(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 549 496**

(51) Int. CI.:

H04W 36/00 (2009.01)
H04W 12/04 (2009.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **17.06.2011 E 11728489 (3)**

(97) Fecha y número de publicación de la concesión europea: **26.08.2015 EP 2583497**

(54) Título: **Procedimientos y aparatos que facilitan la sincronización de configuraciones de seguridad**

(30) Prioridad:

16.06.2011 US 201113162313
18.06.2010 US 356464 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.10.2015

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
International IP Administration 5775 Morehouse Drive
San Diego, CA 92121-1714, US

(72) Inventor/es:

PATIL, KIRAN KISHANRAO;
SANKA, SURESH;
HSU, LIANGCHI y
GHOLMIEH, AZIZ

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Procedimientos y aparatos que facilitan la sincronización de configuraciones de seguridad

Campo

Diversas características se refieren a dispositivos y sistemas de comunicación inalámbrica, y de manera más particular a sincronizar configuraciones de seguridad entre terminales de acceso y entidades de red.

Antecedentes de la invención

La seguridad es una característica importante de un sistema de comunicación inalámbrica. La seguridad, en algunos sistemas de comunicación inalámbrica, convencionalmente puede comprender dos características: la "Integridad de Datos" y el "Cifrado". La "Integridad de Datos" es la característica que asegura que ninguna red maliciosa podrá enviar mensajes de señalización innecesarios con la intención de ocasionar, o realmente provocar algún efecto indeseado en una llamada en curso. El "Cifrado" es la característica que asegura que toda la señalización y mensajes de datos son cifrados sobre la interfaz de aire para evitar que un tercero intercepte los mensajes. En algunos sistemas de comunicación inalámbrica, tal como el Sistema de Telecomunicaciones Móviles Universales (UMTS), la protección de integridad es obligatoria aunque el cifrado es opcional. La protección de integridad puede ser implementada solamente en portadoras de radio de señalización, mientras que el cifrado puede ser implementado en la señalización así como en portadoras de radio de datos.

En una red inalámbrica convencional, una terminal de acceso (AT) típicamente negocia con la red inalámbrica para establecer parámetros de seguridad, tal como claves de encriptación para uso en el encriptado (o cifrado), de comunicaciones entre la terminal de acceso y los componentes de la red. Dichos parámetros de seguridad pueden ser actualizados y/o modificados ocasionalmente para asegurar el secreto de los datos transmitidos entre la terminal de acceso y los componentes de red.

Un ejemplo de un procedimiento convencional para iniciar o actualizar parámetros de seguridad entre la terminal de acceso y la red inalámbrica generalmente incluye que la terminal de acceso reciba un comando de modo de seguridad desde la red inalámbrica y actualice sus parámetros de seguridad con base en el comando de modo de seguridad recibido. Después que la terminal de acceso actualiza sus parámetros de seguridad, y antes de implementar los nuevos parámetros de seguridad, la terminal de acceso envía un mensaje completo de modo de seguridad a la red inalámbrica. Al momento de la recepción del mensaje completo de modo de seguridad, la red inalámbrica comenzará a utilizar los nuevos parámetros de seguridad para proteger cualesquiera mensajes de enlace descendente posteriores enviados a la terminal de acceso.

Sin embargo, la terminal de acceso no comenzará a utilizar los nuevos parámetros de seguridad para proteger cualesquiera mensajes de enlace ascendente enviados a la red inalámbrica hasta que un mensaje de acuse de recibo sea recibido desde la red inalámbrica en respuesta al mensaje completo de modo de seguridad enviado por la terminal de acceso. En otras palabras, la terminal de acceso no comienza a utilizar los nuevos parámetros de seguridad para mensajes enviados desde la terminal de acceso a la red inalámbrica hasta que la terminal de acceso recibe un acuse de recibo desde la red inalámbrica respecto a que el mensaje completo de modo de seguridad fue recibido y autenticado. El documento de descripción y decisión “AS-rekeying in case of inter-cell handover”, de Qualcomm Europe en la reunión 3GPP TSG-RAN WG2 del 12 al 16 de enero de 2009 describe la reintroducción AS en traspaso intercelular.

Como resultado, existe una pequeña ventana entre el tiempo en que se completó el procedimiento de modo de seguridad en la red inalámbrica (por ejemplo, cuando el mensaje completo de modo de seguridad es recibido en la red inalámbrica) y el momento en que el procedimiento de modo de seguridad se completó en la terminal de acceso (por ejemplo, cuando el acuse de recibo es recibido por la terminal de acceso y los parámetros de seguridad son actualizados). Debido a esta ventana de tiempo, es posible que la red inalámbrica sea actualizada a los nuevos parámetros de seguridad, mientras que la terminal de acceso permanece con los viejos parámetros de seguridad. Por ejemplo, las terminales de acceso convencionales típicamente están adaptadas para abortar el procedimiento de modo de seguridad cuando se inician otros procedimientos, tal como un procedimiento de movilidad.

En casos donde la red inalámbrica es actualizada a los nuevos parámetros de seguridad, pero la terminal de acceso continúa con los viejos parámetros de seguridad, la conexión inalámbrica entre los dos típicamente falla, teniendo como resultado llamadas tiradas y una falta de satisfacción por parte del usuario de la terminal de acceso. Por lo tanto, sería benéfico proporcionar procedimientos y aparatos para evitar la situación donde la red inalámbrica es actualizada a nuevos parámetros de seguridad mientras la terminal de acceso continúa con los viejos parámetros de seguridad y/o para sincronizar los parámetros de seguridad cuando ocurre dicha situación.

Sumario

La invención se define en las reivindicaciones, a las que se hace ahora referencia. Diversas características facilitan la sincronización de parámetros de seguridad entre las terminales de acceso y una red de acceso. Una característica proporciona terminales de acceso adaptadas para facilitar dicha sincronización. De acuerdo con una o más

realizaciones, una terminal de acceso (AT) puede comprender una interfaz de comunicaciones inalámbricas acoplada con un circuito de procesamiento. La interfaz de comunicaciones inalámbricas puede estar adaptada para facilitar las comunicaciones inalámbricas de la terminal de acceso.

De acuerdo con al menos una implementación, el circuito de procesamiento puede estar adaptado para conducir un procedimiento de modo de seguridad para reconfigurar parámetros de seguridad de la terminal de acceso. Aunque el procedimiento de modo de seguridad está en curso, el circuito de procesamiento puede iniciar un procedimiento de movilidad. El circuito de procesamiento también puede abortar el procedimiento de modo de seguridad y regresar a los viejos parámetros de seguridad como un resultado de haber iniciado el procedimiento de movilidad. Un mensaje de actualización de movilidad puede ser enviado por el circuito de procesamiento a través de la interfaz de comunicaciones inalámbricas, donde el mensaje de actualización de movilidad incluye un indicador de estatus de seguridad dedicado adaptado para indicar que la terminal de acceso ha regresado a los viejos parámetros de seguridad.

De acuerdo con al menos otra implementación, el circuito de procesamiento puede estar adaptado para conducir un procedimiento de modo de seguridad para reconfigurar parámetros de seguridad de la terminal de acceso. Aunque el procedimiento de modo de seguridad está en curso, el circuito de procesamiento puede iniciar un procedimiento de movilidad, incluyendo el envío de un mensaje de actualización de movilidad. El circuito de procesamiento también puede abortar el procedimiento de modo de seguridad y regresar a los viejos parámetros de seguridad como un resultado de haber iniciado el procedimiento de movilidad. El circuito de procesamiento puede recibir un mensaje de confirmación de actualización de movilidad en respuesta a un mensaje de actualización de movilidad a través de la interfaz de comunicación inalámbrica. Si no se puede decodificar el mensaje de conformación de actualización de movilidad utilizando los viejos parámetros de seguridad, el circuito de procesamiento puede conmutar a los nuevos parámetros de seguridad.

De acuerdo con al menos otra implementación, el circuito de procesamiento puede estar adaptado para conducir un procedimiento de modo de seguridad incluyendo el envío de un mensaje completo de modo de seguridad a una red de acceso a través de la interfaz de comunicación inalámbrica. En respuesta al mensaje completo de modo de seguridad, el circuito de procesamiento puede recibir un mensaje de acuse de recibo a través de la interfaz de comunicación inalámbrica. El circuito de procesamiento se puede actualizar a los nuevos parámetros de seguridad, y puede enviar otro mensaje de acuse de recibo a la red de acceso a través de la interfaz de comunicación inalámbrica, donde el otro mensaje de acuse de recibo está adaptado para indicar que la terminal de acceso se ha actualizado a los nuevos parámetros de seguridad.

También se proporcionan procedimientos operativos en una terminal de acceso de acuerdo con una característica para facilitar la sincronización de parámetros de seguridad entre terminales de acceso y una red de acceso.

En al menos una implementación de dichos procedimientos, un procedimiento de modo de seguridad puede ser conducido para reconfigurar los parámetros de seguridad de la terminal de acceso. Se puede iniciar un procedimiento de movilidad mientras que el procedimiento de modo de seguridad está en curso. El procedimiento de modo de seguridad puede ser abortado como un resultado de iniciar el procedimiento de actualización de movilidad y la terminal de acceso puede regresar a los viejos parámetros de seguridad. Se puede enviar un mensaje de confirmación de actualización de movilidad en respuesta al mensaje de actualización de movilidad. La terminal de acceso puede cambiar a los nuevos parámetros de seguridad si la terminal de acceso no puede decodificar el mensaje de confirmación de actualización de movilidad usando los viejos parámetros de seguridad.

En una o más implementaciones diferentes, dichos procedimientos pueden incluir que se realice un procedimiento de modo de seguridad incluyendo el envío de un mensaje completo de modo de seguridad a una red de acceso. En respuesta al mensaje completo de modo de seguridad, recibir un mensaje de acuse de recibo. La terminal de acceso puede ser actualizada a nuevos parámetros de seguridad. Otro mensaje de acuse de recibo puede ser enviado a la red de acceso, donde el otro mensaje de acuse de recibo está adaptado para indicar que la terminal de acceso se ha actualizado a los nuevos parámetros de seguridad.

Otra característica proporciona entidades de red adaptadas para facilitar la sincronización de parámetros de seguridad entre terminales de acceso y una red de acceso. Dichas entidades de red pueden comprender una interfaz de comunicaciones acoplada con un circuito de procesamiento. En al menos una implementación, el circuito de procesamiento se puede adaptar para recibir un mensaje completo de modo de seguridad desde una terminal de acceso a través de la interfaz de comunicaciones. En respuesta al mensaje completo de modo de seguridad, el circuito de procesamiento se puede actualizar a nuevos parámetros de seguridad. El circuito de procesamiento además puede recibir un mensaje de actualización de movilidad desde la terminal de acceso a través de la interfaz de comunicaciones. El mensaje de actualización de movilidad puede incluir un indicador de estatus de seguridad dedicado adaptado para indicar que la terminal de acceso ha regresado a los viejos parámetros de seguridad. En respuesta al mensaje de actualización de movilidad recibido, el circuito de procesamiento puede regresar a los viejos parámetros de seguridad.

En al menos otra implementación, el circuito de procesamiento se puede adaptar para recibir un mensaje completo de modo de seguridad desde una terminal de acceso a través de la interfaz de comunicaciones. En respuesta al

mensaje completo de modo de seguridad, el circuito de procesamiento se puede actualizar a nuevos parámetros de seguridad. El circuito de procesamiento puede recibir un mensaje de actualización de movilidad desde la terminal de acceso, y puede enviar un mensaje de confirmación de actualización de movilidad a la terminal de acceso en respuesta al mensaje de actualización de movilidad. Si una respuesta al mensaje de confirmación de actualización de movilidad no es recibida desde la terminal de acceso, el circuito de procesamiento puede regresar a los viejos parámetros de seguridad y puede volver a enviar el mensaje de confirmación de actualización de movilidad a la terminal de acceso utilizando los viejos parámetros de seguridad para cifrar el mensaje.

En una o más implementaciones diferentes, el circuito de procesamiento puede ser adaptado para recibir un mensaje completo de modo de seguridad desde una terminal de acceso a través de la interfaz de comunicaciones. El circuito de procesamiento puede enviar un mensaje de acuse de recibo en respuesta al mensaje completo de modo de seguridad. El circuito de procesamiento puede recibir otro mensaje de acuse de recibo desde la terminal de acceso indicando que la terminal de acceso se ha actualizado a los nuevos parámetros de seguridad. En respuesta al otro mensaje de acuse de recibo, el circuito de procesamiento se puede actualizar a los nuevos parámetros de seguridad.

Operaciones del procedimiento en una entidad de red también se proporcionan de acuerdo con una característica para facilitar la sincronización de parámetros de seguridad entre terminales de acceso y una red de acceso.

En al menos otra implementación de dichos procedimientos, un mensaje completo de modo de seguridad puede ser recibido desde una terminal de acceso. En respuesta al mensaje completo de modo de seguridad, la entidad de red puede ser actualizada a nuevos parámetros de seguridad. Un mensaje de actualización puede ser recibido desde la terminal de acceso, y un mensaje de confirmación de actualización de movilidad puede ser enviado a la terminal de acceso en respuesta al mensaje de actualización de movilidad recibido. Si una respuesta al mensaje de confirmación de actualización de movilidad no es recibido desde la terminal de acceso, la entidad de red puede ser regresada a los viejos parámetros de seguridad y el mensaje de confirmación de actualización de movilidad puede ser reenviado a la terminal de acceso utilizando los viejos parámetros de seguridad para cifrar el mensaje de confirmación de actualización de movilidad.

En otra u otras implementaciones todavía de dichos procedimientos, el mensaje completo de modo de seguridad puede ser recibido desde una terminal de acceso. Un mensaje de acuse de recibo puede ser enviado en respuesta al mensaje completo de modo de seguridad. Otro mensaje de acuse de recibo puede ser recibido desde la terminal de acceso indicando que la terminal de acceso se ha actualizado a los nuevos parámetros de seguridad. En respuesta al otro mensaje de acuse de recibo, la entidad de red puede ser actualizada a los nuevos parámetros de seguridad.

Breve descripción de los dibujos

La figura 1 es un diagrama en bloques que ilustra un entorno de red en el cual se pueden utilizar varias características de acuerdo con al menos un ejemplo.

La figura 2 ilustra una jerarquía de claves típica que puede ser implementada dentro de una red de comunicación inalámbrica típica.

La figura 3 ilustra una pila de protocolo ejemplar que puede ser implementada en un dispositivo de comunicación que opera en una red de paquete conmutado.

La figura 4 es un diagrama en bloques que ilustra un sistema de red en el cual se pueden generar las diversas claves de seguridad ilustradas en las figuras 2 y 3.

La figura 5 (que comprende las figuras 5A y 5B) es un diagrama de flujo que ilustra un ejemplo de una operación de sincronización de parámetros de seguridad en la cual una terminal de acceso indica a la red de acceso que el procedimiento de modo de seguridad fue abortado en la terminal de acceso.

La figura 6 es un diagrama de flujo que ilustra un ejemplo de una operación de sincronización de parámetros de seguridad por una terminal de acceso cuando los parámetros de seguridad en la red de acceso son actualizados y los parámetros de seguridad en la terminal de acceso no son actualizados.

La figura 7 es un diagrama de flujo que ilustra un ejemplo de una operación de sincronización de parámetros de seguridad de una terminal de acceso, la red de acceso y la red núcleo para facilitar la actualización de los parámetros de seguridad en la red de acceso solamente después que los parámetros de seguridad son actualizados en la terminal de acceso.

La figura 8 es un diagrama de flujo que ilustra un ejemplo de una operación de sincronización de parámetros de seguridad por una red de acceso cuando los parámetros de seguridad de la red de acceso son actualizados y los parámetros de seguridad de la terminal de acceso no lo son.

La figura 9 es un diagrama en bloques que ilustra componentes selectos de una terminal de acceso de acuerdo con al menos una realización.

La figura 10 es un diagrama de flujo que ilustra un ejemplo de un procedimiento operativo en una terminal de acceso para indicar a una red de acceso cuando la terminal de acceso ha regresado a los viejos parámetros de seguridad.

La figura 11 es un diagrama de flujo que ilustra un ejemplo de un procedimiento operativo en una terminal de acceso para determinar un estatus de los parámetros de seguridad en una red de acceso para comunicarse con la terminal de acceso.

La figura 12 es un diagrama de flujo que ilustra un ejemplo de un procedimiento operativo en una terminal de acceso para indicar a una red de acceso cuando la terminal de acceso se ha actualizado a nuevos parámetros de seguridad.

La figura 13 es un diagrama en bloques que ilustra componentes selectos de una entidad de red de acuerdo con al menos una realización.

La figura 14 es un diagrama de flujo que ilustra un ejemplo de un procedimiento operativo en una entidad de red para determinar que una terminal de acceso ha regresado a viejos parámetros de seguridad.

La figura 15 es un diagrama de flujo que ilustra un ejemplo de un procedimiento operativo en una entidad de red para determinar que una terminal de acceso ha regresado a viejos parámetros de seguridad.

La figura 16 es un diagrama de flujo que ilustra un ejemplo de un procedimiento operativo en una entidad de red para realizar una actualización de los viejos parámetros de seguridad a los nuevos parámetros de seguridad después que la terminal de acceso se ha actualizado a los nuevos parámetros de seguridad.

Descripción detallada de la invención

En la siguiente descripción, se proporcionan detalles específicos para brindar un completo entendimiento de las implementaciones descritas. Sin embargo, un experto en la técnica entenderá que se pueden practicar diversas implementaciones sin estos detalles específicos. Por ejemplo, se pueden mostrar circuitos en diagramas de bloques a fin de no oscurecer las implementaciones con detalles innecesarios. En otros casos, circuitos, estructuras y técnicas bien conocidas se pueden mostrar a detalle para no oscurecer las implementaciones descritas.

La palabra "ejemplar" aquí se utiliza para indicar que "sirve como un ejemplo, caso o ilustración". Cualquier implementación o realización aquí descrita como "ejemplar" no necesariamente se interpretará como preferida o ventajosa sobre otras realizaciones o implementaciones. De igual manera, el término "realizaciones" no requiere que todas las realizaciones incluyan la característica, ventaja o modo de operación analizados. El término "terminal de acceso" tal como aquí se utiliza se interpretará de manera amplia. Por ejemplo, una "terminal de acceso" puede incluir equipo de usuario y/o dispositivos de suscriptor, tales como teléfonos móviles, localizadores, módems inalámbricos, asistentes digitales personales, administradores de información personal (PIM), reproductores de medios personales, ordenadores de mano, ordenadores portátiles, y/u otros dispositivos de computación/comunicación móvil los cuales se comunican, al menos parcialmente, a través de una red inalámbrica o celular.

Perspectiva general

Una o más características facilitan y/o resuelven la sincronización de los parámetros de seguridad entre una terminal de acceso y una o más entidades de una red inalámbrica. De acuerdo con una característica, una terminal de acceso (AT) puede indicar a una entidad de red que la terminal de acceso ha regresado a los viejos parámetros de seguridad. Por ejemplo, la terminal de acceso puede enviar un indicador con un mensaje de actualización de movilidad para informar a la entidad de red respecto al retorno. En otro ejemplo, la terminal de acceso puede enviar un mensaje a la entidad de red para informar a la entidad de red que la terminal de acceso se ha actualizado con éxito a los nuevos parámetros de seguridad.

De acuerdo con una característica, una terminal de acceso puede determinar que una entidad de red se ha actualizado a los nuevos parámetros de seguridad y por consiguiente puede actualizar sus propios parámetros de seguridad. Por ejemplo, después de abortar un procedimiento de modo de seguridad para actualizarse a los nuevos parámetros de seguridad, la terminal de acceso puede determinar que no puede decodificar un mensaje recibido desde la entidad de red. En respuesta a no poder decodificar, la terminal de acceso se puede actualizar a los nuevos parámetros de seguridad e intentar decodificar el mensaje recibido utilizando los nuevos parámetros de seguridad. Si la terminal de acceso es exitosa en decodificar el mensaje recibido con los nuevos parámetros de seguridad, la terminal de acceso puede seguir utilizando los nuevos parámetros de seguridad.

De acuerdo con una característica, una entidad de red puede determinar que una terminal de acceso ha regresado a los viejos parámetros de seguridad y, por consiguiente, pueden revertir sus propios parámetros de seguridad. Por ejemplo, después de actualizarse a los nuevos parámetros de seguridad, la entidad de red puede enviar un mensaje a la terminal de acceso que está cifrado de acuerdo con los nuevos parámetros de seguridad. Si la entidad de red no recibe una respuesta al mensaje enviado, la entidad de red puede regresar a los viejos parámetros de seguridad y enviar el mensaje utilizando los viejos parámetros de seguridad para cifrar el mensaje. Si la entidad de red recibe una respuesta al mensaje enviado utilizando los viejos parámetros de seguridad, la entidad de red puede seguir utilizando los viejos parámetros de seguridad.

Entorno de red ejemplar

La figura 1 es un diagrama en bloques que ilustra un entorno de red en el cual se pueden utilizar varias características de acuerdo con al menos un ejemplo. Una terminal de acceso 102 puede ser adaptada para comunicarse de manera inalámbrica con una red de acceso 104, la cual está comunicativamente acoplada a una red núcleo 106.

Hablando en términos generales, la red de acceso 104 incluye equipo de radio adaptado para permitir que

terminales de acceso 102 tengan acceso a la red, mientras que la red núcleo 106 incluye capacidades de conmutación y enrutamiento para conectarse ya sea a la red de circuito conmutado (por ejemplo, Red de Telefonía Pública Conmutada (PTSN)/Red Digital de Servicios Integrados (ISDN) 108) o a una red de paquete conmutado (por ejemplo, Internet 110). La red núcleo 106 además facilita la movilidad y la administración de ubicación de suscriptor y servicios de autenticación. En cierto ejemplo, tal como el ilustrado en la figura 1, la red núcleo 6 puede ser una red compatible con el Sistema de Telecomunicaciones Móviles Universales (UMTS) o una red compatible con el Sistema Global para Comunicación Móvil (GSM).

