(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 969 664**

(51) Int. Cl.:

H04W 28/02	(2009.01)	***H04L 9/40***	(2012.01)
H04W 12/02	(2009.01)	***H04L 67/50***	(2012.01)
H04W 12/06	(2011.01)		
H04W 24/04	(2009.01)		
H04W 12/033	(2011.01)		
H04W 12/12	(2011.01)		
H04W 12/60	(2011.01)		
H04L 43/062	(2012.01)		
H04L 43/0876	(2012.01)		
H04L 43/16	(2012.01)		

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.08.2018 E 22196027 (1)**

(97) Fecha y número de publicación de la concesión europea: **22.11.2023 EP 4124103**

(54) Título: **Método y sistema para las características de tráfico de plano de usuario y seguridad de la red**

(30) Prioridad:

31.08.2017 US 201715692836

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.05.2024

(73) Titular/es:

MALIKIE INNOVATIONS LIMITED (100.0%)
The Glasshouses GH2, 92 Georges Street Lower
Dun Laoghaire, Dublin A96 VR66, IE

(72) Inventor/es:

ALFANO, NICHOLAS PATRICK;
FERRAZZINI, AXEL y
HE, DAKE

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método y sistema para las características de tráfico de plano de usuario y seguridad de la red

Campo de la descripción

La presente descripción se refiere a comunicaciones en el plano de usuario en una red móvil y, en particular, se refiere a la seguridad de la red con respecto a comunicaciones en el plano de usuario.

Antecedentes

El documento US 2017/230832 da a conocer un sistema para monitorizar el tráfico de datos de IoT entre un dispositivo de IoT y un servidor. Esto da a conocer una unidad de cumplimiento que permite el tráfico de datos solamente si el tráfico se ajusta al perfil de seguridad del dispositivo. El documento WO 2016/119822 da a conocer un método en el que un nodo de red monitoriza un flujo de tráfico del plano de usuario y cuando se detecta una anomalía, se pueden activar acciones de gestión de tráfico y de red.

La integridad y confidencialidad del tráfico entre un equipo de usuario (UE) y la red pueden generar un coste de potencia de procesamiento y también pueden reducir la duración de la batería en un UE. Operar sin seguridad puede habilitar el despliegue de dispositivos con mayor duración de batería y menos potencia de procesamiento.

Sin embargo, el envío de comunicaciones por aire desprotegidas puede introducir riesgos de seguridad para la red y para el UE, incluyendo, entre otros, escuchas ilegales; suplantación de identidad del originador; inyección de datos no válidos; o ataques de denegación de servicio (DoS).

Las conexiones desprotegidas pueden permitir una posible corrupción de los datos en la ruta, lo que puede tener un impacto en la infraestructura o en el rendimiento de la red.

Debido a tales riesgos, los operadores de red dudan en permitir conexiones a su red que no estén protegidas.

Breve descripción de los dibujos

La presente descripción se comprenderá mejor con referencia a los dibujos, en los que:

la fig. 1 es un diagrama de bloques que muestra una arquitectura de red de núcleo de paquetes evolucionados ejemplar;

la fig. 2 es un diagrama de bloques que muestra la confidencialidad del plano de usuario proporcionada por la capa de protocolo de control de paquetes de datos en el núcleo de paquetes evolucionados;

la fig. 3 es un diagrama de bloques que muestra una arquitectura de red de núcleo de paquetes evolucionados ejemplar que tiene una función de cumplimiento de políticas de seguridad añadida a la puerta de enlace de la red de paquetes de datos;

la fig. 4 es un diagrama de bloques que muestra una arquitectura de red de quinta generación que tiene una función de cumplimiento de políticas de seguridad añadida a la función del plano de usuario;

la fig. 5 es un diagrama de flujo de datos que muestra la configuración de características y parámetros en la función de plano de usuario;

la fig. 6 es un diagrama de flujo de datos que muestra un procedimiento de CONEXIÓN ejemplar;

la fig. 7 es un diagrama de proceso que muestra un proceso para monitorizar paquetes de datos para determinar si una cantidad acumulada de datos durante un período de tiempo excede un umbral de parámetro;

la fig. 8 es un diagrama de proceso que muestra un proceso para monitorizar paquetes de datos para determinar una ubicación de un equipo de usuario;

la fig. 9 es un diagrama de proceso que muestra un proceso para monitorizar un tipo de paquetes de datos para garantizar que una red esté transmitiendo un tipo de paquetes de datos esperado;

la fig. 10 es un diagrama de flujo de datos para actualizar una política sobre la detección de una anomalía;

la fig. 11 es un diagrama de flujo de datos que muestra el envío de un mensaje seguro a un equipo de usuario indicando que se ha detectado una anomalía;

la fig. 12 es un diagrama de flujo de datos que muestra la entrega de paquetes del plano de usuario tras la detección de una anomalía y, además, opcionalmente, la liberación de una conexión RRC con el equipo de usuario;

la fig. 13 es un diagrama de flujo de datos que muestra el inicio de un procedimiento de contraverificación tras la detección de una anomalía;

la fig. 14 es un diagrama de flujo de datos que muestra el inicio de una solicitud de autenticación con un equipo de usuario tras la detección de una anomalía;

la fig. 15 es un diagrama de flujo de datos que muestra un procedimiento de DESCONEXIÓN tras la detección de una anomalía;

la fig. 16 es un diagrama de flujo de datos que muestra la RECONFIGURACIÓN_RRC de un equipo de usuario para activar el cifrado y/o la detección de integridad tras la detección de una anomalía;

la fig. 17 es un diagrama de flujo de datos que muestra un procedimiento de DESCONEXIÓN ejemplar;

la fig. 18 es un diagrama de bloques que muestra un dispositivo informático simplificado capaz de utilizarse con el método y las realizaciones de la presente descripción; y

la fig. 19 es un diagrama de bloques de un equipo de usuario ejemplar capaz de utilizarse con los métodos y realizaciones de la presente descripción.

Descripción detallada de los dibujos

La presente descripción proporciona un método en un elemento de red para monitorizar el tráfico del plano de usuario para un equipo de usuario, comprendiendo el método: la configuración de un conjunto de características y un rango de valores para cada uno del conjunto de características para el tráfico del plano de usuario entre el equipo de usuario y el elemento de red; monitorizar el tráfico del plano de usuario para el equipo de usuario en el elemento de red, determinando la monitorización si al menos una característica del tráfico en el plano de usuario cae fuera del rango configurado de valores, dando como resultado una violación de característica; y si al menos una característica del tráfico del plano de usuario cae fuera del rango configurado de valores, la realización de una acción resultante de la violación de la característica.

La presente descripción proporciona además un elemento de red para monitorizar el tráfico del plano de usuario para un equipo de usuario, comprendiendo el elemento de red: un procesador; y un subsistema de comunicaciones, en el que el elemento de red está configurado para: configurar un conjunto de características y un rango de valores para cada uno del conjunto de características para el tráfico del plano de usuario entre el equipo de usuario y el elemento de red; monitorizar el tráfico del plano de usuario para el equipo de usuario en el elemento de red, determinando la monitorización si al menos una característica del tráfico del plano de usuario cae fuera del rango configurado de valores, dando como resultado una violación de característica; y si al menos una característica del tráfico del plano de usuario cae fuera del rango configurado de valores, realizar una acción resultante de la violación de característica.

La presente descripción proporciona además un medio legible por ordenador para almacenar instrucciones de programa para monitorizar el tráfico en el plano de usuario para un equipo de usuario, que cuando se ejecuta por un procesador de un elemento de red hace que el elemento de red: configure un conjunto de características y un rango de valores para cada uno del conjunto de características para el tráfico del plano de usuario entre el equipo de usuario y el elemento de red; monitorizar el tráfico del plano de usuario para el equipo de usuario en el elemento de red, determinando la monitorización si al menos una característica del tráfico del plano de usuario cae fuera del rango configurado de valores, dando como resultado una violación de característica; y si al menos una característica del tráfico del plano de usuario cae fuera del rango configurado de valores, realizar una acción resultante de la violación de característica.

Una amplia gama de tipos de equipos de usuario (UE) utilizarán servicios de quinta generación (5G) o posteriores. Dichos UE pueden incluir dispositivos de Internet de las cosas (IoT), algunos de los cuales pueden tener una potencia de procesamiento y memoria muy limitadas. Como tal, un mecanismo de seguridad único para todos no servirá bien para todos los tipos de dispositivos y puede ser bastante costoso en relación con el mercado al que se dirige el dispositivo.

Por lo tanto, según las realizaciones siguientes, se proporciona un mecanismo diseñado principalmente para soportar dispositivos IoT que se conectan a redes celulares de área amplia, donde se reducen los gastos generales de seguridad para la transmisión, lo que generalmente da como resultado en menores requisitos de potencia de procesamiento y una mayor duración de la batería para el dispositivo.

Si bien las realizaciones que se describen a continuación se proporcionan para redes y dispositivos 5G, en algunos casos las soluciones proporcionadas podrían utilizarse con redes de cuarta generación o podrían utilizarse con redes futuras más allá de 5G. Por lo tanto, la presente descripción no se limita a redes y dispositivos 5G.

Ahora se hace referencia a la fig. 1, que muestra una red de núcleo de paquetes evolucionados en una red 4G. En la realización de la fig. 1, un UE 110 se comunica a través de la red utilizando un nodo de acceso (AN) 120. El AN 120 normalmente es un Nodo B evolucionado (eNB).

Un AN 120 se comunica con un núcleo de paquetes evolucionado (EPC), que en parte comprende una entidad de gestión de movilidad (MME) 130, un servidor de abonado doméstico (HSS) 140, una puerta de enlace de servicio (S-GW) 150 y puerta de enlace (P-GW) de red de paquetes de datos (PDN) 160.

La MME 130 controla el funcionamiento del dispositivo 110 a través de mensajes de señalización utilizando el HSS 140.

La S-GW 150 actúa como enrutador y reenvía datos a la P-GW 170 a través de una interfaz S5/S8.

La P-GW 160 proporciona la interfaz entre la red 4G y otras redes, tales como Internet o redes privadas. La P-GW 160 está conectada a una red pública de datos PDN a través de una interfaz SGi.

Los expertos en la técnica apreciarán que la red inalámbrica puede conectarse a otros sistemas, incluyendo posiblemente otras redes, no mostradas explícitamente en la fig. 1.

En la realización de la fig. 1, el tráfico del plano de usuario fluye entre el UE 110, el AN 120, la MME 130 y el HSS 140.

Además, el tráfico en el plano de usuario fluye entre el UE 110, el AN 120, la SGW 150 y la P-GW 160.

Específicamente, se hace referencia a la fig. 2, que muestra las comunicaciones entre las distintas capas en el UE 210 y el eNB 212.

En particular, para el tráfico 218 del plano de usuario, la comunicación del UE procede de la capa 220 de control de recursos de radio (RRC), a través de la capa 222 del protocolo de convergencia de paquetes de datos (PDCP), de la capa 224 de control de enlace de radio (RLC), de la capa 226 de control de autenticación de mensajes (MAC) y a la capa 228 física (PHY).

De manera similar, en el eNB 212, los datos del plano de control del UE 210 proceden a través de una capa 230 PHY, de una capa 232 MAC, de una capa 234 RLC, de una capa 236 PDCP y a la capa 238 RRC. A continuación, puede fluir hacia la MME.

Para el tráfico 240 del plano de usuario, el tráfico fluye hacia y desde una capa 250 de aplicación (APP) en el UE 210. El tráfico puede fluir a través de la capa 222 PDCP, de la capa 224 RLC, de la capa 226 MAC y a la capa 228 PHY.

En el eNB 212, el tráfico fluye a través de la capa 230 PHY, de la capa 232 MAC, de la capa 234 RLC a la PDCP 236. A continuación, podrá reenviarse a través de la S-GW/P-GW 214 a Internet 216. En un servidor al que se accede a través de Internet 216, una capa 252 de aplicación puede recibir el tráfico 250 del plano de usuario.

En las redes 5G, probablemente habrá numerosas opciones para que un UE seleccione el tipo de servicio que desea recibir de una red. Un elemento de las opciones que se pueden negociar entre el UE y una red puede ser el tipo de seguridad que se aplica al servicio. Estas características de seguridad, que posiblemente ocurran en la interfaz portadora de radio entre el UE y un Nodo B de próxima generación (gNB), podrían ser, por ejemplo, el uso o no uso de protección de integridad, el uso o no uso de confidencialidad (cifrado), la selección del algoritmo de integridad y la selección del algoritmo de cifrado.

La seguridad aplicada a la conexión del UE a la red puede basarse, al menos en parte, en la autenticación mutua del dispositivo del UE y el usuario del UE para verificar que son quienes dicen ser y tienen permiso para acceder a la red. Esta parte de la seguridad de la conexión se llama autenticación mutua. La protección de las comunicaciones intercambiadas entre el UE y la red contra manipulación o suplantación de identidad se conoce como integridad. La integridad se puede lograr principalmente utilizando, por ejemplo, firmas o funciones hash con clave. La protección de las comunicaciones entre el UE y la red contra escuchas ilegales se conoce como confidencialidad. La confidencialidad se puede lograr principalmente utilizando, por ejemplo, cifrado. La confidencialidad y la integridad son los dos componentes básicos que, cuando se combinan, proporcionan un enlace de comunicaciones altamente seguro desde el origen hasta el destino.

En la evolución a largo plazo (LTE), también denominado como redes 4G y 5G, la integridad y la confidencialidad del funcionamiento a través de la interfaz de radio (por el aire) se definen para el tráfico del plano de control y del plano de usuario para garantizar la seguridad de las comunicaciones a través de esta interfaz. La tabla 1 a continuación muestra las opciones definidas para la aplicación de integridad y confidencialidad en 4G y 5G.

Tecnología/Tipo de tráfico	Plano de control (UE - Red)		Plano de usuario (UE - Red)	
	Integridad	Confidencialidad	Integridad	Confidencialidad
4G	Obligatorio	Opcional*	Prohibido	Opcional
5G	Obligatorio	Opcional*	Opcional	Opcional
Notas		*Se recomienda confidencialidad		

Tabla 1: Configuraciones de seguridad de UE a red para 4G y 5G

En el ejemplo de la tabla 1, la integridad garantiza que el UE sea la entidad esperada y la confidencialidad indica que las comunicaciones están cifradas para impedir que los espías lean la comunicación.

La confidencialidad e integridad de 4G están previstas, por ejemplo, en el especificación técnica (TS) 33.401 del proyecto de asociación de tercera generación (3GPP), "Evolución de la arquitectura del sistema 3GPP (SAE); arquitectura de seguridad" (3GPP System Architecture Evolution (SAE); Security architecture), por ejemplo, según lo dispuesto en la versión 15.0.0, de junio de 2017. En particular, la cláusula 5.1.4.1 prevé dicha integridad y confidencialidad. Las secciones de 3GPP TS 33.401 se reproducen, a continuación, en el apéndice A.

