(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 395 946**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/56 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.07.2006 E 06014566 (1)**

(97) Fecha y número de publicación de la concesión europea: **19.09.2012 EP 1753183**

(54) Título: **Método de comprobación de integridad en redes inalámbricas protegidas**

(30) Prioridad:

08.08.2005 US 199348

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.02.2013

(73) Titular/es:

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

(72) Inventor/es:

HUI, ZHAO y
PUTCHA, PADMAJA

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Método de comprobación de integridad en redes inalámbricas protegidas

Campo de la descripción

Esta descripción se refiere de manera general a comunicaciones radiotelefónicas y, en particular, a la comprobación de integridad de mensajes de señalización en una estación móvil.

Antecedentes de la descripción

De acuerdo con la Especificación Técnica 25.331 del Proyecto de Cooperación 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 recursos radio (RRC). El estado de protección de integridad puede ser o bien "no iniciado" o bien "iniciado". Si la variable INTEGRITY_PROTECTION_INFO tiene el valor "iniciado", cualquier mensaje de RRC recibido por la MS se comprobará para una "información de comprobación de Integridad" del elemento de información (IE). Si la "información de comprobación de Integridad" del IE no está presente, la MS descartará el mensaje.

De acuerdo con la Especificación Técnica 24.008 del 3GPP, la señalización protegida de integridad es obligatoria cuando una estación móvil está en un modo conectado de UMTS con una red. Hay algunas excepciones, no obstante, al requerimiento de que todos los mensajes de señalización de capa 3 estén protegidos de integridad. Por ejemplo, los mensajes de "petición de autentificación" del dominio de circuitos conmutados (CS) y "petición de autentificación y cifrado" del dominio de paquetes conmutados (PS) no necesitan estar protegidos de integridad. De esta manera, estos tipos de mensajes pueden estar omitiendo la "información de comprobación de Integridad" del IE.

Cuando las conexiones del dominio de CS y dominio de PS entre una red y una estación móvil se están estableciendo concurrentemente, se puede recibir un mensaje de capa 3 no protegido de integridad del dominio en la estación móvil después de otro mensaje del dominio que inicia la protección de integridad. El requerimiento de la Especificación Técnica 25.331 del 3GPP puede provocar a una MS descartar el mensaje de capa 3 no protegido de integridad. La consecuencia de este descarte puede provocar una incapacidad de completar una llamada. Por ejemplo, si un mensaje de "petición de autentificación" del dominio de CS (y su copia) se descarta consecuentemente por la MS, entonces la llamada no puede completarse y se caerá finalmente.

En otras palabras, cuando se recibe un mensaje de capa 3 no protegido de integridad en un dominio por una MS después de un comando para iniciar la protección de integridad en otro dominio, la MS descarta el mensaje de capa 3 no protegido de integridad. Por otra parte, si el mismo mensaje de capa 3 no protegido de integridad en un dominio fue recibido por la MS antes del comando para iniciar la protección de integridad en otro dominio, entonces la MS procesa adecuadamente el mensaje de capa 3 no protegido de integridad. Debido a que los mensajes de RRC (Estrato de Acceso) y los mensajes de capa 3 (Estrado de No Acceso) usan diferentes portadores radio y tiene diferentes prioridades, hay un riesgo real de que un mensaje no protegido de integridad para un dominio y un mensaje de iniciación de protección de integridad para otro dominio se recibirán fuera de servicio por una MS.

La US 2003/236085 A1 revela un equipo de usuario (UE) que puede procesar dos mensajes de RRC uno independientemente del otro, cada uno de los cuales puede contener un valor START para el mismo dominio. Un método para la reconfiguración del modo de seguridad se conoce a partir de la US 2003/0100291 A1.

Hay una oportunidad para una MS para procesar mensajes de capa 3 no protegido de integridad fuera de servicio e iniciación de protección de integridad para reducir el número de llamadas caídas. Esto se logra mediante el método de la reivindicación 1. Los diversos aspectos, rasgos y ventajas de la descripción llegarán a ser evidentes más plenamente a aquellos que tienen experiencia habitual en la técnica tras la consideración cuidadosa de los siguientes Dibujos y la Descripción Detallada anexa.

Breve descripción de los dibujos

La FIG. 1 muestra un sistema 3GPP simplificado con una estación móvil y una red de acuerdo con una realización.

La FIG. 2 muestra un diagrama de flujo de un método de modo de seguridad para la estación móvil mostrada en la FIG. 1 de acuerdo con una primera realización.

La FIG. 3 muestra un primer diagrama de flujo de señal ejemplo para un método de modo de seguridad en el sistema 3GPP mostrado en la FIG. 1 de acuerdo con la primera realización.

La FIG. 4 muestra un segundo diagrama de flujo de señal ejemplo para un método de modo de seguridad en el sistema 3GPP mostrado en la FIG. 1 de acuerdo con la primera realización.

La FIG. 5 muestra un diagrama de flujo de un método de modo de seguridad para la estación móvil mostrada en la FIG. 1 de acuerdo con una segunda realización.

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

Descripción detallada

Tanto en los dominios de circuitos conmutados (CS) y los de paquetes conmutados (PS), una red central puede iniciar un mensaje de señalización de capa 3 no protegido de integridad antes de iniciar un mensaje de control de recursos radio (RRC) para iniciar la protección de integridad. Cuando tanto una red central de CS como una red central de PS están estableciendo concurrentemente una conexión con una estación móvil (MS), un mensaje de señalización de capa 3 no protegido de integridad para un dominio puede llegar a una MS o bien antes o bien después de un mensaje de iniciación de protección de integridad para otro dominio. Debido a que los mensajes de RRC (Estrato de Acceso) y mensajes de capa 3 (Estrato de No Acceso) se envían con diferentes prioridades sobre diferentes portadores radio, hay un riesgo real de que un MS recibirá un mensaje de señalización de capa 3 no protegido de integridad para un dominio después de recibir un mensaje de RRC (Estrato de Acceso) para iniciar la protección de integridad en otro dominio.

Un método de modo de seguridad de estación móvil recibe un mensaje de capa 3 o bien en el dominio de paquetes conmutados (PS) o bien de circuitos conmutados (CS), determina si el mensaje de capa 3 está protegido de integridad, determina si la protección de integridad se ha iniciado en ese dominio, y reenvía el mensaje de capa 3 a la capa de gestión de movilidad del dominio adecuado en la MS si el mensaje de capa 3 no está protegido de integridad y la protección de integridad no se ha iniciado en ese dominio. Si la protección de integridad se ha iniciado en ese dominio, entonces se descarta el mensaje de capa 3. Este método acomoda una situación en que una MS recibe un mensaje de capa 3 no protegido de integridad para un dominio después de recibir un mensaje de iniciación de protección de integridad en otro dominio.

La FIG. 1 muestra un sistema 3GPP simplificado 100 con una estación móvil 180 y una red 190 de acuerdo con una realización. En las realizaciones discutidas, se muestra un sistema de comunicación inalámbrico 3GPP; no obstante, los principios revelados se pueden aplicar a otros tipos de sistemas de comunicación inalámbricos que incluyen versiones futuras del sistema 3GPP. La estación móvil 180, algunas veces referida como un dispositivo móvil o equipo de usuario (UE), puede ser un radioteléfono, ordenador portátil con conexión inalámbrica, dispositivo de mensajería inalámbrico, u otro tipo de dispositivo de comunicación inalámbrico compatible con la red 190.