La red de acceso 104 puede incluir uno o más nodos de acceso 112 (por ejemplo, estación base, nodo B, etc.) y un controlador de red de radio (RNC) 114. Cada nodo de acceso 112 típicamente está asociado con una célula, o sector, que comprende un área geográfica de cobertura de recepción y transmisión. Las células o sectores se pueden traslapar entre sí. El controlador de red de radio (RNC) 114 se puede adaptar para controlar los nodos de acceso 112 que están comunicativamente conectados a éste. El controlador de red de radio (RNC) 114 además se puede adaptar para llevar a cabo la administración de recursos de radio, algunas de las funciones de administración de movilidad, y puede ser el punto donde la encriptación es ejecutada antes que los datos de usuario sean enviados hacia y desde la terminal de acceso 102. El controlador de red de radio (RNC) 114 está comunicativamente acoplado a la red núcleo 106 a través de un nodo de soporte (SGSN) del Servicio de Radio de Paquete General (GPRS) 116 en servicio para llamadas de paquete conmutado y a través de un centro de conmutación móvil (MSC) 118, el cual puede incluir un registro de ubicación de visitante (VLR), para llamadas de circuito conmutado. Un registro de ubicación de casa (HLR) y un Centro de Autenticación (AuC) 120 pueden servir para autenticar terminales de acceso antes de proporcionar servicios de comunicación a través de la red núcleo 106. Observar que, en otros tipos de red, las funciones del HLR/AuC 120 y otros componentes (tal como el MSC/VLR 118) pueden ser ejecutadas por otras entidades de red equivalentes. Por ejemplo, en una red de Evolución a Largo Plazo (LTE), algunas o todas las funciones del HLR/AuC 120 pueden ser ejecutadas por un servidor de suscriptor de casa (HSS). La red núcleo 106 también puede incluir una entidad de administración móvil (MME), ejecuta la activación/desactivación de portadora de terminales de acceso, ayuda a autenticar terminales de acceso, y/o ejecuta rastreo de terminales de acceso y/o procedimientos de localización (incluyendo retransmisiones) para las terminales de acceso acopladas a la red núcleo.

Cuando una terminal de acceso 102 intenta conectarse a la red de acceso 104, la terminal de acceso 102 inicialmente es autenticada a fin de verificar la identidad de la terminal de acceso 102. La terminal de acceso 102 también autentica la red para verificar que ésta esté conectada a una red de acceso 104 que está autorizada a utilizar. La negociación típicamente surge entre la terminal de acceso 102 y la red de acceso 104 y/o la red núcleo 106 para establecer parámetros de seguridad, tal como claves de encriptación para uso en la encriptación de comunicaciones entre la terminal de acceso 102 y los componentes de red (por ejemplo, red de acceso 104 y/o red núcleo 106). Dichos parámetros de seguridad pueden ser actualizados y/o cambiados ocasionalmente para asegurar el secreto de los datos transmitidos entre la terminal de acceso 102 y los componentes de red.

La figura 2 ilustra una jerarquía de claves típica 200 que puede ser implementada para establecer los parámetros de seguridad (por ejemplo, claves de encriptación) para uso en la encriptación de comunicaciones entre la terminal de acceso 102 y los componentes de red (por ejemplo, red de acceso 104 y/o red núcleo 106). Aquí, un Módulo de Identidad de Suscriptor Universal (USIM), en la terminal de acceso 102, y la red núcleo 106 (por ejemplo, un Centro de Autenticación (HLR/AuC 120 en la figura 1)) utilizan una clave maestra K 202 para generar una clave de cifrado (CK) 204 y la clave de integridad (1K) 206. La clave de cifrado (CK) 204 y la clave de integridad (IK) 206 pueden entonces ser utilizadas por el dispositivo de comunicación y la red núcleo 106 (por ejemplo, un Registro de Ubicación de Casa (HLR)) para generar una clave de Entidad de Administración de Seguridad de Acceso K ASME 208. La activación de seguridad de una terminal de acceso 102 se puede lograr a través de un procedimiento de Acuerdo de Autenticación y Clave (AKA), procedimiento de Configuración de Modo de Seguridad (NAS SMC) de Estrato de No Acceso (NAS) y procedimiento de Configuración de Modo de Seguridad (AS SMC) de Estrato de Acceso (AS). El AKA es utilizado para derivar la clave K ASME 208, la cual entonces es utilizada como una clave base para el cálculo de claves NAS (Estrato de No Acceso) 210 y 212 y claves AS (Estrato de Acceso) 214, 216, 218 y 220. La terminal de acceso 102 y la red núcleo 106 pueden entonces utilizar la KASME 208 para generar una o más de estas claves de seguridad.

Las redes de paquete conmutado pueden ser estructuradas en múltiples capas de protocolo jerárquicas, donde las capas de protocolo inferiores proporcionan servicios a las capas superiores y cada capa es responsable de diferentes tareas. Por ejemplo, la figura 3 ilustra una pila de protocolo ejemplar que puede ser implementada en un dispositivo de comunicación que opera en una red de paquete conmutado. En este ejemplo, la pila de protocolo 302 incluye una capa Física (PHY) 304, una capa de Control de Acceso de Medio (MAC) 306, una capa de Control de Enlace de Radio (RLC) 308, una Capa de Protocolo de Convergencia de Datos en Paquete (PDCP), una Capa de Control de Recursos de Radio (RRC) 312, una Capa de Estrato de No Acceso (NAS) 314, y una Capa de Aplicación (APP) 316.

Las capas debajo de la Capa NAS 314 con frecuencia son referidas como la Capa de Estrato de Acceso (AS) 318. La Capa RLC 308 puede incluir uno o más canales 320. La Capa RRC 312 puede implementar varios modos de monitoreo para la terminal de acceso, incluyendo estado conectado y estado inactivo. La Capa de Estrato de No Acceso (NAS) 314 puede mantener el contexto de administración de movilidad del dispositivo de comunicación, el

contexto de datos en paquete y/o sus direcciones IP. Observar que pueden estar presentes otras capas en la pila de protocolo 302 (por ejemplo, encima, debajo y/o en medio de las capas ilustradas), pero han sido omitidas para el propósito de ilustración.

Haciendo referencia a las figuras 1-3, portadoras de radio/sesión 322 pueden ser establecidas, por ejemplo, en la Capa RRC 312 y/o Capa NAS 314. En consecuencia, la Capa NAS 314 puede ser utilizada por una terminal de acceso 102 y la red núcleo 106 para generar las claves de seguridad K NAS-enc 210 y K_NAS-int 212 que se muestran en la figura 2. De manera similar, la Capa RRC 312 puede ser utilizada por la terminal de acceso 102 y la re de acceso 104 (por ejemplo, RNC 114) para generar las claves de seguridad del Estrato de Acceso (AS) K UP-enc 216, K RRC-enc 218, y K RRC-int 220. Aunque las claves de seguridad K_UP-enc 216, K_RRC-enc 218, y K RRC-int 220 pueden ser generadas en la Capa RRC 312, estas claves pueden ser utilizadas por la Capa PDCP 310 para asegurar la señalización y/o comunicaciones de usuario/datos. Por ejemplo, la clave K_UP-enc 216 puede ser utilizada por la Capa PDCP 310 para asegurar las comunicaciones del plano de usuario/datos (UP), mientras que las claves KRRC-enc 218, y K RRC-int 220 pueden ser utilizas para asegurar las comunicaciones de señalización (es decir, control) en la Capa .PDCP 310.

En la derivación de estas claves de seguridad, utilizadas para cifrado y algoritmos de integridad, tanto en el AS (plano de Usuario y RRC) como en el NAS, requiere que una identidad de algoritmo individual sea proporcionada como una de las entradas. Al nivel de AS, los algoritmos que se van a utilizar son proporcionados por un Comando de Modo de Seguridad del Control de Recursos de Radio (RRC).

La figura 4 es un diagrama en bloques que ilustra un sistema de red en el cual se pueden generar las diversas claves de seguridad ilustradas en las figuras 2 y 3. Aquí, una terminal de acceso 402 puede implementar una pila de comunicación que incluye varias capas (por ejemplo, APP, NAS, RRC, RLC, MAC y PHY). Una red de acceso 404 puede proporcionar conectividad inalámbrica a la terminal de acceso 402 de manera que se puede comunicar con la red. Un centro de autenticación (AuC) 406 y la terminal de acceso 402 puede conocer o tener acceso a una clave raíz (K) la cual puede ser utilizada para generar u obtener una clave de cifrado (CK) y/o una clave de integridad (IK). La terminal de acceso 402 y/o un registro de ubicación de casa (HLR) 408 entonces puede utilizar la clave de cifrado (CK) y/o clave de integridad (IK) para generar una Clave de Entidad de Administración de Seguridad de Acceso K ASME. Al utilizar la clave KASME, la terminal de acceso 402 y una entidad de administración de movilidad (MME) 410 pueden entonces generar las claves KNAS-enc y KNAS-int. La terminal de acceso 402 y MME 410 también pueden generar una clave específica de red de acceso K eNB/NH. Al utilizar la clave específica de red de acceso K eNB/N14, la terminal de acceso 402 y la red de acceso 404 pueden generar las claves KUP-enc y KRRC-enc y KRRC-int.

Se proporcionan detalles referentes a la derivación de estas calves en 3GPP STD-T63-33.401 "Evolución de Arquitectura de Sistema (SAE): Arquitectura de Seguridad" (conocido como 3GPP TS 33.401) Versión 8, el cual se incorpora aquí por referencia.

Haciendo referencia nuevamente a la figura 1, la terminal de acceso 102 típicamente está adaptada para cambiar entre células (por ejemplo, nodos de acceso 112) a las cuales está conectada de forma activa. Por ejemplo, a medida que una terminal de acceso 102 se desplaza a través de un área geográfica, diferentes células (por ejemplo, nodos de acceso 112) pueden proporcionar una mejor conectividad (por ejemplo, señal más fuerte). La terminal de acceso 102 por consiguiente puede cambiar de una célula (por ejemplo, nodo de acceso 112) a otra célula (por ejemplo, nodo de acceso 112). En redes convencionales, dicha movilidad de una terminal de acceso 102 que requiere cambios de una célula (por ejemplo, nodo de acceso 112) a otra célula (por ejemplo, nodo de acceso 112) puede tener como resultado la cancelación de cualquier actualización en curso de parámetros de seguridad (por ejemplo, actualización a parámetros de seguridad de Estrato de Acceso K UP-enc, K RRC-enc y/o K RRC-int). Por ejemplo, como resultado de la movilidad de la terminal de acceso 102, se puede iniciar un procedimiento de movilidad, teniendo como resultado una cancelación de un procedimiento de modo de seguridad en curso. A manera de ejemplo y no limitación, un procedimiento de movilidad puede incluir una reselección de célula, error irrecuperable del Control de Enlace de Radio (RLC), problema relacionado con fuera de servicio, etc. Por consiguiente, algunos ejemplos no limitativos de los mensajes de actualización de movilidad que pueden ser enviados como parte de un procedimiento de movilidad pueden incluir un mensaje de reselección de célula, un mensaje de error irrecuperable del Control de Enlace de Radio (RLC), un mensaje de fuera de servicio, etc.

En casos donde se cancela un procedimiento de modo de seguridad en curso, existe la posibilidad de que los parámetros de seguridad sean actualizados en la red de acceso 104, pero no actualizados en la terminal de acceso 102, tal como se describirá con mayor detalle a continuación. Como un resultado, los parámetros de seguridad son actualizados en la red de acceso 104 pero no en la terminal de acceso 102, puede ocurrir un error de decodificación de datos/mensaje permanente y pérdida de conexión entre la terminal de acceso 102 y la red de acceso 104 (por ejemplo, teniendo como resultado llamadas tiradas).

De acuerdo con una característica, cuando la terminal de acceso 102 inicia un procedimiento de movilidad (por ejemplo, reselección de un nodo de acceso 112) después que la red de acceso 104 se ha actualizado a nuevos parámetros de seguridad, la terminal de acceso 102 se puede adaptar para enviar una indicación a la red de acceso 104 informando a la red de acceso 104 que la terminal de acceso 102 se ha revertido a los viejos parámetros de

seguridad. Por ejemplo, la terminal de acceso 102 puede incluir una indicación con el mensaje de actualización de movilidad enviado a la red de acceso 104.

De acuerdo con otra característica, la red de acceso 104 se puede adaptar para regresar a los viejos parámetros de seguridad cuando la terminal de acceso 102 falla en responder a un mensaje de confirmación de actualización de movilidad de la red de acceso 104 que está encriptado de acuerdo con los nuevos parámetros de seguridad. Es decir, después que la red de acceso 104 ha enviado un mensaje de confirmación de actualización de movilidad a la terminal de acceso 102, un número específico de veces sin recibir una respuesta de la terminal de acceso 102, la red de acceso 104 puede regresar a los viejos parámetros de seguridad y enviar el mensaje de confirmación de actualización de movilidad encriptado de acuerdo con los viejos parámetros de seguridad. Si la terminal de acceso 102 entonces responde al mensaje de confirmación de actualización de movilidad que está encriptado de acuerdo con los viejos parámetros de seguridad, entonces la red de acceso 104 sabe que la actualización de los parámetros de seguridad no fue exitosa y la red de acceso 104 sigue utilizando los viejos parámetros de seguridad.

De acuerdo con otra característica, la red de acceso 104 se puede adaptar para actualizar los parámetros de seguridad solamente después de recibir un mensaje de acuse de reciboacuse de recibo adicional desde la terminal de acceso 102. Es decir, después que un mensaje de confirmación de actualización de movilidad es enviado desde la red de acceso 104 a la terminal de acceso 102, la red de acceso 104 puede esperar otro mensaje de acuse de recibo desde la terminal de acceso 102 antes que la red de acceso 104 actualice los parámetros de seguridad. De esta manera, si la terminal de acceso 102 ha abortado la actualización de los parámetros de seguridad, la red de acceso 104 no actualizará, sin conocimiento, sus parámetros de seguridad de forma prematura.

De acuerdo con otra característica todavía, la terminal de acceso 102 se puede adaptar para identificar su falla para decodificar un mensaje de confirmación de actualización de movilidad de la red de acceso 104 después que éste es enviado un número específico de veces. Si la terminal de acceso 102 no puede decodificar el mensaje después del número específico de veces, la terminal de acceso 102 se puede adaptar para cambiar a los nuevos parámetros de seguridad e intentar decodificar el mensaje de confirmación de actualización de movilidad utilizando los nuevos parámetros. Si la terminal de acceso 102 tiene éxito en decodificar el mensaje de confirmación de actualización de movilidad utilizando los nuevos parámetros, entonces la terminal de acceso 102 puede continuar desde ese punto hacia delante para utilizar los nuevos parámetros de seguridad en la comunicación con la red de acceso 104.

Procedimientos ejemplares para sincronizar los parámetros de seguridad entre terminales de acceso y redes de acceso

La figura 5 (que comprende las figuras 5A y 5B) es un diagrama de flujo que ilustra un ejemplo de una operación de sincronización de parámetros de seguridad por una red de acceso cuando los parámetros de seguridad de la red de acceso son actualizados y los parámetros de seguridad de la terminal de acceso no lo son. Aunque el ejemplo ilustrado en la figura 5 así como los ejemplos de las figuras 6-8 están dirigidos a implementaciones que involucran un procedimiento de modo de seguridad de Estrato de Acceso (AS) para iniciar y actualizar los parámetros de seguridad de Estrato de Acceso, las características aquí descritas pueden ser implementadas en otros procedimientos de modo de seguridad, tal como procedimientos de modo de seguridad de Estrato de No Acceso (NAS). La terminal de acceso 102, red de acceso 104 y red núcleo 106 de la figura 1 se utilizan para propósitos ilustrativos.

Inicialmente, la terminal de acceso 102 puede establecer una conexión de control de recursos de radio (RRC) 502 con la red de acceso 104. El mensaje transmitido desde la terminal de acceso 102 a la red de acceso 104 cuando la conexión de control de recursos de radio (RRC) es establecida puede incluir la información de capacidad de seguridad de la terminal de acceso. La información de capacidad de seguridad de la terminal de acceso está adaptada para informar a la red de acceso 104 respecto de los algoritmos de cifrado (o encriptación) y los algoritmos de integridad que son soportados por la terminal de acceso 102. La información de capacidad de seguridad opcionalmente también puede incluir un mensaje de marca de clase indicando los algoritmos de seguridad GSM soportados por la terminal de acceso 102 (por ejemplo, marcas de clase GSM 2 y 3) y/o valores START para el dominio de servicio de circuito conmutado y el dominio de servicio de paquete conmutado. La información del mensaje de establecimiento de conexión de control de recursos de radio (RRC) puede ser almacenado 504 en la red de acceso 104.

La terminal de acceso 102 entonces puede enviar un mensaje de transferencia directa inicial 506 a la red núcleo 106. El mensaje de transferencia directa inicial 506 puede incluir, entre otra información, una identidad de usuario y un identificador de conjunto de claves (KSI) asignado por el dominio de servicio de circuito conmutado o el dominio de servicio de paquete conmutado en la última autenticación para esta red de núcleo 106. De acuerdo con al menos una implementación, el mensaje de transferencia directa inicial puede comprender un mensaje capa 3 (L3), tal como una solicitud de actualización de ubicación, una solicitud de servicio CM, una solicitud de actualización de área de enrutamiento, una solicitud de unión, una respuesta de localización u otro mensaje L3. El mensaje de transferencia directa inicial puede ser enviado, por ejemplo, a un registro de ubicación de visitante (VLR) para el dominio de servicio de circuito conmutado de la red núcleo 106 o un nodo de soporte GPRS (SGSN) para el dominio de servicio de paquete conmutado de la red núcleo 106.

La autenticación de la terminal de acceso 102 y la generación de nuevas claves de seguridad (por ejemplo, clave de integridad (IK), clave de cifrado (CK)) pueden ser ejecutadas entre la terminal de acceso 102 y la red núcleo 106 utilizando un procedimiento de acuerdo de autenticación y clave (AKA) 508. Como parte del acuerdo de autenticación y clave 508, opcionalmente se puede asignar un nuevo identificador de conjunto de claves (KSI).

Siguiendo el acuerdo de autenticación y clave, las nuevas claves de seguridad (por ejemplo, la clave de integridad (IK) y la clave de cifrado (CK)) pueden ser empleadas para calcular las claves de Estrato de Acceso (AS). Por ejemplo, la red núcleo 106 puede decidir cuál algoritmo de cifrado y algoritmo de integridad van a ser utilizados en orden de preferencia en 510. La red núcleo 106 entonces puede enviar un mensaje de comando de modo de seguridad de Estrato de Acceso (AS) 512 a la red de acceso 104. El mensaje de comando de modo de seguridad de Estrato de Acceso (AS) 512 puede ser enviado de acuerdo con un protocolo de parte de aplicación de red de acceso de radio (RANAP), y puede ser dirigido al controlador de red de radio (RNC) de la red de acceso 104. Este mensaje de comando de modo de seguridad 512 puede incluir una lista de algoritmos de integridad permitidos en orden de preferencia, y la clave de integridad (IK) que se va a utilizar. Si se va a iniciar el cifrado, el mensaje de comando de modo de seguridad 512 también puede incluir una lista de algoritmos de cifrado permitidos en orden de preferencia, y la clave de cifrado (CK) que se va a utilizar. Si se ha ejecutado el acuerdo de autenticación y clave (AKA), esto será indicado a la red de acceso 104 de manera que los valores START serán restablecidos cuando las nuevas claves sean iniciadas para uso.

La red de acceso 104 (por ejemplo, el controlador de red de radio RNC)) decide qué algoritmos (por ejemplo, algoritmo de integridad, algoritmo de cifrado) utilizar, genera un valor aleatorio RAND, e inicia la protección de integridad en 514. La red de acceso 104 entonces puede generar un mensaje de control de recursos de radio (RRC) 516 que comprende un mensaje de comando de modo de seguridad de Estrato de Acceso (AS), y envía el mensaje a la terminal de acceso 102. El mensaje de comando de modo de seguridad AS 516 puede incluir la capacidad de seguridad de la terminal de acceso 102, el algoritmo de integridad y el valor aleatorio RAND que se van a utilizar. Si se va a iniciar el cifrado, el mensaje 516 también puede incluir el algoritmo de cifrado que se va a utilizar. También se puede incluir información adicional. Debido a que la terminal de acceso 102 puede tener dos conjuntos de claves de cifrado e integridad, la red puede indicar cuál conjunto de claves se va a utilizar. Antes de enviar el mensaje de comando de modo de seguridad AS 516 a la terminal de acceso 102, la red de acceso 104 genera un código de autenticación de mensaje para integridad (MAC-I) y une esta información al mensaje de comando de modo de seguridad AS 516.

Volviendo ahora a la figura 5B, la terminal de acceso 102 recibe el mensaje de comando de modo de seguridad AS, verifica que la capacidad de seguridad sea la misma que la enviada en el mensaje de establecimiento de conexión del control de recursos de radio (RRC) y verifica el mensaje comparando el MAC-I con un XMAC-I generado en 518. La terminal de acceso 102 puede calcular XMAC-I en el mensaje recibido utilizando al menos el algoritmo de integridad indicado y el parámetro de valor aleatorio RAND recibido. Si todas las verificaciones son exitosas, entonces la terminal de acceso 102 envía un mensaje completo de modo de seguridad de Estrato de Acceso (AS) 520 incluyendo un MAC-1. Si las verificaciones no fueron exitosas, entonces se habría enviado un mensaje de rechazo de modo de seguridad.

Cuando la red de acceso 104 recibe el mensaje completo de modo de seguridad AS, éste verifica la integridad del mensaje generando XMAC-I y comparándolo con MAC-I incluido en el mensaje completo de modo de seguridad AS 522. Un mensaje completo de modo de seguridad AS 524 es enviado desde la red de acceso 104 a la red núcleo 106 como un mensaje de parte de aplicación de red de acceso de radio (RANAP) indicando los algoritmos seleccionados para integridad y cifrado. Un mensaje de acuse de recibo 526 es enviado desde la red de acceso 104 a la terminal de acceso 102 para reconocer la recepción del mensaje completo de modo de seguridad AS. De acuerdo con al menos algunas implementaciones, el mensaje de acuse de recibo 526 puede comprender un acuse de recibo L2.

El mensaje completo de modo de seguridad AS (por ejemplo, 520) de la terminal de acceso 102 a la red de acceso 104 inicia la protección de integridad de enlace descendente, es decir, los mensajes de enlace descendente posteriores enviados a la terminal de acceso 102 quedan protegidos en su integridad utilizando los nuevos parámetros de seguridad. Sin embargo, la protección de la integridad de enlace ascendente no comienza hasta que la terminal de acceso 102 recibe el mensaje de acuse de recibo en el paso 526 desde la red de acceso 104, con lo cual la terminal de acceso 102 actualiza sus parámetros de seguridad en el paso 528. En otras palabras, la terminal de acceso 102 no comienza a utilizar los nuevos parámetros de seguridad de Estrato de Acceso (AS) para mensajes enviados desde la terminal de acceso 102 a la red de acceso 104 hasta que la terminal de acceso 102 recibe un acuse de recibo desde la red de acceso 104 respecto a que el mensaje completo de modo de seguridad de Estrato de Acceso (AS) fue recibido y autenticado.