La confidencialidad e integridad de 5G están previstas, por ejemplo, en 3GPP TS 33.501, "Arquitectura y procedimientos de seguridad para el sistema 5G" (Security architecture and procedures for 5G system), por ejemplo, según lo dispuesto en la versión 0.2.0, de junio de 2017. Además, el informe técnico 3GPP (TR) 33.899, "Estudio sobre los aspectos de seguridad del sistema de próxima generación" (Study on the security aspects of the next generation system) también prevé dicha confidencialidad e integridad.

En las redes 3GPP actuales, incluyendo la segunda generación (2G), la tercera generación (3G) y LTE, la protección de integridad y confidencialidad se logra mediante el uso de una clave compartida (K) entre el UE y la red. Por ejemplo, los detalles de autenticación para un sistema de paquetes mejorado (EPS) se encuentran en 3GPP TS 33.401, sección 6.1, reproducido en el apéndice B de la presente descripción.

Generalmente, la seguridad aplicada a una conexión de radio del UE a la red es la seguridad más sólida que pueden soportar mutuamente el UE y el equipo de red. En particular, la red intentaría utilizar la seguridad más sólida posible para ofrecer protección al UE, así como proteger el equipo de red contra ataques.

La confidencialidad del plano de usuario se proporciona mediante cifrado en la capa 222 o 236 PDCP. Es en la capa 222 o 236 PDCP donde se realiza el uso o no uso de la confidencialidad para el plano de usuario. La decisión de configurar la capa PDCP para utilizar o no la confidencialidad se puede tomar en la capa 238 RRC (en el eNB 212) o algún otro equipo, posiblemente la MME. La capa 222 o 236 PDCP soporta la integridad de los datos del usuario utilizando MAC, donde cada mensaje que llegue a la capa PDCP estaría protegido por su integridad.

Normalmente, los protocolos de capa superior (por encima de la capa PDCP) aplican seguridad a la transmisión de comunicación, aunque esto no es necesario para las realizaciones de la presente descripción. La seguridad de capa superior podría ser, por ejemplo, seguridad de la capa de transporte (TLS) o TLS de datagramas (DTLS), capa de conexión segura (SSL), protocolo de transferencia de hipertexto seguro (HTTPS) y seguridad del protocolo de Internet (IPSec). Además, si no se aplica la seguridad en las capas superiores, a continuación, las realizaciones de la presente descripción podrían utilizarse para proporcionar seguridad mejorada a aquellas transmisiones desprotegidas.

Basándose en lo anterior, el impacto de seguridad en la infraestructura de red y el tráfico de datos del usuario basado en la selección de los aspectos opcionales del uso de integridad y confidencialidad del plano de usuario que se muestran en tabla 1 se abordan mediante las realizaciones que se describen a continuación.

3GPP TR 23.799, "Estudio de Arquitectura para Sistemas de Próxima Generación" (Study on Architecture for Next Generation System), en la cláusula 5.10: infraestructura de políticas, estados;

- En el sistema EPC, las funciones de red se pueden configurar mediante políticas del operador. Se espera que esta tendencia continúe en el sistema de próxima generación. Estas políticas de operador ayudan a dar forma a una variedad de comportamientos de red, tales como los relacionados con:

- Cumplimiento de la calidad de servicio (QoS).
- Control de cobro.
- Apertura y cierre.
- Enrutamiento del tráfico.
- Gestión de la congestión.
- Encadenamiento de servicios.
- Selección de red (por ejemplo, PLMN).
- Selección del tipo de acceso.
- Itinerancia.
- Movilidad.
- Políticas relacionadas con grupo de usuarios.
- Manejo de servicios de terceros.

• El aprovisionamiento y el cumplimiento de estas políticas pueden ocurrir en:

- El UE.
- Las entidades del plano de control.
- Las entidades del plano de usuario.

Por lo tanto, en algunos casos, las realizaciones de la presente descripción pueden ser parte de la infraestructura de políticas para 5G al proporcionar supervisión de las características del tráfico de un UE.

La presente descripción proporciona a un operador de red más información sobre el uso de un servicio de red por parte de un UE. Siempre que las transmisiones observadas cumplan con el comportamiento descrito de un UE, el operador de red debería tener confianza en que el tráfico del UE no ha sido modificado en ruta o que el UE no ha sido manipulado.

Específicamente, una buena seguridad es la combinación de integridad y confidencialidad en un flujo de datos. Eliminar uno, el otro o ambos afecta a aspectos de seguridad.

Por ejemplo, la integridad puede proteger al receptor de la manipulación de la carga útil de datos, ya que la carga útil de datos o una parte de ella se utiliza para generar la firma de integridad. La integridad también puede proteger contra ataques DoS, ya que los paquetes adicionales o duplicados que llegan a un destino no pasarían la verificación de integridad. La integridad también garantiza que la conexión no haya sido secuestrada por un atacante que se haga pasar por el verdadero creador/usuario de la conexión de datos.

La confidencialidad protege los datos contra escuchas ilegales y puede proporcionar cierta protección contra la manipulación. Por ejemplo, podría descartarse un paquete que no ha pasado la verificación de confidencialidad porque se ha cambiado la carga útil de datos.

La tabla 2 a continuación ilustra una combinación de características de seguridad y cómo pueden proteger contra una vulnerabilidad o exponerla. La manipulación incluye tanto la carga útil de datos como la información de control del protocolo (PCI o paquete de metadatos). Cuando la confidencialidad está desactivada y no se aplica en una capa superior, toda la PCI queda expuesta, incluyendo la información crítica, tal como la dirección de protocolo de Internet (IP) de origen y destino.

Característica de seguridad/vulnerabilidad	Escuchas ilegales	Manipulación	Denegación de servicio
Integridad ACTIVADA; Confidencialidad ACTIVADA	Seguro	Seguro	Seguro
Integridad ACTVADA; Confidencialidad DESACTIVADA	Expuesto	Riesgo (datos de usuario)	¿Riesgo?
Integridad DESACTIVADA; Confidencialidad ACTIVADA	Seguro	Riesgo (metadatos)	Expuesto
Integridad DESACTIVADA; Confidencialidad DESACTIVADA	Expuesto	Expuesto	Expuesto

Tabla 2: Impacto de las opciones de seguridad en la seguridad aérea

Es posible que ciertos tipos de dispositivos, en particular los empleados en aplicaciones de tipo IoT, no requieran una gran cantidad de protección de seguridad si los datos que intercambian son de bajo valor. Este puede ser el caso de muchos tipos de dispositivos IoT, donde el coste del dispositivo y su vida útil en servicio son cuestiones más importantes que el valor de un intercambio de datos individual. Algunos ejemplos de datos y aplicaciones que pueden tener poco valor incluyen:

- Datos de medición (parquímetros)
- Recopilación de datos meteorológicos
- Algunas aplicaciones de monitorización del hogar (temperatura interna)
- Seguimiento de ubicación de objetos que se mueven lentamente (barrera de troncos)

Estos dispositivos normalmente ejecutarían una aplicación específica que se conecta a un solo destino y también pueden operar un protocolo de seguridad en una capa superior o en la propia aplicación. Por lo tanto, la seguridad de la capa de radio puede suponer un coste adicional, innecesario.

Para 5G, la protección de integridad de los datos de usuario es opcional en la capa de radio. Por lo tanto, es posible tener una sesión de datos de usuario entre el UE y el eNB funcionando sin integridad ni protección de confidencialidad.

Por lo tanto, la presente descripción aborda el problema en el que se puede permitir que dispositivos de bajo coste con funciones de seguridad integradas mínimas que soportan la integridad y la confidencialidad se conecten a una red móvil terrestre pública (PLMN) y no introduzcan riesgos de seguridad a la infraestructura de la red ni a otros usuarios de la red. Esto aborda específicamente el escenario en el que no se aplica ninguna seguridad (integridad desactivada, confidencialidad desactivada) a las transmisiones OTA. Los problemas de seguridad abordados en la presente descripción se aplican al plano de usuario e incluyen manipulación, uso indebido de la conexión y ataques de denegación de servicio.

Las realizaciones descritas en la presente memoria también se pueden utilizar para otros beneficios de seguridad que están fuera del alcance de la interfaz de radio del UE a la red. Los parámetros configurados en las realizaciones de la presente descripción pueden observar características del dispositivo y de la aplicación, tales como la frecuencia de transmisión de datos, el volumen de datos y la ubicación del dispositivo (geocercado), la dirección de origen y destino de los datos. Si, por ejemplo, el dispositivo ha sido robado y trasladado a otra ubicación y, a continuación se utiliza para transportar otros datos, las realizaciones de la presente descripción podrían detectar estos cambios en el comportamiento de transmisión de datos del dispositivo y/o en la ubicación del dispositivo.

Por lo tanto, la presente descripción proporciona para la configuración, en un nodo de red determinado, un conjunto de características y rangos de valores para cada una de estas características. La presente descripción proporciona además la monitorización del tráfico del plano de usuario para observar el conjunto de características para identificar cualquier comportamiento anómalo cuando una o más de las características caen fuera del rango configurado. La presente descripción proporciona además la invocación de acciones adecuadas al observar un comportamiento anómalo.

Ahora se hace referencia a fig. 3. La realización de la fig. 3 muestra un ejemplo de configuración de red de cuarta generación similar a la de la fig. 1. Números similares a los de la fig. 1 se utilizan en la realización de la fig. 3.

En la realización de la fig. 3, sin embargo, la P-GW 160 es elegida como nodo de red responsable de identificar cualquier comportamiento anómalo. En este sentido, una función de cumplimiento de políticas de seguridad (SPEF) 310 se añade a la P-GW 160. En la SPEF 310 de P-GW 160 se configura un conjunto de características y un rango de valores para cada una de estas características.

La realización de la fig. 3 sin embargo, es sólo un ejemplo y la SPEF 310 podría implementarse en diferentes nodos de red. Además, en algunas realizaciones, se podrían implementar diferentes funcionalidades dentro de la SPEF en diferentes nodos de red. Por lo tanto, el uso de la SPEF 310 en la P-GW 160 se proporciona simplemente como ejemplo.

Ahora se hace referencia a la fig. 4, que muestra un ejemplo de una red 5G. En particular, en la realización de la fig. 4, un UE 410 se comunica con una red 420 de acceso (por radio) ((R)AN). La (R)AN 420 también puede denominarse Nodo B de próxima generación (gNB).

El UE 410 puede comunicarse además con una función 420 de gestión de acceso y movilidad (AMF).

La AMF 420 se comunica con la función 422 del servidor de autenticación (AUSF) y además con un módulo 424 de gestión unificada de datos (UDM).

Además, la AMF 420 también se comunica con la función 426 de gestión de sesiones (SMF).

Una función 430 de control de políticas (PCF) es responsable del control de políticas y se comunica con la SMF 426 y con la función 432 de aplicación (AF).

La (R)AN 412 se comunica además con la AMF 420 y con la función 450 de plano de usuario (UPF). La UPF 450 es similar a la P-GW 160 de las realizaciones de la figs. 1 y 3.

La UPF 450 se comunica con la red 452 de datos, que pueden ser servicios de operador de red, Internet, servicios de terceros, entre otras opciones.

Según la realización de la fig. 4, la SPEF 460 se añade a la UPF 450. De esta manera, la SPEF 460 puede identificar cualquier comportamiento anómalo mediante la monitorización del tráfico del plano de usuario.

Como se ha indicado anteriormente, las realizaciones de la presente descripción proporcionan tres aspectos. En un primer aspecto se configura la SPEF. En un segundo aspecto, la SPEF monitoriza el tráfico del plano de usuario para observar el conjunto de características e identificar cualquier comportamiento anómalo. En un tercer aspecto, se actúa sobre el comportamiento anómalo detectado invocando acciones adecuadas en un elemento de red. Cada uno se describe a continuación.

Configuración

Según una realización de la presente descripción, una SPEF puede configurarse con un conjunto de características para las comunicaciones entre un equipo de usuario y una red. Estas características están relacionadas principalmente con la comunicación de datos del plano del usuario. Las características se conocen de antemano y/o se pueden establecer de antemano y, por lo tanto, la infraestructura de red puede monitorizar una sesión frente al comportamiento observado de las transmisiones.

Cuando se identifica una desviación de las características predefinidas, esto indicaría un posible problema de seguridad.

Un conjunto de características se proporciona a continuación en Tabla 3.

Nombre	Valores de rango de ejemplo	Descripción
SPE_LOC	- Coordenadas GPS dentro de las cuales se ubicará el UE. - Lista de ID de celda válidas o ID de área de seguimiento del UE	- Ubicación del UE: coordenadas GPS que incluyen comportamiento de ubicación/movimiento/velocidad u otra información sobre la ubicación física del UE (ID de celda). Estos pueden ser conocidos a priori para muchos UE, tales como UE estacionarios (por ejemplo, medidores inteligentes).
SPE_VOLUME	- Cantidad máxima de datos en un período de tiempo determinado o Máximo de bytes por segundo o Volumen máximo de datos en un día/mes, etc.	- Volumen de carga útil de datos estimado. Esto puede especificarse en los parámetros de suscripción (por ejemplo, disponible en el HSS)
SPE_TOD	- Hora prevista de llegada (algunos ejemplos a continuación) o de 01:00 a 02:00 am todos los días o solo entre semana o solo fines de semana	- Hora prevista del día/día de la semana/día del mes, etc., para la configuración de la conexión
SPE_CONNS	- número máximo de conexiones TCP/IP o número máximo de sesiones de datos de PDU por UE	- Número esperado de conexiones de datos simultáneas (TCP/IP) desde el UE
SPE_DUR	- duración máxima esperada de una sesión (por ejemplo, a continuación) o duración máxima 20 minutos	- Duración prevista de la conexión
SPE_FREQ	- número máximo de paquetes de datos enviados en un período de tiempo determinado (ejemplos a continuación) o Número de paquetes IP en una hora o Número de paquetes IP por día/semana	- Frecuencia estimada de transmisión de datos (una vez por hora/minuto/segundo, o continua)

Nombre	Valores de rango de ejemplo	Descripción
SPE_DATATYPE	- Tipos de datos permitidos o Datos de imagen o Datos de vídeo o tipo VoIP o ftp o etc. Obsérvese que esto puede identificarse basándose en el campo DSCP en el encabezado IP Alternativamente, esto también puede identificarse basándose en el tipo de carga útil del paquete IP (por ejemplo, carga útil de tipo TCP o UDP, etc.). También es factible una mayor identificación del nivel de aplicación si el nodo es capaz de realizar una inspección profunda de paquetes.	- Tipo de datos; texto, numérico, transmisión de video, transmisión de audio, gráficos (.jpg, .gif, .pdf), carga útil cifrada (donde el cifrado se realiza en una capa por encima de la capa de radio, es decir, la capa de aplicación)
SPE_IPADDR	- dirección IP/números de puerto de origen y/o destino permitidos	- Dirección de destino normal (dirección IP, URI o nombre de dominio o subdominio)
SPE_BYTES	- número máximo de bytes	- Intercambio de recuentos de bytes transmitidos y recibidos entre el UE y la red a través de una conexión específica. Véase la sección técnica anterior a continuación.
SPE_CAPABILITY	- Esto es similar al SPE_DATATYPE mencionado anteriormente.	- Uso de suscripción permitido. Por ejemplo, solo datos (no se permite tráfico de SMS, multimedia o voz (VoIP)).

