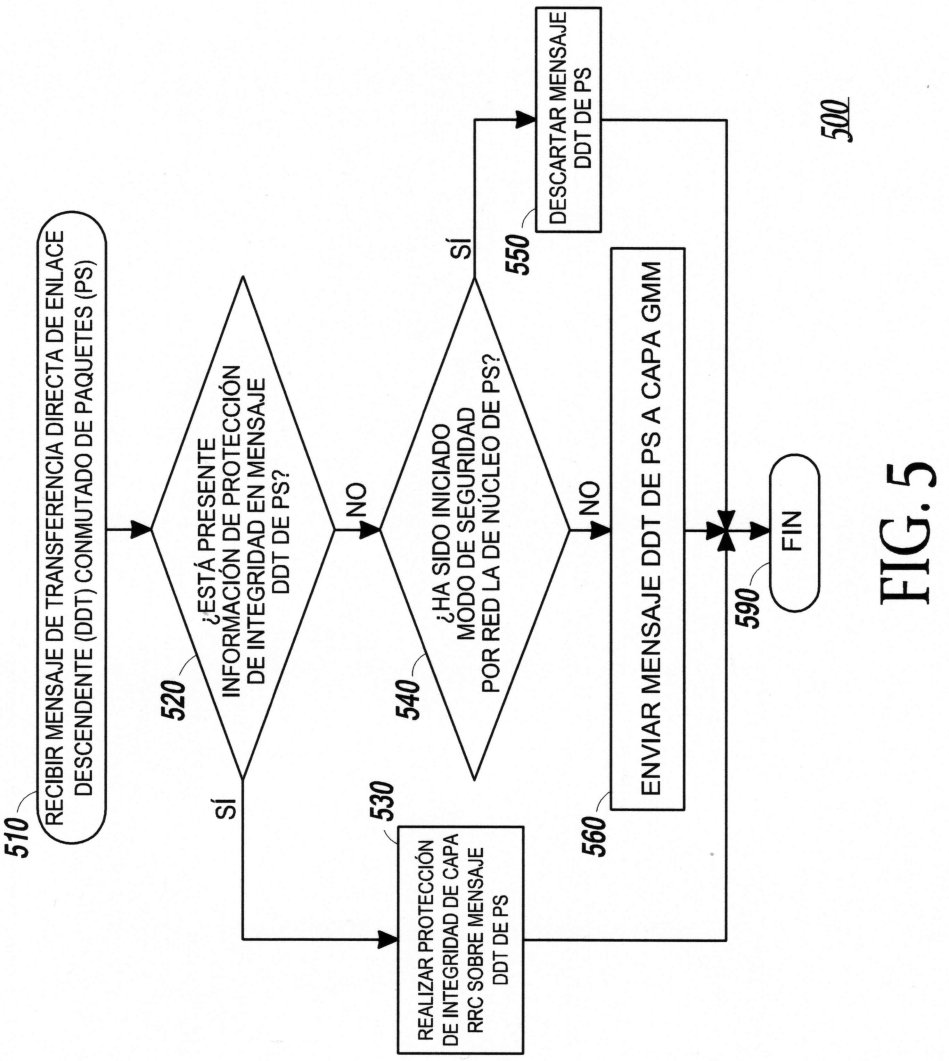
500
510
RECIBIR MENSAJE DE TRANSFERENCIA DIRECTA DE ENLACE DESCENDENTE (DDT) CONMUTADO DE PAQUETES (PS)
520
¿ESTÁ PRESENTE INFORMACIÓN DE PROTECCIÓN DE INTEGRIDAD EN MENSAJE DDT DE PS?
SÍ
NO
530
REALIZAR PROTECCIÓN DE INTEGRIDAD DE CAPA RRC SOBRE MENSAJE DDT DE PS
540
¿HA SIDO INICIADO MODO DE SEGURIDAD POR RED LA DE NÚCLEO DE PS?
SÍ
NO
550
DESCARTAR MENSAJE DDT DE PS
560
ENVIAR MENSAJE DDT DE PS A CAPA GMM
590
FIN

FIG. 5

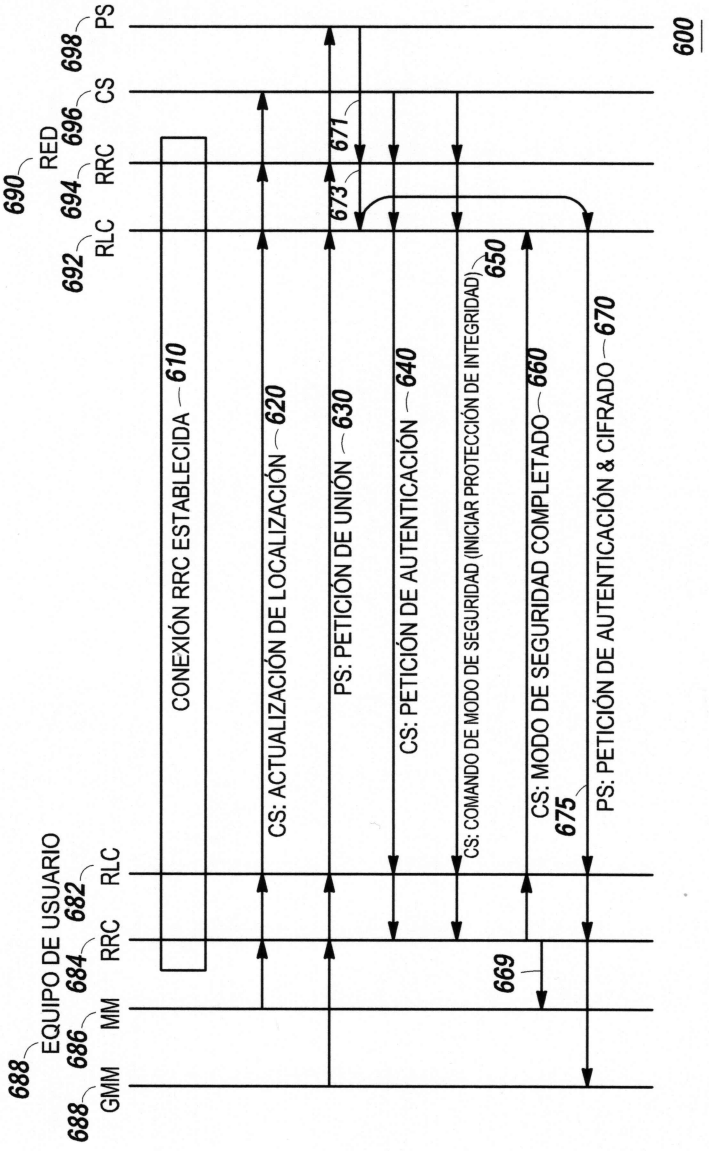
600
688 EQUIPO DE USUARIO
688 GMM
686 MM
684 RRC
682 RLC
692 RLC
694 RRC
696 CS
698 PS
690 RED
CONEXIÓN RRC ESTABLECIDA 610
CS: ACTUALIZACIÓN DE LOCALIZACIÓN 620
PS: PETICIÓN DE UNIÓN 630
CS: PETICIÓN DE AUTENTICACIÓN 640
CS: COMANDO DE MODO DE SEGURIDAD (INICIAR PROTECCIÓN DE INTEGRIDAD) 650
CS: MODO DE SEGURIDAD COMPLETADO 660
PS: PETICIÓN DE AUTENTICACIÓN & CIFRADO 670
669
671
673
675

FIG. 6