Existe una ventana pequeña entre el tiempo en que el procedimiento de modo de seguridad de Estrato de Acceso (AS) es completado en la red de acceso 104 (por ejemplo, cuando el mensaje completo de modo de seguridad de Estrato de Acceso (AS) 520 es recibido en la red de acceso 104) y cuando el procedimiento de modo de seguridad AS es completado en la terminal de acceso 102 (por ejemplo, cuando el mensaje de acuse de recibo 526 es recibido por la terminal de acceso 102 y los parámetros de seguridad de Estrato de Acceso (AS) son actualizados en 528). Debido a esta ventana de tiempo, es posible que la red de acceso 104 se actualice a los nuevos parámetros de

seguridad de Estrato de Acceso (AS), mientras que la terminal de acceso 102 permanece con los viejos parámetros de seguridad de Estrato de Acceso (AS).

Por ejemplo, la terminal de acceso 102 típicamente está adaptada para abortar el procedimiento de modo de seguridad de Estrato de Acceso (AS) cuando se inicia un procedimiento de movilidad, tal como en la situación en que un mensaje de actualización de movilidad es enviado desde la terminal de acceso 102 a la red de acceso 104. En consecuencia, la terminal de acceso 102 puede iniciar un procedimiento de movilidad, incluyendo la generación y envío de un mensaje de actualización de movilidad 530 después que el mensaje completo de modo de seguridad de Estrato de Acceso (AS) 520 es enviado a la red de acceso 104, y antes de recibir el acuse de recibo 526 y/o actualizar los parámetros de seguridad de la terminal de acceso. Como un resultado de haber iniciado el procedimiento de movilidad, la terminal de acceso 102 aborta el procedimiento de modo de seguridad y regresa a los viejos parámetros de seguridad de Estrato de Acceso (AS) 528. La terminal de acceso 102 puede recibir un acuse de recibo 526 después que se inicia el procedimiento de movilidad, pero la terminal de acceso 102 ha abortado el procedimiento de modo de seguridad del Estrato de Acceso (AS) y, por lo tanto, no se ha actualizado a los nuevos parámetros de seguridad del Estrato de Acceso (AS), desconocido para la red de acceso 104.

De acuerdo con la implementación mostrada en la figura 5B, el mensaje de actualización de movilidad 530 incluye un indicador que informa a la red de acceso 104 que la terminal de acceso 102 ha abortado el procedimiento de modo de seguridad AS y ha regresado a los viejos parámetros de seguridad AS. En al menos algunas implementaciones, el indicador puede comprender un nuevo elemento de información (IE) en el mensaje de actualización de movilidad. En alguna implementación, el indicador puede comprender uno o más bits del mensaje de actualización de movilidad.

En el momento de la recepción del mensaje de actualización de movilidad incluyendo el indicador, la red de acceso 104 regresa a los viejos parámetros de seguridad de Estrato de Acceso (AS) 532. La red de acceso 104 entonces puede generar y enviar un mensaje de confirmación de actualización de movilidad 534 a la terminal de acceso 102 que es cifrado utilizando los viejos parámetros de seguridad AS.

De acuerdo con otra característica, la terminal de acceso 102 se puede adaptar para ajustarse a los nuevos parámetros de seguridad cuando ante la terminal de acceso 102 pareciera que la red de acceso 104 está operando con los nuevos parámetros de seguridad mientras la terminal de acceso 102 está operando con los viejos parámetros de seguridad. La figura 6 es un diagrama de flujo que ilustra un ejemplo de una operación de sincronización de parámetros de seguridad por una terminal de acceso cuando los parámetros de seguridad en la red de acceso son actualizados y los parámetros de seguridad en la terminal de acceso no lo son. Los pasos mostrados en la figura 6 corresponden a los pasos siguiendo todos los pasos descritos y mostrados en relación a la figura 5A. Es decir, la figura 6 pretende mostrar los pasos que siguen después que los pasos de la figura 5A son completados.

Como se observó anteriormente con referencia a la figura 5B, al momento de la recepción del mensaje de comando de modo de seguridad de Estrato de Acceso (AS), la terminal de acceso 102 verifica que la capacidad de seguridad sea la misma que la enviada en el mensaje de establecimiento de conexión de control de recursos de radio (RRC), calcula XMAC-I y verifica la integridad del mensaje de comando de modo de seguridad AS comparando el MAC-I recibido con el XMAC-I generado 602. Si todas las verificaciones son exitosas, entonces la terminal de acceso 102 envía un mensaje completo de modo de seguridad de Estrato de Acceso (AS) 604 incluyendo un MAC-1. Si las verificaciones no fueron exitosas, entonces un mensaje de rechazo de modo de seguridad de Estrato de Acceso (AS) habría sido enviado. Cuando la red de acceso 104 recibe el mensaje completo de modo de seguridad AS, ésta verifica la integridad del mensaje en el paso 606, y envía un mensaje completo de modo de seguridad AS 608 a la red núcleo 106 indicando los algoritmos de encriptación e integridad seleccionados.

Como se observó anteriormente, en algunos casos la red de acceso 104 se puede actualizar a los nuevos parámetros de seguridad del Estrato de Acceso (AS) mientras que la terminal de acceso 102 falla en actualizarse a los nuevos parámetros de seguridad AS. Por ejemplo, después de enviar el mensaje completo de modo de seguridad AS 604 a la red de acceso 104, y antes de recibir un acuse de recibo y/o actualizar los parámetros de seguridad del Estrato de Acceso (AS), la terminal de acceso 102 puede comenzar un procedimiento de movilidad en el cual la terminal de acceso 102 genera y envía un mensaje de actualización de movilidad 610 a la red de acceso 104. En respuesta a iniciar el procedimiento de movilidad, la terminal de acceso 102 aborta el procedimiento de modo de seguridad y se revierte a los viejos parámetros de seguridad del Estrato de Acceso (AS) 612. La terminal de acceso 102 puede recibir un mensaje de acuse de recibo 614 después de iniciar el procedimiento de movilidad, pero la terminal de acceso 102 ya habrá abortado el procedimiento de modo de seguridad de Estrato de Acceso (AS) y, por lo tanto, no se actualiza a los nuevos parámetros de seguridad de Estrato de Acceso (AS), desconocidos para la red de acceso 104.

En dichos casos, el mensaje de actualización de movilidad enviado en el paso 610 típicamente no está encriptado, teniendo como resultado que la red de acceso 104 pueda recibir y procesar el mensaje de actualización de movilidad incluso cuando la terminal de acceso 102 está operando con los viejos parámetros de seguridad del Estrato de Acceso (AS). En la implementación mostrada en la figura 6, la red de acceso 104 recibe el mensaje de actualización de movilidad 610 y responde con una confirmación de actualización de movilidad 616 que está cifrada con los

nuevos parámetros de seguridad AS y, por lo tanto, no puede ser decodificada por la terminal de acceso 102 utilizando los viejos parámetros de seguridad AS. Cuando la red de acceso 104 falla en recibir una respuesta al mensaje de confirmación de actualización de movilidad, la red de acceso 104 reenvía la confirmación de actualización de movilidad. La terminal de acceso 102 puede ser adaptada para mantener un registro del número de veces que ésta recibe y falla en decodificar el mensaje de confirmación de actualización de movilidad. Después de un número predeterminado de intentos (N), la terminal de acceso 102 puede cambiar a los nuevos parámetros de seguridad AS 618. Después de cambiar a los nuevos parámetros de seguridad AS, la terminal de acceso 102 puede intentar decodificar el mensaje de confirmación de actualización de movilidad utilizando los nuevos parámetros de seguridad AS. Si tiene éxito, la terminal de acceso 102 continuará utilizando los nuevos parámetros de seguridad AS desde ese punto en adelante.

De acuerdo con otra característica, la red de acceso 104 se puede adaptar para completar el procedimiento de modo de seguridad y actualizar sus parámetros de seguridad solamente después de recibir un mensaje de acuse de recibo final desde la terminal de acceso 102. La figura 7 es un diagrama de flujo que ilustra un ejemplo de una operación de sincronización de parámetros de seguridad de una terminal de acceso 102, red de acceso 104 y red núcleo 106 para facilitar la actualización de los parámetros de seguridad en la red de acceso 104 solamente después que los parámetros de seguridad son actualizados en la terminal de acceso 102. Los pasos mostrados en la figura 7 corresponden a los pasos que siguen a todos los pasos descritos y mostrados en relación a la figura SA. Es decir, la figura 7 está destinada a mostrar los pasos que siguen después que los pasos de la figura 5A son completados.

Como se observó anteriormente con referencia a la figura 5B, al momento de la recepción del mensaje de comando de modo de seguridad del Estrato de Acceso (AS), la terminal de acceso 102 verifica que la capacidad de seguridad sea la misma que aquella enviada en el mensaje de establecimiento de conexión de control de recursos de radio (RRC), calcula XMAC-I y verifica la integridad del mensaje comparando el MAC-I recibido con el XMAC-I generado 702. Si todas las verificaciones son exitosas, entonces la terminal de acceso 102 envía un mensaje completo de modo de seguridad de Estrato de Acceso (AS) 704 incluyendo un MAC-I. Si las verificaciones no fuesen exitosas entonces se habría enviado un mensaje de rechazo de modo de seguridad AS. Cuando la red de acceso 104 recibe el mensaje completo de modo de seguridad AS, ésta verifica la integridad del mensaje en el paso 706, y envía un mensaje completo de modo de seguridad AS 708 a la red núcleo 106 indicando los algoritmos de encriptación e integridad seleccionados.

En la implementación mostrada en la figura 7, la red de acceso 104 no completa el procedimiento de modo de seguridad AS al momento de la recepción y verificación de un mensaje completo de modo de seguridad AS. Es decir, la red de acceso 104 está adaptada para no actualizarse a los nuevos parámetros de seguridad AS al momento de la recepción y verificación del mensaje completo de modo de seguridad AS 704. Por el contrario, la red de acceso 104 envía un mensaje de acuse de recibo 710 a la terminal de acceso 102. El mensaje de acuse de recibo 710 puede comprender un mensaje de acuse de recibo L2. En respuesta a la recepción del mensaje de acuse de recibo 710, la terminal de acceso 102 se actualiza a los nuevos parámetros de seguridad AS 712. La terminal de acceso 102 puede enviar un mensaje de acuse de recibo 714 a la red de acceso 104. Por ejemplo, la terminal de acceso 102 puede enviar un mensaje de acuse de recibo L3 a la red de acceso 104 para indicar que se ha actualizado a los nuevos parámetros de seguridad AS. La red de acceso 104 entonces se actualiza a los nuevos parámetros de seguridad AS 716 en respuesta a la recepción del mensaje de acuse de recibo 714 de la terminal de acceso 102.

De acuerdo con la implementación en la figura 7, si la terminal de acceso 102 aborta el procedimiento de modo de seguridad de Estrato de Acceso (AS) (por ejemplo, inicia un procedimiento de movilidad) después de enviar el mensaje completo de modo de seguridad AS 704 a la red de acceso 104, pero antes de actualizarse a los nuevos parámetros de seguridad, la red de acceso 104 no recibirá el acuse de recibo 714 y no se actualizará a los nuevos parámetros de seguridad AS. En otras palabras, si la terminal de acceso 102 aborta el procedimiento de modo de seguridad AS antes de completar el procedimiento (por ejemplo, antes de actualizarse a los nuevos parámetros de seguridad AS), entonces el mensaje de acuse de recibo 714 no será enviado y la red de acceso 104 no será actualizada a los nuevos parámetros de seguridad AS.

De acuerdo con otra característica, la red de acceso 104 puede ser actualizada para revertirse a los viejos parámetros de seguridad cuando a criterio de la red de acceso 104 la terminal de acceso 102 está operando con los viejos parámetros de seguridad mientras la red de acceso 104 está operando con los nuevos parámetros de seguridad. La figura 8 es un diagrama de flujo que ilustra un ejemplo de una operación de sincronización de parámetros de seguridad por una red de acceso cuando los parámetros de seguridad de la red de acceso son actualizados y los parámetros de seguridad de la terminal de acceso no lo son. Los pasos mostrados en la figura 8 corresponden a los pasos posteriores a todos los pasos descritos y mostrados en relación a la figura SA. Es decir, la figura 8 pretende mostrar los pasos que siguen después que se completan los pasos de la figura 5A.

Como se observó anteriormente con referencia a la figura 5B, al momento de la recepción del mensaje de comando de modo de seguridad de Estrato de Acceso (AS), la terminal de acceso 102 verifica que la capacidad de seguridad sea la misma que aquélla enviada en el mensaje de establecimiento de conexión RRC, calcula XMAC-I, y verifica la integridad del mensaje de comando de modo de seguridad AS comparando el MAC-I recibido con el XMAC-I generado 802. Si todas las verificaciones son exitosas, entonces la terminal de acceso 102 envía un mensaje

completo de modo de seguridad de Estrato de Acceso (AS) 804 incluyendo un MAC-I. Si las verificaciones no fueron exitosas, entonces se habría enviado un mensaje de rechazo de modo de seguridad AS. Cuando la red de acceso 104 recibe este mensaje completo de modo de seguridad AS 804, éste verifica la integridad del mensaje 806, y envía un mensaje completo de modo de seguridad AS 808 a la red núcleo 106 indicando los algoritmos de encriptación e integridad seleccionados.

Como se observó anteriormente, en algunos casos, la red de acceso 104 se puede actualizar a los nuevos parámetros de seguridad AS mientras la terminal de acceso 102 falla en actualizarse a los nuevos parámetros de seguridad AS. Por ejemplo, después de enviar el mensaje completo de modo de seguridad AS 804 a la red de acceso 104, y antes de recibir un acuse de recibo y/o actualizar la terminal de acceso a los nuevos parámetros de seguridad AS, la terminal de acceso 102 puede iniciar un procedimiento de movilidad, incluyendo la generación y envío de un mensaje de actualización de movilidad 810. Como un resultado de iniciar el procedimiento de movilidad, la terminal de acceso 102 aborta el procedimiento de modo de seguridad AS y se revierte a los viejos parámetros de seguridad AS 812. La terminal de acceso 102 puede recibir un mensaje de acuse de recibo 814 después de iniciar el procedimiento de movilidad, pero la terminal de acceso 102 ya habrá abortado el procedimiento de modo de seguridad AS y, por lo tanto, no se actualizará a los nuevos parámetros de seguridad AS, desconocidos para la red de acceso 104.

En dichos casos, el mensaje de actualización de movilidad 810 no está convenientemente encriptado, de manera que la red de acceso 104 puede recibir y procesar el mensaje de actualización de movilidad 810 incluso cuando la terminal de acceso 102 está operando con los viejos parámetros de seguridad AS. Sin embargo, cuando la red de acceso 104 envía un mensaje de confirmación de actualización de movilidad 816, ese mensaje 816 es cifrado con los nuevos parámetros de seguridad AS y, por lo tanto, no podrá ser decodificado por la terminal de acceso 102.

En la implementación mostrada en la figura 8, la red de acceso 104 puede ser adaptada para enviar la confirmación de actualización de movilidad 816 una o más veces. Después que la red de acceso 104 ha enviado el mensaje a la terminal de acceso 102 un número especificado de veces sin recibir una respuesta de la terminal de acceso 102, la red de acceso se puede adaptar para revertirse a los viejos parámetros de seguridad AS 518 y reenviar el mensaje de confirmación de actualización de movilidad 820 utilizando los viejos parámetros de seguridad AS. Si la red de acceso 104 recibe una respuesta al mensaje de confirmación de actualización de movilidad enviado utilizando los viejos parámetros de seguridad As, entonces la red de acceso 104 puede seguir utilizando los viejos parámetros de seguridad AS.

Terminal de Acceso Ejemplar

La figura 9 es un diagrama en bloques que ilustra componentes selectos de una terminal de acceso 900 de acuerdo con al menos una realización. La terminal de acceso 900 generalmente incluye un circuito de procesamiento 902 acoplado a un medio de almacenamiento 904 y una interfaz de comunicaciones inalámbricas 906.

El circuito de procesamiento 902 está acomodado para obtener, procesar y/o enviar datos, controlar el acceso y almacenamiento de datos, emitir comandos, y controlar otras operaciones deseadas. El circuito de procesamiento 902 puede ser implementado como uno o más de un procesador, un controlador, una pluralidad de procesadores y/u otra estructura configurada para ejecutar instrucciones ejecutables incluyendo, por ejemplo, instrucciones de software y/o microprogramación cableada, y/o circuitería de hardware. Realizaciones del circuito de procesamiento 902 pueden incluir un procesador de propósito general, un procesador de señal digital (DSP), un circuito integrado de aplicación específica (ASIC), un arreglo de puerta programable en campo (FPGA), u otro componente lógico programable, compuerta discreta o lógica de transistor, componentes de hardware discretos, o cualquier combinación de los mismos diseñada para ejecutar las funciones aquí descritas. Un procesador de propósito general puede ser un microprocesador pero, en la alternativa, el procesador puede ser cualquier procesador, controlador, microcontrolador, o máquina de estado convencional. Un procesador también puede ser implementado como una combinación de componentes de computación, tal como una combinación de un DSP y un microprocesador, un número de microprocesadores, uno o más microprocesadores en conjunto con un DSP núcleo, o cualquier otra configuración de este tipo. Estos ejemplos del circuito de procesamiento 902 son para ilustración y también se tienen contempladas otras configuraciones convenientes dentro del alcance de la presente divulgación.

El circuito de procesamiento 902 puede incluir un módulo de indicación y/o determinación de parámetros de seguridad 908. El módulo de indicación y/o determinación de parámetros de seguridad 908 puede comprender circuitería y/o programación adaptada para ejecutar procedimientos de indicación de parámetros de seguridad y/o procedimientos de determinación de parámetros de seguridad.

El medio de almacenamiento 904 puede representar uno o más dispositivos para almacenar programación y/o datos, tal como un código ejecutable por procesador o instrucciones (por ejemplo, software, microprogramación cableada), datos electrónicos, bases de datos, u otra información digital. El medio de almacenamiento 904 puede ser cualquier medio disponible al que pueda tener acceso un procesador de propósito especial o de propósito general. A modo de ejemplo y no limitación, el medio de almacenamiento 904 puede incluir memoria de solo lectura (por ejemplo, ROM, EPROM, EEPROM), memoria de acceso aleatorio (RAM), medios de almacenamiento de disco magnético, medios de almacenamiento óptico, dispositivos de memoria Flash, y/u otros medios legibles por ordenador no transitorios

para almacenamiento de información. El medio de almacenamiento 904 puede estar acoplado al circuito de procesamiento 902 de manera que el circuito de procesamiento 902 puede leer información de, y escribir información en el medio de almacenamiento 904. En la alternativa, el medio de almacenamiento 904 puede ser parte integral del circuito de procesamiento 902.

El medio de almacenamiento 904 puede incluir operaciones de indicación de parámetros de seguridad y/u operaciones de determinación de parámetros de seguridad 910, de acuerdo con una o más realizaciones. Las operaciones de indicación de parámetros de seguridad y/u operaciones de determinación de parámetros de seguridad 910 pueden ser implementadas por el circuito de procesamiento 902, por ejemplo, en el módulo de indicación y/o determinación de parámetros de seguridad 909. En algunas implementaciones, operaciones de indicación de parámetros de seguridad pueden comprender operaciones que pueden ser implementadas por el circuito de procesamiento 902 para indicar un estatus de los parámetros de seguridad de la terminal de acceso 900 a una red de acceso, tal como incluyendo un indicador en un mensaje de actualización de movilidad respecto a que la terminal de acceso 900 se ha revertido a los viejos parámetros de seguridad y/o enviando un mensaje indicando que la terminal de acceso 900 se ha actualizado con éxito a los nuevos parámetros de seguridad. En algunas implementaciones, las operaciones de determinación de parámetros de seguridad pueden comprender operaciones que pueden ser implementadas por el circuito de procesamiento 902 para determinar un estatus de los parámetros de seguridad en una red de acceso para comunicarse con la terminal de acceso 900, tal como determinando su falla para decodificar un mensaje de confirmación de actualización de movilidad recibido desde la red de acceso.

La interfaz de comunicaciones 906 está configurada para facilitar las comunicaciones inalámbricas de la terminal de acceso 900. Por ejemplo, la interfaz de comunicaciones 906 se puede configurar para comunicar información bidireccionalmente con respecto a una red de acceso y/u otras terminales de acceso. El circuito de comunicaciones 906 puede estar acoplado a una antena (que no se muestra) y puede incluir circuitería de transceptor inalámbrico, incluyendo al menos un transmisor 912 y/o al menos un receptor 914 (por ejemplo, una o más cadenas de transmisor/receptor).

De acuerdo con una o más características de la terminal de acceso 900, el circuito de procesamiento 902 se puede adaptar para ejecutar cualquiera o todos los procesos, funciones, pasos y/o rutinas relacionadas con las diversas terminales de acceso aquí descritas anteriormente con referencia a las figura 1-8 (por ejemplo, la terminal de acceso 102 y/o 402). Tal como aquí se utiliza, el término "adaptado" en relación al circuito de procesamiento 902 se puede referir al circuito de procesamiento 902 que es uno o más de configurado, empleado, implementado o programado para ejecutar un proceso, función, paso y/o rutina particular de acuerdo con las diversas características aquí descritas.

La figura 10 es un diagrama de flujo que ilustra un ejemplo de un procedimiento operativo en una terminal de acceso, tal como la terminal de acceso 900, para indicar a una red de acceso cuando la terminal de acceso se ha revertido a los viejos parámetros de seguridad. Haciendo referencia a las figuras 9 y 10, una terminal de acceso 900 puede conducir un procedimiento de modo de seguridad en el paso 1002. Por ejemplo, el circuito de procesamiento 902 se puede comunicar con una red de acceso a través de la interfaz de comunicaciones 906 para conducir el procedimiento de modo de seguridad. Como parte del procedimiento de modo de seguridad, el circuito de procesamiento 902 puede generar y enviar un mensaje completo de modo de seguridad a la red de acceso. De acuerdo con al menos algunas implementaciones, el procedimiento de modo de seguridad puede comprender un procedimiento de modo de seguridad de Estrato de Acceso (AS), donde el circuito de procesamiento 902 genera y envía un mensaje completo de modo de seguridad de Estrato de Acceso (AS). El circuito de procesamiento 902 puede enviar dicho mensaje completo de modo de seguridad AS utilizando una capa de control de recursos de radio (RRC) de la pila de protocolo para comunicarse con la red de acceso.