Tabla 3: Parámetros de la función de cumplimiento de políticas de seguridad

En la tabla 3 anterior, SPE se refiere al cumplimiento de políticas de seguridad. Los nombres del cumplimiento de políticas de seguridad especificadas en la tabla 3 son, sin embargo, meros ejemplos. Otras características de cumplimiento podrían definirse en la SPEF.

En la tabla 3 anterior, se podría establecer una característica de ubicación que puede incluir comportamiento de ubicación, de movimiento o velocidad, u otra información con respecto a la ubicación física del UE. Las coordenadas del ID de celda o del sistema global de navegación por satélite (GNSS) se pueden utilizar para verificar la ubicación del UE y verificar su posición con un valor de red contenido en el perfil de usuario del UE para garantizar que el UE esté en la ubicación que debería estar, o en la región de su operación prevista. Un dispositivo que se encuentre funcionando fuera de su ubicación esperada podría marcarse como un posible dispositivo robado.

Además, se puede establecer la información de volumen estimando el volumen de datos de carga útil que se enviaría desde un UE o a un UE.

Se puede configurar la información de la hora del día, incluyendo cuándo pueden ocurrir las transmisiones esperadas hacia o desde el UE.

También se pueden configurar varias conexiones simultáneas esperadas. La duración prevista de dichas conexiones puede ser otra característica que podría monitorizarse.

Además, en algunas realizaciones se puede conocer la frecuencia estimada de transmisión de datos. Así, por ejemplo, si se espera que una baliza meteorológica transmita cada 30 minutos, dicha frecuencia podría fijarse con esta característica.

Un tipo de datos para el tipo de datos que se enviarían desde el UE también podría conocerse o establecerse como una característica de los datos que se esperan de ese UE.

Las balizas pueden tener un destino particular al que reportar. Por ejemplo, utilizando el ejemplo de la baliza meteorológica, la baliza meteorológica puede enviar datos a un servidor particular y a ninguna otra ubicación. En este caso, una característica podría ser la dirección de destino normal de las comunicaciones.

Una característica adicional que se puede establecer puede ser el número de bytes que se espera transmitir en las comunicaciones. Por ejemplo, utilizando nuevamente el sistema de baliza meteorológica, el UE puede enviar un paquete de datos que tiene un tamaño relativamente conocido y, por lo tanto, se podrían establecer límites superiores en el tamaño de la transmisión como una característica.

Además, se podrían establecer capacidades para el UE, indicando por ejemplo que el UE enviará datos y no SMS, paquetes multimedia, paquetes de voz, entre otros.

Muchos de los parámetros anteriores están relacionados con el flujo de tráfico. Además, si se utiliza la inspección de la carga útil del paquete, muchos de los parámetros anteriores se pueden utilizar con el contenido de la carga útil.

Como se describe a continuación, la red puede utilizar las características y rangos anteriores para comparar el tráfico observado con los parámetros proporcionados. Si el tráfico observado cae dentro de los rangos de perímetro proporcionados, la red puede tener confianza en que el tráfico es válido.

Un cambio en el flujo de tráfico puede verse como una posible amenaza a la red. Por ejemplo, los cambios en el tráfico con respecto a la frecuencia o el volumen pueden estar asociados con un ataque de denegación de servicio, cambios en el tráfico en la duración de la conexión, tipo de datos, ubicación, hora del día, capacidad, dirección IP de origen o destino, recuento de bytes, entre otros podría indicar manipulación. Como se describe a continuación, la red puede, entonces tomar las medidas adecuadas.

Además, en algunas realizaciones, un dispositivo que funcione fuera de sus parámetros esperados podría ser simplemente un dispositivo que no funciona correctamente. A continuación, los operadores pueden tomar medidas para proteger la red de un dispositivo corrupto o que se comporte mal y los propietarios del dispositivo pueden ser notificados del problema.

Las características y rangos de la tabla 3 anterior pueden estar configurados previamente en el nodo que contiene la información de suscripción. Por ejemplo, en la arquitectura de red 3GPP, la funcionalidad puede residir en la PCF en redes 5G o en el HSS en redes 4G.

Alternativamente, la información con respecto a las características puede obtenerse directamente de un UE para cada sesión. En una realización, la información del UE con respecto a las características puede proporcionarse sólo en mensajes de integridad protegida para garantizar la validez de los parámetros.

Por ejemplo, durante un procedimiento de CONEXIÓN, un UE se autentica y posiblemente puede enviar de forma segura las características esperadas de la sesión en un mensaje de integridad protegida. Dado que sólo un UE autenticado puede enviar un mensaje de integridad protegida, la red puede confiar en los valores de los parámetros incluidos en el mensaje. Basándose en la información se puede determinar el conjunto de características y un rango de valores correspondientes a las características. Estos valores podrán, a continuación, configurarse, por ejemplo, en la SPEF de la P-GW para redes 4G y en la UPF para redes 5G.

Por ejemplo, ahora se hace referencia a la fig. 5, que muestra la configuración de características de la UPF en una red 5G.

En particular, en la realización de la fig. 5, un UE 510 de próxima generación (NG-UE) se comunica con una red 5G, incluyendo la AMF 512, la SMF 514, la UPF con SPEF 516 y la infraestructura 518 de acceso al cumplimiento de seguridad (SEAF).

Como se ve en bloque 520, el UE está conectado a la red. Esta etapa implica la autenticación mutua de la red y el UE.

Opcionalmente, en bloque 520, el UE puede proporcionar las características esperadas de la sesión en un mensaje seguro y de integridad protegida. Un ejemplo de dicho mensaje de integridad protegida es un mensaje 522 de solicitud de establecimiento de sesión de PDU del UE.

El mensaje 522 puede incluir una identidad así como un nombre de red de datos (DNN). En una realización, la capacidad de seguridad del UE, que incluye las capacidades de seguridad del plano de usuario, se almacena en la AMF durante el procedimiento de CONEXIÓN. Alternativamente, el NG-UE 510 puede proporcionar sus capacidades de seguridad del plano de usuario en el mensaje 522.

Posteriormente, en el bloque 524, la AMF determina una SMF basada en el DNN proporcionado por el NG-UE 510.

La AMF 512, una vez que ha elegido una SMF adecuada, activa el procedimiento de establecimiento de sesión enviando una solicitud de establecimiento de sesión de PDU a la SMF, que se muestra mediante un mensaje 530. El mensaje 530 incluye la identidad del UE, DNN y capacidad de seguridad.

La SMF 514, a continuación, puede recuperar una política de seguridad de la PCF 532, como lo muestra la flecha 534. En una realización, la política de seguridad puede incluir un conjunto de características y el rango de valores para cada característica, como se muestra en las dos primeras columnas de la tabla 3 anterior.

Alternativamente, la SMF 514 puede determinar las características y rangos basándose en una política recuperada de la PCF. En otras realizaciones, algunos o todos los valores también pueden obtenerse directamente desde el UE durante la solicitud 522 de establecimiento de sesión de CONEXIÓN o PDU. En este caso, los valores se pasan a la SMF 514 desde la AMF 512.

En el bloque 536, la SMF puede verificar si el NG-UE 510 está autorizado a establecer la sesión de PDU solicitada y determina la terminación de seguridad del plano de usuario.

Si el NG-UE 510 está autorizado para establecer la sesión de PDU y se requiere la terminación de seguridad UPF para la sesión de PDU, la SMF 512 podrán solicitar una clave para la UPF. La SMF 514 proporciona la SEAF 518 con la identidad del UE, DNN e identidad de la SMF en el mensaje 540.

La SEAF obtiene una clave UPF (K_{UPF}) de la K_{SEAF} incorporando los parámetros recibidos de la SMF 514 y un contador gestionado localmente (por ejemplo CNT_{UPF}) para la derivación de la clave UPF. La derivación de la clave se muestra en el bloque 542.

La SEAF 518, a continuación, envía un mensaje 544 de respuesta de clave a la SMF 514. La respuesta de clave incluye la K_{UPF} y CNT_{UPF} utilizadas para la derivación de la clave. Así, el contador en el bloque 542 es devuelto.

Al recibir el mensaje 544, la SMF 514 envía una solicitud de configuración de sesión de PDU a la UPF que contiene la información de configuración de seguridad para la sesión de PDU. Esto puede incluir, por ejemplo, el algoritmo de cifrado y/o de protección de integridad, incluyendo la K_{UPF} y características del tráfico para la sesión de PDU. Esto se envía en el mensaje 550 en la realización de la fig. 5.

La UPF con la SPEF 516 instala la K_{UPF} para la sesión como parte de la configuración de la sesión de PDU y deriva claves posteriores, tales como K_{UPFEnc} y K_{UPFInt}. Dichas claves se derivan basándose en la información de configuración de seguridad. Las claves están asociadas con un ID de clave, que también puede incorporarse en la derivación de clave. Sin embargo, si no se aplican la protección de integridad y confidencialidad a la sesión de PDU y la K_{UPF} es nula, es posible que no haya derivación de las claves posteriores. Además, la UPF configura la función de cumplimiento de política de seguridad con los parámetros característicos del tráfico recibidos de la PCF desde esta sesión de PDU. La instalación clave se muestra en el bloque 552 en la realización de la fig. 5.

La UPF, a continuación, envía una respuesta 554 de configuración de sesión de PDU a la SMF 514 que contiene un ID de sesión de PDU, un ID de clave y otros parámetros, si existen, utilizados para la derivación de la clave.

La SMF 514, a continuación, envía una respuesta de establecimiento de sesión de PDU al NG-UE 510 mediante la AMF 512, mostrada por el mensaje 556. Este mensaje de respuesta incluye todos los materiales clave, tales como CNT_{UPF}, ID de clave, entre otros, que se necesitan para que el NG-UE 510 derive las mismas claves que la UPF.

El NG-UE 510 deriva la K_{UPF} y claves posteriores basándose en la respuesta de establecimiento de sesión en el bloque 558.

El NG-UE 510, a continuación, envía un mensaje 560 de establecimiento de sesión de PDU completo a la SMF 514 mediante la AMF 512.

Después de completar el envío del mensaje 560, el NG-UE 510 y la UPF protegen en el plano de usuario los paquetes basándose en la configuración de seguridad de sesión de PDU que termina en la UPF, que incluye la SPEF.

Los cambios a 3GPP TR 33.899 que pueden adaptarse a lo anterior se muestran, por ejemplo, en el apéndice C a continuación. Los añadidos a TR se muestran en negrita.

De manera similar, las características podrían proporcionarse a la P-GW con una SPEF en una red 4G. Por ejemplo, ahora se hace referencia a la fig. 6.

En la realización de la fig. 6, un UE 610 se comunica con el eNB 612. Además, los elementos de red incluyen una MME 614, una S-GW 616, una P-GW 618 y una función 620 de reglas de política y cobro (PCRF).

Al principio, el UE 610 realiza una solicitud de CONEXIÓN al eNB 612, como se muestra en el mensaje 630.

El eNB 612 reenvía la solicitud de CONEXIÓN a la MME 614, como se muestra en el mensaje 632.

A partir de entonces, se realiza un procedimiento de CONEXIÓN, como se define por ejemplo en 3GPP TS 23.401, y concretamente las etapas 1-11 en la sección 5.3.2.1, como se muestra en el bloque 640 en la realización de la fig. 6.

Si el contexto de suscripción no indica que el APN es para una conexión PDN, la MME 614 selecciona una puerta de enlace 616 de servicio. A continuación, envía una solicitud 650 de creación de sesión. Dicha solicitud de creación de sesión puede incluir diversa información de solicitud de sesión, incluyendo parámetros de cumplimiento de políticas de seguridad.

Una vez que la puerta de enlace 616 de servicio recibe la solicitud 650, a continuación, puede enviar una solicitud de creación de sesión con información estándar, así como parámetros de cumplimiento de políticas de seguridad, a la P-GW 618, mostrada como la solicitud 652.

La P-GW 618, a continuación, puede realizar un procedimiento de establecimiento de sesión IP-CAN con PCRF 620, como se define por ejemplo en 3GPP TS 23.203, y de ese modo obtiene reglas de control de política y cobro (PCC) predeterminadas para el UE. Esto se muestra con una flecha 654 en la realización de la fig. 6.

La P-GW 618 crea una nueva entrada en su tabla de contexto de portadora EPS y genera un ID de cobro para la portadora predeterminada. La nueva entrada permite a la P-GW 618 enrutar las PDU del plano de usuario entre la S-GW 616 y la red de paquetes de datos. Si los parámetros SPEF están presentes, la función SPEF se invocará en la P-GW 618 y comenzará a monitorizar las PDU del plano de usuario para el UE 610.

La P-GW 618 devolverá a la S-GW 616 una respuesta de creación de sesión, que se muestra como respuesta 660.

Si la CONEXIÓN no se basa en un traspaso, a continuación, se pueden recibir los primeros datos de enlace descendente, mostrados por la flecha 662. En este punto, la S-GW 616 puede enviar una respuesta de creación de sesión a la MME 614, como se muestra en el mensaje 664.

Monitorización del tráfico del plano de usuario

Al configurarse con un conjunto de características y sus rangos válidos, como por ejemplo se describe con respecto a la figs. 5 y 6 anteriormente, la SPEF puede comenzar a monitorizar el tráfico originado y terminado en dispositivos móviles. Si una o más características de los datos del plano de usuario están más allá del rango configurado, la SPEF puede detectar una anomalía, lo que puede indicar una posible vulnerabilidad de seguridad y puede activar una acción adecuada basada en la causa de la anomalía identificada.

La monitorización puede ser para características particulares. En una realización, la monitorización puede ocurrir teniendo cada una de las características configuradas en la SPEF monitorizadas por separado. En otras realizaciones, la monitorización puede realizarse para una pluralidad de características.

A continuación se muestran ejemplos de monitorización con respecto a las realizaciones de la figs. 7, 8 y 9. Sin embargo, las realizaciones en estas figuras se proporcionan simplemente a modo de ilustración, y otros ejemplos de monitorización de características particulares resultarán evidentes para los expertos en la técnica teniendo en cuenta la presente descripción.

Con referencia a la fig. 7, la realización muestra un proceso en la SPEF para monitorizar el volumen de datos. En particular, el proceso de la fig. 7 comienza en el bloque 710 y procede al bloque 712 en el que se reciben nuevos paquetes de datos que están destinados a un UE o son de un UE.

El proceso, a continuación, procede al bloque 714 en el que se realiza un cálculo sobre la cantidad acumulada de datos que ha recibido un UE o se ha enviado al UE durante un período de tiempo particular. Por ejemplo, si la configuración para un UE se ha establecido con una característica que espera una cierta cantidad de datos para el UE para cada día determinado, el cálculo en el bloque 714 podrá calcular los datos acumulados para ese período de tiempo. En otras realizaciones, el período de tiempo puede ser una hora, una cantidad de minutos, una semana, un mes, entre otros períodos de tiempo.