La red 190 incluye una red central de circuitos conmutados (CS) 196 así como una red central de paquetes conmutados (PS) 198. La red central de CS 196 y la red central de PS 198 funcionan independientemente una de la otra. Por ejemplo, la red central de PS puede iniciar la protección de integridad en un momento, y la red central de CS puede iniciar la protección de integridad en un momento posterior que no está coordinado con la iniciación de la protección de integridad de la red central de PS. La red central de CS 196 y la red central de PS 198 llegan juntas a un control de recursos radio (RRC) de Controlador de Red Radio (RNC) 194 y una entidad de control de enlace radio (RLC) dentro de la red 190 y de esta manera tanto los mensajes de PS como de CS se transmiten a través de un enlace de comunicación inalámbrico 110 a la estación móvil 180. La estación móvil 180 comunica con la red 190 a través del enlace de comunicación inalámbrico 110 también.

La FIG. 2 muestra un diagrama de flujo 200 de un método de modo de seguridad para la estación móvil 180 mostrada en la FIG. 1 de acuerdo con una primera realización. En el paso 210, la estación móvil 180 recibe el mensaje de transferencia directa de enlace descendente (DDT) de capa 3 de circuitos conmutados (CS) desde una red tal como la red 190 mostrada en la FIG. 1. El mensaje de DDT de CS podría ser un mensaje de petición de autentificación, un mensaje de rechazo de autentificación, un mensaje de petición de identidad, un mensaje de aceptación de actualización de ubicación, un mensaje de rechazo de actualización de ubicación, un mensaje de abortar, o un mensaje de otros diversos tipos de mensajes de capa 3. En el paso 220, la estación móvil 180 determina si la información de protección de integridad está presente en el mensaje de DDT de CS. De acuerdo con la Especificación Técnica 25.331 del 3GPP, una “información de comprobación de Integridad” del elemento de información (IE) indica convenientemente si la información de comprobación de integridad está en el mensaje de capa 3. En esta realización, si la “información de comprobación de Integridad” del IE está presente, entonces hay información de protección de integridad presente en el mensaje de DDT de CS de acuerdo con el paso 220. Si está presente la información de protección de integridad, el paso 230 realiza la protección de integridad de capa de RRC estándar en el mensaje DDT de CS y el flujo finaliza en el paso 290.

Si la información de protección de integridad no está presente en el mensaje de DDT de CS, el paso 240 determina si se ha iniciado un procedimiento de modo de seguridad de protección de integridad por la red central de CS. Si la estación móvil 180 ha recibido un mensaje de comando de modo de seguridad de CS para iniciar la protección de integridad, entonces se ha iniciado un procedimiento de modo de seguridad de protección de integridad por la red central de CS y el paso 250 descarta el mensaje de DDT de CS antes de que el flujo finalice en el paso 290. Descartar el mensaje de DDT de CS bajo estas condiciones cumple los requerimientos de la Especificación Técnica 25.331 del 3GPP. Alternativamente, si la variable INTEGRITY_PROTECTION_INFO fue modificada para incluir estados iniciados y no iniciados separados para los dominios de CS y el de PS, el paso 240 se podría determinar comprobando la variable INTEGRITY_PROTECTION_INFO de la estación móvil.

Si el paso 240 determina que un procedimiento de modo de seguridad de protección de integridad no se ha iniciado por la red central de CS (por ejemplo, un modo de seguridad solamente se ha iniciado por la red central de PS o que tampoco la red central ha iniciado un modo de seguridad), el paso 260 reenvía el mensaje de DDT de CS a la capa de gestión de movilidad (MM) de circuitos conmutados de la estación móvil 180 antes de que el flujo finalice en el paso 290. Debido a que la Especificación Técnica 24.008 del 3GPP proporciona flexibilidad para procesar un mensaje de capa 3 no protegido de integridad en un dominio particular cuando la protección de integridad para ese dominio no se ha iniciado, el diagrama de flujo 200 impide que se caiga una llamada cuando un mensaje de señalización de capa 3 y un mensaje de iniciación de protección de integridad se reciben fuera de servicio.

La FIG. 3 muestra un primer diagrama de flujo de señal ejemplo 300 para un método de modo de seguridad en el sistema 3GPP 100 mostrado en la FIG. 1 de acuerdo con la primera realización. En este primer ejemplo, un mensaje de petición de autentificación de CS no protegido de integridad 370 se inicia por una red central de CS 396 antes de que se inicie un mensaje de iniciación de protección de integridad 350 por una red central de PS, pero el mensaje no protegido de integridad 370 se recibe en la estación móvil 380 después de que se recibe el mensaje de iniciación de protección de integridad 350 en la estación móvil 380. En este ejemplo, cuando una estación móvil 380 está iniciando una llamada, en lugar de descartar el mensaje de petición de autentificación de CS no protegido de integridad 370, la estación móvil 380 pasa el mensaje 370 a su capa de gestión de movilidad (MM) de dominio de circuitos conmutados 386.

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

También se muestran cuatro capas de una red 390 en el primer diagrama de flujo de señal ejemplo 300. La red 390 tiene una capa de control de enlace radio (RLC) 392 y una capa de control de recursos radio (RRC) 394 las cuales son contrapartidas a las capas de RLC y de RRC 382, 384 en la estación móvil 380. La red 390 también tiene una red central de CS 396 y una red central de PS 398, las cuales se muestran en la FIG. 1 como la red central de CS 196 y la red central de PS 198. Como se indicó previamente, la red central de CS 396 y la red central de PS 398 funcionan independientemente una de la otra.

Después de que se establece una conexión de RRC entre la estación móvil 380 y la red 390 usando varios mensajes 310, se genera un mensaje de actualización de ubicación de CS 320 por la capa de MM de circuitos conmutados 386 y se pasa a la capa de RRC 384, se vuelve a empaquetar para la capa de RLC 382, y se transmite desde la capa de RLC de la estación móvil 380 como el mensaje 325. El mensaje 325 se recibe en la capa de RLC 392 de la red, se convierte y se envía a la capa de RRC 394, la cual reenvía el mensaje a la red central de CS 396 para procesamiento. En el lado de conmutación por paquetes, un mensaje de petición de adjunto 330 se genera en la capa de GMM de paquetes conmutados 388, se vuelve a empaquetar en la capa de RRC 384, y se transmite desde la estación móvil 380 a través de la capa de RLC 382 como el mensaje 335. La capa de RLC 392 de la red 390 recibe el mensaje 335 y lo convierte para la capa de RRC 394, la cual entonces lo procesa y lo reenvía a la red central de PS 398. El mensaje de actualización de ubicación de CS 320 y el mensaje de petición de adjunto de PS 330 no están coordinados uno con el otro y puede ocurrir en cualquier secuencia de tiempo.

En respuesta al mensaje de actualización de ubicación de CS 320, la red 390 envía un mensaje de petición de autentificación de CS no protegido de integridad 370 seguido por un comando de modo de seguridad de CS (no se muestra) para iniciar la protección de integridad. La petición de autentificación se genera por la red central de CS 396 como el mensaje 371, y se empaqueta por la capa de RRC 394 como el mensaje 373. Dependiendo del tamaño y prioridad del mensaje 373, puede transcurrir algún tiempo antes de que la capa de RLC 392 de la red 390 transmita un mensaje no protegido de integridad 375 que contiene el mensaje de petición de autentificación de CS 370. Mientras tanto, en respuesta al mensaje de petición de adjunto 330, la red central de PS 398 ha iniciado un mensaje de petición de autentificación y cifrado 340 seguido por un comando de modo de seguridad 350 para iniciar la protección de integridad. La estación móvil 380 inicia la protección de integridad y prepara un mensaje completo de modo de seguridad 360 para la capa de RLC 382 cuando los procedimientos de modo de seguridad se completan en la estación móvil 380. Mientras tanto, también se notifica a la capa de GMM de paquetes conmutados 388 que el modo de seguridad de PS se ha completado usando el mensaje 369 desde la capa de RRC 384.