En el paso 1004, después que la terminal de acceso 900 envía un mensaje completo de modo de seguridad a la red de acceso, un procedimiento de movilidad puede ser iniciado mientras el procedimiento de modo de seguridad sigue estando activo. Por ejemplo, como resultado de la movilidad de la terminal de acceso 900, el circuito de procesamiento 902 puede iniciar un procedimiento de movilidad. Ejemplos de procedimiento de movilidad pueden incluir reselección de células, errores irrecuperables de control de enlace de radio (RLC), que la terminal de acceso esté fuera de servicio, etc.

En respuesta a iniciar un procedimiento de movilidad antes de actualizar sus parámetros de seguridad (por ejemplo, antes de recibir un acuse de recibo del mensaje completo de modo de seguridad o antes de la actualización en respuesta al acuse de recibo), la terminal de acceso 900 aborta el procedimiento de modo de seguridad en curso y se revierte a los viejos parámetros de seguridad en el paso 1006. Por ejemplo, el circuito de procesamiento 902 puede abortar el procedimiento de modo de seguridad activo y revertirse al empleo de los viejos parámetros de seguridad (por ejemplo, los viejos parámetros de seguridad de Estrato de Acceso (AS)) en respuesta a iniciar el procedimiento de movilidad.

En el paso 1008, la terminal de acceso 900 puede generar y enviar un mensaje de actualización de movilidad a la red de acceso. El mensaje de actualización de movilidad incluye un indicador adaptado para informar a la terminal de acceso que la terminal de acceso 900 se ha revertido a los viejos parámetros de seguridad. Por ejemplo, el circuito de procesamiento 902 puede ser adaptado para generar un mensaje de actualización de movilidad

incluyendo un elemento de información (IE) que indica que la terminal de acceso 900 se ha revertido a los viejos parámetros de seguridad abortando el procedimiento de modo de seguridad en curso. En al menos una implementación, el módulo de indicación y/o determinación de parámetros de seguridad 908 puede comprender un módulo de indicación de parámetros de seguridad que está adaptado para ejecutar operaciones de indicación de parámetros de seguridad 910 almacenados en el medio de almacenamiento 904 para generar el mensaje de actualización de movilidad con el elemento de información (IE) que comprende un indicador de estatus de seguridad dedicado adaptado para indicar que la terminal de acceso 900 se ha revertido por los viejos parámetros de seguridad.

El circuito de procesamiento 902 puede enviar el mensaje de actualización de movilidad generado incluyendo el indicador a la red de acceso a través de la interfaz de comunicaciones 906. El mensaje de actualización de movilidad puede ser enviado por el circuito de procesamiento 902 como un mensaje de control de recursos de radio (RRC) en la capa de control de recursos de radio (RRC) de la pila de protocolo. De acuerdo con al menos algunas implementaciones, el mensaje de actualización de movilidad enviado por el circuito de procesamiento 902 puede no estar cifrado (es decir, puede no estar encriptado) de manera que la red de acceso puede recibir y procesar el mensaje sin un conocimiento de los parámetros de seguridad activamente implementados por la terminal de acceso 900. El mensaje de actualización de movilidad puede comprender cualquier mensaje que resulte de la movilidad de la terminal de acceso 900 tal como, por ejemplo, un mensaje de reselección de célula, un mensaje de error irrecuperable de control de enlace de radio (RLC), un mensaje de fuera de servicio, etc.

La terminal de acceso 900 puede recibir, en respuesta al mensaje de actualización de movilidad, un mensaje de confirmación de actualización de movilidad que está cifrado de acuerdo con los viejos parámetros de seguridad. Por ejemplo, el circuito de procesamiento 902 puede recibir un mensaje de confirmación de actualización de movilidad a través de la interfaz de comunicaciones 906. El mensaje de confirmación de actualización de movilidad recibido está cifrado de acuerdo con los viejos parámetros de seguridad y puede ser decodificado por el circuito de procesamiento 902 empleando los viejos parámetros de seguridad de acuerdo con un algoritmo de acuerdo.

La figura 11 es un diagrama de flujo que ilustra un ejemplo de un procedimiento operativo en una terminal de acceso, tal como la terminal de acceso 900, para determinar un estatus de los parámetros de seguridad en una red de acceso para comunicación con la terminal de acceso. Haciendo referencia a las figuras 9 y 11, una terminal de acceso 900 puede conducir un procedimiento de modo de seguridad en el paso 1102. Por ejemplo, el circuito de procesamiento 902 se puede comunicar con una red de acceso a través de la interfaz de comunicaciones 906 para conducir el procedimiento de modo de seguridad. Como parte del procedimiento de modo de seguridad, el circuito de procesamiento 902 puede generar y enviar un mensaje completo de modo de seguridad a la red de acceso. El circuito de procesamiento 902 puede enviar el mensaje completo de modo de seguridad como un mensaje de control de recursos de radio (RRC) a la red de acceso.

En el paso 1104, después que la terminal de acceso 900 envía un mensaje completo de modo de seguridad a la red de acceso, un procedimiento de actualización de movilidad puede ser iniciado mientras el procedimiento de modo de seguridad sigue estando activo. Por ejemplo, como resultado de la movilidad de la terminal de acceso 900, el circuito de procesamiento 902 puede iniciar un procedimiento de movilidad. Ejemplos de procedimientos de movilidad pueden incluir la reselección de células, errores irrecuperables de control de enlace de radio (RLC), que la terminal de acceso esté fuera de servicio, etc. Como parte del procedimiento de movilidad, la terminal de acceso 900 envía un mensaje de actualización de movilidad a la red de acceso.

En respuesta a iniciar un procedimiento de movilidad, y antes de actualizar sus parámetros de seguridad (por ejemplo, antes de recibir un acuse de recibo L2 o antes de realizar una actualización en respuesta al acuse de recibo L2), la terminal de acceso 900 aborta el procedimiento de modo de seguridad en curso y se revierte a los viejos parámetros de seguridad en el paso 1106. Por ejemplo, el circuito de procesamiento 902 puede abortar el procedimiento de modo de seguridad activo y revertirse al empleo de los viejos parámetros de seguridad como un resultado de iniciar el procedimiento de movilidad.

En respuesta al mensaje de actualización de movilidad enviado a la red de acceso como parte del procedimiento de movilidad, la terminal de acceso 900 recibe un mensaje de confirmación de actualización de movilidad desde la red de acceso en el paso 1108. Por ejemplo, el circuito de procesamiento 902 puede recibir un mensaje de confirmación de actualización de movilidad a través de la interfaz de comunicaciones 906. En el paso 1110, el circuito de procesamiento 902 intenta decodificar el mensaje de confirmación de actualización de movilidad utilizando los viejos parámetros de seguridad. Por ejemplo, el circuito de procesamiento 902 puede incluir un módulo de determinación de parámetros de seguridad 908 adaptado para ejecutar operaciones de determinación de parámetros de seguridad 910 almacenadas en el medio de almacenamiento 904. Si el circuito de procesamiento 902 puede decodificar el mensaje de confirmación de actualización de movilidad, entonces la terminal de acceso envía un mensaje de respuesta a la red de acceso en el paso 1112. En este caso, el mensaje de respuesta sería cifrado utilizando los viejos parámetros de seguridad.

Sin embargo, si el circuito de procesamiento 902 (por ejemplo, el módulo de determinación de parámetros de seguridad 908) no puede decodificar el mensaje de confirmación de actualización de movilidad, entonces el circuito de procesamiento 902 puede cambiar a los nuevos parámetros de seguridad en el paso 1114 y puede intentar

decodificar el mensaje de confirmación de actualización de movilidad utilizando los nuevos parámetros de seguridad. De acuerdo con al menos una implementación, el circuito de procesamiento 902 (por ejemplo, el módulo de determinación de parámetros de seguridad 908) puede ser adaptado para conmutar a los nuevos parámetros de seguridad después de cierto número predeterminado de intentos fallidos por decodificar el mensaje de confirmación de actualización de movilidad (por ejemplo, uno o más intentos).

Si el circuito de procesamiento 902 es exitoso en decodificar el mensaje de confirmación de actualización de movilidad utilizando los nuevos parámetros de seguridad, entonces el circuito de procesamiento 902 se puede adaptar para seguir utilizando los nuevos parámetros de seguridad en el paso 1118. El circuito de procesamiento 902 puede entonces enviar un mensaje de respuesta a la red de acceso a través de la interfaz de comunicaciones 906 utilizando los nuevos parámetros de seguridad en el paso 1112. Si el circuito de procesamiento 902 no tiene éxito en decodificar el mensaje de confirmación de actualización de movilidad utilizando los nuevos parámetros de seguridad, entonces la llamada puede fallar.

La figura 12 es un diagrama de flujo que ilustra un ejemplo de un procedimiento operativo en una terminal de acceso, tal como la terminal de acceso 900, para indicar a una red de acceso cuando la terminal de acceso se ha actualizado a los nuevos parámetros de seguridad. Haciendo referencia a las figuras 9 y 12, una terminal de acceso 900 que conduce un procedimiento de modo de seguridad puede generar y enviar un mensaje completo de modo de seguridad a la red de acceso en el paso 1202. Por ejemplo, el circuito de procesamiento 902 (por ejemplo, un módulo de indicación de parámetros de seguridad 908) puede generar y enviar un mensaje completo de modo de seguridad a través de la interfaz de comunicaciones 906. El circuito de procesamiento 902 puede enviar el mensaje completo de modo de seguridad como un mensaje de control de recursos de radio (RRC) a la red de acceso.

En el paso 1204, el circuito de procesamiento 902 puede recibir, a través de la interfaz de comunicaciones 906, un mensaje de acuse de recibo de la red de acceso. El mensaje de acuse de recibo es recibido en respuesta al mensaje completo de modo de seguridad y puede comprender' una transmisión L2. El mensaje de acuse de recibo puede indicar al circuito de procesamiento 902 que el mensaje completo de modo de seguridad fue recibido con éxito por la red de acceso. En respuesta a la recepción del mensaje de acuse de recibo, el circuito de procesamiento 902 actualiza los parámetros de seguridad de la terminal de acceso 900 a los nuevos parámetros de seguridad en el paso 1206.

Después que la terminal de acceso 900 es actualizada a los nuevos parámetros de seguridad, el circuito de procesamiento 902 envía una indicación a la red de acceso en el paso 908 para informar a la terminal de acceso que la terminal de acceso 900 se ha actualizado con éxito a los nuevos parámetros de seguridad. Por ejemplo, el circuito de procesamiento 902 (por ejemplo, el módulo de indicación de parámetros de seguridad 908) puede generar y enviar un mensaje de acuse de recibo L3 a la red de acceso a través de la interfaz de comunicaciones 906 para indicar que la terminal de acceso 900 se ha actualizado con éxito a los nuevos parámetros de seguridad.

Entidad de red ejemplar

La figura 13 es un diagrama en bloques que ilustra componentes selectos de una entidad de red 1300 de acuerdo con al menos una realización. De acuerdo con al menos algunas implementaciones, la entidad de red 1300 puede comprender un controlador de red de radio (RNC) de una red de acceso, tal como RNC 114 en la figura 1. La entidad de red 1300 generalmente incluye un circuito de procesamiento 1302 acoplado a un medio de almacenamiento 1304 y una interfaz de comunicaciones 1306.

El circuito de procesamiento 1302 está acomodado para obtener, procesar y/o enviar datos, controlar el acceso y almacenamiento de datos, emitir comandos, y controlar otras operaciones deseadas. El circuito de procesamiento 1302 puede comprender circuitería configurada para implementar programación deseada proporcionada por medios apropiados en al menos una realización. Por ejemplo, el circuito de procesamiento 1302 puede ser implementado como uno o más de un procesador, un controlador, una pluralidad de procesadores y/u otra estructura configurada para ejecutar instrucciones ejecutables incluyendo, por ejemplo, instrucciones de software y/o microprogramación cableada, y/o circuitería de hardware. Realizaciones del circuito de procesamiento 1302 pueden incluir un procesador de propósito general, un procesador de señal digital (DSP), un circuito integrado de aplicación específica (ASIC), un arreglo de puerta programable en campo (FPGA), u otro componente lógico programable, compuerta discreta o lógica de transistor, componentes de hardware discretos, o cualquier combinación de los mismos diseñada para ejecutar las funciones aquí descritas. Un procesador de propósito general puede ser un microprocesador pero, en la alternativa, el procesador puede ser cualquier procesador, controlador, microcontrolador, o máquina de estado convencional. Un procesador también puede ser implementado como una combinación de componentes de computación, tal como una combinación de un DSP y un microprocesador, un número de microprocesadores, uno o más microprocesadores en conjunto con un DSP núcleo, o cualquier otra configuración de este tipo. Estos ejemplos del circuito de procesamiento 1302 son para ilustración y también se tienen contempladas otras configuraciones convenientes dentro del alcance de la presente divulgación.

El circuito de procesamiento 1302 puede incluir un módulo de reversión y/o actualización de parámetros de seguridad 1308. El módulo de reversión y/o actualización de parámetros de seguridad 1308 puede comprender circuitería y/o programación adaptada para ejecutar procedimientos para revertirse a viejos parámetros de seguridad

y/o procedimientos para actualizarse a los nuevos parámetros de seguridad, de acuerdo con varias implementaciones.

El medio de almacenamiento 1304 puede representar uno o más dispositivos para almacenar programación y/o datos, tal como un código ejecutable por procesador o instrucciones (por ejemplo, software, microprogramación cableada), datos electrónicos, bases de datos, u otra información digital. El medio de almacenamiento 904 puede ser cualquier medio disponible al que pueda tener acceso un procesador de propósito especial o de propósito general. A manera de ejemplo y no de limitación, el medio de almacenamiento 1304 puede incluir memoria de solo lectura (por ejemplo, ROM, EPROM, EEPROM), memoria de acceso aleatorio (RAM), medios de almacenamiento de disco magnético, medios de almacenamiento óptico, dispositivos de memoria Flash, y/u otros medios legibles por computadora no transitorios para almacenamiento de información. El medio de almacenamiento 1304 puede estar acoplado al circuito de procesamiento 1302 de manera que el circuito de procesamiento 1302 puede leer información de, y escribir información en el medio de almacenamiento 1304. En la alternativa, el medio de almacenamiento 1304 puede ser parte integral del circuito de procesamiento 1302.

El medio de almacenamiento 1304 puede incluir operaciones de reversión y/o actualización de parámetros de seguridad 1310, de acuerdo con una o más realizaciones. Las operaciones de reversión y/o actualización de parámetros de seguridad 1310 pueden ser implementadas por el circuito de procesamiento 1302, por ejemplo, en el módulo de reversión y/o actualización de parámetros de seguridad 1308. En algunas implementaciones, operaciones de reversión de parámetros de seguridad pueden comprender operaciones que pueden ser implementadas por el circuito de procesamiento 1302 para determinar si se revierte a viejos parámetros de seguridad y llevar a cabo la reversión nuevamente a los viejos parámetros de seguridad. En algunas implementaciones, las operaciones de actualización de parámetros de seguridad pueden comprender operaciones que pueden ser implementadas por el circuito de procesamiento 1302 para actualizar los parámetros de seguridad.

La interfaz de comunicaciones 1306 está configurada para facilitar las comunicaciones inalámbricas de la entidad de red 1300. Por ejemplo, la interfaz de comunicaciones 1306 se puede configurar para comunicar información bidireccionalmente con respecto a una o más terminales de acceso y/u otras entidades de red. El circuito de comunicaciones 1306 puede estar acoplado a una antena (que no se muestra) y puede incluir circuitería de transceptor inalámbrico, incluyendo al menos un transmisor 1312 y/o al menos un receptor 1314 (por ejemplo, una o más cadenas de transmisor/receptor).

De acuerdo con una o más características de la entidad de red 1300, el circuito de procesamiento 1302 se puede adaptar para ejecutar cualquiera o todos los procesos, funciones, pasos y/o rutinas relacionadas con una o más de las diversas entidades de red aquí descritas anteriormente con referencia a las figura 1-8 (por ejemplo, una entidad de red de acceso 104, tal como el nodo de acceso 112 y/o el controlador de red de radio (RNC) 114, o una entidad de red núcleo 106, tal como el nodo de soporte GPRS en servicio (SGSN) 116 y/o el centro de conmutación móvil (MSC) 118). Tal como aquí se utiliza, el término "adaptado" en relación al circuito de procesamiento 1302 se puede referir al circuito de procesamiento 1302 que es uno o más de configurado, empleado, implementado o programado para ejecutar un proceso, función, paso y/o rutina particular de acuerdo con las diversas características aquí descritas.

La figura 14 es un diagrama de flujo que ilustra un ejemplo de un procedimiento operativo en una entidad de red, tal como la entidad de red 1300, para determinar que una terminal de acceso se ha revertido a los viejos parámetros de seguridad. Haciendo referencia a las figuras 13 y 14, una entidad de red 1300 puede recibir un mensaje completo de modo de seguridad desde una terminal de acceso en el paso 1402. Por ejemplo, el circuito de procesamiento 1302 puede recibir un mensaje completo de modo de seguridad a través de la interfaz de comunicaciones 1306. En al menos algunas implementaciones, el mensaje completo de modo de seguridad puede comprender un mensaje completo de modo de seguridad de Estrato de Acceso (AS). El mensaje completo de modo de seguridad AS puede ser recibido a través de la interfaz de comunicaciones 1306 en una capa de control de recursos de radio (RRC) de la pila de protocolo.

En respuesta al mensaje completo de modo de seguridad recibido desde la terminal de acceso, la entidad de red 1300 se puede actualizar a nuevos parámetros de seguridad para comunicaciones entre la entidad de red 1300 y la terminal de acceso en el paso 1404. En al menos una implementación, el circuito de procesamiento 1302 se puede adaptar para actualizar los parámetros de seguridad asociados con la terminal de acceso a nuevos parámetros de seguridad en respuesta a la recepción del mensaje completo de modo de seguridad. En implementaciones donde el mensaje completo de modo de seguridad comprende un mensaje completo de modo de seguridad AS, los nuevos parámetros de seguridad pueden comprender nuevos parámetros de seguridad de Estrato de Acceso (AS). El circuito de procesamiento 1302 se puede adaptar para conservar los viejos parámetros de seguridad por un periodo de tiempo especificado después de la actualización a los nuevos parámetros de seguridad. Por ejemplo, el circuito de procesamiento 1302 puede almacenar los viejos parámetros de seguridad en el medio de almacenamiento 1304 por un periodo de tiempo (por ejemplo, hasta que una comunicación es recibida desde la terminal de acceso empleando los nuevos parámetros de seguridad).

En el paso 1406, la entidad de red 1300 puede recibir un mensaje de actualización de movilidad desde la terminal de acceso, donde el mensaje de actualización de movilidad incluye un indicador de estatus de seguridad dedicado

adaptado para indicar a la entidad de red 1300 que la terminal de acceso se ha revertido a los viejos parámetros de seguridad. Por ejemplo, el circuito de procesamiento 1302 puede recibir el mensaje de actualización de movilidad a través de la interfaz de comunicaciones 1306. El mensaje de actualización de movilidad puede ser recibido como un mensaje de control de recursos de radio (RRC). De acuerdo con al menos una implementación, el mensaje de actualización de movilidad no está cifrado, y puede ser leído por el circuito de procesamiento 1302 sin decodificar el mensaje primero. El mensaje de actualización de movilidad puede comprender un mensaje enviado por la terminal de acceso por motivos de movilidad. A manera de ejemplo y no limitación, el mensaje de actualización de movilidad puede comprender un mensaje de reselección de células, un mensaje de error irrecuperable de control de enlace de radio (RLC), un mensaje de fuera de servicio, etc.

En algunas implementaciones, el indicador de estatus dedicado incluido con el mensaje de actualización de movilidad puede comprender un elemento de información (IE) adaptado para indicar que la terminal de acceso se ha revertido a los viejos parámetros de seguridad. En algunas implementaciones, el indicador de estatus dedicado incluido con el mensaje de actualización de movilidad puede comprender uno o más bits adaptados para indicar que la terminal de acceso se ha revertido a los viejos parámetros de seguridad.

En el paso 1408, la entidad de red 1300 se revierte a los viejos parámetros de seguridad. Por ejemplo, el circuito de procesamiento 1302 se puede revertir a los viejos parámetros de seguridad en respuesta al mensaje de actualización de movilidad recibido incluyendo el indicador de estatus de seguridad dedicado. En algunas implementaciones, el módulo de reversión y/o actualización de parámetros de seguridad 1308 puede ejecutar las operaciones de reversión y/o actualización de parámetros de seguridad 1310 al momento de la recepción del indicador de estatus de seguridad dedicado informando a la entidad de red 1300 que la terminal de acceso se ha revertido a los viejos parámetros de seguridad. Como parte de las operaciones de reversión y/o actualización de parámetros de seguridad 1310, el módulo de reversión y/o actualización de parámetros de seguridad 1308 puede retener una asociación entre la terminal de acceso y los viejos parámetros de seguridad para poder reemplazar los nuevos parámetros de seguridad con los parámetros de seguridad previos (o viejos). De esta manera, el circuito de procesamiento 1302 puede emplear los viejos parámetros de seguridad para posteriores comunicaciones con la terminal de acceso.

En respuesta al mensaje de actualización de movilidad recibido, la entidad de red 1300 puede enviar un mensaje de confirmación de actualización de movilidad a la terminal de acceso en el paso 1410 para reconocer la recepción del mensaje de actualización de movilidad. El mensaje de confirmación de actualización de movilidad puede ser cifrado de acuerdo con los viejos parámetros de seguridad. En al menos algunas implementaciones, el circuito de procesamiento 1302 puede generar un mensaje de confirmación de actualización de movilidad y puede cifrar el mensaje de confirmación de actualización de movilidad de acuerdo con los viejos parámetros de seguridad. El circuito de procesamiento 1302 puede entonces enviar el mensaje de confirmación de actualización de movilidad cifrado a la terminal de acceso a través de la interfaz de comunicaciones 1306.

La figura 15 es un diagrama de flujo que ilustra un ejemplo de un procedimiento operativo en una entidad de red, tal como la entidad de red 1300, para determinar que una terminal de acceso se ha revertido a los viejos parámetros de seguridad. Haciendo referencia a las figuras 13 y 15, una entidad de red 1300 puede recibir un mensaje completo de modo de seguridad desde una terminal de acceso en el paso 1502. Por ejemplo, el circuito de procesamiento 1302 puede recibir un mensaje completo de modo de seguridad a través de la interfaz de comunicaciones 1306.