El proceso, a continuación, procede al bloque 716 en el que se realiza una verificación para determinar si la cantidad de datos recibidos en el período de tiempo excede un umbral para la cantidad esperada de datos desde el UE o hacia el UE. Por ejemplo, si se espera que el UE envíe menos de 1 MB de datos por día y la cantidad

acumulada de datos enviados desde el UE ha excedido 1 MB, a continuación la verificación en el bloque 716 es afirmativa y el proceso procede al bloque 718.

En el bloque 718, si la cantidad de datos ha superado el umbral, a continuación, se invoca una acción adecuada relacionada con la causa del gran volumen de datos. A continuación se describen acciones ejemplares.

Por el contrario, si la cantidad de datos es menor que el umbral, a continuación, el proceso continúa desde el bloque 716 vuelve al bloque 712 en el que el proceso espera a que se reciban los siguientes datos para o desde el UE.

Desde el bloque 718 el proceso procede al bloque 720 y termina.

Así, según la realización de la fig. 7, un elemento de red puede monitorizar el tráfico de datos hacia o desde un UE para garantizar que la cantidad de datos no exceda un umbral durante un período de tiempo.

Ahora se hace referencia a la fig. 8, que muestra un proceso para monitorizar la ubicación de un UE en la SPEF. En particular, el proceso comienza en el bloque 810 y pasa al bloque 812 en el que se ha recibido un nuevo paquete de datos que está destinado a un UE o se ha recibido un nuevo paquete de datos desde un UE.

El proceso, a continuación, procede al bloque 814 en el que se determina la ubicación del UE. Por ejemplo, en una realización la ubicación puede determinarse basándose en el identificador de celda del UE. Este puede ser, por ejemplo, el identificador de red de acceso por radio (RAN ID) o el identificador eNB para la interfaz N3 en una realización. Sin embargo, la ubicación puede determinarse de diversas maneras y la obtención de la ubicación del bloque 814 podría utilizar diferentes métodos.

Desde el bloque 814 el proceso procede al bloque 816 en el que se realiza la verificación para determinar si el identificador celular está dentro de una lista de identificadores celulares configurados como una característica para ese UE en particular. Por ejemplo, si se supone que un UE es un UE estacionario, como un parquímetro, entonces el movimiento del UE a un ID de celda diferente puede indicar que el UE ha sido robado o está siendo falsificado.

Desde el bloque 816, si el ID de celda está dentro de la lista de parámetros para la característica de ubicación, el proceso regresa al bloque 814 para esperar nuevos paquetes de datos hacia o desde el UE.

Por el contrario, si el ID de celda no está dentro de la lista de parámetros de ID de celda, según lo determinado en el bloque 816, a continuación, el proceso procede al bloque 818 en el que se invocan acciones adecuadas relacionadas con la causa de una ubicación inesperada del UE. A continuación se describen ejemplos de acciones.

Desde el bloque 818 el proceso procede al bloque 820 y termina.

Así, basándose en la fig. 8, la SPEF puede monitorizar la ubicación de un UE para garantizar que la ubicación del UE sea la esperada.

Ahora se hace referencia a la fig. 9, que muestra un proceso en una SPEF para la funcionalidad de monitorización de tipos de datos. En particular, el proceso de la fig. 9 comienza en el bloque 910 y procede al bloque 912 en el que se recibe un nuevo paquete de datos destinado a un UE o un nuevo paquete de un UE.

El proceso, a continuación, procede al bloque 914 en el que se identifica un tipo de datos para el paquete de datos. Por ejemplo, el tipo de datos puede identificarse inspeccionando el campo punto de código de servicios diferenciados (DSCP) en el encabezado IP o identificando si el paquete es un paquete de tipo protocolo de control de transmisión/Protocolo de datagramas de usuario (TCP/UDP).

También son posibles otros métodos para definir el tipo de datos y la presente descripción no se limita a ningún método particular para identificar el tipo de datos en el bloque 914.

Desde el bloque 914 el proceso procede al bloque 916 y comprueba si el tipo de datos es el tipo de datos correcto. La verificación podría utilizar parámetros asociados con características de tipo de datos que se han configurado para el UE. Dichos parámetros permiten a la SPEF determinar si el UE puede enviar el paquete con el tipo de datos identificado en el bloque 914.

Si el tipo de datos es el tipo de datos correcto, el proceso procede al bloque 912 en el que el proceso espera el siguiente paquete de datos hacia o desde el UE.

Por el contrario, si el tipo de datos en el bloque 916 se identifica como un tipo de datos incorrecto, a continuación, el proceso procede al bloque 918 en el que se invoca una acción adecuada relacionada con una causa, donde la causa se establece en un tipo de datos inesperado. Por ejemplo, en el ejemplo del parquímetro, se puede esperar que el parquímetro envíe paquetes TCP. Sin embargo, si se recibe un mensaje del servicio de

mensajes cortos (SMS), esto podría identificarse como un tipo de datos incorrecto y se podría invocar una acción en el bloque 918 hecho para reflejar esto. Las acciones se describen a continuación.

El proceso procede al bloque 920 y termina.

Así, la realización de la fig. 9 muestra un proceso ejemplar para monitorizar tipos de datos para el tráfico que se origina desde un UE o el tráfico destinado a un UE.

Los ejemplos de la figs. 7, 8 y 9 se proporcionan a modo de ilustración. Se podrían utilizar procesos similares para las diferentes características configuradas en la SPEF para que el UE determine si el tráfico en el plano de usuario está o no dentro de los parámetros especificados para tales características.

Activación de acciones adecuadas

Al detectar una o más anomalías en el tráfico del plano de usuario, la SPEF puede activar una acción adecuada específica para el conjunto de anomalías detectadas. Algunas acciones pueden incluir una funcionalidad simple del plano de usuario, tal como descartar paquetes, mientras que otras acciones pueden incluir una funcionalidad del plano de control, tal como activar procedimientos específicos del plano de control 3GPP.

A continuación se proporcionan varios ejemplos de acciones. Sin embargo, la lista de acciones se proporciona simplemente a modo de ilustración, y también podrían realizarse otras acciones. Las acciones que se describen a continuación no tienen por tanto carácter limitativo.

Activar alarmas enviadas a una función de gestión de red PLMN

Se hace referencia a la fig. 10. En un primer ejemplo de una acción, nodos del plano de control, tales como la SMF 1014, la AMF 1012 y la PCF 1030 pueden estar involucrados en la ejecución de la acción. En particular, la acción en el ejemplo de la fig. 10 implica actualizaciones de políticas con la PCF 1030.

En el ejemplo de la fig. 10, la UPF con la SPEF 1016 puede identificar una anomalía y la causa de la anomalía en el bloque 1020. Basándose en la anomalía y la causa, la UPF puede, a continuación, enviar un mensaje 1022 a la SMF 1014 indicando que se ha detectado una anomalía de seguridad. El mensaje 1022 puede incluir una causa, así como un identificador del equipo de usuario.

La SMF 1014, a continuación, puede reenviar el contenido del mensaje 1022 a la AMF 1012, mostrado como mensaje 1024, con la causa y el identificador del equipo de usuario.

Al recibir el mensaje 1024, la AMF 1012 puede actualizar el registro de políticas en la PCF 1030, mostrado con la actualización 1032 de políticas. La actualización puede activar acciones adicionales, tales como notificación al usuario, la demanda de seguridad del plano de usuario, entre otras acciones, como se establece a continuación.

Activar una notificación al propietario del dispositivo

Ahora se hace referencia a la fig. 11, que muestra una acción que puede invocar los nodos del plano de control SMF 1114, AMF 1112 y la UPF con la SPEF 1116. En el ejemplo de la fig. 11, el UE 1110 recibe una notificación.

En el ejemplo de la fig. 11, la UPF con la SPEF 1116 identifica una anomalía en una causa, mostrada en el bloque 1120. La UPF puede, a continuación, enviar un mensaje 1122 a la SMF 1114, indicando que se ha detectado una anomalía de seguridad. El mensaje 1122 puede incluir una causa y un identificador del equipo de usuario.

La SMF 1114, a continuación, puede reenviar el contenido del mensaje 1122 a la AMF 1112, mostrado como mensaje 1124.

La AMF 1112, a continuación, puede reenviar al UE 1110, un mensaje indicando que se ha detectado una vulnerabilidad y la causa de la misma. Esto se muestra como mensaje 1126 en la realización de la fig. 11. El mensaje 1126 puede ser un mensaje seguro de estrato de acceso a la red (NAS) en una realización. Así, el mensaje 1126 puede cifrarse y/o protegerse la integridad para garantizar que sólo el UE auténtico esté informado sobre la vulnerabilidad detectada, ya que sólo el UE auténtico tendrá las claves necesarias para la integridad y el descifrado.

Entregar los paquetes hacia o desde el UE en cuestión

En otra realización, sólo un nodo del plano de usuario, tal como la UPF, puede estar involucrado en la acción. Ahora se hace referencia a la fig. 12 que muestra una UPF con la SPEF 1216 que está involucrada con el tráfico del plano de usuario. Además, los mensajes pueden reenviarse a través de la SMF 1214, la AMF 1212, y el gNB 1218. Además, el UE 1210 recibe mensajes del plano de control.

En la realización de la fig. 12, la UPF con la SPEF 1216 identifica una anomalía y una causa en el bloque 1220 y, a continuación, puede entregar los paquetes hacia y desde el UE en el bloque 1222.

En una realización, este puede ser el final de la acción.

En otras realizaciones, la UPF puede opcionalmente activar el gNB para entregar los paquetes desde el UE, lo que podría ahorrar el tráfico que llega a los nodos de la red central entre el nodo RAN y la UPF. En este caso, un nodo del plano de control, tal como la AMF 1212 y la SMF 1214 es posible que deba participar en dicha funcionalidad.

En particular, en la realización de la fig. 12, la UPF podrá enviar un mensaje 1230 para entregar paquetes desde el UE, incluyendo un identificador de equipo de usuario y una causa. El mensaje 1230 puede ser enviado a la SMF 1214.

La SMF 1214, a continuación, puede reenviar el contenido del mensaje 1230, mostrado como mensaje 1232, a la AMF 1212.

La AMF 1212, a continuación, puede reenviar el contenido del mensaje 1232, mostrado como mensaje 1234, al gNB 1218.

Al recibir el mensaje 1234, el gNB 1218 puede descartar el tráfico del plano de usuario (UP) desde el UE e/o invocar el procedimiento de liberación de RRC para el UE, como se muestra en el bloque 1240. En el último caso, si se invoca una liberación de RRC, a continuación, la liberación de RRC se envía al UE, como se muestra con la flecha 1242 y el UE puede, a continuación, entrar en un modo INACTIVO, como se muestra en el bloque 1250.

Activar un procedimiento de verificación o de contraverificación de integridad

En una acción adicional, un nodo RAN, tal como el gNB en redes 5G puede iniciar un procedimiento. Sin embargo, un accionador para iniciar el procedimiento puede provenir de cualquier nodo de la red central.

Ahora se hace referencia a la fig. 13. En la realización de la fig. 13, la SPEF puede hacer que el nodo RAN active un procedimiento de contraverificación al detectar una anomalía específica.

En la realización de la fig. 13, el UE 1310 puede comunicarse con un nodo RAN, tal como el gNB 1318. Además, un nodo de la red central, tal como la AMF 1312 y la SMF 1314 puede participar en la comunicación con la UPF y la SPEF 1316.

La UPF con la SPEF 1316 puede identificar una anomalía y una causa, como se muestra en el bloque 1320, y puede, en una realización, entregar los paquetes del plano de usuario hacia y desde el UE como se muestra en el bloque 1322.

Además, en la realización de la fig. 13, la UPF con la SPEF 1316 puede indicar que se ha detectado una anomalía de seguridad, junto con una causa y un identificador de equipo de usuario, y enviarlo como un mensaje 1330 a la SMF 1314.

La SMF 1314 puede reenviar el contenido del mensaje 1330, mostrado como el mensaje 1332, a la AMF 1312.

La AMF 1312, a continuación, puede reenviar el contenido del mensaje 1332 al gNB 1318, como se muestra en el mensaje 1334.

Al recibir el mensaje 1334, el gNB 1318 podrá iniciar un procedimiento de contraverificación. Si la contraverificación falla, la conexión RRC puede liberarse y esto puede indicarse a la AMF 1312 y a una realización. Además, si la contraverificación tiene éxito, el gNB 1318 puede indicar el éxito de la AMF 1312.

El procedimiento de contraverificación inicial se muestra en el bloque 1340 en la realización de la fig. 13.

Basándose en la verificación en el bloque 1340, si la contraverificación falla, se puede iniciar una liberación de RRC como lo muestra la flecha 1342 en la fig. 13.

Al recibir la liberación de RRC, el UE puede entrar a un modo inactivo, mostrado en el bloque 1350.

Activar un procedimiento de autenticación

En otra acción más, al detectar una anomalía, la SPEF puede activar un procedimiento de autenticación para el UE. Ahora se hace referencia a la fig. 14.

En la realización de la fig. 14, la AMF activa un procedimiento de autenticación de NAS. Específicamente, el UE 1410 se comunica con la AMF 1412. Además, la red central incluye la SMF 1414 y los datos del plano de usuario son monitorizados por la UPF con la SPEF 1416.

La UPF con la SPEF 1416 identifica una anomalía y su causa, como se muestra en el bloque 1420, y basándose en la anomalía y su causa detectadas proporciona un mensaje 1422 a la SMF 1414 indicando que se ha detectado una anomalía de seguridad. El mensaje 1422 puede incluir una causa y un identificador del equipo de usuario.

La SMF 1414, a continuación, reenvía el contenido del mensaje 1422 a la AMF 1412, mostrado como el mensaje 1424.

Basándose en el mensaje 1424, la AMF 1412 inicia un procedimiento de autenticación. En particular, un mensaje 1430 de solicitud de autenticación puede ser enviado al UE 1410.

En respuesta, un mensaje 1432 de respuesta de autenticación puede ser proporcionado desde el UE 1410 de vuelta a la AMF 1412.

La AMF 1412 verifica la respuesta en el mensaje 1432 para determinar si la autenticación ha tenido éxito o ha fallado. Además, la ausencia de una respuesta también puede indicar que la autenticación ha fallado. La verificación de autenticación se muestra en el bloque 1440 en la realización de la fig. 14.

Si la autenticación falla, se puede iniciar un procedimiento de DESCONEXIÓN para el UE. A continuación se describe un procedimiento de DESCONEXIÓN ejemplar con respecto a la fig. 17.

Por el contrario, si la autenticación tiene éxito, la sesión continúa y se puede enviar una indicación a la SPEF mediante la SMF 1414.

Así, si la autenticación tiene éxito, el UE se vuelve a autenticar como se muestra en el mensaje 1442 entre la AMF 1412 y la SMF 1414. La SMF 1414, a continuación, reenvía el contenido del mensaje 1442 a la UPF 1416, mostrado como el mensaje 1444.