Así cuando el mensaje no protegido de integridad 375 que porta un mensaje de petición de autentificación del dominio de circuitos conmutados 370 desde la red 390 llega a la estación móvil 380, la estación móvil 380 está en modo de seguridad para el dominio de PS. Usando el diagrama de flujo 200 mostrado en la FIG. 2, la estación móvil 380 determina que el mensaje 375 no contiene información de protección de integridad, que la protección de integridad no se ha iniciado en el dominio de CS, y de esta manera reenvía la petición de autentificación de CS a la capa de MM de circuitos conmutados 386. Hablando en términos generales, el mensaje de petición de autentificación 370 sería seguido por un mensaje de comando de modo de seguridad de circuitos conmutados para iniciar la protección de integridad.

Sin el diagrama de flujo 200 mostrado en la FIG. 2, el mensaje de petición de autentificación del dominio de CS 375 se habría descartado por la estación móvil 380 debido a que el mensaje 375 no contenía información de protección de integridad y un modo de seguridad se ha iniciado. Descartar este mensaje 375 (y sus copias) habría provocado eventualmente una llamada caída.

La FIG. 4 muestra un diagrama de flujo de señal ejemplo 400 para un método de modo de seguridad en el sistema 3GPP 100 mostrado en la FIG. 1 de acuerdo con la primera realización. En este segundo ejemplo, donde una estación móvil 480 está siendo buscada en preparación para recibir una llamada entrante, se inicia un mensaje de petición de autentificación de CS no protegido de integridad 470 por una red central de CS 496 antes de que se inicie un mensaje de iniciación de protección de integridad de PS, excepto que el mensaje no protegido de integridad 470 se reciba en la estación móvil 480 después de que el mensaje de iniciación de protección de integridad 450 se reciba en la estación móvil 480. En este ejemplo, en lugar de descartar el mensaje de petición de autentificación de CS no protegido de integridad 470, la estación móvil 480 pasa el mensaje 470 a su capa de gestión de movilidad de circuitos conmutados 486.

Este segundo diagrama de flujo de señal ejemplo 400 muestra cuatro capas de una estación móvil 480: una capa de control de enlace radio (RLC) 482, una capa de control de recursos radio (RRC) 484, una capa de gestión de movilidad (MM) de circuitos conmutados 486, y una capa de gestión de movilidad de GPRS (GMM) del dominio de paquetes conmutados 488. También se muestran cuatro capas de red 490 en el segundo diagrama de flujo de señal ejemplo 400. La red 490 tiene una capa de control de enlace radio (RLC) 492 y una capa de control de recursos radio (RRC) 494 las cuales son contrapartidas a las capas de RLC y RRC 482, 484 en la estación móvil 480. La red 490 también tiene una red central de CS 496 y una red central de PS 498, las cuales se muestran en la FIG. 1 como red central de CS 196 y red central de PS 198. Como se indicó previamente, la red central de CS 496 y la red central de PS 498 funcionan independientemente una de otra.

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

La estación móvil 480 entonces proporciona un mensaje de respuesta de búsqueda de CS 420 desde la capa de MM 486 a la capa de RRC 484, el cual se convierte a un mensaje para la capa de RLC 482 y se transmite a la red 490. El mensaje de respuesta de búsqueda de CS recibido se convierte por la capa de RLC 492 y envía a la capa de RRC 494 y finalmente alcanza la red central de CS 496. Mientras tanto, la capa de GMM 488 de la estación móvil 480 prepara un mensaje de petición de servicio de PS 430 para el servicio de UMTS solamente. El mensaje inicial desde la capa de GMM 488 se convierte a la capa de RRC 484 y se transmite desde la capa de RLC 482. Cuando la capa de RLC 492 de la red 490 recibe el mensaje 430, lo pasa a la capa de RRC 494, la cual a su vez pasa una forma del mensaje a la red central de PS 498.

Aunque el mensaje de respuesta de búsqueda de CS 420 y el mensaje de petición de servicio de PS 430 están descoordinados uno con respecto al otro, un mensaje de petición de autentificación de CS posterior 470 seguido por un comando de modo de seguridad de CS (no se muestra) se desencadena mediante la recepción del mensaje de respuesta de búsqueda 420 en la red 490. Después de que se procesa el mensaje de respuesta de búsqueda de CS 420 por la red central de CS 496, la red central de CS 496 responde con un mensaje de petición de autentificación de CS 470. Este mensaje comienza como un mensaje 471 desde la red central de CS 496, se convierte a un mensaje 473 por la capa de RRC 494, y puede tardar un tiempo para que la capa de RLC 492 lo transmita como un mensaje 475.

Mientras tanto, la red central de PS 498 ha respondido al mensaje de petición de servicio de PS 430 con un mensaje de petición de autentificación y cifrado de PS 440 seguido por un mensaje de comando de modo de seguridad de PS 450 para iniciar la protección de integridad. Cuando la estación móvil 480 recibe el mensaje de iniciación de protección de integridad 450, lo pasa a la capa de RRC 484. La capa de RRC inicia la protección de integridad e informa a la red 490 usando un mensaje completo de modo de seguridad 460. La capa de RRC 484 también usa un mensaje 469 para informar a la capa de GMM de paquetes conmutados 488 cuando el modo de seguridad está completo.

La estación móvil 480 entonces recibe el mensaje de petición de autentificación de CS 470 a través del mensaje 475 después de que el modo de seguridad de PS está completo. Usando el diagrama de flujo 200 mostrado en la FIG. 2, la estación móvil 480 determina que el mensaje 475 no contiene información de protección de integridad, que no se ha iniciado la protección de integridad en el dominio de CS, y de esta manera reenvía la petición de autentificación 470 a la capa de MM de circuitos conmutados 486. Hablando en términos generales, el mensaje de petición de autentificación 470 sería seguido por el mensaje de comando de modo de seguridad de circuitos conmutados para iniciar la protección de integridad.

Sin el diagrama de flujo 200 mostrado en la FIG. 2, el mensaje de petición de autentificación de CS 475 habría sido descartado por la estación móvil 480 debido a que el mensaje 475 no contenía información de protección de integridad y un modo de seguridad se ha iniciado. Descartar este mensaje 475 habría impedido que la llamada

entrante suene en la estación móvil 480.

Los conceptos mostrados en la FIG. 2 se pueden repetir para el dominio de PS. La FIG. 5 muestra un diagrama de flujo 500 de un método de modo de seguridad para la estación móvil 180 mostrada en la FIG. 1 de acuerdo con una segunda realización. En el paso 510, la estación móvil 180 recibe un mensaje de transferencia directa de enlace descendente (DDT) de capa 3 de paquetes conmutados (PS) desde una red tal como la red 190 mostrada en la FIG. 1. El mensaje de DDT de PS podría ser un mensaje de petición de autentificación y cifrado, un mensaje de rechazo de autentificación y cifrado, un mensaje de petición de identidad, un mensaje de aceptación de actualización de área de encaminamiento, un mensaje de rechazo de actualización de área de encaminamiento, un mensaje de rechazo de servicio, o uno de otros diversos tipos de mensajes de capa 3. En el paso 520, la estación móvil 180 determina si la información de protección de integridad está presente en el mensaje de DDT de PS. De acuerdo con la Especificación Técnica 25.331 del 3GPP, una "información de comprobación de Integridad" de elemento de información (IE) registra convenientemente si la información de integridad está en el mensaje de capa 3. En esta realización, si está presente la "información de comprobación de Integridad", entonces hay información de protección de integridad presente en el mensaje de DDT de PS de acuerdo con el paso 520. Si la información de protección de integridad está presente, el paso 530 realiza la protección de integridad de capa de RRC estándar en el mensaje de DDT de PS y el flujo finaliza en el paso 590.