En respuesta al mensaje completo de modo de seguridad recibido desde la terminal de acceso, la entidad de red 1300 se puede actualizar a nuevos parámetros de seguridad para comunicaciones entre la entidad de red 1300 y la terminal de acceso en el paso 1504. En al menos una implementación, el circuito de procesamiento 1302 puede estar adaptado para actualizar los parámetros de seguridad asociados con la terminal de acceso a nuevos parámetros de seguridad en respuesta a la recepción del mensaje completo de modo de seguridad. El circuito de procesamiento 1302 se puede adaptar para retener los viejos parámetros de seguridad durante un periodo de tiempo especificado después de la actualización a los nuevos parámetros de seguridad. Por ejemplo, el circuito de procesamiento 1302 puede almacenar los viejos parámetros de seguridad en el medio de almacenamiento 1304 durante un periodo de tiempo (por ejemplo, hasta que una comunicación es recibida desde la terminal de acceso que emplea los nuevos parámetros de seguridad).

En el paso 1506, la entidad de red 1300 puede recibir un mensaje de actualización de movilidad desde la terminal de acceso. Por ejemplo, el circuito de procesamiento 1302 puede recibir el mensaje de actualización de movilidad a través de la interfaz de comunicaciones 1306. El mensaje de actualización de movilidad puede ser recibido como un mensaje de control de recursos de radio (RRC). De acuerdo con al menos una implementación, el mensaje de actualización de movilidad no está cifrado, y puede ser leído por el circuito de procesamiento 1302 sin decodificar el mensaje primero.

En respuesta al mensaje de actualización de movilidad recibido, la entidad de red 1300 genera y envía un mensaje de confirmación de actualización de movilidad en el paso 1508. Por ejemplo, el circuito de procesamiento 1302 puede generar un mensaje de confirmación de actualización de movilidad y puede cifrar el mensaje de acuerdo con los nuevos parámetros de seguridad. El circuito de procesamiento 1302 puede entonces enviar el mensaje de confirmación de actualización de movilidad cifrado a través de la interfaz de comunicaciones 1306 a la terminal de

acceso.

En el paso 1510, la entidad de red 1300 determina si una respuesta al mensaje de confirmación de actualización de movilidad ha sido recibida desde la terminal de acceso. Por ejemplo, el circuito de procesamiento 1302 puede monitorear comunicaciones recibidas a través de la interfaz de comunicaciones 1306 para una respuesta al mensaje de confirmación de actualización de movilidad. En al menos algunas implementaciones, las operaciones de reversión y/o actualización de parámetros de seguridad 1310 pueden ocasionar que el módulo de reversión y/o actualización de parámetros de seguridad 1308 monitoree la respuesta recibida. Si una respuesta es recibida, el circuito de procesamiento 1302 puede seguir utilizando los nuevos parámetros de seguridad.

Si no se recibe una respuesta, entonces el módulo de reversión y/o actualización de parámetros de seguridad 1308 puede revertirse a los viejos parámetros de seguridad en el paso 1512 para determinar si la terminal de acceso está empleando los viejos parámetros de seguridad. En algunas implementaciones, el circuito de procesamiento 1302 (por ejemplo, las operaciones de reversión y/o actualización de parámetros de seguridad 1310) puede estar adaptado para reenviar el mensaje de confirmación de actualización de movilidad después de una falla para recibir una respuesta, y esperar otra respuesta al mensaje de confirmación de actualización de movilidad reenviado. Si no se recibe una respuesta después de un número de veces predeterminado que se envía el mensaje de confirmación de actualización de movilidad, el circuito de procesamiento 1302 (por ejemplo, las operaciones de reversión y/o actualización de parámetros de seguridad 1310) se puede adaptar para revertirse a los viejos parámetros de seguridad a fin de determinar si la terminal de acceso está empleando los viejos parámetros de seguridad.

Al emplear los viejos parámetros de seguridad, la entidad de red 1300 genera y envía otro mensaje de confirmación de actualización de movilidad en el paso 1514. En algunas implementaciones, el circuito de procesamiento 1302 puede generar un mensaje de confirmación de actualización de movilidad y puede cifrar el mensaje. A diferencia de los mensajes de confirmación de actualización de movilidad previos cifrados de acuerdo con los nuevos parámetros de seguridad, este mensaje de confirmación de actualización de movilidad es cifrado de acuerdo con los viejos parámetros de seguridad. El circuito de procesamiento 1302 puede entonces enviar el mensaje de confirmación de actualización de movilidad cifrado a través de la interfaz de comunicaciones 1306 a la terminal de acceso.

En el paso 1516, la entidad de red 1300 determina si una respuesta al mensaje de confirmación de actualización de movilidad cifrado de acuerdo con los viejos parámetros de seguridad ha sido recibida desde la terminal de acceso. Por ejemplo, el circuito de procesamiento 1302 puede monitorear las comunicaciones recibidas a través de la interfaz de comunicaciones 1306 para una respuesta al mensaje de confirmación de actualización de movilidad. Si se recibe una respuesta al mensaje de confirmación de actualización de movilidad cifrado de acuerdo con los viejos parámetros de seguridad, el módulo de reversión y/o actualización de parámetros de seguridad 1308 puede determinar que la terminal de acceso se ha revertido a los viejos parámetros de seguridad, y puede ocasionar que la entidad de red 1300 continúe utilizando los viejos parámetros de seguridad en el paso 1518. Si no se recibe una respuesta al mensaje de confirmación de actualización de movilidad cifrado de acuerdo con los viejos parámetros de seguridad, el circuito de procesamiento 1302 puede ocasionar que la llamada se caiga con la terminal de acceso.

La figura 16 es un diagrama de flujo que ilustra un ejemplo de un procedimiento operativo en una entidad de red, tal como la entidad de red 1300, para actualizarse de los viejos parámetros de seguridad a los nuevos parámetros de seguridad después que la terminal de acceso se ha actualizado a los nuevos parámetros de seguridad. Haciendo referencia a las figuras 13 y 16, una entidad de red 1300 puede recibir un mensaje completo de modo de seguridad desde una terminal de acceso en el paso 1602. Por ejemplo, el circuito de procesamiento 1302 puede recibir un mensaje completo de modo de seguridad a través de la interfaz de comunicaciones 1306.

En respuesta al mensaje completo de modo de seguridad, la entidad de red 1300 envía un mensaje de acuse de recibo a la terminal de acceso en el paso 1604. El mensaje de acuse de recibo puede comprender una transmisión L2 adaptada para indicar a la terminal de acceso que el mensaje completo de modo de seguridad fue recibido y verificado con éxito por la entidad de red. De acuerdo con al menos una implementación, el circuito de procesamiento 1302 puede generar y enviar el mensaje de acuse de recibo a la terminal de acceso a través de la interfaz de comunicaciones 1306.

En el paso 1606, la entidad de red 1300 recibe un mensaje de acuse de recibo desde la terminal de acceso. El mensaje de acuse de recibo recibido puede comprender un mensaje de acuse de recibo L3 adaptado para indicar que la terminal de acceso se ha actualizado con éxito a los nuevos parámetros de seguridad. En al menos una implementación, el circuito de procesamiento 1302 (por ejemplo, el módulo de reversión y/o actualización de parámetros de seguridad 1308) puede recibir el mensaje de acuse de recibo L3 a través de la interfaz de comunicaciones 1306.

En respuesta a recibir el mensaje de acuse de recibo desde la terminal de acceso, la entidad de red 1300 se puede actualizar a los nuevos parámetros de seguridad para comunicaciones entre la entidad de red 1300 y la terminal de acceso en el paso 1608. Por ejemplo, el circuito de procesamiento 1302 (por ejemplo, el módulo de reversión y/o actualización de parámetros de seguridad 1308) puede actualizar los parámetros de seguridad asociados con la terminal de acceso a los nuevos parámetros de seguridad en respuesta a la recepción del mensaje de acuse de recibo adaptado para indicar que la terminal de acceso se ha actualizado a los nuevos parámetros de seguridad. El

circuito de procesamiento 1302 entonces puede emplear los nuevos parámetros de seguridad para posteriores comunicaciones con la terminal de acceso.

Uno o más de los componentes, pasos, características y/o funciones ilustrados en las figuras 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15 y/o 16 se pueden reacomodar y/o combinar en un solo componente, paso, característica o función o se puede incorporar en varios componentes, pasos o funciones. Elementos, componentes, pasos y/o funciones adicionales también se pueden agregar sin apartarse de la presente divulgación. Los aparatos, dispositivos y/o componentes ilustrados en las figuras 1, 4, 9 y/o 13 se pueden configurar para ejecutar uno o más de los procedimientos, características o pasos descritos con referencia a las figuras 2, 3, 5, 6, 7, 8, 10, 11, 12, 14, 15 y/o 16. Los algoritmos novedosos aquí descritos también pueden ser implementados de manera eficiente en software y/o incorporados en microprogramación cableada.

También, se observa que al menos algunas implementaciones han sido descritas como un proceso que se muestra como un gráfico de flujo, un diagrama de flujo, un diagrama de estructura, o un diagrama en bloques. Aunque un gráfico de flujo puede describir las operaciones como un proceso secuencial, muchas de las operaciones pueden ser ejecutadas en paralelo o de manera concurrente. Además, el orden de las operaciones se puede reacomodar. Un proceso finaliza cuando se completan sus operaciones. Un proceso puede corresponder a un procedimiento, una función, un procedimiento, una subrutina, o subprograma, etc. Cuando un proceso corresponde a una función, su terminación corresponde a un retorno de la función a la función de llamada o la función principal.

Además, las realizaciones pueden implementarse por hardware, software, microprogramación cableada, soporte intermedio, microcódigo o cualquier combinación de los mismos. Cuando se implementa en software, microprogramación cableada, soporte intermedio o microcódigo, el código de programa o segmentos de código para ejecutar las tareas necesarias pueden ser almacenados en un medio legible por máquina tal como un medio de almacenamiento u otros almacenamientos. Un procesador puede ejecutar las tareas necesarias. Un segmento de código puede representar un procedimiento, una función, un subprograma, un programa, una rutina, una subrutina, un módulo, un paquete de software, una clase, o cualquier combinación de instrucciones, estructuras de datos o divulgaciones de programa. Un segmento de código se puede acoplar a otro segmento de código o un circuito de pasados, reenviados o transmitidos a través de cualquier medio conveniente incluyendo el reparto de memoria, pase de mensajes, pase de componentes léxicos, transmisión de red, etc.

Los términos "medio legible por máquina", "medio legible por ordenador", y/o "medio legible por procesador" pueden incluir, pero no se limitan a dispositivos de almacenamiento portátiles o fijos, dispositivos de almacenamiento óptico, y otros medios no transitorios con la capacidad para almacenar, contener o llevar instrucciones y/o datos. Por lo tanto, los diversos procedimientos aquí descritos pueden ser parcial o completamente implementados por instrucciones y/o datos que pueden ser almacenados en un "medio legible por máquina", "medio legible por computadora", y/o "medio legible por procesador" y ejecutados por uno o más procesadores, máquinas y/o dispositivos.

Los procedimientos o algoritmos descritos en relación con los ejemplos aquí divulgados pueden ser incorporados directamente en hardware, en un módulo de software ejecutable por un procesador, o en una combinación de ambos, en la forma de unidad de procesamiento, instrucciones de programación, u otras direcciones, y pueden estar contenidos en un solo dispositivo o distribuidos a través de múltiples dispositivos. Un módulo de software puede residir en memoria RAM, memoria Flash, memoria ROM, memoria EPROM, memoria EEPROM, registros, disco duro, disco removible, un CD-ROM, o cualquier forma de medio de almacenamiento no transitorio conocido en la técnica. Un medio de almacenamiento puede estar acoplado al procesador de manera que el procesador puede leer información de, y escribir información en el medio de almacenamiento. En la alternativa, el medio de almacenamiento puede ser parte integral del procesador.

Los expertos en la técnica además apreciarán que los diversos bloques lógicos ilustrativos, módulos, circuitos y pasos de algoritmo descritos en conexión con las realizaciones aquí divulgadas pueden ser implementados como hardware electrónico, software de computadora, o combinaciones de ambos. Para ilustrar claramente esta capacidad de intercambio de hardware y software, varios componentes ilustrativos, bloques, módulos, circuitos y pasos han sido descritos antes generalmente en términos de su funcionalidad. Si dicha funcionalidad es implementada como hardware o software depende de la aplicación particular y las restricciones de diseño impuestas sobre el sistema en general.

Las diversas características de la invención aquí descritas pueden ser implementadas en diferentes sistemas sin apartarse de la invención. Se debiera observar que las realizaciones anteriores son simplemente ejemplos y no se interpretarán como una limitación de la invención. La descripción de las realizaciones está destinada a ser ilustrativa, y no a limitar el alcance de la divulgación. Debido a esto, las presentes enseñanzas pueden ser fácilmente aplicadas a otros tipos de aparatos y muchas alternativas, modificaciones y variaciones serán aparentes para aquellos expertos en la técnica.

REIVINDICACIONES

1. Una terminal de acceso (900), que comprende:

medios para conducir un procedimiento de modo de seguridad para reconfigurar los parámetros de seguridad de la terminal de acceso (902, 910);
medios para iniciar un procedimiento de movilidad mientras el procedimiento de modo de seguridad sigue su curso (902, 910);
medios para abortar el procedimiento de modo de seguridad y revertir a los viejos parámetros de seguridad como un resultado de iniciar el procedimiento de movilidad (902, 910); **caracterizada por**
medios para enviar un mensaje de actualización de movilidad incluyendo un indicador de estatus dedicado adaptado para indicar que la terminal de acceso se ha revertido a los viejos parámetros de seguridad (902, 914).

2. La terminal de acceso de acuerdo con la reivindicación 1, en la que el procedimiento de modo de seguridad comprende un procedimiento de modo de seguridad de Estrato de Acceso utilizando una capa de control de recursos de radio (RRC) de una pila de protocolo para reconfigurar los parámetros de seguridad del Estrato de Acceso de la terminal de acceso.

3. La terminal de acceso de acuerdo con la reivindicación 1, en la que los medios se proporcionan mediante una interfaz de comunicaciones inalámbricas adaptada para facilitar las comunicaciones inalámbricas y un circuito de procesamiento, estando el circuito de procesamiento además adaptado para:

generar y enviar un mensaje completo de modo de seguridad a la red de acceso a través de la interfaz de comunicaciones inalámbricas como parte del procedimiento de modo de seguridad (804).

4. La terminal de acceso de acuerdo con la reivindicación 1, en la que el mensaje de actualización de movilidad comprende:

(i) un mensaje de control de recursos de radio (RRC); o
(ii) uno de un mensaje de reselección de célula, un mensaje de error irrecuperable de control de enlace de radio (RLC) o un mensaje de fuera de servicio.

5. La terminal de acceso de acuerdo con la reivindicación 1, en la que el indicador de estatus de seguridad dedicado comprende:

(i) un elemento de información (IE) del mensaje de actualización de movilidad; o
(ii) uno o más bits del mensaje de actualización de movilidad.

6. La terminal de acceso de acuerdo con la reivindicación 1, en la que los medios se proporcionan mediante una interfaz de comunicaciones inalámbricas adaptada para facilitar las comunicaciones inalámbricas y un circuito de procesamiento, estando el circuito de procesamiento también adaptado para abortar el procedimiento de modo de seguridad y revertirse a los viejos parámetros de seguridad cuando un mensaje de acuse de reciboacuse de recibo no es recibido desde la red de acceso antes que se inicie el procedimiento de movilidad.

7. La terminal de acceso de acuerdo con la reivindicación 1, en la que los medios se proporcionan mediante una interfaz de comunicaciones inalámbricas adaptada para facilitar las comunicaciones inalámbricas y un circuito de procesamiento, estando el circuito de procesamiento también adaptado para:

recibir un mensaje de confirmación de actualización de movilidad desde la red de acceso, en la que el mensaje de confirmación de actualización de movilidad está cifrado de acuerdo con los viejos parámetros de seguridad.

8. Un procedimiento operativo en una terminal de acceso, que comprende:

conducir un procedimiento de modo de seguridad para reconfigurar parámetros de seguridad de la terminal de acceso (1002);
iniciar un procedimiento de movilidad mientras el procedimiento de modo de seguridad sigue su curso (1004);
abortar el procedimiento de modo de seguridad y revertirse a los viejos parámetros de seguridad como un resultado de iniciar el procedimiento de movilidad (1006); **caracterizado por**
enviar un mensaje de actualización de movilidad incluyendo un indicador de estatus dedicado adaptado para indicar que la terminal de acceso se ha revertido a los viejos parámetros de seguridad (1008).

9. El procedimiento de acuerdo con la reivindicación 8, en el que:

iniciar el procedimiento de movilidad comprende iniciar un procedimiento de actualización de células; y
enviar el mensaje de actualización de movilidad comprende enviar un mensaje de actualización de células desde uno de un mensaje de reselección de células, o un mensaje de error irrecuperable de control de enlace de radio (RLC) o un mensaje de fuera de servicio.

10. El procedimiento de acuerdo con la reivindicación 8, en el que el envío del mensaje de actualización de movilidad incluyendo el indicador de estatus dedicado adaptado para indicar que la terminal de acceso se ha revertido a los viejos parámetros de seguridad comprende:

enviar el mensaje de actualización de movilidad incluyendo:

(i) un elemento de información (IE) adaptado para indicar que la terminal de acceso se ha revertido a los viejos parámetros de seguridad; o
(ii) uno o más bits adaptados para indicar que la terminal de acceso se ha revertido a los viejos parámetros de seguridad.

11. Un procedimiento operativo en una entidad de red, que comprende:

recibir un mensaje completo de modo de seguridad desde una terminal de acceso (1402; 1502);
actualizarse a nuevos parámetros de seguridad en respuesta al mensaje completo de modo de seguridad (1404; 1504); y
revertir a los viejos parámetros de seguridad, **caracterizado por**
recibir un mensaje de actualización de movilidad desde la terminal de acceso, incluyendo el mensaje de actualización de movilidad un indicador de estatus de seguridad dedicado adaptado para indicar que la terminal de acceso se ha revertido a los viejos parámetros de seguridad (1406); en el que el paso de reversión a los viejos parámetros de seguridad es en respuesta al mensaje de actualización de movilidad recibido.

12. El procedimiento de acuerdo con la reivindicación 11, que además comprende:

enviar un mensaje de confirmación de actualización de movilidad a la terminal de acceso, en el que el mensaje de confirmación de actualización de movilidad está cifrado de acuerdo con los viejos parámetros de seguridad (1514).

13. Una entidad de red (1300), que comprende:

medios para recibir un mensaje completo de modo de seguridad desde una terminal de acceso (1314);
medios para actualizarse a los nuevos parámetros de seguridad en respuesta al mensaje completo de modo de seguridad (1302, 1308, 1310);
medios para revertirse a los viejos parámetros de seguridad (1302, 1308, 1310); **caracterizada por**
medios para recibir un mensaje de actualización de movilidad desde la terminal de acceso (1314), incluyendo el mensaje de actualización de movilidad un indicador de estatus de seguridad dedicado adaptado para indicar que la terminal de acceso se ha revertido a los viejos parámetros de seguridad; en la que los medios de reversión a los viejos parámetros de seguridad responden al mensaje de actualización de movilidad recibido.

14. La entidad de red de acuerdo con la reivindicación 13, en la que la entidad de red comprende un controlador de red de radio (RNC) (114).

15. Un medio legible por procesador que comprende instrucciones, las cuales cuando son ejecutadas por un procesador hacen que el procesador realice el procedimiento de cualquiera de las reivindicaciones 8 a 10 cuando es operativo en una terminal de acceso o realice el procedimiento de cualquiera de las reivindicaciones 11 a 12 cuando es operativo en una entidad de red.

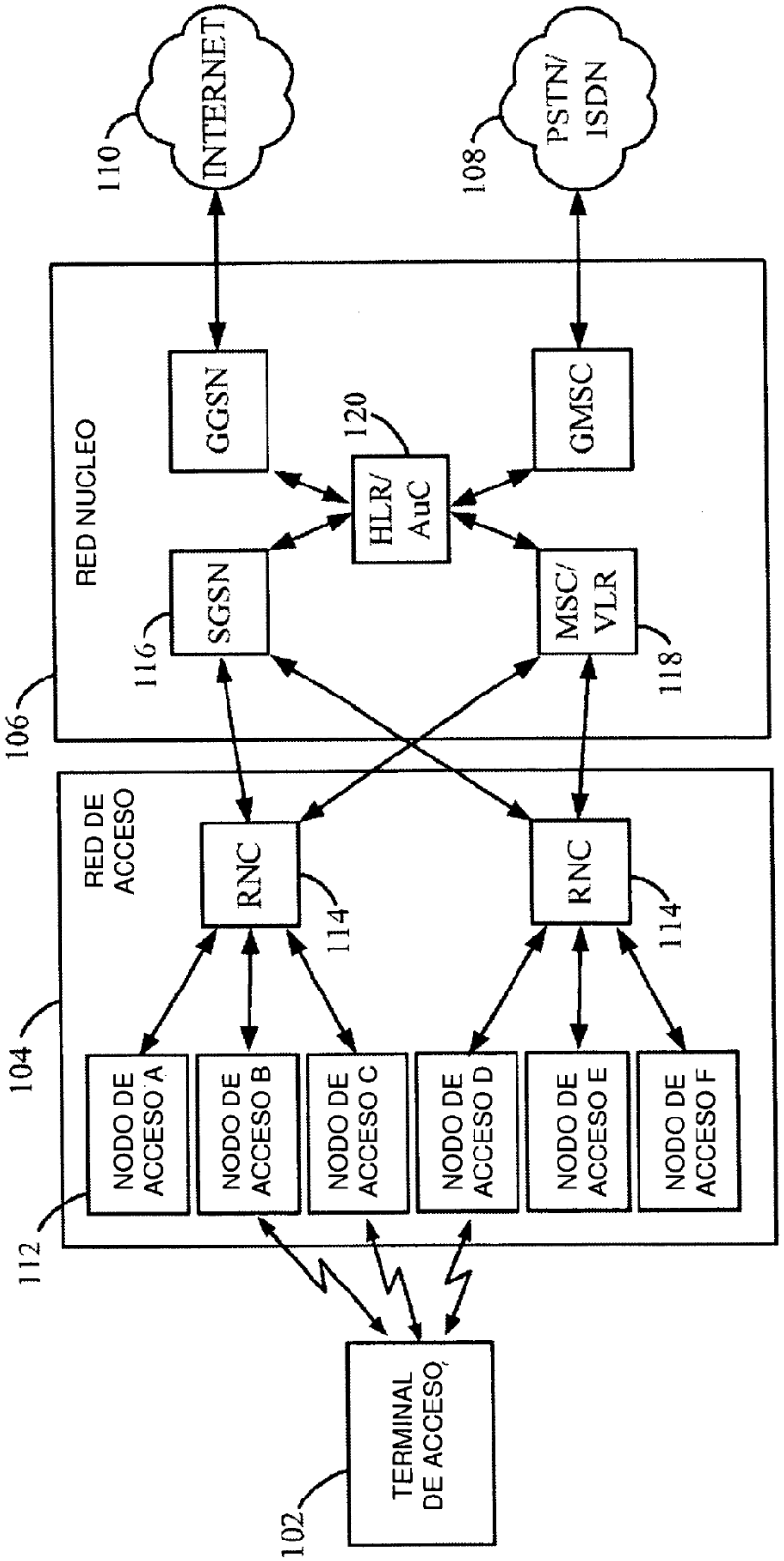

INTERNET
110
PSTN/
ISDN
108
RED NUCLEO
GGSN
120
HLR/
AuC
GMSC
SGSN
116
MSC/
VLR
118
106
RED DE
ACCESO
RNC
114
RNC
114
104
NODO DE
ACCESO A
NODO DE
ACCESO B
NODO DE
ACCESO C
NODO DE
ACCESO D
NODO DE
ACCESO E
NODO DE
ACCESO F
112
TERMINAL
DE ACCESO
102