Activar un procedimiento de restablecimiento de conexión

Una acción adicional que puede ocurrir sería activar un procedimiento de DESCONEXIÓN para el UE al detectar una anomalía. En este caso, un UE genuino puede realizar un nuevo procedimiento de CONEXIÓN, incluyendo la autenticación posterior al procedimiento de DESCONEXIÓN.

Ahora se hace referencia a la fig. 15. En particular, en la realización de la fig. 15, el UE 1510 se comunica con la red utilizando el gNB 1518. La red central incluye la AMF 1512 y la SMF 1514. Además, la UPF con la SPEF 1516 proporciona el tráfico del plano de usuario.

La UPF con la SPEF 1516 identifica una anomalía y una causa en el bloque 1520. La UPF con la SPEF 1516, a continuación, indica que se ha detectado una anomalía de seguridad, incluyendo la causa y un identificador del equipo de usuario, en un mensaje 1530 a la SMF 1514.

La SMF 1514, a continuación, puede reenviar el contenido del mensaje 1530 a la AMF 1512, mostrado como el mensaje 1532.

La AMF 1512, a continuación, puede enviar un mensaje de ACEPTACIÓN de DESCONEXIÓN 1534 al gNB 1518, lo que puede causar una liberación de RRC 1540 con el UE 1510.

Como se ha indicado anteriormente, un UE 1510 genuino, a continuación, podría realizar un procedimiento de CONEXIÓN con la seguridad de autenticación.

Se muestra un procedimiento de DESCONEXIÓN ejemplar con respecto a la fig. 17 a continuación.

Activar el cifrado y/o la protección de integridad

En una acción adicional, la SPEF puede activar el nodo de radio para activar el cifrado y/o la protección de integridad de los datos. Dicho activador puede ser un activador temporal en algunas realizaciones. Ahora se hace referencia a la fig. 16.

El UE 1610 se comunica utilizando el gNB 1618. Además, la red central incluye la AMF 1612 y la SMF 1614. Una UPF con la SPEF 1616 prevé el tráfico del plano de usuario.

En la realización de la fig. 16, la UPF con la SPEF 1616 identifica una anomalía y una causa en el bloque 1620 y proporciona un mensaje 1630 a la SMF 1614 indicando que se ha detectado una anomalía de seguridad. El mensaje 1630 puede incluir una causa y un identificador del equipo de usuario.

La SMF 1614, a continuación, puede reenviar el contenido del mensaje 1630 a la AMF 1612, mostrado como el mensaje 1632.

La AMF 1612, a continuación, puede activar una modificación de sesión para activar el cifrado o la protección de integridad, como se muestra en el mensaje 1634, con el gNB 1618.

Basándose en la recepción del mensaje 1634, el gNB 1618, a continuación, puede causar una reconfiguración de RRC. La reconfiguración 1640 de RRC puede incluir la reconfiguración de la portadora de radio de datos para utilizar cifrado y/o protección de integridad.

Una vez que el UE 1610 recibe la reconfiguración 1640 de RRC, sólo un UE genuino puede tener éxito en activar el cifrado y/o la protección de integridad, ya que esto requiere que el UE esté en posesión de las claves de seguridad adecuadas.

DESCONEXIÓN

En las acciones mostradas respecto a la figs. 14 y 15 anteriores, se hace que el UE se DESCONECTE. Esto se puede lograr de varias maneras.

Se proporciona un ejemplo de desconexión para una red 4G con respecto a la fig. 17. En particular, la realización de la fig. 17 muestra una red 4G que provoca una nueva notificación 1720 de DESCONEXIÓN para ser enviada entre una P-GW 1710 y una MME 1712. Por ejemplo, la notificación 1720 de DESCONEXIÓN puede ser enviada desde la SPEF asociada con la P-GW 1710.

La notificación 1720 de DESCONEXIÓN proporciona una indicación de que el comportamiento del tráfico observado está fuera del rango esperado.

Al recibir la notificación 1720 de DESCONEXIÓN, la MME puede realizar un procedimiento de DESCONEXIÓN como, por ejemplo, se describe en 3GPP TR 23.401 y en particular en la sección 5.8.3.1 de ese TR. Dicho procedimiento de DESCONEXIÓN se muestra en el bloque 1730 en la realización de la fig. 17.

Basándose en el procedimiento de DESCONEXIÓN, la P-GW 1710 recibirá una solicitud de eliminación de sesión y enviará una respuesta de eliminación de sesión para la sesión de PDU de datos de usuario solicitada (no mostrada).

Al finalizar el procedimiento de DESCONEXIÓN en el bloque 1730, la MME 1712 envía un acuse de recibo de DESCONEXIÓN final, que se muestra mediante un mensaje 1740, a la P-GW 1710. En particular, el acuse de recibo de DESCONEXIÓN 1740 puede enviarse a la SPEF asociada con la P-GW 1710.

A continuación en el apéndice E se muestra un ejemplo de cambios a 3GPP TR 23.401 que podrían realizarse para el procedimiento de desconexión anterior.

Para una red 5G, se podría utilizar un procedimiento de desconexión similar.

Por lo tanto, lo anterior proporciona la capacidad de reducir la potencia de procesamiento y aumentar la duración de la batería de potencialmente millones de UE desplegados en aplicaciones de IoT al eliminar la necesidad de ejecutar la integridad y la confidencialidad en la interfaz de radio. Además, se crea una reducción en la transferencia de datos por aire que se necesita para soportar la integridad, lo que resulta en más ancho de banda disponible para que la red soporte a otros clientes.

Las realizaciones ofrecen además protección a la red contra un posible uso indebido de la interfaz de radio contra suplantación de identidad y ataques DoS.

Las realizaciones descritas anteriormente también pueden proporcionar protección para el propietario o usuario de un dispositivo si el dispositivo ha sido robado y/o la suscripción se ha utilizado de manera fraudulenta.

Además, se puede detectar un dispositivo que funciona mal según las realizaciones descritas anteriormente, protegiendo así, a la red y al propietario o usuario del dispositivo.

Los módulos, entidades móviles y equipos de usuario y dispositivos descritos anteriormente pueden ser cualquier dispositivo informático o nodo de red. Dicho dispositivo informático o nodo de red puede incluir cualquier tipo de dispositivo electrónico, incluyendo, entre otros, dispositivos móviles, tales como teléfonos inteligentes o teléfonos celulares. Los ejemplos pueden incluir además equipos de usuario fijos o móviles, tales como dispositivos de Internet de las cosas (IoT), terminales, dispositivos de automatización del hogar, equipos médicos en entornos hospitalarios o domésticos, dispositivos de seguimiento de inventario, dispositivos de monitorización ambiental, dispositivos de gestión de energía, dispositivos de gestión de infraestructura, vehículos o dispositivos para vehículos, dispositivos electrónicos fijos, entre otros. Los vehículos incluyen vehículos a motor (por ejemplo, automóviles, coches, camiones, autobuses, motocicletas, etc.), aeronaves (por ejemplo, aviones, vehículos

aéreos no tripulados, sistemas de aeronaves no tripuladas, drones, helicópteros, etc.), naves espaciales (por ejemplo, aviones espaciales, lanzaderas, cápsulas espaciales, estaciones espaciales, satélites, etc.), embarcaciones (por ejemplo, barcos, botes, aerodeslizadores, submarinos, etc.), vehículos sobre raíles (por ejemplo, trenes y tranvías, etc.) y otros tipos de vehículos, incluyendo cualesquiera combinaciones de cualquiera de los anteriores, ya sean existentes actualmente o después de surgir.

Se muestra un diagrama simplificado de un dispositivo informático con respecto a la fig. 18. El dispositivo informático de la fig. 18 podría ser cualquier UE, entidad móvil (ME), nodo de red tal como UPF, SPEF u otro nodo como se ha descrito anteriormente.

En la fig. 18, el dispositivo 1810 incluye un procesador 1820 y un subsistema 1830 de comunicaciones, donde el procesador 1820 y el subsistema 1830 de comunicaciones cooperan para realizar los métodos de las realizaciones descritas anteriormente. El subsistema 1820 de comunicaciones puede, en algunas realizaciones, comprender múltiples subsistemas, por ejemplo para diferentes tecnologías de radio.

El procesador 1820 está configurado para ejecutar lógica programable, que puede almacenarse, junto con los datos, en el dispositivo 1810, y se muestra en el ejemplo de la fig. 18 como la memoria 1840. La memoria 1840 puede ser cualquier medio de almacenamiento tangible, no transitorio, legible por ordenador. El medio de almacenamiento legible por ordenador puede ser un medio tangible o transitorio/no transitorio tal como óptico (por ejemplo, CD, DVD, etc.), magnético (por ejemplo, cinta), una unidad flash, un disco duro u otra memoria conocida en la técnica.

Alternativamente, o además de la memoria 1840, el dispositivo 1810 puede acceder a datos o lógica programable desde un medio de almacenamiento externo, por ejemplo a través del subsistema 1830 de comunicaciones.

El subsistema 1830 de comunicaciones permite al dispositivo 1810 comunicarse con otros dispositivos o elementos de red y puede variar basándose en el tipo de comunicación que se realiza. Además, el subsistema 1830 de comunicaciones puede comprender una pluralidad de tecnologías de comunicaciones, incluyendo cualquier tecnología de comunicaciones por cable o inalámbricas.

Las comunicaciones entre los distintos elementos del dispositivo 1810 puede ser a través de un bus 1860 interno en una realización. Sin embargo, son posibles otras formas de comunicación.

Además, si la estación informática es un equipo de usuario, a continuación se describe un equipo de usuario ejemplar con respecto a la fig. 19.

El equipo de usuario 1900 puede comprender un dispositivo de comunicación inalámbrica bidireccional que tiene capacidades de comunicación de voz o datos, o ambas. El equipo de usuario 1900 generalmente tiene la capacidad de comunicarse con otros sistemas informáticos. Dependiendo de la funcionalidad exacta proporcionada, el equipo de usuario puede denominarse dispositivo de mensajería de datos, un buscapersonas bidireccional, un dispositivo de correo electrónico inalámbrico, un teléfono inteligente, un teléfono celular con capacidad de mensajería de datos, un dispositivo de Internet inalámbrico, un dispositivo inalámbrico, un dispositivo móvil, una entidad móvil, un módem celular integrado o un dispositivo de comunicación de datos, como ejemplos.

Donde el equipo de usuario 1900 está habilitado para comunicación bidireccional, puede incorporar un subsistema 1911 de comunicación, incluyendo un receptor 1912 y un transmisor 1914, así como componentes asociados, tales como uno o más elementos 1916 y 1918 de antena, osciladores locales (LO) 1913 y un módulo de procesamiento, tal como un procesador 1920 de señales digitales (DSP). Como resultará evidente para los expertos en el campo de las comunicaciones, el diseño particular del subsistema 1911 de comunicación dependerá de la red de comunicación en la que se pretende que funcione el equipo de usuario.

Los requisitos de acceso a la red también variarán dependiendo del tipo de red 1919. En algunas redes, el acceso a la red está asociado con un abonado o usuario del equipo de usuario 1900. Un equipo de usuario puede estar provisto de un módulo de identidad de usuario (RUIM) incorporado o extraíble o una tarjeta de módulo de identidad de abonado (SIM) o una SIM UMTS (USIM) con el fin de operar en una red. La interfaz 1944 USIM/SIM/RUIM normalmente es similar a una ranura para tarjetas en la que se puede insertar y expulsar una tarjeta USIM/SIM/RUIM. La tarjeta USIM/SIM/RUIM puede tener memoria y contener muchas configuraciones clave 1951, y otra información 1953, tal como identificación e información relacionada con el abonado. En otros casos, en lugar de una red 1919, el equipo de usuario 1900 puede comunicarse con un nodo sin acceso, tal como un vehículo, una infraestructura de carretera, otro equipo de usuario u otra comunicación entre pares.

Cuando se hayan completado los procedimientos requeridos de registro o activación de red, el equipo de usuario 1900 puede enviar y recibir señales de comunicación a través de la red 1919. Como se ilustra en la fig. 19, la red 1919 puede incluir múltiples estaciones base que se comunican con el equipo de usuario.

Las señales recibidas por la antena 1916 a través de la red 1919 de comunicación son entradas al receptor 1912, que puede realizar funciones de receptor tan comunes como amplificación de señal, conversión descendente de frecuencia, filtrado, selección de canal y similares. La conversión analógica a digital (A/D) de una señal recibida permite realizar funciones de comunicación más complejas, tales como la demodulación y la decodificación, en el DSP 1920. De manera similar, las señales a transmitir se procesan, incluyendo modulación y codificación, por ejemplo, mediante DSP 1920 y entrada al transmisor 1914 para conversión de digital a analógico (D/A), conversión ascendente de frecuencia, filtrado, amplificación y transmisión a través de la red 1919 de comunicación mediante la antena 1918. El DSP 1920 no sólo procesa señales de comunicación, sino que también proporciona control del receptor y del transmisor. Por ejemplo, las ganancias aplicadas a las señales de comunicación en el receptor 1912 y transmisor 1914 pueden controlarse de forma adaptativa a través de algoritmos de control automático de ganancia implementados en DSP 1920.

El equipo de usuario 1900 generalmente incluye un procesador 1938 que controla el funcionamiento general del dispositivo. Las funciones de comunicación, incluyendo las comunicaciones de datos y voz, se realizan a través del subsistema 1911 de comunicación. El procesador 1938 también interactúa con otros subsistemas del dispositivo, tales como el dispositivo 1922 de presentación, la memoria 1924 flash, La memoria 1926 de acceso aleatorio (RAM), subsistemas 1928 auxiliares de entrada/salida (E/S), el puerto 1930 serie, uno o más teclados o teclados numéricos 1932, el altavoz 1934, el micrófono 1936, otro subsistema 1940 de comunicación, tal como un subsistema de comunicaciones de corto alcance o un subsistema DSRC, y cualquier otro subsistema de dispositivo generalmente indicado como 1942. El puerto 1930 serie podría incluir un puerto USB, un puerto de diagnóstico a bordo (OBD) u otro puerto conocido por los expertos en la técnica.

Algunos de los subsistemas mostrados en la fig. 19 realiza funciones relacionadas con la comunicación, mientras que otros subsistemas pueden proporcionar funciones "residentes" o en el dispositivo. En particular, algunos subsistemas, tales como el teclado 1932 y el dispositivo 1922 de presentación, por ejemplo, se pueden utilizar tanto para funciones relacionadas con la comunicación, como para introducir un mensaje de texto para su transmisión a través de una red de comunicación, y funciones residentes en el dispositivo, tales como una calculadora o una lista de tareas.

El software del sistema operativo utilizado por el procesador 1938 puede almacenarse en un almacén persistente, tal como una memoria 1924 flash, que puede ser en cambio una memoria de sólo lectura (ROM) o un elemento de almacenamiento similar (no mostrado). Los expertos en la técnica apreciarán que el sistema operativo, las aplicaciones específicas del dispositivo o partes de los mismos se pueden cargar temporalmente en una memoria volátil, tal como la RAM 1926. Las señales de comunicación recibidas también pueden almacenarse en la RAM 1926.