Si la información de protección de integridad no está presente en el mensaje de DDT de PS, el paso 540 determina si un modo de seguridad de protección de integridad se ha iniciado por la red central de PS. Si la estación móvil 180 ha recibido un mensaje de comando de modo de seguridad de PS para iniciar la protección de integridad, entonces se ha iniciado un modo de seguridad de protección de integridad por la red central de PS y el paso 550 descarta el mensaje de DDT de PS antes de que el flujo finalice en el paso 590. Descartar el mensaje de DDT de PS bajo estas condiciones cumple con los requerimientos de la Especificación Técnica 25.331 del 3GPP. Alternativamente, si la variable INTEGRITY_PROTECTION_INFO fue modificada para incluir estados iniciados y no iniciados separados para los dominios de CS y de PS, el paso 540 se podría determinar comprobando la variable INTEGRITY_PROTECTION_INFO de la estación móvil.

Si el paso 540 determina que no se ha iniciado un modo de seguridad de protección de integridad por la red central de PS (por ejemplo, un modo de seguridad se ha iniciado solamente por la red central de CS o que tampoco la red central ha iniciado un modo de seguridad), el paso 560 reenvía el mensaje de DDT de PS a la capa de GMM de paquetes conmutados de la estación móvil 180 antes de que el flujo finalice en el paso 590. Debido a que la Especificación Técnica 24.008 del 3GPP proporciona flexibilidad para procesar un mensaje de capa 3 no protegido de integridad en un dominio particular cuando la protección de integridad para ese dominio no se ha iniciado, el diagrama de flujo 500 impide que una llamada se caiga cuando un mensaje de señalización de capa 3 y un mensaje de iniciación de protección de integridad se reciben fuera de servicio.

La FIG. 6 muestra un tercer diagrama de señal ejemplo 600 para un método de modo de seguridad en el sistema del 3GPP mostrado en la FIG. 1 de acuerdo con la segunda realización. En este tercer ejemplo, un mensaje de petición de autentificación y cifrado de PS no protegido de integridad 670 se inicia por una red central de PS 698 antes de que se inicie un mensaje de iniciación de protección de integridad 650, excepto que el mensaje no protegido de integridad 670 se reciba en la estación móvil 680 después de que se reciba el mensaje de iniciación de protección de integridad 650 en la estación móvil 680. En este ejemplo, cuando una estación móvil 680 está iniciando una llamada, en lugar de descartar el mensaje de petición de autentificación y cifrado de PS no protegido de integridad 670, la estación móvil 680 pasa el mensaje 670 a su capa de gestión de movilidad de dominio de paquetes conmutados, la capa de GMM 688.

Este tercer diagrama de flujo de señal ejemplo 600 muestra cuatro capas de una estación móvil 680: una capa de control de enlace radio (RLC) 682, una capa de control de recursos radio (RRC) 684, una capa de gestión de movilidad (MM) del dominio de circuitos conmutados 686, y una capa de gestión de movilidad GPRS (GMM) del dominio de paquetes conmutados 688. Una red 690 también se muestra en el tercer diagrama de flujo de señal ejemplo 600. La red 690 tiene una capa de control de enlace radio (RLC) 692 y una capa de control de recursos radio (RRC) 694 las cuales son contrapartidas a las capas de RLC y RRC 682, 684 en la estación móvil 680. La red 690 también tiene una red central de CS 696 y una red central de PS 698, las cuales se muestran en la FIG. 1 como la red central de CS 196 y la red central de PS 198. Como se indicó previamente, la red central de CS 696 y la red central de PS 698 funcionan independientemente una de la otra.

Después de que se establece una conexión de RRC entre la estación móvil 680 y la red 690 usando varios mensajes 610, se genera un mensaje de actualización de ubicación de CS 620 por la capa de MM 686 se pasa a la capa de RRC 684 para volver a empaquetar, y se transmite desde la capa de RLC 682 de la estación móvil 680. El mensaje 620 se recibe en la capa de RLC 692 de la red, se convierte y se envía a la capa de RRC 694, la cual reenvía el mensaje a la red central de CS 696 para procesamiento. En el dominio de paquetes conmutados, se genera un mensaje de petición de adjunto 630 en la capa de GMM 688, se vuelve a empaquetar en la capa de RRC 684, y se transmite desde la estación móvil 680 a través de la capa de RLC 682. La capa de RLC 692 de la red 690 recibe el mensaje 630, lo convierte para la capa de RRC 694, la cual lo reenvía a la red central de PS 698. El mensaje de actualización de ubicación de CS 620 y el mensaje de petición de adjunto de PS 630 no están coordinados uno con el otro y pueden ocurrir en cualquier secuencia de tiempo.

En respuesta al mensaje de petición de adjunto de PS 630, la red 690 envía un mensaje de petición de autentificación y cifrado de PS 670. La petición de autentificación y cifrado se genera por la red central de PS 698 como el mensaje 671, y se empaqueta por la capa de RRC 694 como el mensaje 673. Dependiendo del tamaño y la prioridad del mensaje 673, puede trascurrir algún tiempo antes de que la capa de RLC de la red 690 transmita un mensaje no protegido de integridad 675 que contiene el mensaje de petición de autentificación y cifrado de PS 670.

Mientras tanto, en respuesta al mensaje de actualización de ubicación de CS 620, la red central de CS 696 ha enviado un mensaje de petición de autentificación de CS 640 seguido por un mensaje de comando de modo de seguridad de CS 650 que dirige el inicio de la protección de integridad. Cuando el mensaje de comando de modo de seguridad de CS 650 se recibe por la estación móvil 680 en la capa de RLC 682 y se pasa a la capa de RRC 684, la estación móvil 680 inicia la protección de integridad. Cuando los procedimientos de modo de seguridad están completos en la estación móvil 680, se envía un mensaje completo de modo de seguridad 660 a la red 690. Mientras tanto, también se notifica a la capa de MM del dominio de circuitos conmutados 686 que el modo de seguridad de CS se ha completado usando el mensaje 669 desde la capa de RRC 684.

Así cuando el mensaje no protegido de integridad 675 que porta un mensaje de petición de autentificación y cifrado 670 desde la red 690 llega a la estación móvil 680, la estación móvil 680 está en modo de seguridad para el dominio de CS. Usando el diagrama de flujo 500 mostrado en la FIG. 500, la estación móvil 680 determina que el mensaje 675 no contiene información de protección de integridad, la protección de integridad no se ha iniciado en el dominio de PS, y de esta manera reenvía el mensaje de petición de autentificación y cifrado de PS 670 a la capa de GMM 688. Hablando en términos generales, el mensaje de petición de autentificación y cifrado 670 se seguiría por un mensaje de comando de modo de seguridad de paquetes conmutados para iniciar la protección de integridad.