FIGURA 1

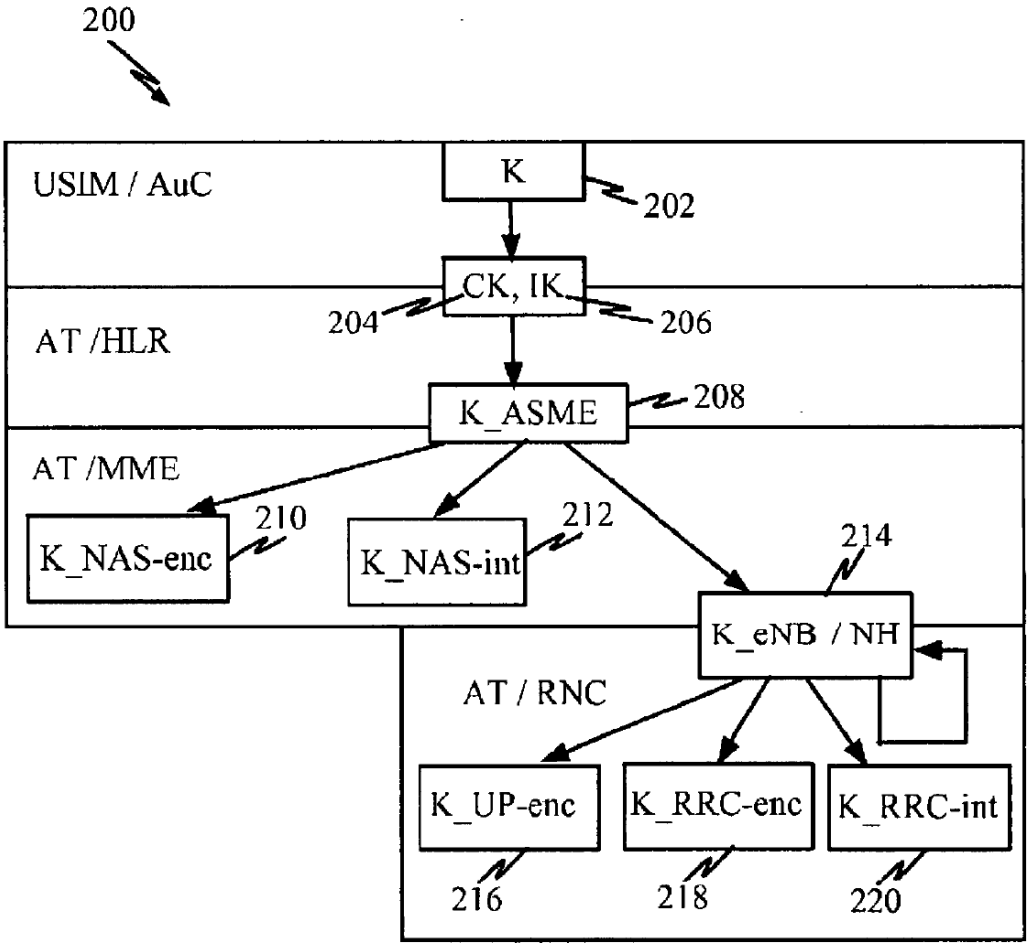

200
USIM / AuC
K
202
CK, IK
204
206
AT /HLR
K_ASME
208
AT /MME
K_NAS-enc
210
K_NAS-int
212
214
K_eNB / NH
AT / RNC
K_UP-enc
K_RRC-enc
K_RRC-int
216
218
220

FIGURA 2

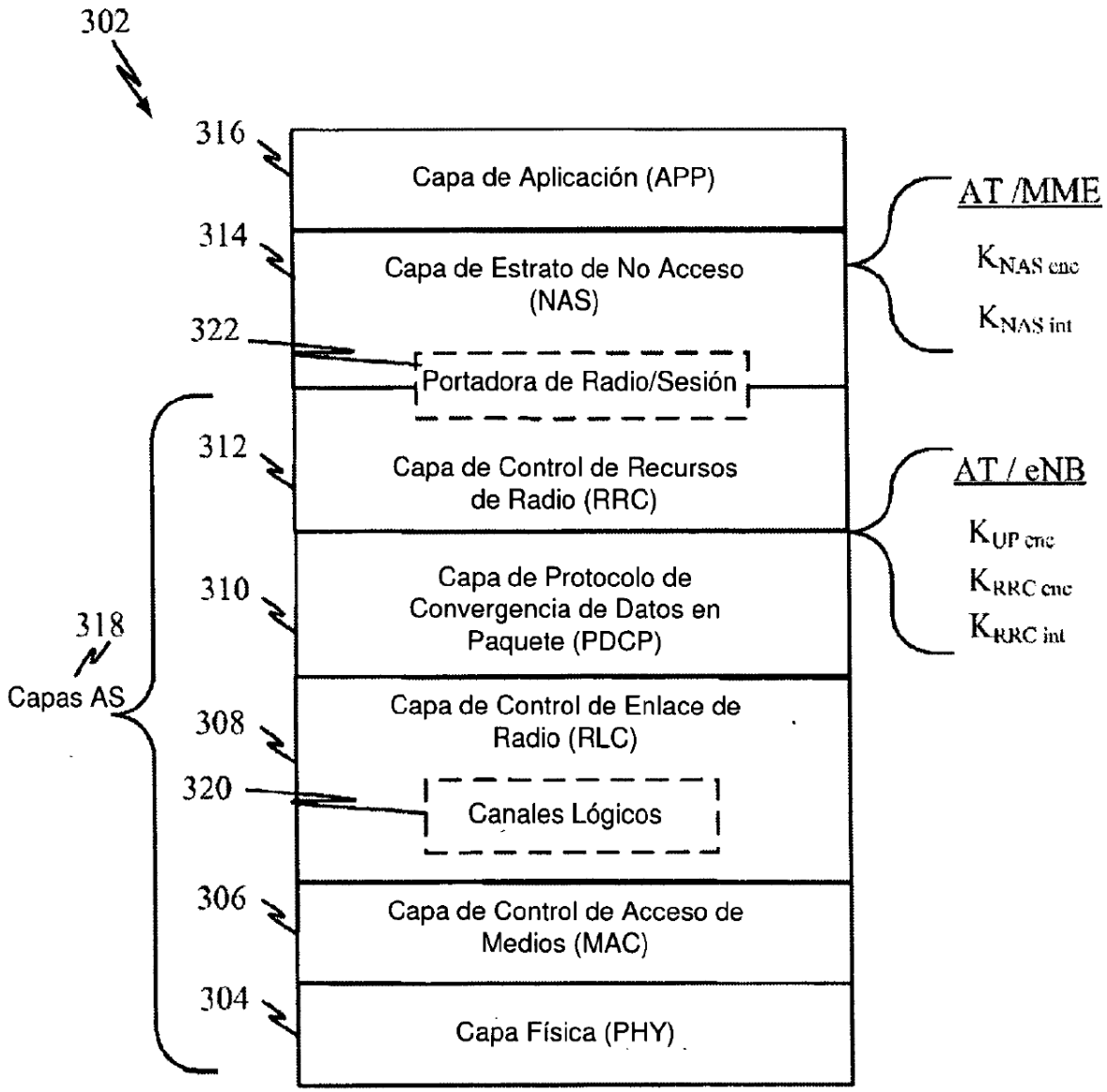

302
316
Capa de Aplicación (APP)
314
Capa de Estrato de No Acceso (NAS)
322
Portadora de Radio/Sesión
312
Capa de Control de Recursos de Radio (RRC)
310
Capa de Protocolo de Convergencia de Datos en Paquete (PDCP)
308
Capa de Control de Enlace de Radio (RLC)
320
Canales Lógicos
306
Capa de Control de Acceso de Medios (MAC)
304
Capa Física (PHY)
318
Capas AS
AT /MME
$K_{NAS\ enc}$
$K_{NAS\ int}$
AT / eNB
$K_{UP\ enc}$
$K_{RRC\ enc}$
$K_{RRC\ int}$

FIGURA 3

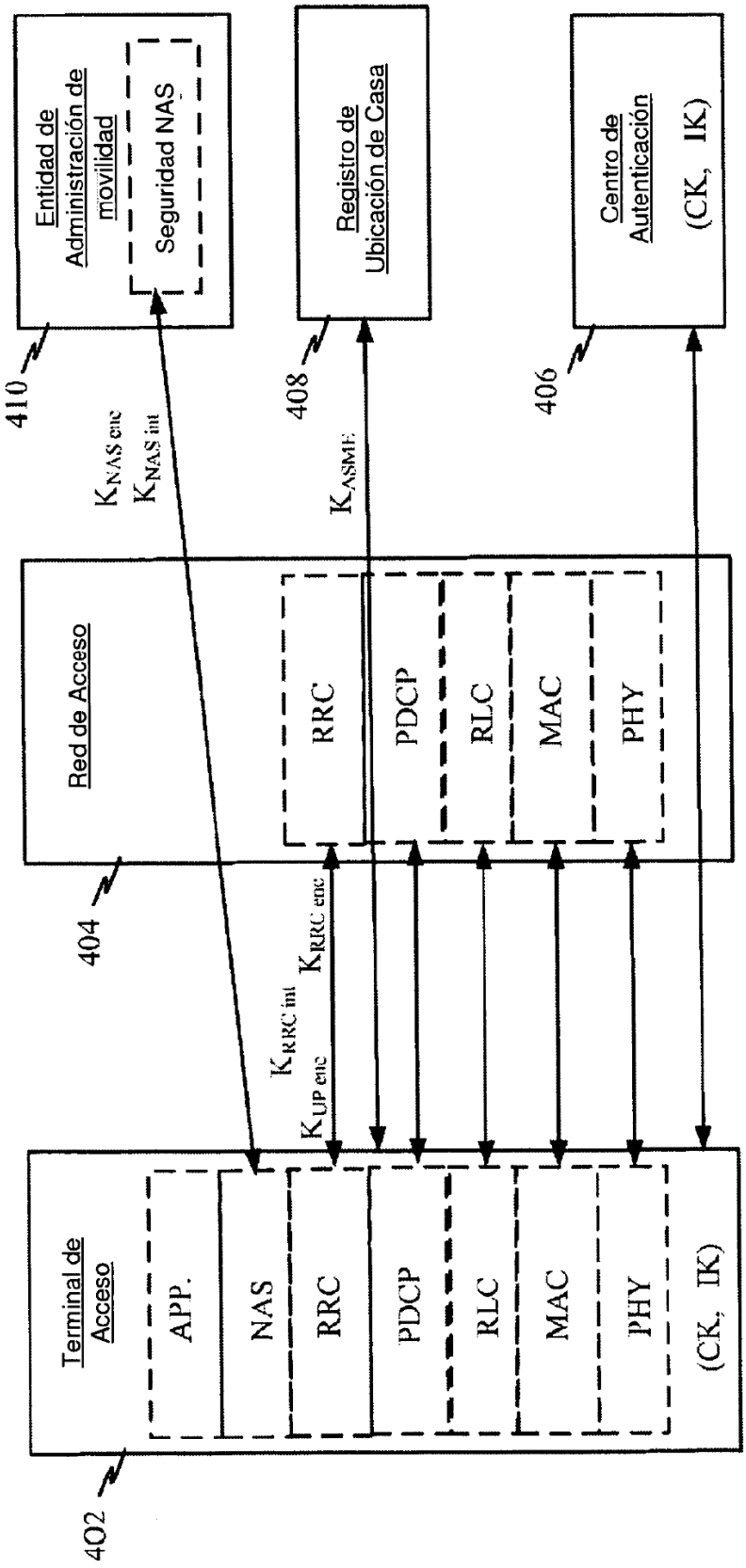

Entidad de Administración de movilidad
Seguridad NAS
Registro de Ubicación de Casa
Centro de Autenticación
(CK, IK)
410
408
406
$K_{NAS\ enc}$
$K_{NAS\ int}$
K_{ASME}
Red de Acceso
RRC
PDCP
RLC
MAC
PHY
404
$K_{RRC\ enc}$
$K_{RRC\ int}$
$K_{UP\ enc}$
Terminal de Acceso
APP.
NAS
RRC
PDCP
RLC
MAC
PHY
(CK, IK)
402

FIGURA 4

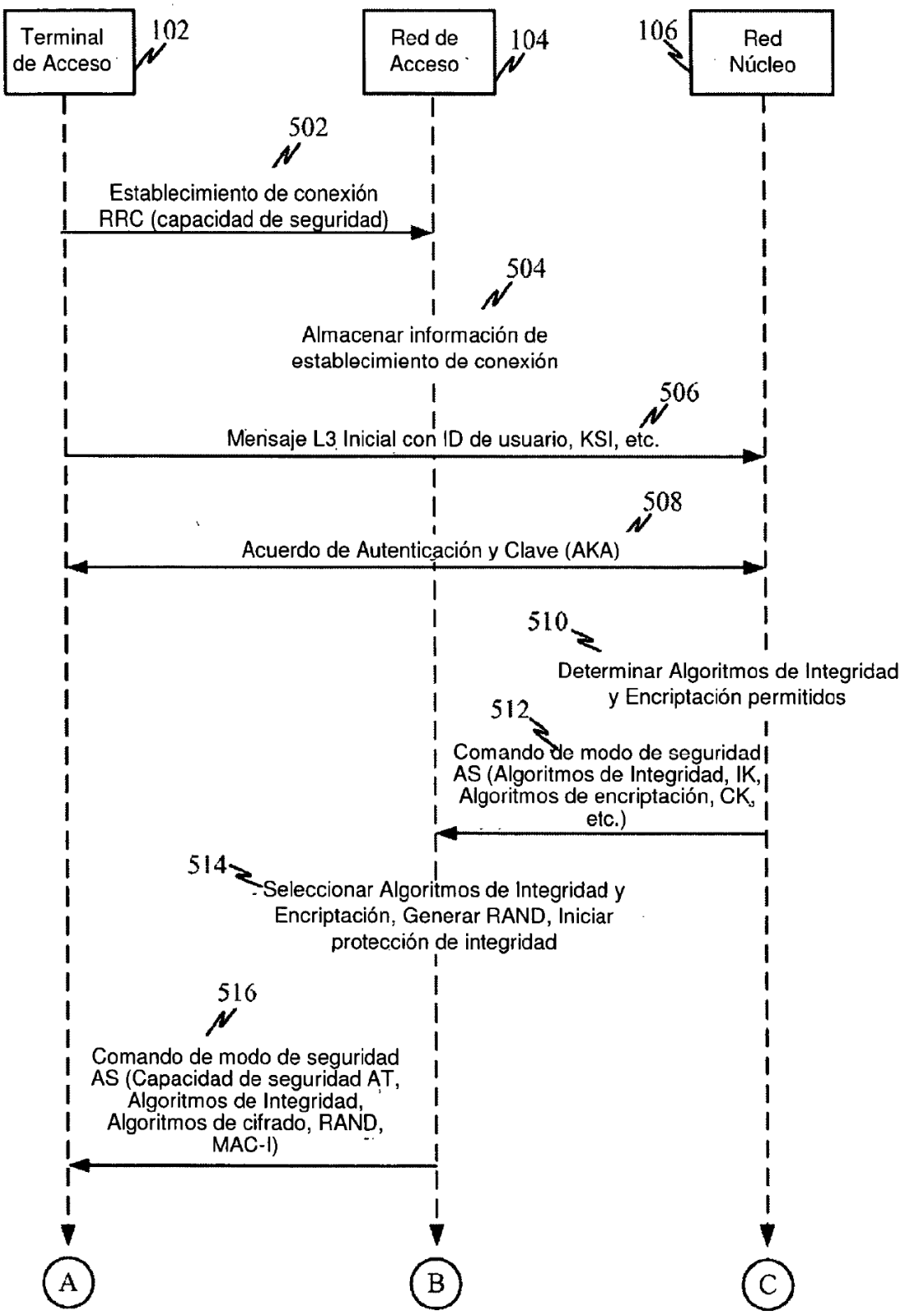

Terminal de Acceso
102
Red de Acceso
104
106
Red Núcleo
502
Establecimiento de conexión RRC (capacidad de seguridad)
504
Almacenar información de establecimiento de conexión
506
Mensaje L3 Inicial con ID de usuario, KSI, etc.
508
Acuerdo de Autenticación y Clave (AKA)
510
Determinar Algoritmos de Integridad y Encriptación permitidos
512
Comando de modo de seguridad AS (Algoritmos de Integridad, IK, Algoritmos de encriptación, CK, etc.)
514
Seleccionar Algoritmos de Integridad y Encriptación, Generar RAND, Iniciar protección de integridad
516
Comando de modo de seguridad AS (Capacidad de seguridad AT, Algoritmos de Integridad, Algoritmos de cifrado, RAND, MAC-I)
A
B
C

FIGURA 5A

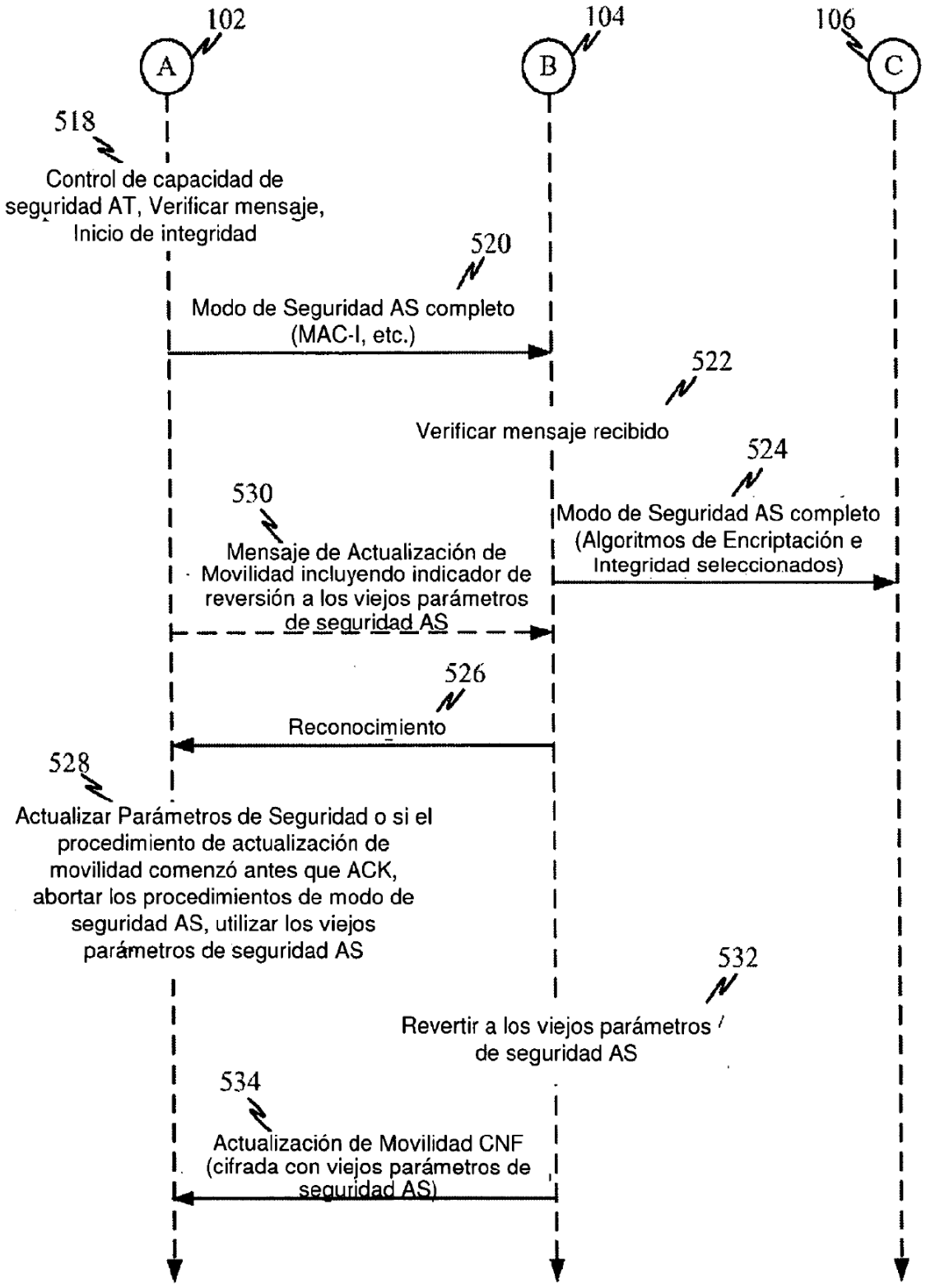

102
104
106
A
B
C
518
Control de capacidad de seguridad AT, Verificar mensaje, Inicio de integridad
520
Modo de Seguridad AS completo (MAC-I, etc.)
522
Verificar mensaje recibido
524
Modo de Seguridad AS completo (Algoritmos de Encriptación e Integridad seleccionados)
530
Mensaje de Actualización de Movilidad incluyendo indicador de reversión a los viejos parámetros de seguridad AS
526
Reconocimiento
528
Actualizar Parámetros de Seguridad o si el procedimiento de actualización de movilidad comenzó antes que ACK, abortar los procedimientos de modo de seguridad AS, utilizar los viejos parámetros de seguridad AS
532
Revertir a los viejos parámetros de seguridad AS
534
Actualización de Movilidad CNF (cifrada con viejos parámetros de seguridad AS)