Como se muestra, la memoria 1924 flash se puede segregar en diferentes áreas tanto para programas 1958 informáticos como para almacenamiento 1950, 1952, 1954 y 1956 de datos de programa. Estos diferentes tipos de almacenamiento indican que cada programa puede asignar una parte de la memoria 1924 flash para sus propios requisitos de almacenamiento de datos. El procesador 1938, además de las funciones de su sistema operativo, puede habilitar la ejecución de aplicaciones de software en el equipo de usuario. Normalmente se instalará en el equipo de usuario 1900 un conjunto predeterminado de aplicaciones que controlan las operaciones básicas, incluyendo potencialmente aplicaciones de comunicación de voz y datos, por ejemplo, durante la fabricación. Otras aplicaciones podrían instalarse posteriormente o de forma dinámica.

Las aplicaciones y el software pueden almacenarse en cualquier medio de almacenamiento legible por ordenador. El medio de almacenamiento legible por ordenador puede ser un medio tangible o transitorio/no transitorio tal como óptico (por ejemplo, CD, DVD, etc.), magnético (por ejemplo, cinta) u otra memoria conocida en la técnica.

Una aplicación de software puede ser una aplicación de administrador de información personal (PIM) que tiene la capacidad de organizar y gestionar elementos de datos relacionados con el usuario del equipo de usuario tales como, entre otros, correo electrónico, mensajes, eventos de calendario, correos de voz, citas y elementos de tareas. También se pueden cargar en el equipo de usuario 1900 otras aplicaciones, incluyendo aplicaciones de productividad, aplicaciones de redes sociales, juegos, entre otros, a través de la red 1919, un subsistema 1928 de E/S auxiliar, un puerto 1930 serie, un subsistema 1940 de comunicaciones de corto alcance o cualquier otro subsistema 1942 adecuado, e instalado por un usuario en la RAM 1926 o un almacén no volátil (no mostrado) para su ejecución por el procesador 1938. Tal flexibilidad en la instalación de aplicaciones aumenta la funcionalidad del dispositivo y puede proporcionar funciones mejoradas en el dispositivo, funciones relacionadas con la comunicación o ambas.

En un modo de comunicación de datos, el subsistema 1911 de comunicación procesará una señal recibida, tal como un mensaje de texto o la descarga de una página web y la entrada al procesador 1938, que puede procesar aún más la señal recibida para enviarla al dispositivo 1922 de presentación, o alternativamente a un dispositivo 1928 de E/S auxiliar.

Un usuario de equipo de usuario 1900 también puede redactar elementos de datos, tales como mensajes, por ejemplo, utilizando el teclado 1932, que puede ser un teclado alfanumérico completo o un teclado tipo teléfono, ya sea físico o virtual, entre otros, en combinación con el dispositivo 1922 de presentación y posiblemente un dispositivo 1928 de E/S auxiliar. Dichos elementos compuestos pueden, a continuación, transmitirse a través de una red de comunicación a través del subsistema 1911 de comunicación.

Cuando se proporcionen comunicaciones de voz, el funcionamiento general del equipo de usuario 1900 es similar, excepto que las señales recibidas normalmente pueden enviarse a un altavoz 1934 y las señales para la transmisión pueden ser generadas por un micrófono 1936. También se pueden implementar subsistemas de E/S de voz o audio alternativos, tales como un subsistema de grabación de mensajes de voz, en el equipo de usuario 1900. Aunque la salida de la señal de voz o audio preferiblemente se logra principalmente a través del altavoz 1934, el dispositivo 1922 de presentación también se puede utilizar para proporcionar una indicación de la identidad de la persona que llama, la duración de una llamada de voz u otra información relacionada con la llamada de voz, por ejemplo.

El puerto 1930 serie en la fig. 19 puede implementarse en un equipo de usuario para el cual puede ser deseable la sincronización con el ordenador de escritorio de un usuario (no mostrada), pero es un componente de dispositivo opcional. Tal puerto 1930 puede habilitar a un usuario para establecer preferencias a través de un dispositivo externo o una aplicación de software y puede ampliar las capacidades del equipo de usuario 1900 proporcionando información o descargas de software al equipo de usuario 1900 que no sea a través de una red de comunicación inalámbrica. Como apreciarán los expertos en la técnica, el puerto 1930 serie además se puede utilizar para conectar el equipo de usuario a un ordenador para que actúe como módem o para cargar una batería en el equipo de usuario.

Otros subsistemas 1940 de comunicaciones, tal como un subsistema de comunicaciones de corto alcance, es un componente adicional que puede proporcionar comunicación entre los equipos del usuario 1900 y diferentes sistemas o dispositivos, que no necesariamente tienen que ser dispositivos similares. Por ejemplo, el subsistema 1940 puede incluir un dispositivo de infrarrojos y circuitos y componentes asociados o un módulo de comunicación Bluetooth™ o Bluetooth™ de bajo consumo de energía para proporcionar comunicación con sistemas y dispositivos habilitados de manera similar. El subsistema 1940 puede incluir además comunicaciones no celulares, tales como Wi-Fi o WiMAX, o comunicaciones de campo cercano, y según las realizaciones anteriores dicha radio puede poder dividirse en algunas circunstancias.

Las realizaciones descritas en la presente memoria son ejemplos de estructuras, sistemas o métodos que tienen elementos correspondientes a elementos de las técnicas de esta aplicación. Esta descripción escrita puede habilitar a los expertos en la técnica para realizar y utilizar realizaciones que tengan elementos alternativos que también correspondan a los elementos de las técnicas de esta aplicación. El alcance previsto de las técnicas de esta aplicación incluye así, otras estructuras, sistemas o métodos que no difieren de las técnicas de esta aplicación como se describen en la presente memoria, e incluye además otras estructuras, sistemas o métodos con diferencias insustanciales de las técnicas de esta aplicación como se ha descrito en la presente memoria.

Si bien las operaciones se representan en los dibujos en un orden particular, esto no debería comprenderse como que requiere que dichas operaciones se realicen en el orden particular que se muestra o en orden secuencial, o que se realicen todas las operaciones ilustradas, para lograr resultados deseables. En determinadas circunstancias, se puede emplear multitarea y procesamiento paralelo. Además, no debería comprenderse que la separación de varios componentes del sistema en la implementación descrita anteriormente requiere dicha separación en todas las implementaciones, y debería comprenderse que los componentes y sistemas del programa descritos generalmente pueden integrarse juntos en un producto de software de señal o empaquetarse en múltiples productos de software.

También, las técnicas, sistemas, subsistemas y métodos descritos e ilustrados en las diversas implementaciones como discretos o separados pueden combinarse o integrarse con otros sistemas, módulos, técnicas o métodos. Otros elementos mostrados o dados a conocer como acoplados o directamente acoplados o comunicándose entre sí pueden estar indirectamente acoplados o comunicándose a través de alguna interfaz, dispositivo o componente intermedio, ya sea eléctrica, mecánicamente o de otro modo. Un experto en la técnica puede determinar y realizar otros ejemplos de cambios, sustituciones y alteraciones.

Si bien la descripción detallada anterior ha mostrado, descrito y señalado las características novedosas fundamentales de la descripción, aplicadas a diversas implementaciones, se comprenderá que se pueden realizar diversas omisiones, sustituciones y cambios en la forma y detalles del sistema ilustrado por los expertos en la técnica. Además, el orden de las etapas del método no está implícito en el orden en que aparecen en las reivindicaciones.

Cuando los mensajes se envían hacia/desde un dispositivo electrónico, dichas operaciones pueden no ser inmediatas o directamente desde el servidor. Pueden entregarse de forma síncrona o asíncrona desde un servidor u otra infraestructura de sistema informático que soporta los dispositivos/métodos/sistemas descritos en la presente memoria. Las etapas anteriores pueden incluir, total o parcialmente, comunicaciones

síncronas/asíncronas hacia/desde el dispositivo/infraestructura. Además, la comunicación desde el dispositivo electrónico puede ser hacia uno o más terminales en una red. Estos terminales pueden ser atendidos por un servidor, un sistema informático distribuido, un procesador de flujo, etc. Las redes de entrega de contenido (CDN) también pueden proporcionar comunicación a un dispositivo electrónico. Por ejemplo, en lugar de una respuesta típica del servidor, el servidor también puede proporcionar o indicar datos para la red de entrega de contenido (CDN) para esperar la descarga por parte del dispositivo electrónico en un momento posterior, tal como una actividad posterior del dispositivo electrónico. Así, los datos pueden enviarse directamente desde el servidor u otra infraestructura, tal como una infraestructura distribuida o una CDN, como parte del sistema o separada del mismo.

Normalmente, los medios de almacenamiento pueden incluir cualquiera o alguna combinación de los siguientes: un dispositivo de memoria semiconductor tal como una memoria de acceso aleatorio dinámica o estática (una DRAM o SRAM), una memoria de sólo lectura borrable y programable (EPROM), una memoria de solo lectura borrable y programable eléctricamente (EEPROM) y una memoria flash; un disco magnético tal como un disco fijo, flexible y extraíble; otro medio magnético que incluye una cinta; un medio óptico tal como un disco compacto (CD) o un disco de vídeo digital (DVD); u otro tipo de dispositivo de almacenamiento. Obsérvese que las instrucciones dadas a conocer anteriormente se pueden proporcionar en un medio de almacenamiento legible por ordenador o por máquina, o alternativamente, se pueden proporcionar en múltiples medios de almacenamiento legibles por ordenador o por máquina distribuidos en un sistema grande que tiene posiblemente una pluralidad de nodos. Dicho medio o medios de almacenamiento legibles por ordenador o por máquina se consideran parte de un artículo (o artículo de fabricación). Un artículo o artículo de fabricación puede referirse a cualquier componente único o múltiples componentes fabricados. El medio o medios de almacenamiento pueden ubicarse en la máquina que ejecuta las instrucciones legibles por máquina o ubicarse en un sitio remoto desde el cual se pueden descargar instrucciones legibles por máquina a través de una red para su ejecución.

En la descripción anterior, se exponen numerosos detalles para proporcionar una comprensión del tema descrito en la presente memoria. Sin embargo, las implementaciones pueden practicarse sin algunos de estos detalles. Otras implementaciones pueden incluir modificaciones y variaciones de los detalles dados a conocer anteriormente. Se pretende que las reivindicaciones adjuntas cubran dichas modificaciones y variaciones.

APÉNDICE A - Extracto de 33.401

5.1.3 Confidencialidad de los datos de usuario y de los datos de señalización

5.1.3.1 Requisitos de cifrado

Se puede proporcionar cifrado a la señalización RRC para impedir el seguimiento del UE basándose en informes de medición a nivel de celda, asignación de mensajes de traspaso o encadenamiento de identidad a nivel de celda. La confidencialidad de la señalización RRC es una opción del operador.

Todos los mensajes S1 y X2 transportados entre RN y DeNB estarán protegidos por la confidencialidad.

NOTA 0: El cifrado está sujeto a regulación nacional.

Se garantizará la sincronización de los parámetros de entrada para el cifrado para los protocolos implicados en el cifrado.

La señalización NAS puede estar protegida de forma confidencial. La confidencialidad de la señalización NAS es una opción del operador.

NOTA 1: Se recomienda utilizar la protección de confidencialidad de la señalización RRC y NAS.

Cuando no se puede realizar con éxito la autenticación de las credenciales en la UICC durante una llamada de emergencia en el modo de servicio limitado, como se define en TS 23.401 [2], se omitirá la protección de confidencialidad de la señalización RRC y NAS y del plano de usuario (véase cláusula 15). Esto lo logrará la red seleccionando EEA0 para la protección de confidencialidad de NAS, RRC y del plano de usuario.

La protección de confidencialidad del plano de usuario sobre el estrato de acceso se realizará en la capa PDCP y es una opción del operador.

NOTA 2: Se recomienda utilizar la protección de confidencialidad del plano del usuario.

NOTA 3: La protección de confidencialidad para RRC y UP se aplica en la capa PDCP y ninguna capa por debajo de PDCP está protegida por la confidencialidad. La protección de confidencialidad para NAS la proporciona el protocolo NAS.

Los datos del usuario enviados mediante MME pueden estar protegidos de forma confidencial

NOTA 4: Se recomienda utilizar la protección de confidencialidad de los datos del usuario enviados mediante MME.

5.1.4 Integridad de los datos de usuario y de los datos de señalización

5.1.4.1 Requisitos de integridad

Se garantizará la sincronización de los parámetros de entrada para la protección de integridad para los protocolos implicados en la protección de integridad.

Se proporcionará protección de integridad y protección de reproducción a la señalización NAS y RRC.

Todos los mensajes de señalización NAS, excepto aquellos enumerados explícitamente en TS 24.301 [9] como excepciones, estarán protegidos por su integridad. Todos los mensajes de señalización RRC, excepto aquellos enumerados explícitamente en TS 36.331 [21] como excepciones, estarán protegidos por su integridad.

Cuando la autenticación de las credenciales en la UICC durante una llamada de emergencia en modo de servicio limitado, como se define en TS 23.401 [2], no se puede realizar con éxito, se omitirá la integridad y la protección de reproducción de la señalización RRC y NAS (véase cláusula 15). Esto lo logrará la red seleccionando EIA0 para la protección de integridad de NAS y RRC. EIA0 sólo se utilizará para llamadas de emergencia no autenticadas.

Los paquetes del plano de usuario entre el eNB y el UE no estarán protegidos por su integridad en la interfaz Uu. Los paquetes del plano de usuario entre la RN y el UE no estarán protegidos por su integridad. Todos los paquetes del plano de usuario que transporten mensajes S1 y X2 entre RN y DeNB estarán protegidos por su integridad. Puede soportarse la protección de integridad para todos los demás paquetes del plano de usuario entre RN y DeNB.

Todos los paquetes de datos de usuario enviados mediante la MME estarán protegidos por su integridad.

7.3 Mecanismos de seguridad del UP (PLANO DE USUARIO)

7.3.1 Mecanismos de confidencialidad del UP (PLANO DE USUARIO)

Los datos del plano de usuario se cifran mediante el protocolo PDCP entre el UE y el eNB como se especifica en TS 36.323 [12].

El uso y modo de funcionamiento de los algoritmos 128-EEA se especifican en el anexo B. Los parámetros de entrada a los algoritmos EEA de 128 bits descritos en el anexo B son una clave de cifrado K_{UPenc} de 128 bits como CLAVE, una identidad de portadora PORTADORA de 5 bits cuyo valor se asigna según lo especificado en TS 36.323 [12], la dirección de transmisión DIRECCIÓN de 1 bit, la longitud LONGITUD del flujo de claves requerida y un RECUENTO de entrada de 32 bits dependiente del tiempo y de la dirección, específico de la portadora que corresponde al RECUENTO de PDCP de 32 bits.