Sin el diagrama de flujo 500 mostrado en la FIG. 5, el mensaje de petición de autentificación y cifrado de paquetes conmutados 675 habría sido descartado por la estación móvil 680 debido a que el mensaje 675 no contenía información de protección de integridad y se ha iniciado un modo de seguridad. Descartar este mensaje 675 (y sus copias) habría provocado eventualmente una llamada caída.

De esta manera, un método de modo de seguridad cumple con las especificaciones técnicas del 3GPP y aún diferencia entre modos de seguridad en diferentes dominios. Si un dispositivo móvil recibe un mensaje sin protección de integridad en un dominio, y se determina que un modo de seguridad no se ha iniciado para ese dominio, entonces el mensaje se puede procesar por el dispositivo móvil. Diferenciando entre modos de seguridad en diferentes dominios, las llamadas caídas se pueden reducir – especialmente para situaciones en que se reciben mensajes de capa 3 en un dominio después de mensajes de iniciación de protección de integridad desde otro dominio, lo cual es muy posible cuando se están configurando concurrentemente conexiones de PS y CS.

Aunque esta descripción incluye que están consideradas en este momento para ser las realizaciones preferentes y los mejores modos de la invención descritos de una manera que establecen posesión de la misma por los inventores y que permite a aquellos expertos habituales en la técnica hacer y usar la invención, se entenderá y apreciará que hay muchos equivalentes a las realizaciones preferentes reveladas aquí dentro y que se pueden hacer modificaciones y variaciones sin salirse del alcance y espíritu de la invención, las cuales van a estar limitados no por las realizaciones preferentes sino por las reivindicaciones adjuntas, incluyendo cualquier modificación hecha durante la tramitación de esta solicitud y todos los equivalentes de aquellas reivindicaciones que se emiten.

Además se entiende que el uso de términos relacionales tales como primero y segundo, y similares, se usan solamente para distinguir una entidad, elemento, o acción de otra sin requerir o implicar necesariamente ninguna real de tal relación u orden entre tales entidades, elementos o acciones. Gran parte de la funcionalidad inventiva y muchos de los principios inventivos se implementan mejor con o en programas o instrucciones de soporte lógico. Se espera que un experto habitual, a pesar del esfuerzo posiblemente significativo y muchas opciones de diseño motivadas, por ejemplo, por el tiempo disponible, tecnología actual, y consideraciones económicas, cuando se guía por los conceptos y principios revelados aquí dentro serán fácilmente capaces de generar tales instrucciones y programas de soporte lógico con mínima experimentación. Por lo tanto, la discusión adicional de tal soporte lógico, en su caso, estará limitada en el interés de la brevedad y minimización de cualquier riesgo de oscurecer los principios y conceptos de acuerdo con la presente invención.

REIVINDICACIONES

1. Un método de modo de seguridad que comprende recibir (210) un mensaje de capa 3 en un primer dominio desde una red, determinar (220) si el mensaje de capa 3 tiene información de protección de integridad, y averiguar (240) si se ha iniciado un modo de seguridad en el primer dominio, el método caracterizado por:

detectar (240) si un modo de seguridad se ha iniciado en un segundo dominio; y

reenviar (260) el mensaje de capa 3 a una capa superior, si el mensaje de capa 3 carece de información de protección de integridad y un modo de seguridad no se ha iniciado en el primer dominio y se ha iniciado en el segundo dominio.

2. Un método de modo de seguridad de acuerdo con la reivindicación 1 que además comprende:

realizar (230) protección de integridad en el mensaje de capa 3, si el mensaje de capa 3 tiene información de protección de integridad.

3. Un método de modo de seguridad de acuerdo con la reivindicación 1 que además comprende:

descartar (250) el mensaje de capa 3, si el mensaje de capa 3 carece de información de protección de integridad y un modo de seguridad se ha iniciado en el primer dominio.

4. Un método de modo de seguridad de acuerdo con la reivindicación 1 en el que determinar (220) si el mensaje de capa 3 tiene información de protección de integridad además comprende:

comprobar una “información de comprobación de Integridad” del elemento de información.

5. Un método de modo de seguridad de acuerdo con la reivindicación 1 en el que averiguar (240) si se ha iniciado un modo de seguridad en el primer dominio comprende:

comprobar la recepción de un mensaje de comando de iniciación de protección de integridad en el primer dominio.

6. Un método de modo de seguridad de acuerdo con la reivindicación 1 en el que detectar (240) si se ha iniciado un modo de seguridad en un segundo dominio comprende:

comprobar la recepción de un mensaje de comando de iniciación de protección de integridad en el segundo dominio.

7. Un método de modo de seguridad de acuerdo con la reivindicación 1 en el que averiguar (240) si se ha iniciado un modo de seguridad en el primer dominio comprende:

comprobar una variable para un valor que indica que la protección de integridad ha comenzado en el primer dominio.

8. Un método de modo de seguridad de acuerdo con la reivindicación 1 en el que detectar (240) si se ha iniciado un modo de seguridad en un segundo dominio comprende:

comprobar una variable para un valor que indica que la protección de integridad ha comenzado en el segundo dominio.

9. Un método de modo de seguridad de acuerdo con la reivindicación 1 en el que la capa superior es una capa de gestión de movilidad para el primer dominio.

10. Un método de modo de seguridad de acuerdo con la reivindicación 1 en el que el primer dominio es de circuitos conmutados (196) y el segundo dominio es de paquetes conmutados (198).

11. Un método de modo de seguridad de acuerdo con la reivindicación 1 en el que el primer dominio es de paquetes conmutados (198) y el segundo dominio es de circuitos conmutados (196).

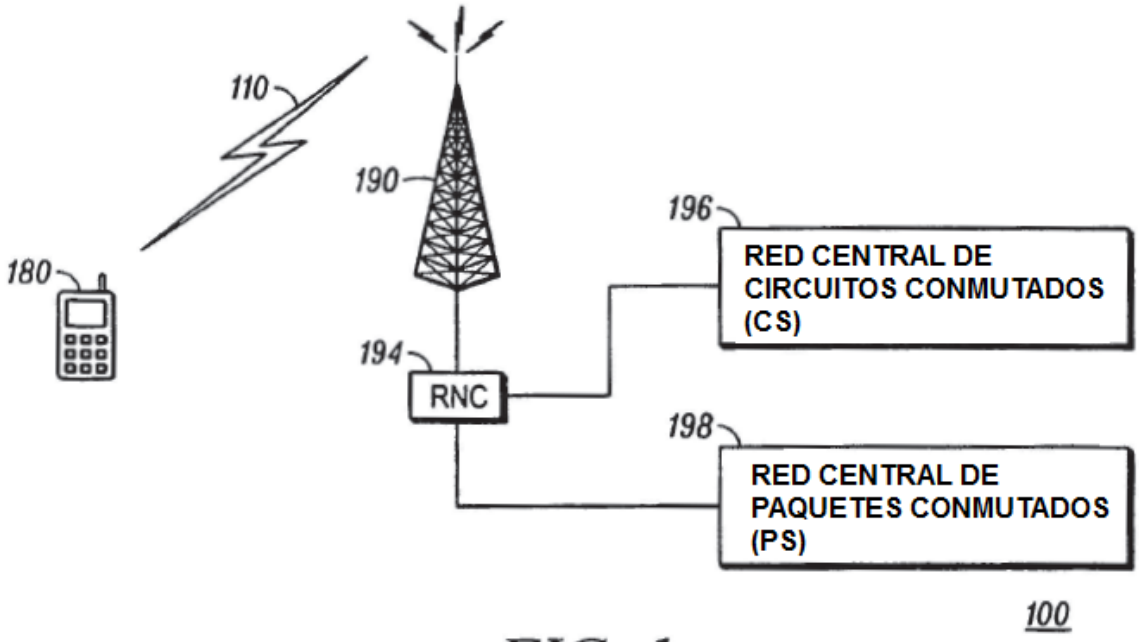
110
190
196
RED CENTRAL DE CIRCUITOS CONMUTADOS (CS)
180
194
RNC
198
RED CENTRAL DE PAQUETES CONMUTADOS (PS)
100