FIGURA 5B

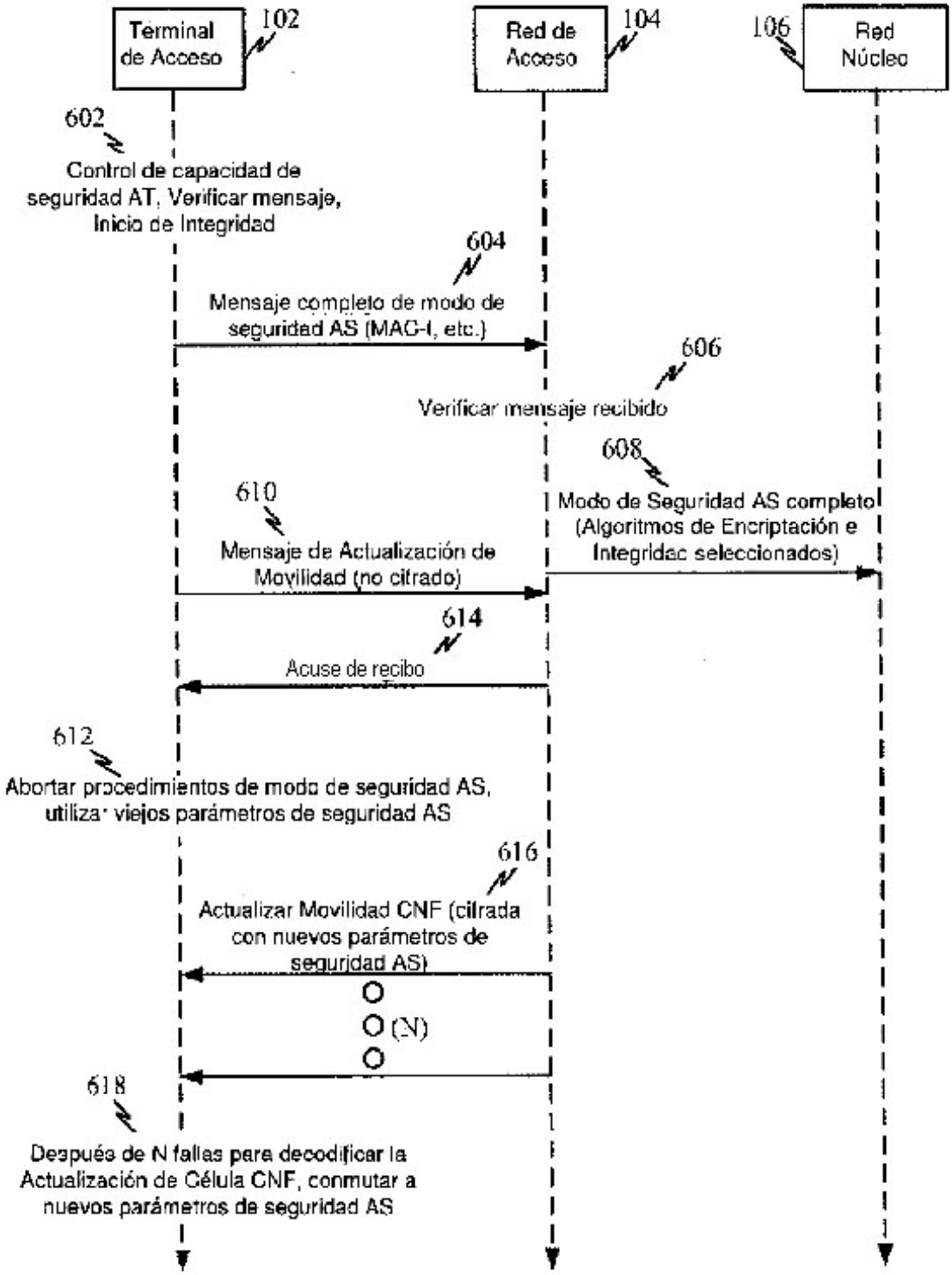

Terminal de Acceso
102
Red de Acceso
104
106
Red Núcleo
602
Control de capacidad de seguridad AT, Verificar mensaje, Inicio de Integridad
604
Mensaje completo de modo de seguridad AS (MAC-I, etc.)
606
Verificar mensaje recibido
608
Modo de Seguridad AS completo (Algoritmos de Encriptación e Integridad seleccionados)
610
Mensaje de Actualización de Movilidad (no cifrado)
614
Acuse de recibo
612
Abortar procedimientos de modo de seguridad AS, utilizar viejos parámetros de seguridad AS
616
Actualizar Movilidad CNF (cifrada con nuevos parámetros de seguridad AS)
(N)
618
Después de N fallas para decodificar la Actualización de Célula CNF, conmutar a nuevos parámetros de seguridad AS

FIGURA 6

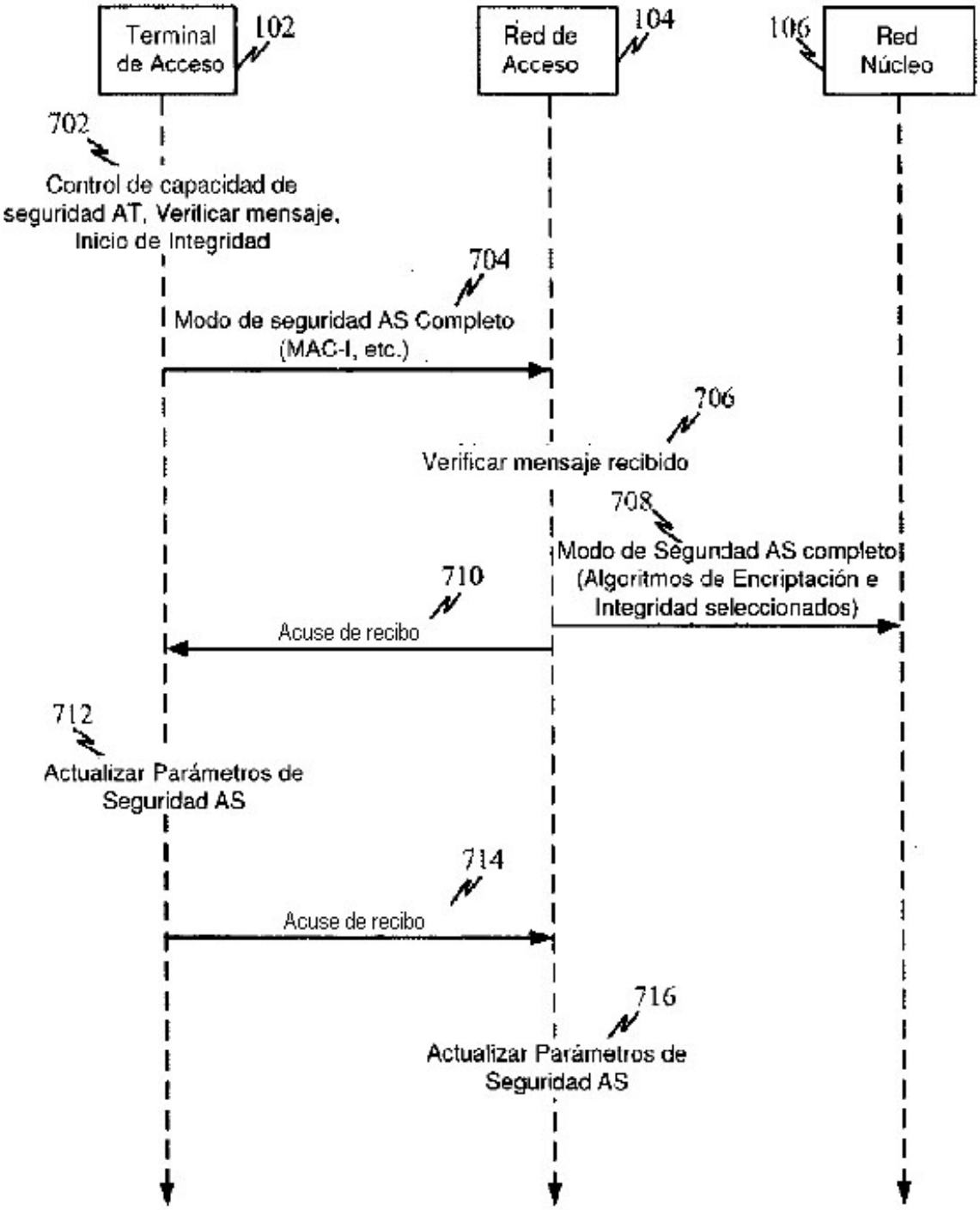

Terminal de Acceso
102
Red de Acceso
104
106
Red Núcleo
702
Control de capacidad de seguridad AT, Verificar mensaje, Inicio de Integridad
704
Modo de seguridad AS Completo (MAC-I, etc.)
706
Verificar mensaje recibido
708
Modo de Seguridad AS completo (Algoritmos de Encriptación e Integridad seleccionados)
710
Acuse de recibo
712
Actualizar Parámetros de Seguridad AS
714
Acuse de recibo
716
Actualizar Parámetros de Seguridad AS

FIGURA 7

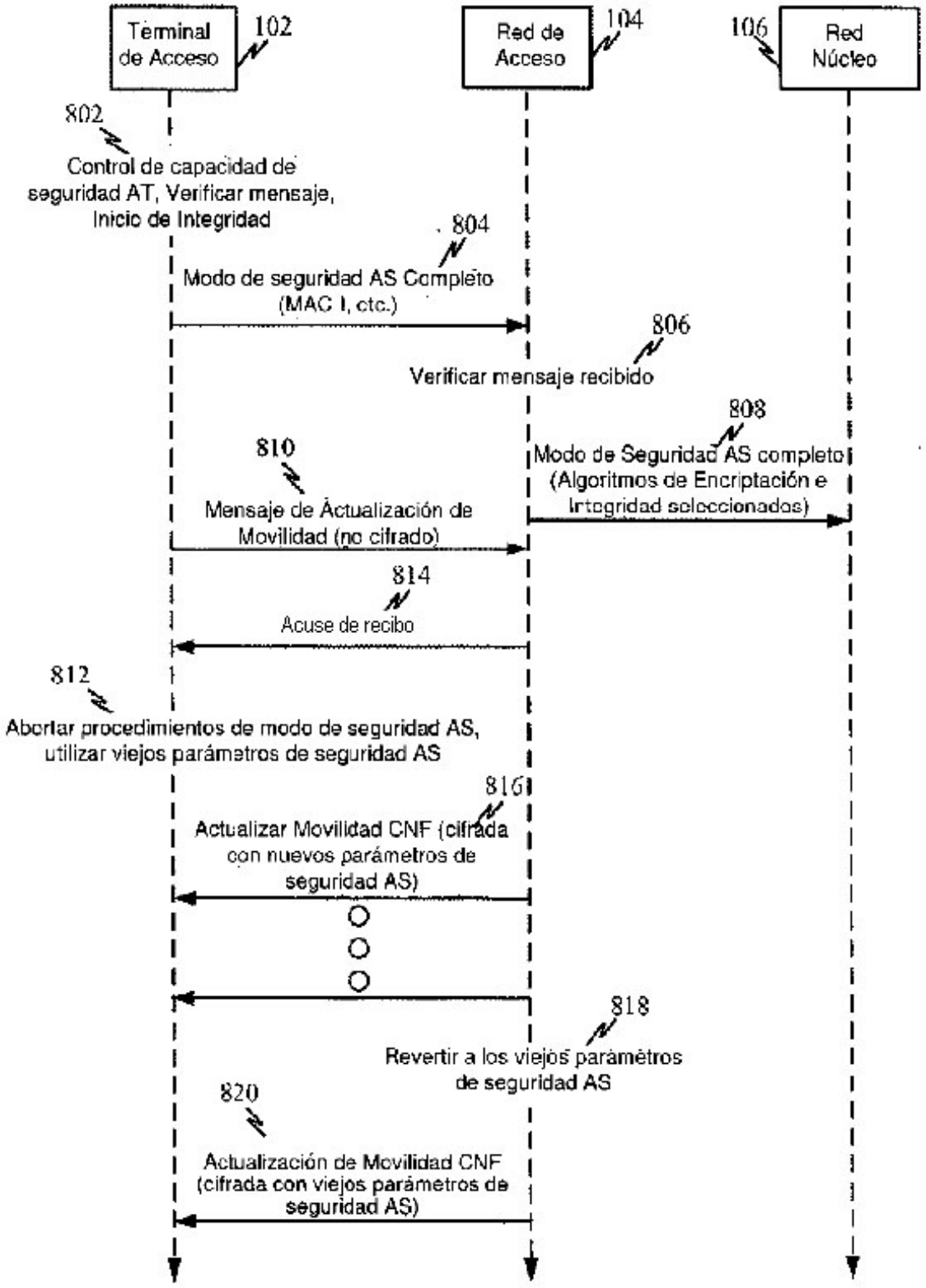

Terminal de Acceso
102
Red de Acceso
104
106
Red Núcleo
802
Control de capacidad de seguridad AT, Verificar mensaje, Inicio de Integridad
804
Modo de seguridad AS Completo (MAC I, etc.)
806
Verificar mensaje recibido
808
Modo de Seguridad AS completo (Algoritmos de Encriptación e Integridad seleccionados)
810
Mensaje de Actualización de Movilidad (no cifrado)
814
Acuse de recibo
812
Abortar procedimientos de modo de seguridad AS, utilizar viejos parámetros de seguridad AS
816
Actualizar Movilidad CNF (cifrada con nuevos parámetros de seguridad AS)
818
Revertir a los viejos parámetros de seguridad AS
820
Actualización de Movilidad CNF (cifrada con viejos parámetros de seguridad AS)

FIGURA 8

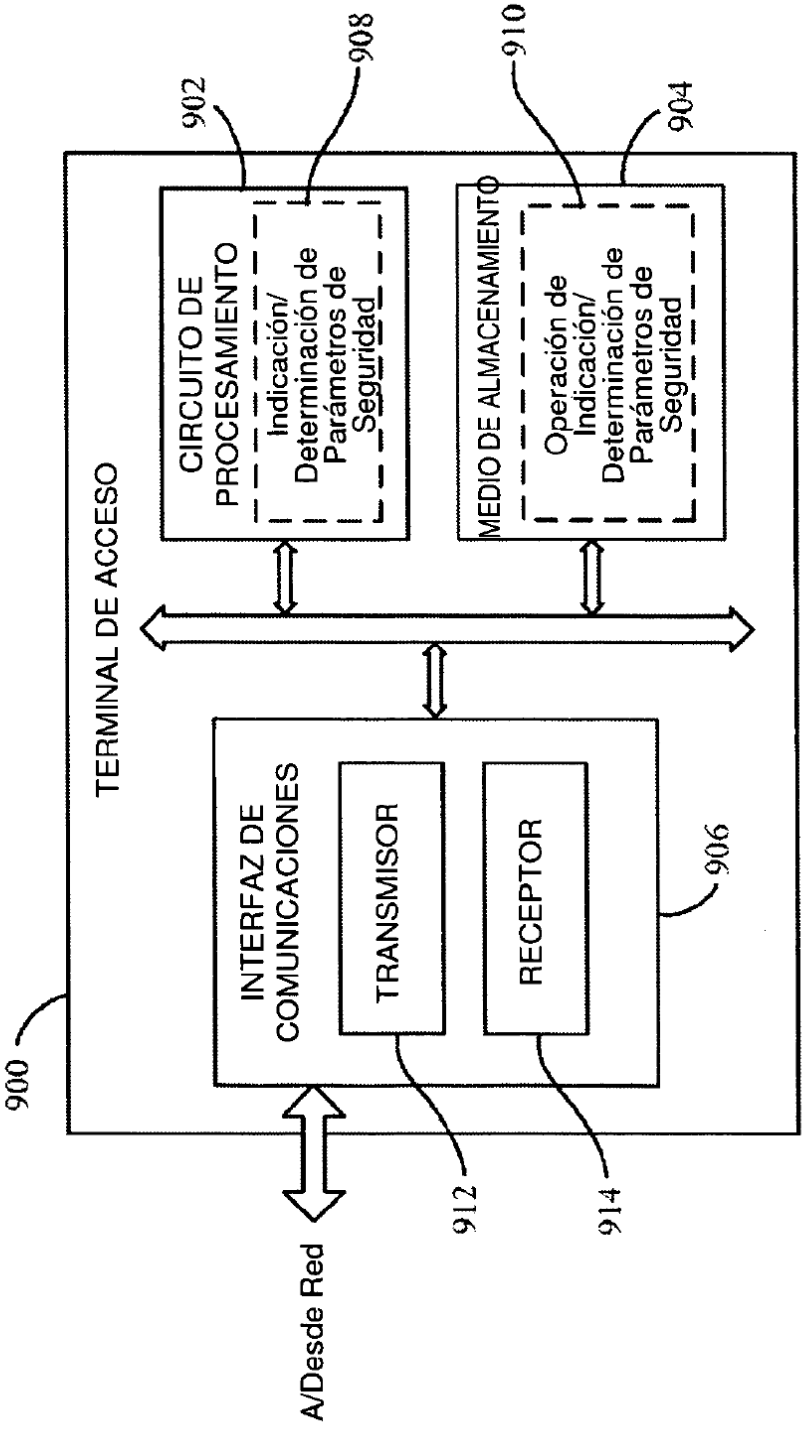

900
TERMINAL DE ACCESO
902
CIRCUITO DE PROCESAMIENTO
908
Indicación/ Determinación de Parámetros de Seguridad
910
MEDIO DE ALMACENAMIENTO
904
Operación de Indicación/ Determinación de Parámetros de Seguridad
INTERFAZ DE COMUNICACIONES
TRANSMISOR
RECEPTOR
906
912
914
A/Desde Red

FIGURA 9

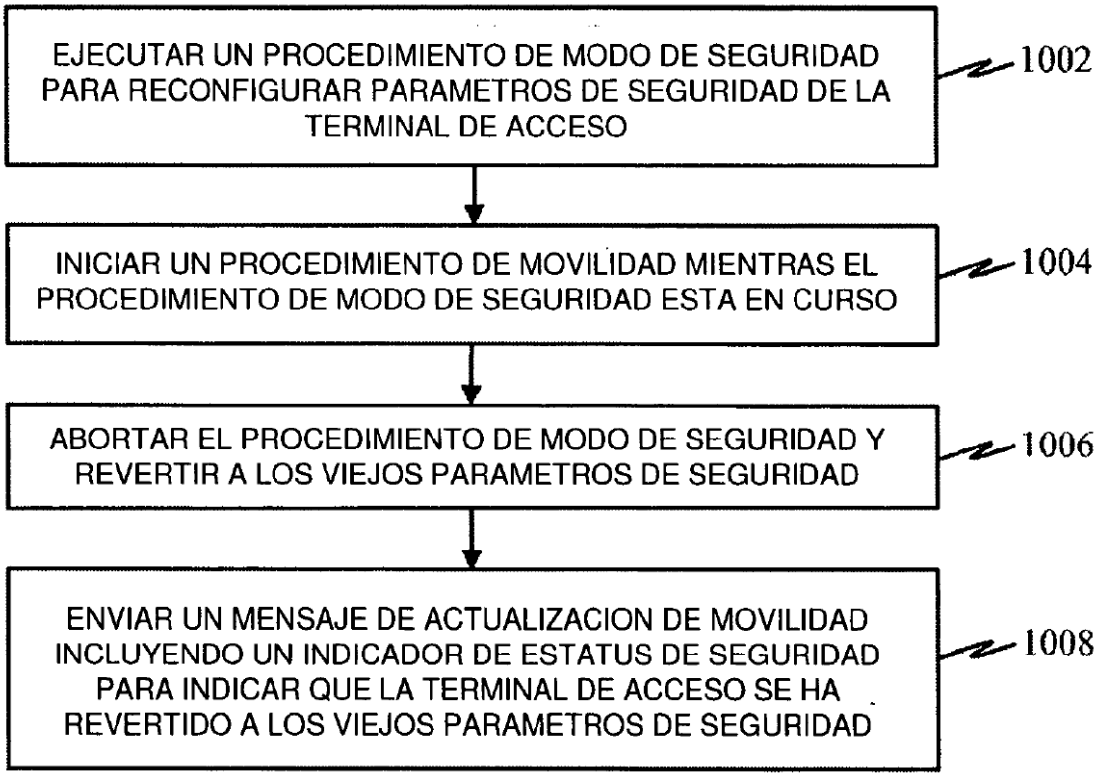

EJECUTAR UN PROCEDIMIENTO DE MODO DE SEGURIDAD PARA RECONFIGURAR PARAMETROS DE SEGURIDAD DE LA TERMINAL DE ACCESO
1002
INICIAR UN PROCEDIMIENTO DE MOVILIDAD MIENTRAS EL PROCEDIMIENTO DE MODO DE SEGURIDAD ESTA EN CURSO
1004
ABORTAR EL PROCEDIMIENTO DE MODO DE SEGURIDAD Y REVERTIR A LOS VIEJOS PARAMETROS DE SEGURIDAD
1006
ENVIAR UN MENSAJE DE ACTUALIZACION DE MOVILIDAD INCLUYENDO UN INDICADOR DE ESTATUS DE SEGURIDAD PARA INDICAR QUE LA TERMINAL DE ACCESO SE HA REVERTIDO A LOS VIEJOS PARAMETROS DE SEGURIDAD
1008