7.3.2 Mecanismos de integridad del UP (PLANO DE USUARIO)

Esta subcláusula se aplica únicamente al plano de usuario en la interfaz Un entre RN y DeNB:

Los datos del plano de usuario están protegidos por su integridad mediante el protocolo PDCP entre el RN y el DeNB como se especifica en TS 36.323 [12]. La protección de reproducción se activará cuando se active la protección de integridad. La protección de reproducción garantizará que el receptor sólo acepte cada valor entrante de CONTADOR PDCP particular una vez utilizando el mismo contexto de seguridad AS.

El uso y modo de funcionamiento de los algoritmos 128-EIA se especifican en el anexo B. Los parámetros de entrada a los algoritmos EIA de 128 bits, tal como se describen en el anexo B, son una clave de integridad K_{UPInt} de 128 bits como CLAVE, una identidad de portadora de PORTADORA de 5 bits cuyo valor se asigna según lo especificado en TS 36.323 [12], la dirección de transmisión DIRECCIÓN de 1 bit, y un RECUENTO de entrada de 32 bits, dependiente del tiempo y de la dirección, específico de la portadora que corresponde al RECUENTO PDCP de 32 bits.

La supervisión de las verificaciones de integridad del UP fallidas se realizará tanto en la RN como en el DeNB. En caso de que se detecte una verificación de integridad fallida (es decir, MAC-I defectuosa o faltante) después del inicio de la protección de integridad, se descartará el mensaje en cuestión. Esto puede suceder en el lado de DeNB o en el lado de RN.

NOTA: El manejo de fallos de verificación de integridad del UP por parte de una RN es un problema de implementación. TS 36.323 [12] intencionadamente no exige ninguna acción en caso de una verificación de integridad fallida (ni siquiera envía una indicación de fallo a capas superiores). Por consiguiente, dependiendo de

la implementación, el mensaje de que falla en la verificación de integridad se descarta silenciosamente o no. Esto contrasta con el manejo de una verificación de integridad RRC fallida por parte de un UE, cf. la NOTA de la cláusula 7.4. 1 del presente documento.

APÉNDICE B - Extracto de 33.401 Sección 6 Autenticación

6.1 Autenticación y acuerdo de claves.

6.1.1 Procedimiento AKA

NOTA 1: Los datos de autenticación en esta subcláusula representan un vector o vectores de autenticación EPS.

AKA EPS es el procedimiento de autenticación y acuerdo de claves que se utilizará en E-UTRAN.

Una aplicación USIM Ver-99 o posterior en una UICC será suficiente para acceder a E-UTRAN, siempre que la aplicación USIM no haga uso del bit de separación de la AMF de la manera descrita en TS 33.102 [4] anexo F. No se concederá el acceso a E-UTRAN con una SIM 2G o una aplicación SIM en una UICC.

Un ME que tenga capacidad de radio E-UTRAN deberá soportar la interfaz USIM-ME como se especifica en TS 31.102

El AKA EPS producirá material de claves que sirva de base para las claves de cifrado del plano de usuario (UP), RRC y NAS, así como para las claves de protección de integridad de RRC y NAS.

NOTA 2: Los requisitos de derivación de claves de AS y NAS se pueden encontrar en la subcláusula 7.2.1.

La MME envía a la USIM mediante ME el desafío aleatorio RAND y un token de autenticación AUTN para la autenticación de red desde el vector de autenticación seleccionado. También incluye una KSI_{ASME} para el ME que se utilizará para identificar la K_{ASME} (y otras claves derivadas de la K_{ASME}) que resulta del procedimiento AKA EPS.

Al recibir este mensaje, la USIM verificará la actualidad del vector de autenticación verificando si AUTN puede aceptarse como se describe en TS 33.102. Si es así, la USIM calcula una respuesta RES. USIM calculará CK e IK que se envían al ME. Si la USIM calcula una Kc (es decir, Kc GPRS) a partir de CK e IK utilizando la función de conversión c3 como se describe en TS 33.102, y lo envía al ME, a continuación, el ME ignorará dicho Kc GPRS y no almacenará la Kc GPRS en la USIM o en ME. Si la verificación falla, la USIM indica al ME el motivo del fallo y en el caso de un fallo de sincronización pasa el parámetro AUTS (véase TS 33.102).

Un ME que acceda a E-UTRAN deberá verificar durante la autenticación que el "bit de separación" en el campo AMF de AUTN esté establecido en 1. El "bit de separación" es el bit 0 del campo AMF de AUTN.

NOTA 3: Este bit de separación en la AMF ya no se puede utilizar para fines específicos del operador como se describe en TS 33.102, anexo F.

NOTA 4: Si las claves CK, IK resultantes de una ejecución de AKA EPS se han almacenado en los campos ya disponibles en la USIM para almacenar las claves CK e IK, esto podría provocar que se sobrescriban las claves resultantes de una ejecución anterior de AKA UMTS. Esto conduciría a problemas cuando el contexto de seguridad EPS y el contexto de seguridad UMTS se mantuvieran simultáneamente (como es el caso cuando el contexto de seguridad se almacena, por ejemplo, para fines de reducción de señalización en modo inactivo). Por lo tanto, la "itinerancia plástica" en la que se inserta una UICC en otro ME requerirá una ejecución de autenticación AKA EPS si la USIM no soporta el almacenamiento de parámetros EMM.

El UE responderá con un mensaje de respuesta de autenticación de usuario que incluya RES en caso de verificación AUTN con éxito y verificación AMF con éxito como se ha descrito anteriormente. En este caso el ME calculará K_{ASME} desde CK, IK y la identidad de la red de servicio (ID SN) utilizando la KDF como se especifica en la cláusula A.2. El enlace de ID SN autentica implícitamente la identidad de la red de servicio cuando las claves derivadas de K_{ASME} se utilizan con éxito.

NOTA 5: Esto no impide que una USIM (véase TS 31.102) en versiones posteriores tenga la capacidad de derivar K_{ASME}.

De lo contrario, el UE enviará un mensaje de error de autenticación con un valor CAUSA que indique el motivo del error. En caso de un error de sincronización de AUTN (como se describe en TS 33.102), el UE también incluye AUTS proporcionado por la USIM. Al recibir un mensaje de error de autenticación, la MME puede iniciar solicitudes de identidad y autenticaciones adicionales hacia el UE. (véase TS 24.301).

La MME verifica que RES sea igual a XRES. Si es así, la autenticación tiene éxito. De lo contrario, dependiendo del tipo de identidad utilizada por el UE en el mensaje NAS inicial, la MME puede iniciar solicitudes de identidad adicionales o enviar un mensaje de rechazo de autenticación al UE (véase TS 24.301 [9]).

La fig. 6.1.1-1 describe el procedimiento AKA EPS, que se basa en AKA UMTS (véase TS 33.102[4]). Las siguientes claves se comparten entre UE y HSS:

K es la clave permanente almacenada en la USIM en una UICC y en el Centro de autenticación AuC.

CK, IK es el par de claves derivadas en AuC y en USIM durante una ejecución de AKA. CK, IK se manejarán de manera diferente dependiendo de si se utilizan en un contexto de seguridad EPS o en un contexto de seguridad heredado, como se describe en la subcláusula 6.1.2.

Como resultado de la autenticación y el acuerdo de claves, se crea una clave intermedia K_{ASME} que se compartirá entre UE y MME, es decir, la ASME para EPS.

APÉNDICE C - Cambios a TR 33.866

En el área de seguridad nº 1 aspectos arquitectónicos de la seguridad de próxima generación, añadir

**** PRIMER CAMBIO ****

[Todo el texto a continuación es nuevo, es posible que sea necesario corregir la numeración de las secciones]

5.1.3.22 Problema de clave #1.22: Función de cumplimiento de políticas de seguridad de sesión del UP

5.1.3.22.1 Detalles del problema de clave

Los UE que seleccionan establecer una sesión de datos que no utiliza la integridad o confidencialidad del UP pueden proporcionar un medio para que un atacante utilice la sesión para atacar la red en la RAN o en capas superiores.

5.1.3.22.2 Amenazas de seguridad

Un atacante podría secuestrar una sesión de datos sin protección de integridad o confidencialidad. Nos interesan principalmente las amenazas a la red, ya que si el UE ha seleccionado una sesión de datos sin integridad o confidencialidad se supone que ha aceptado riesgos, tales como las escuchas ilegales. Las amenazas a la red son el interés en este problema de clave; una sesión de datos desprotegida podría permitirle a un atacante;

- Inundar la red con datos no autorizados (un ataque DoS), donde la inundación de datos iría más allá del eNB hasta la UPF, ya que no hay protección en la capa PDCP.
- Suplantar al UE y enviar datos maliciosos o corruptos al receptor.
- Secuestrar la conexión de la sesión para sus propios fines.

5.1.3.22.3 Posibles requisitos de seguridad

El requisito de seguridad es proteger la red en una capa más allá de la RAN o por encima de la capa PDCP, pero tampoco reducir los beneficios para la aplicación/UE que se pueden obtener mediante una sesión del UP que no invoca integridad y confidencialidad.

Un requisito para proteger la red de una manera que sea pasiva para el usuario de la conexión de datos del UP, pero que garantice que la red pueda estar al tanto de un mal uso de su servicio.

**** Segundo CAMBIO ****

[Todo el texto a continuación es nuevo, es posible que sea necesario corregir la numeración de las secciones]

5.1.4.40 Solución #1.40: Función de aplicación de políticas de seguridad de sesión de UP

5.1.4.40.1 Introducción

Esta solución propone una función de aplicación de políticas de seguridad (SPEF) de sesión UP en la UPF y es una solución para el problema de clave nº 22 en 5.1.3.22

5.1.4.40.2 Detalles de la solución

El operador de red utiliza un conjunto de parámetros asociados con las características del tráfico del UE para proporcionar a la UPF los parámetros que necesita para garantizar que el UE se comporte dentro de los límites

de las características esperadas. Estos valores se pueden configurar manualmente en PCF o SPCF (o la información de suscripción de UE en HSS en LTE). Estos valores pueden ser, entre otros:

Nombre	Descripción
SPE_LOC	Ubicación del UE: coordenadas GPS que incluyen comportamiento de ubicación/movimiento/velocidad u otra información sobre la ubicación física del UE (ID de celda). Estos pueden ser conocidos a priori para muchos UE, tales como UE estacionarios (por ejemplo, medidores inteligentes).
SPE_VOLUME	Volumen de carga útil de datos estimado. Esto puede especificarse en los parámetros de suscripción (por ejemplo, disponible en el HSS)
SPE_TOD	Hora prevista del día/día de la semana/día del mes, etc., para la configuración de la conexión
SPE_CONNS	Número esperado de conexiones de datos simultáneas (TCP/IP) desde el UE
SPE_DUR	Duración prevista de la conexión
SPE_FREQ	Frecuencia estimada de transmisión de datos (una vez por hora/minuto/segundo, o continua)
SPE_DATATYPE	Tipo de datos; texto, numérico, transmisión de video, transmisión de audio, gráficos (.jpg, .gif, .pdf), carga útil cifrada (donde el cifrado se realiza en una capa por encima de la capa de radio, es decir, la capa de aplicación)
SPE_IPADDR	Dirección de destino normal (dirección IP, URI o nombre de dominio o subdominio)
SPE_BYTES	Intercambio de recuentos de bytes transmitidos y recibidos entre el UE y la red a través de una conexión específica. Véase la sección técnica anterior a continuación.
SPE_CAPABILITY	Uso de suscripción permitido. Por ejemplo, solamente datos (no se permite tráfico de SMS, multimedia ni voz (VoIP)).

Tabla 1: Parámetros de la función de cumplimiento de políticas de seguridad

Estos valores son utilizados por la SPEF en la UPF para monitorizar el tráfico a través de una sesión de PDU específica desde un UE específico. Si las características del tráfico observadas caen fuera del rango de valores aceptables, la SPEF y señalan la AMF para terminar la conexión o restablecer la conexión utilizando protección de integridad y/o confidencialidad.

Esta solución se basa en la arquitectura 5G donde la seguridad del UP termina en la UPF.

Desde 23.501 v0.3.0, la fig. 4.2.3-2: Arquitectura del sistema 5G sin itinerancia en representación del punto de referencia

Un NG-UE solicita el establecimiento de sesión de PDU para una DN (red de datos) utilizando un mensaje NAS. Cuando la AMF recibe el establecimiento de sesión de PDU del NG-UE, la AMF determina una SMF basándose en el DNN (nombre de red de datos) y reenvía el establecimiento de sesión a la SMF junto con la identidad del NG-UE y el DNN. La SMF interactúa con la PCF para obtener los requisitos para la sesión de PDU.

La SMF obtiene una clave (es decir, K_{UPF}) para la seguridad de UPF por parte de la SEAF y proporciona la clave (K_{UPF}) a la UPF como parte de la configuración de sesión de PDU en la UPF de manera que la UPF pueda aplicar la seguridad de la UPF para el NG-UE. Incluido en esta configuración de sesión de PDU en la UPF son los parámetros para monitorizar las características de tráfico del NG-UE. La SMF también proporciona la información de sesión y los parámetros de derivación de claves al NG-UE de manera que el NG-UE derive la misma clave que la UPF e inicie la protección de seguridad de la UPF. En el caso de una sesión de PDU sin integridad ni confidencialidad la clave proporcionada a la UPF (K_{UPF}) sería nula.

5.1.4.40.2.1 Procedimiento

10. Solicitud de configuración de sesión de PDU (identidad, DNN, K_{UPF})

Fig. 5.1.4.x.2.1.3-1. Establecimiento de sesión de PDU para terminación de seguridad del UP en la UPF (VER FIG. 5)

1. El NG-UE se conecta a la red.

2. El NG-UE envía una solicitud de establecimiento de sesión de PDU a la AMF con DNN.

NOTA: Se supone que la capacidad de seguridad del UE (incluyendo la capacidad de seguridad del UP) se almacena en la AMF durante la conexión. Alternativamente, el NG-UE puede proporcionar su capacidad de seguridad del UP en esta etapa.

3. La AMF determina una SMF basándose en el DNN proporcionado por el NG-UE.

4. La AMF reenvía la solicitud de establecimiento de sesión de PDU a la SMF con la identidad del UE, el DNN y la capacidad de seguridad.

5. La SMF interactúa con la PCF para recuperar el perfil de suscripción del UE relacionado con la sesión de PDU solicitada.

6. La SMF verifica si el NG-UE está autorizado a establecer la sesión de PDU solicitada y determina la terminación de seguridad del UP.

7. Si el NG-UE está autorizado a establecer la sesión de PDU y se requiere la terminación de seguridad de la UPF para la sesión de PDU, la SMF solicita una clave para la UPF a la SEAF. La SMF proporciona a la SEAF la identidad del UE, el DNN y el ID de SMF.

8. La SEAF deriva una clave UPF (K_{UPF}) de la K_{SEAF} incorporando los parámetros recibidos de la SMF y un contador gestionado localmente (es decir, CNT_{UPF}) para la derivación de claves UPF.