FIG. 1

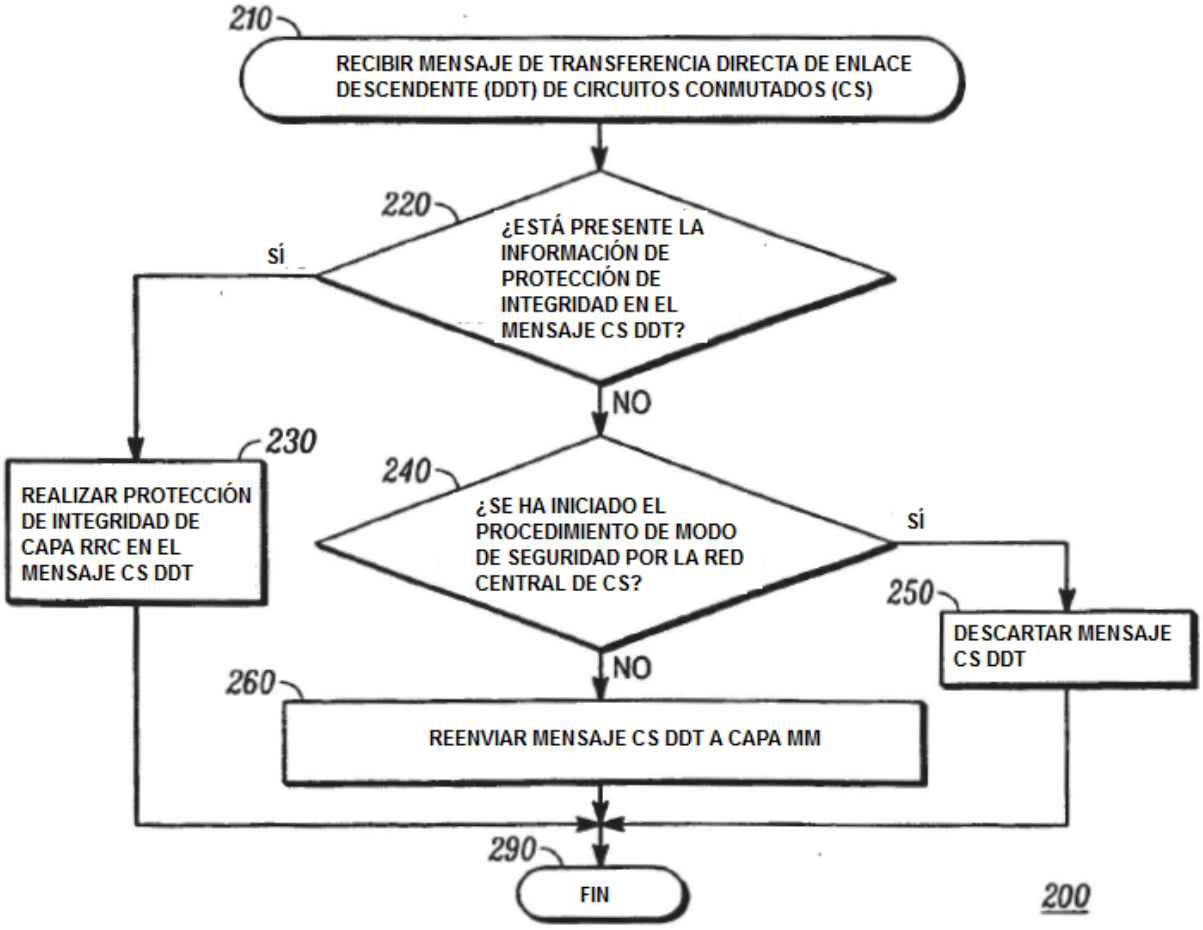
210
RECIBIR MENSAJE DE TRANSFERENCIA DIRECTA DE ENLACE DESCENDENTE (DDT) DE CIRCUITOS CONMUTADOS (CS)
220
¿ESTÁ PRESENTE LA INFORMACIÓN DE PROTECCIÓN DE INTEGRIDAD EN EL MENSAJE CS DDT?
SÍ
NO
230
REALIZAR PROTECCIÓN DE INTEGRIDAD DE CAPA RRC EN EL MENSAJE CS DDT
240
¿SE HA INICIADO EL PROCEDIMIENTO DE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

FIG. 2

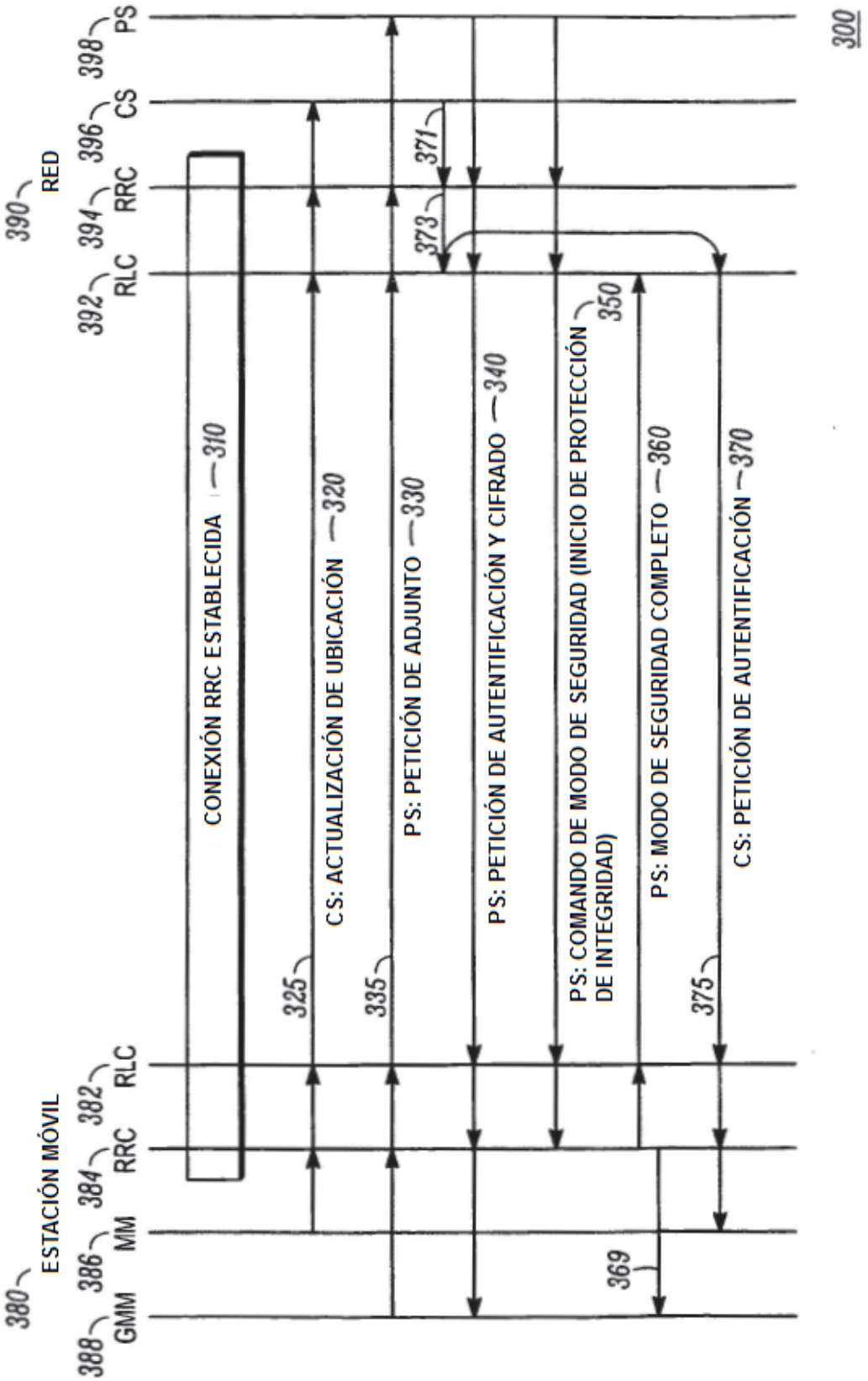
300
380
ESTACIÓN MÓVIL
388 GMM
386 MM
384 RRC
382 RLC
390
RED
392 RLC
394 RRC
396 CS
398 PS
CONEXIÓN RRC ESTABLECIDA 310
325
CS: ACTUALIZACIÓN DE UBICACIÓN 320
335
PS: PETICIÓN DE ADJUNTO 330
PS: PETICIÓN DE AUTENTIFICACIÓN Y CIFRADO 340
PS: COMANDO DE MODO DE SEGURIDAD (INICIO DE PROTECCIÓN DE INTEGRIDAD)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