FIGURA 10

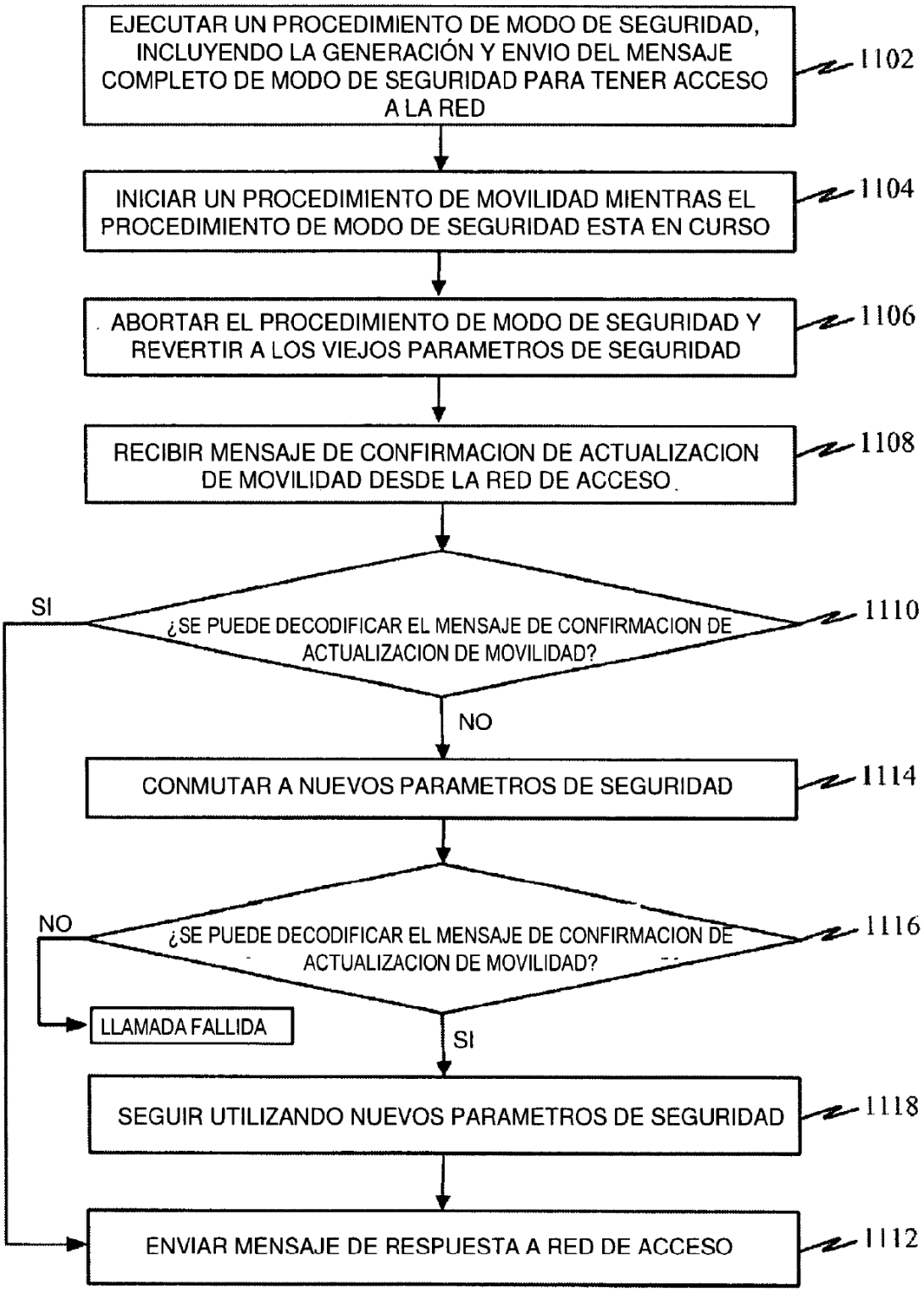

EJECUTAR UN PROCEDIMIENTO DE MODO DE SEGURIDAD, INCLUYENDO LA GENERACIÓN Y ENVIO DEL MENSAJE COMPLETO DE MODO DE SEGURIDAD PARA TENER ACCESO A LA RED
1102
INICIAR UN PROCEDIMIENTO DE MOVILIDAD MIENTRAS EL PROCEDIMIENTO DE MODO DE SEGURIDAD ESTA EN CURSO
1104
ABORTAR EL PROCEDIMIENTO DE MODO DE SEGURIDAD Y REVERTIR A LOS VIEJOS PARAMETROS DE SEGURIDAD
1106
RECIBIR MENSAJE DE CONFIRMACION DE ACTUALIZACION DE MOVILIDAD DESDE LA RED DE ACCESO
1108
SI
¿SE PUEDE DECODIFICAR EL MENSAJE DE CONFIRMACION DE ACTUALIZACION DE MOVILIDAD?
1110
NO
CONMUTAR A NUEVOS PARAMETROS DE SEGURIDAD
1114
NO
¿SE PUEDE DECODIFICAR EL MENSAJE DE CONFIRMACION DE ACTUALIZACION DE MOVILIDAD?
1116
LLAMADA FALLIDA
SI
SEGUIR UTILIZANDO NUEVOS PARAMETROS DE SEGURIDAD
1118
ENVIAR MENSAJE DE RESPUESTA A RED DE ACCESO
1112

FIGURA 11

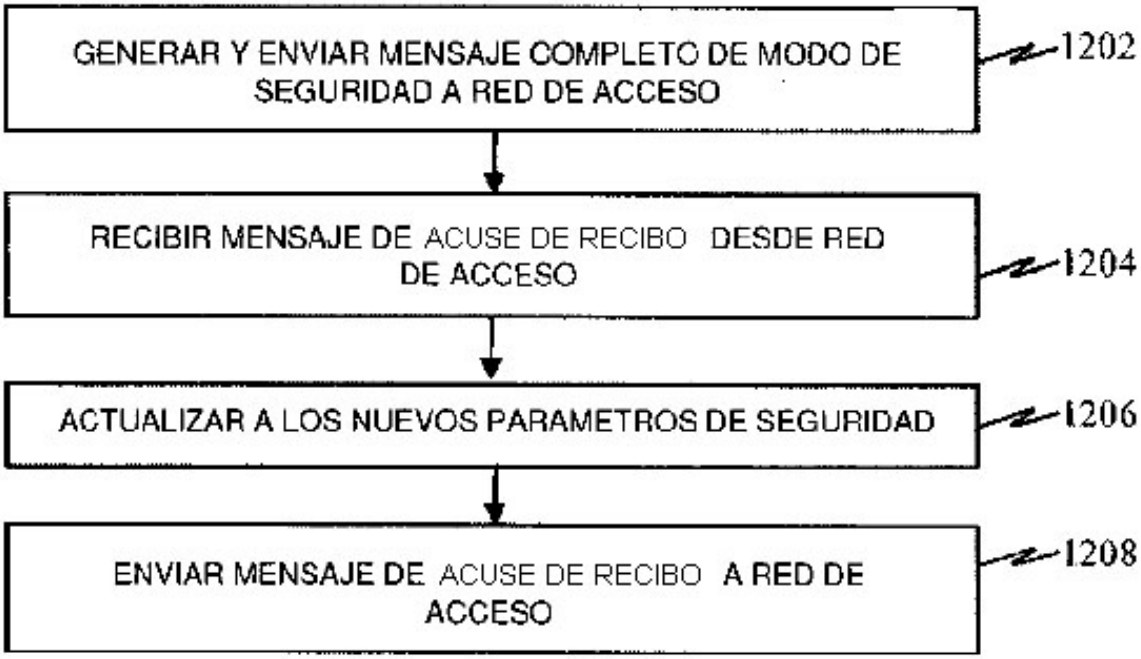

GENERAR Y ENVIAR MENSAJE COMPLETO DE MODO DE SEGURIDAD A RED DE ACCESO
1202
RECIBIR MENSAJE DE ACUSE DE RECIBO DESDE RED DE ACCESO
1204
ACTUALIZAR A LOS NUEVOS PARAMETROS DE SEGURIDAD
1206
ENVIAR MENSAJE DE ACUSE DE RECIBO A RED DE ACCESO
1208

FIGURA 12

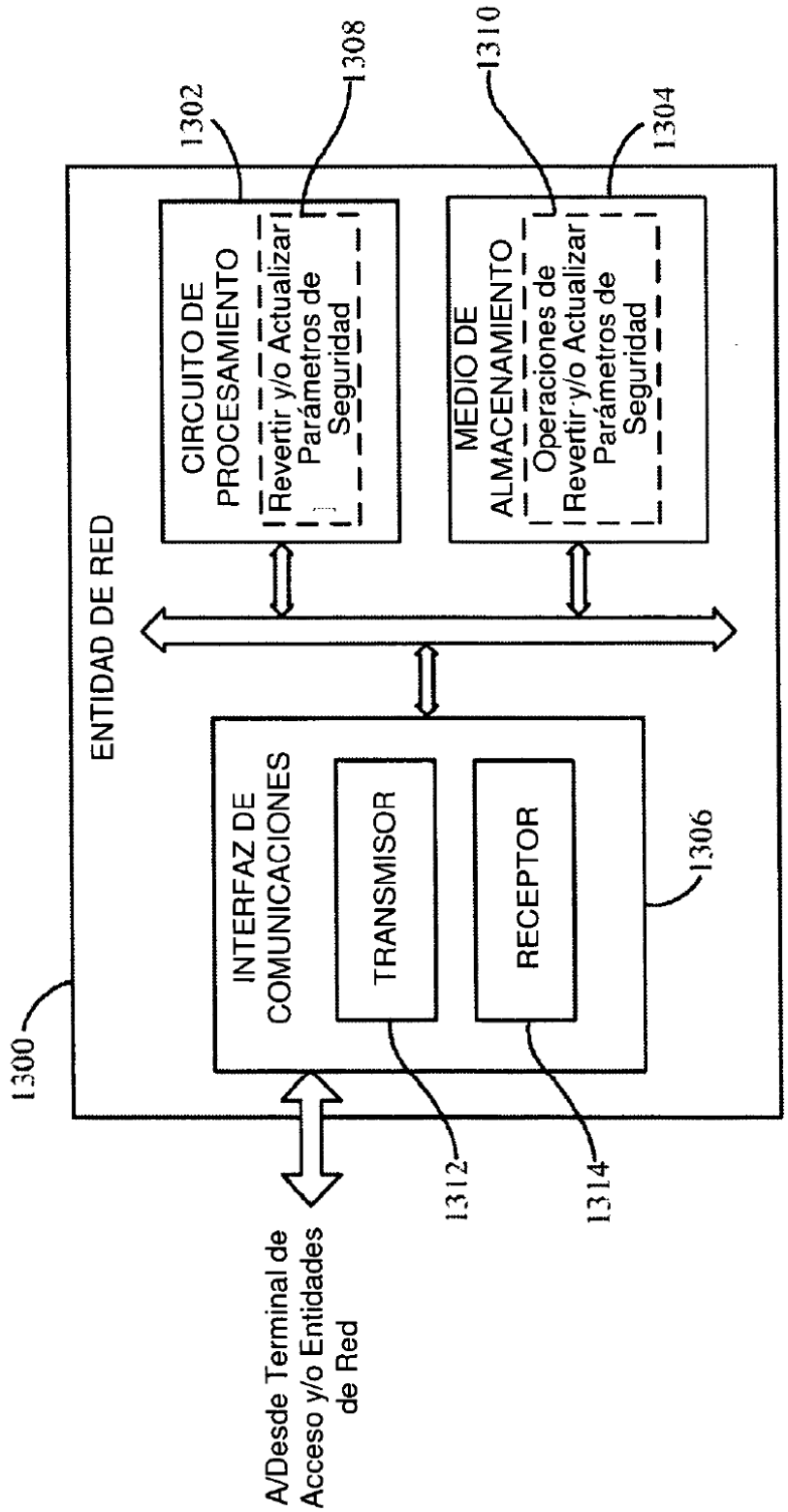

1300
ENTIDAD DE RED
1302
CIRCUITO DE PROCESAMIENTO
Revertir y/o Actualizar Parámetros de Seguridad
1308
1310
MEDIO DE ALMACENAMIENTO
Operaciones de Revertir y/o Actualizar Parámetros de Seguridad
1304
INTERFAZ DE COMUNICACIONES
TRANSMISOR
RECEPTOR
1306
1312
1314
A/Desde Terminal de Acceso y/o Entidades de Red

FIGURA 13

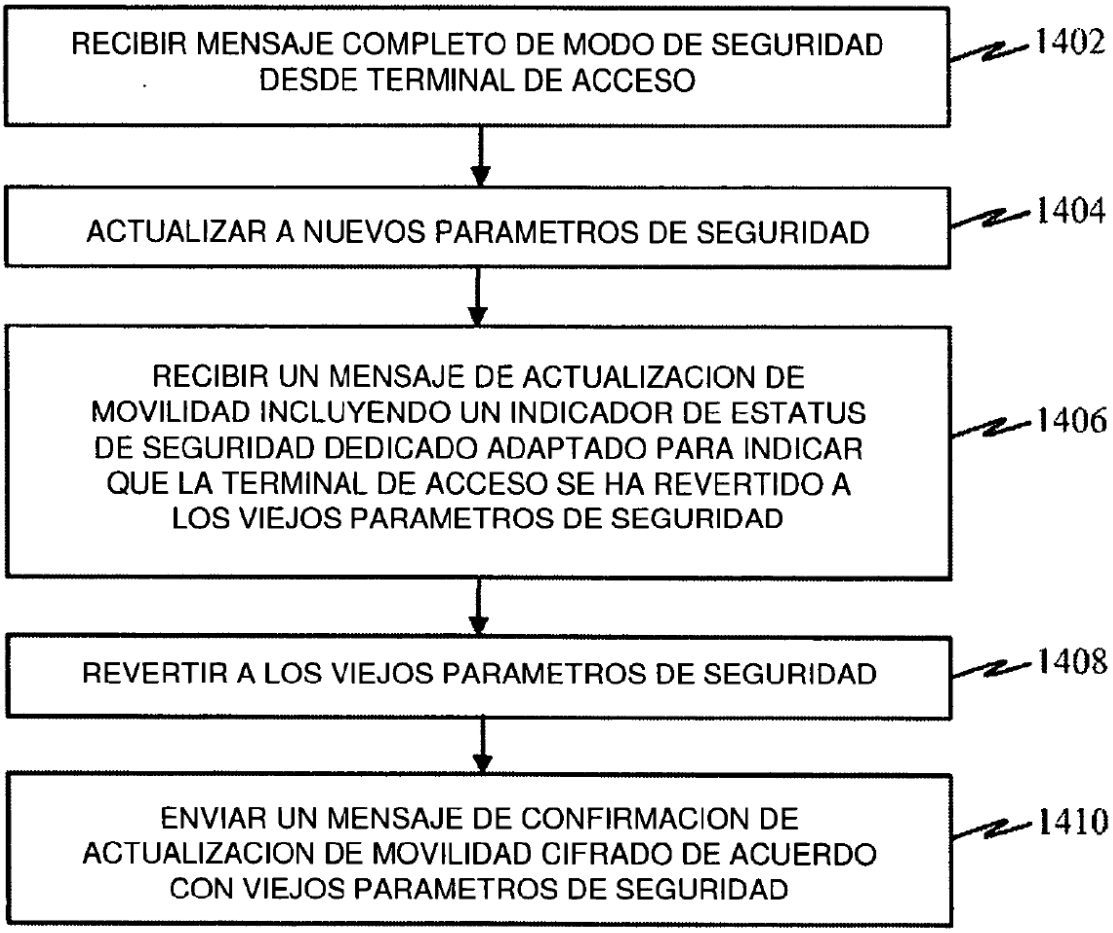

RECIBIR MENSAJE COMPLETO DE MODO DE SEGURIDAD DESDE TERMINAL DE ACCESO
1402
ACTUALIZAR A NUEVOS PARAMETROS DE SEGURIDAD
1404
RECIBIR UN MENSAJE DE ACTUALIZACION DE MOVILIDAD INCLUYENDO UN INDICADOR DE ESTATUS DE SEGURIDAD DEDICADO ADAPTADO PARA INDICAR QUE LA TERMINAL DE ACCESO SE HA REVERTIDO A LOS VIEJOS PARAMETROS DE SEGURIDAD
1406
REVERTIR A LOS VIEJOS PARAMETROS DE SEGURIDAD
1408
ENVIAR UN MENSAJE DE CONFIRMACION DE ACTUALIZACION DE MOVILIDAD CIFRADO DE ACUERDO CON VIEJOS PARAMETROS DE SEGURIDAD
1410

FIGURA 14

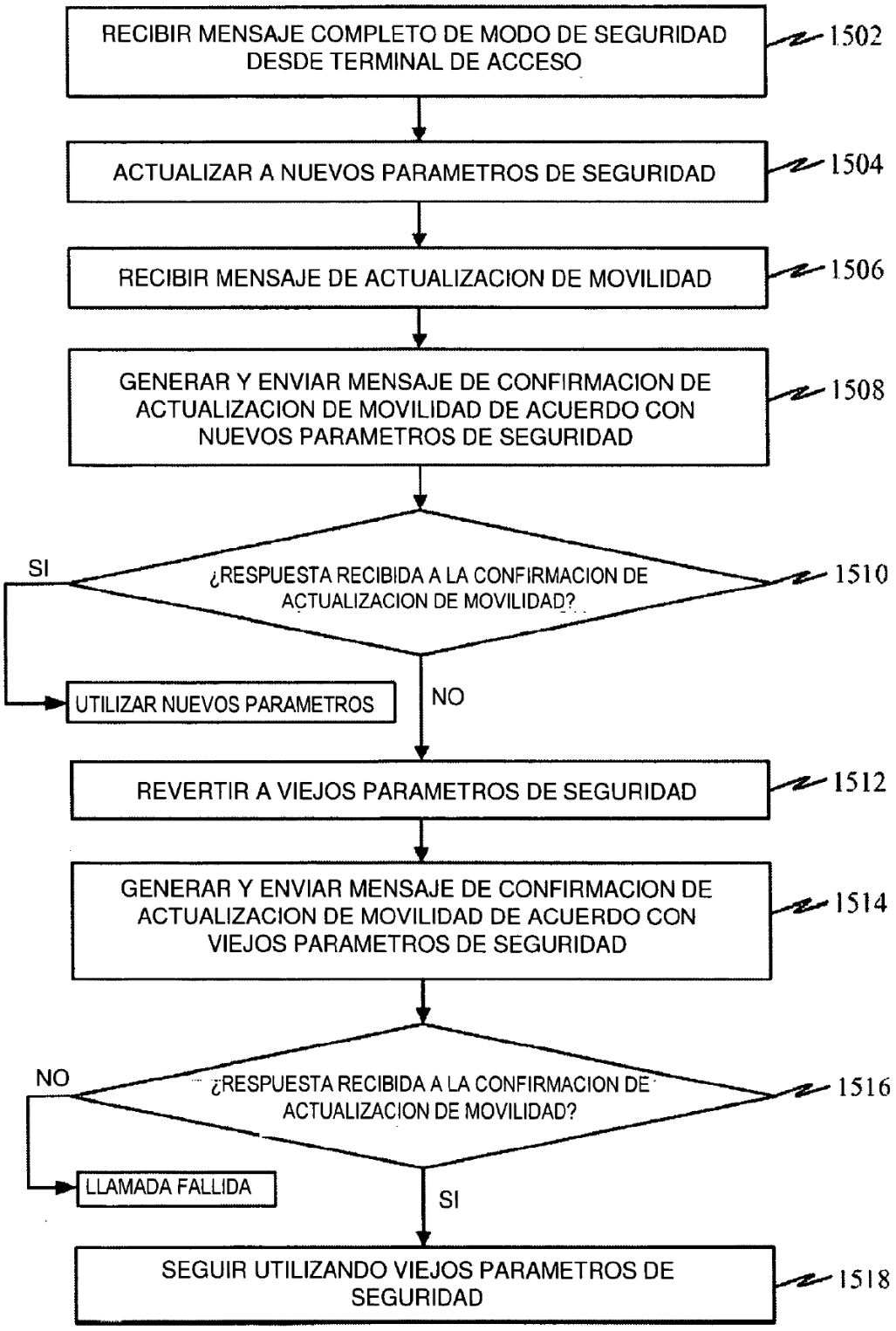

RECIBIR MENSAJE COMPLETO DE MODO DE SEGURIDAD DESDE TERMINAL DE ACCESO
1502
ACTUALIZAR A NUEVOS PARAMETROS DE SEGURIDAD
1504
RECIBIR MENSAJE DE ACTUALIZACION DE MOVILIDAD
1506
GENERAR Y ENVIAR MENSAJE DE CONFIRMACION DE ACTUALIZACION DE MOVILIDAD DE ACUERDO CON NUEVOS PARAMETROS DE SEGURIDAD
1508
¿RESPUESTA RECIBIDA A LA CONFIRMACION DE ACTUALIZACION DE MOVILIDAD?
1510
SI
UTILIZAR NUEVOS PARAMETROS
NO
REVERTIR A VIEJOS PARAMETROS DE SEGURIDAD
1512
GENERAR Y ENVIAR MENSAJE DE CONFIRMACION DE ACTUALIZACION DE MOVILIDAD DE ACUERDO CON VIEJOS PARAMETROS DE SEGURIDAD
1514
¿RESPUESTA RECIBIDA A LA CONFIRMACION DE ACTUALIZACION DE MOVILIDAD?
1516
NO
LLAMADA FALLIDA
SI
SEGUIR UTILIZANDO VIEJOS PARAMETROS DE SEGURIDAD
1518

FIGURA 15

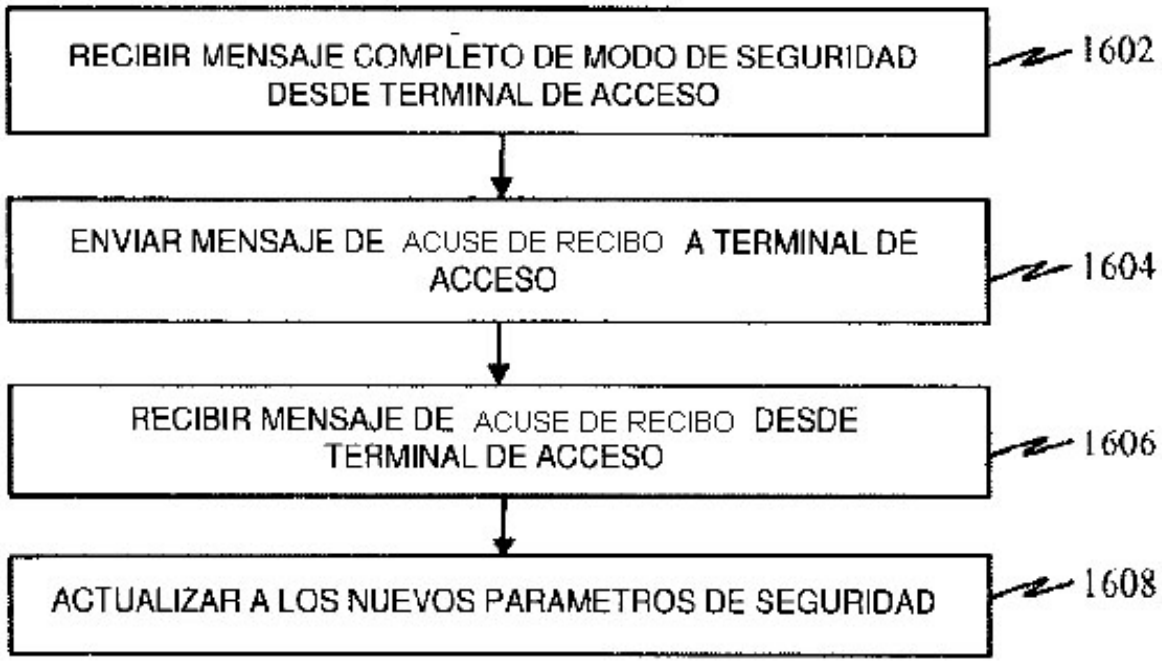

RECIBIR MENSAJE COMPLETO DE MODO DE SEGURIDAD DESDE TERMINAL DE ACCESO
1602
ENVIAR MENSAJE DE ACUSE DE RECIBO A TERMINAL DE ACCESO
1604
RECIBIR MENSAJE DE ACUSE DE RECIBO DESDE TERMINAL DE ACCESO
1606
ACTUALIZAR A LOS NUEVOS PARAMETROS DE SEGURIDAD
1608

FIGURA 16