FIG. 3

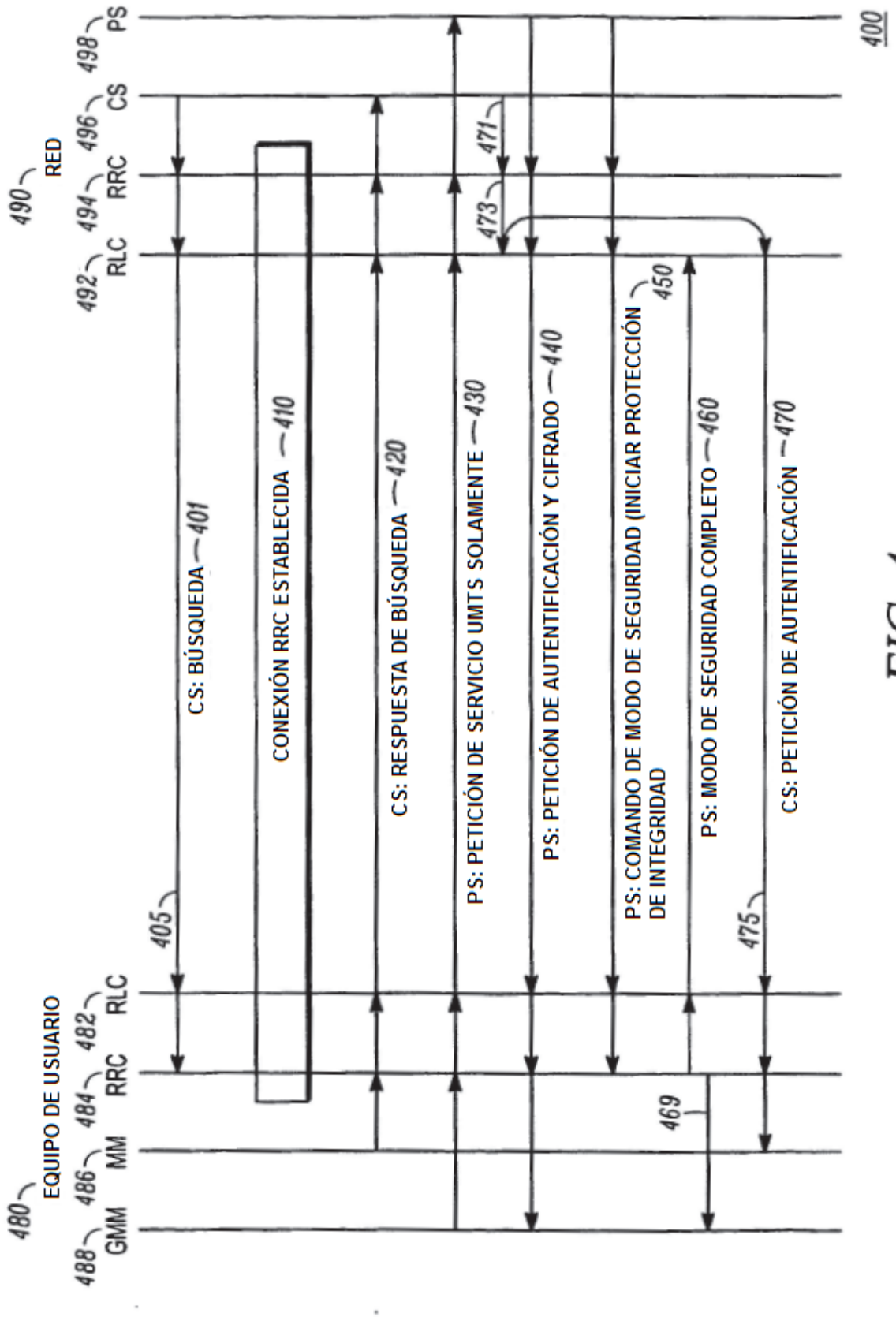
400
EQUIPO DE USUARIO
480
GMM 488
MM 486
RRC 484
RLC 482
RED
490
RRC 494
CS 496
PS 498
RLC 492
405
CS: BÚSQUEDA 401
CONEXIÓN RRC ESTABLECIDA 410
CS: RESPUESTA DE BÚSQUEDA 420
PS: PETICIÓN DE SERVICIO UMTS SOLAMENTE 430
PS: PETICIÓN DE AUTENTIFICACIÓN Y CIFRADO 440
PS: COMANDO DE MODO DE SEGURIDAD (INICIAR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

FIG. 4

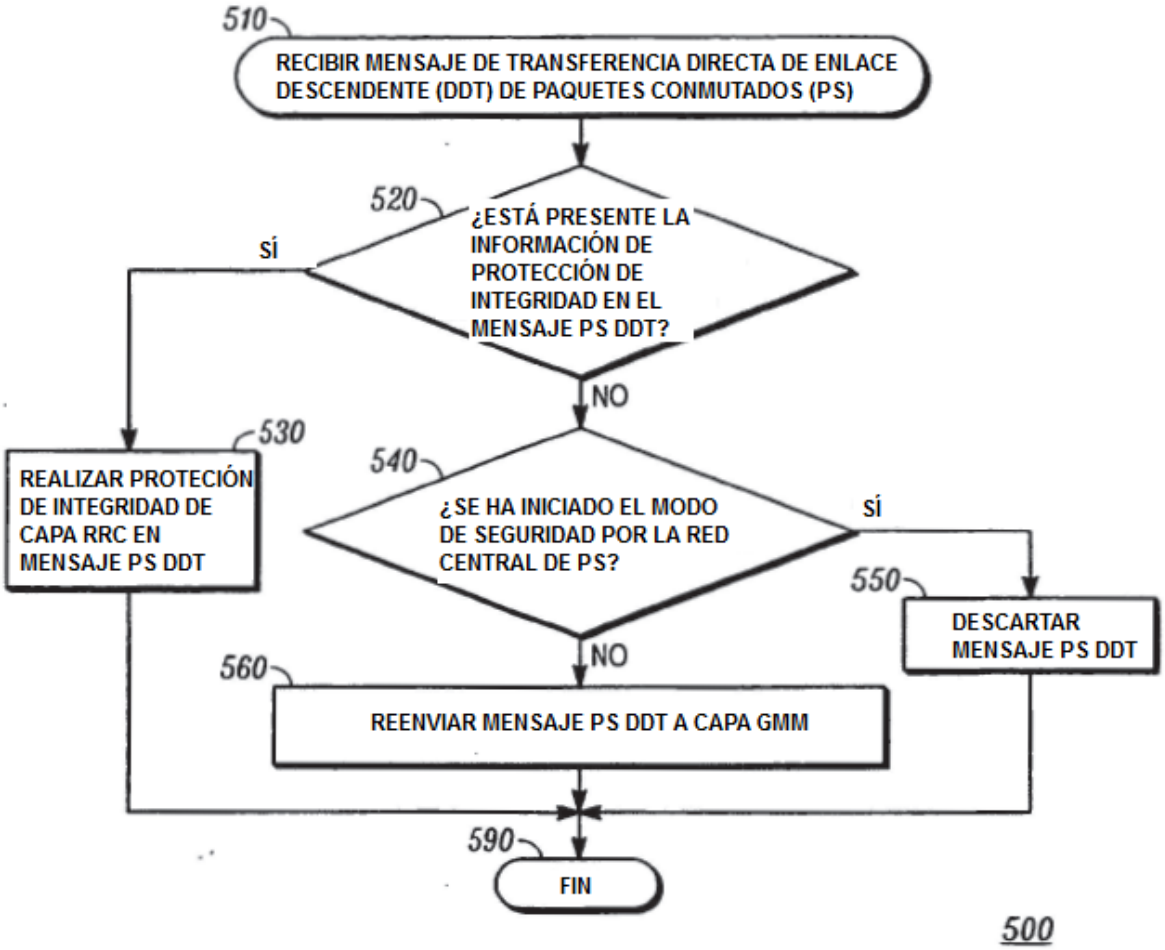
510
RECIBIR MENSAJE DE TRANSFERENCIA DIRECTA DE ENLACE DESCENDENTE (DDT) DE PAQUETES CONMUTADOS (PS)
520
¿ESTÁ PRESENTE LA INFORMACIÓN DE PROTECCIÓN DE INTEGRIDAD EN EL MENSAJE PS DDT?
SÍ
NO
530
REALIZAR PROTECIÓN DE INTEGRIDAD DE CAPA RRC EN MENSAJE PS DDT
540
¿SE HA INICIADO EL MODO DE SEGURIDAD POR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

FIG. 5

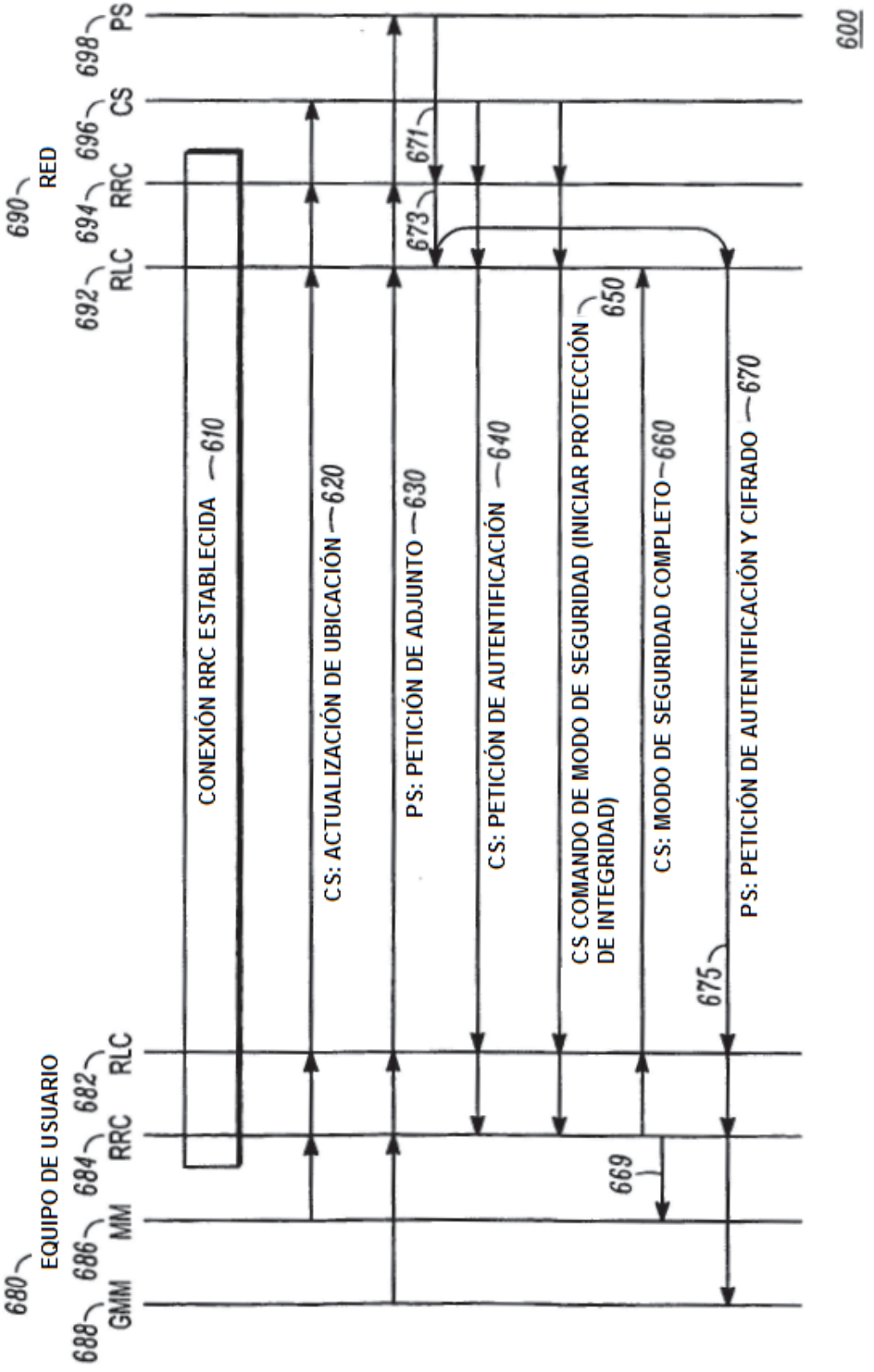
600
690 RED
698 PS
696 CS
694 RRC
692 RLC
671
673
CONEXIÓN RRC ESTABLECIDA 610
CS: ACTUALIZACIÓN DE UBICACIÓN 620
PS: PETICIÓN DE ADJUNTO 630
CS: PETICIÓN DE AUTENTIFICACIÓN 640
CS COMANDO DE MODO DE SEGURIDAD (INICIAR PROTECCIÓN DE INTEGRIDAD) 650
CS: MODO DE SEGURIDAD COMPLETO 660
PS: PETICIÓN DE AUTENTIFICACIÓN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

FIG. 6