9. La SEAF envía una respuesta de clave a la SMF. La respuesta clave incluye la K_{UPF} y CNT_{UPF} utilizadas para la derivación de claves (por ejemplo, el contador en la etapa 8).

10. La SMF envía una solicitud de configuración de sesión de PDU a la UPF que contiene la información de configuración de seguridad para la sesión de PDU (por ejemplo, cifrado y/o algoritmo de protección de integridad), incluyendo la K_{UPF}, y características de tráfico para la sesión de PDU.

11. La UPF instala la K_{UPF} para la sesión como parte de la configuración de la sesión de PDU y derivar claves posteriores (K_{UPFEnc}, K_{UPFInt}) basándose en la información de configuración de seguridad. Las claves están asociadas con un ID de clave, que también puede incorporarse en la derivación de claves. Si no se aplica la protección de integridad y confidencialidad a la sesión de PDU, la K_{UPF} es nula y no se derivan claves posteriores.

Además, la UPF configura la función de cumplimiento de políticas de seguridad con los parámetros característicos del tráfico recibidos de la PCF para esta sesión de PDU.

12. La UPF envía una respuesta de configuración de sesión de PDU a la SMF que contiene el ID de sesión de PDU, el ID de clave y otros parámetros (si existen) utilizados para la derivación de claves.

13. La SMF envía una respuesta de establecimiento de sesión de PDU al NG-UE mediante la AMF. Este mensaje de respuesta incluye todos los materiales de claves (por ejemplo, CNT_{UPF}, ID de clave) que son necesarios para que el NG-UE derive las mismas claves que la UPF.

14. El NG-UE deriva K_{UPF} y claves posteriores basándose en la respuesta de establecimiento de sesión.

15. El NG-UE envía un mensaje de establecimiento de sesión de PDU completo a la SMF mediante la AMF.

Después de completar la etapa 15, el NG-UE y la UPF protegen los paquetes del UP basándose en la configuración de seguridad de sesión de PDU que termina en la UPF, la cual incluiría la SPEF.

5.1.40.3 Evaluación

Por determinar

**** FIN DE LOS CAMBIOS ****

APÉNDICE D - Cambios en TR 23.401 Conexión

Este CR añade parámetros al mensaje de solicitud de creación de sesión enviado desde la MME a la puerta de enlace de servicio y a la PDN-GW que transportará los parámetros necesarios por la SPEF en la PDN-GW. La MME obtiene la SPEF del contexto de suscripción HSS para el UE.

El parámetro agregado incluye;

Nombre	Descripción
SPE_LOC	Ubicación del UE: coordenadas GPS que incluyen comportamiento de ubicación/movimiento/velocidad u otra información sobre la ubicación física del UE (ID de celda). Estos pueden ser conocidos a priori para muchos UE, tales como UE estacionarios (por ejemplo, contadores inteligentes).
SPE_VOLUME	Volumen de carga útil de datos estimado. Esto puede especificarse en los parámetros de suscripción (por ejemplo, disponible en el HSS)
SPE_TOD	Hora prevista del día/día de la semana/día del mes, etc., para la configuración de la conexión
SPE_CONNS	Número previsto de conexiones de datos simultáneas (TCP/IP) desde el UE
SPE_DUR	Duración prevista de la conexión
SPE_FREQ	Frecuencia estimada de transmisión de datos (una vez por hora/minuto/segundo, o continua)
SPE_DATATYPE	Tipo de datos; texto, numérico, transmisión de video, transmisión de audio, gráficos (.jpg, .gif, .pdf), carga útil cifrada (donde el cifrado se realiza en una capa por encima de la capa de radio, es decir, la capa de aplicación)
SPE_IPADDR	Dirección de destino normal (dirección IP, URI o nombre de dominio o subdominio)
SPE_BYTES	Intercambio de recuento de bytes transmitidos y recibidos entre el UE y la red a través de una conexión específica. Véase la sección técnica anterior a continuación.
SPE_CAPABILITY	Uso de suscripción permitido. Por ejemplo, solamente datos (no se permite tráfico de SMS, multimedia ni voz (VoIP)).

Tabla 1: Parámetros de la función de cumplimiento de políticas de seguridad

**** PRIMER CAMBIO ****

[Las etapas que no son relevantes para el cambio se eliminan para mayor claridad]

5.3.2.1 Conexión inicial de E-UTRAN

[VÉASE FIG. 6]

12. Si no se ha incluido un recipiente ESM en la solicitud de conexión, se omiten las etapas 12, 13, 14, 15, 16.

Para una conexión de emergencia, la MME aplica los parámetros de los datos de configuración de emergencia de la MME para el establecimiento de la portadora de emergencia realizado en esta etapa y la MME ignora cualquier dato de suscripción relacionado con IMSI potencialmente almacenado. Si el UE realiza una conexión inicial o de traspaso mediante una celda CSG y no hay suscripción para ese CSG o la suscripción al CSG ha expirado, la MME rechazará la solicitud de conexión con una causa adecuada. Si el UE tiene este ID de CSG y la PLMN asociada en su lista de CSG permitidos, el UE eliminará el ID de CSG y la PLMN asociada de la lista cuando reciba esta causa de rechazo.

Si se asigna una dirección PDN suscrita para el UE para este APN, el contexto de suscripción PDN contiene la dirección IPv4 del UE y/o el prefijo IPv6 y, opcionalmente, la identidad GW de PDN. Si el contexto de suscripción PDN contiene una dirección IPv4 y/o un prefijo IPv6 suscritos, la MME lo indica en la dirección PDN. Para el tipo de solicitud que indica "solicitud inicial", si el UE no proporciona un APN, la MME utilizará la GW PDN

correspondiente al APN predeterminado para la activación de la portadora predeterminada. Si el UE proporciona un APN, este APN se empleará para la activación de la portadora predeterminada. Para el tipo de solicitud que indica "traspaso", si el UE proporciona un APN, la MME utilizará la GW PDN correspondiente al APN predeterminado para la activación de la portadora predeterminada. Si el UE no proporciona un APN y el contexto de suscripción del HSS contiene una identidad de GW PDN correspondiente al APN predeterminado, la MME utilizará la GW PDN correspondiente al APN predeterminado para la activación de la portadora predeterminada. El caso en el que el tipo de solicitud indica "traspaso" y el UE no proporcione un APN, y el contexto de suscripción del HSS no contenga una identidad de GW PDN correspondiente al APN predeterminado constituye un caso de error. Si el tipo de solicitud indica "solicitud inicial" y el contexto de suscripción de PDN seleccionado no contiene ninguna identidad de GW PDN, la nueva MME selecciona una GW PDN como se describe en la cláusula 4.3.8.1 sobre la función de selección de GW PDN (accesos 3GPP). Si el contexto de suscripción de PDN contiene una identidad de GW PDN asignada dinámicamente y el tipo de solicitud no indica "traspaso", la MME puede seleccionar una nueva GW PDN como se describe en la cláusula función de selección de GW PDN, por ejemplo, para asignar una GW PDN que permita un enrutamiento más eficiente.

Para la conexión de emergencia inicial y de traspaso, la MME utiliza la función de selección de GW PDN definida en la cláusula 4.3.12.4 para seleccionar una GW PDN.

Si el contexto de suscripción no indica que el APN es para una conexión PDN a una SCEF, la nueva MME selecciona una GW de servicio como se describe en la cláusula 4.3.8.2 sobre la función de selección de GW de servicio y asigna una identidad de portadora EPS para la portadora predeterminada asociada con el UE. A continuación, se envía un mensaje de solicitud de creación de sesión (IMSI, MSISDN, MME TEID para el plano de control, dirección GW PDN, dirección PDN, APN, tipo RAT, QoS de portadora EPS predeterminada, tipo PDN, APN-AMBR, identidad de portadora EPS, opciones de configuración de protocolo, indicación de traspaso, identidad ME (IMEISV), información de ubicación del usuario (ECGI), zona horaria del UE, información CSG del usuario, indicación de soporte de informes de cambio de información MS, modo de selección, características de cobro, referencia de seguimiento, tipo de seguimiento, ID de activación, identidad OMC, restricción máxima de APN, indicador de portadora de dirección dual, tipo de protocolo sobre S5/S8, red de servicio, parámetros de aplicación de políticas de seguridad) a la GW de servicio seleccionada. Si se aplica la optimización CIoT EPS del plano de control, a continuación, la MME también indicará la tunelización S11-U de los datos del usuario NAS y enviará su propia dirección IP S11-U y el TEID DL de MME para el reenvío de datos DL por parte de la SGW. La información del usuario CSG incluye ID de CSG, modo de acceso e indicación de membresía de CSG.

Para el tipo de PDN "no IP" cuando las optimizaciones CIoT EPS del plano de control están habilitadas para el UE, si los datos de suscripción de APN indican que se necesita utilizar una conexión SCEF, a continuación, la MME asigna una identidad de portadora EPS para la portadora predeterminada asociada con el UE y establece una conexión con la dirección SCEF indicada en los datos de suscripción según TS 23.682 [74] y las etapas 12, 13, 14, 15, 16 no se ejecutan. El resto de interacciones con el UE se aplican como se especifica a continuación.

Si la MME determina que la conexión PDN solamente utilizará la optimización CIoT EPS del plano de control, la MME incluirá un indicador de conexión PDN solamente del plano de control en la solicitud de creación de sesión.

Si el tipo de solicitud indica "Emergencia", no se realizará el control de restricción máxima de APN.

Para los UE conectados de emergencia, se incluye la IMSI si está disponible y, si la IMSI no se puede autenticar, a continuación, la IMSI se marcará como no autenticada.

El tipo RAT se proporciona en este mensaje para la decisión posterior del PCC. El tipo RAT distinguirá entre los tipos NB-IoT y WB-E-UTRA. En este mensaje también se proporciona el APN-AMBR suscrito para el APN. El MSISDN se incluye si se proporciona en los datos de suscripción del HSS. La indicación de traspaso se incluye si el tipo de solicitud indica traspaso. El modo de selección indica si se ha seleccionado un APN suscrito o si se ha seleccionado un APN no suscrito enviado por el UE. Las características de cobro indican de qué tipo de cobro es responsable el contexto de la portadora. La MME puede cambiar el tipo de PDN solicitado según los datos de suscripción para este APN como se describe en la cláusula 5.3.1.1. La MME establecerá el indicador de portadora de dirección dual cuando el tipo de PDN esté configurado en IPv4v6 y todos los SGSN a los que se puede traspasar el UE sean de la versión 8 o superior y soporten direccionamiento dual, lo cual se determina basándose en la configuración previa del nodo por parte del operador. El tipo de protocolo sobre S5/S8 se proporciona a la GW de servicio cuyo protocolo debería utilizarse sobre la interfaz S5/S8.

Las características de cobro para la suscripción de PS y los APN suscritos individualmente, así como la forma de manejar las características de cobro y si enviarlas o no a la P-GW se definen en TS 32.251 [44]. La MME incluirá la referencia de seguimiento, el tipo de seguimiento, el ID del activador y la identidad OMC si el seguimiento de S-GW y/o P-GW está activado. La MME copiará la referencia de seguimiento, el tipo de seguimiento y la identidad de OMC de la información de seguimiento recibida del HLR o del OMC.

La restricción máxima de APN indica la restricción más estricta requerida por cualquier contexto de portadora ya activo. Si ya no hay contextos de portadora activos, este valor se establece en el tipo menos restrictivo (véase la

cláusula 15.4 de TS 23.060 [7]). Si la P-GW recibe la restricción máxima de APN, a continuación, la P-GW verificará si el valor de restricción máxima de APN no entra en conflicto con el valor de restricción de APN asociado con esta solicitud de contexto de portadora. Si no hay conflicto, se permitirá la solicitud; de lo contrario, se rechazará enviando una causa de error adecuada al UE.

Si la MME requiere que el eNB verifique si las capacidades de radio del UE son compatibles con la configuración de red (por ejemplo, si el SRVCC o el soporte de frecuencia del UE coincide con el de la red) para poder configurar la indicación de soporte de sesión PS sobre voz IMS (véase la cláusula 4.3.5.8), a continuación, la MME puede enviar una solicitud de coincidencia de capacidad de radio del UE al eNB como se define en la cláusula 5.3.14.

13. La GW de servicio crea una nueva entrada en su tabla de portadoras EPS y envía un mensaje de solicitud de creación de sesión (IMSI, MSISDN, APN, dirección de GW de servicio para el plano de usuario, TEID de GW de servicio del plano de usuario, TEID de GW de servicio del plano de control, tipo RAT, QoS de portadora EPS predeterminado, tipo de PDN, dirección PDN, APN-AMBR suscrito, identidad de portadora EPS, opciones de configuración del protocolo, indicación de traspaso, identidad ME, información de ubicación del usuario (ECGI), zona horaria del UE, información CSG del usuario, Indicación de soporte de informe de cambio de información MS, indicación de soporte de pausa de cobro PDN, modo de selección, características de cobro, referencia de seguimiento, tipo de seguimiento, ID de activación, identidad OMC, restricción máxima de APN, indicador de portadora de dirección dual, red de servicio, parámetros de cumplimiento de políticas de seguridad) a la GW PDN indicada por la dirección GW PDN recibida en la etapa anterior. Después de esta etapa, la GW de servicio almacena en memoria intermedia cualquier paquete de enlace descendente que pueda recibir de la GW PDN sin enviar un mensaje de notificación de datos de enlace descendente a la MME hasta que reciba el mensaje de solicitud de modificación de portadora en la etapa 23 a continuación. El MSISDN se incluye si se recibe de la MME.

Si la GW de servicio ha recibido el indicador de conexión PDN solamente del plano de control en la etapa 12, la GW de servicio informa a la PGW de esta información en la solicitud de creación de sesión. La GW de servicio y la GW PDN indicarán el uso de CP únicamente en sus CDR.

Las GW PDN no realizarán ninguna verificación de la restricción máxima de APN si la solicitud de creación de portadora predeterminada incluye el APN de emergencia.

Para los UE conectados de emergencia, se incluye la IMSI si está disponible y, si la IMSI no se puede autenticar, a continuación, la IMSI se marcará como no autenticada.

En el caso de conexión de traspaso, y si la PGW detecta que el estado de UE sin datos del PS 3GPP ha cambiado, la PGW indicará este evento al sistema de cobro para el cobro en línea y fuera de línea.

14. Si se despliega un PCC dinámico y la indicación de traspaso no está presente, la GW PDN realiza un procedimiento de establecimiento de sesión IP-CAN como se define en TS 23.203 [6] y, por lo tanto, obtiene las reglas PCC predeterminadas para el UE. Esto puede llevar al establecimiento de varias portadoras dedicadas siguiendo los procedimientos definidos en la cláusula 5.4.1 en asociación con el establecimiento de la portadora predeterminada, que se describe en el anexo F.

La IMSI, APN, dirección IP de UE, información de ubicación del usuario (ECGI), zona horaria del UE, red de servicio, tipo RAT, APN-AMBR, QoS de portadora de EPS predeterminada, ETFTU (si no se proporciona ETFTU, significa que el UE y/o la GW PDN no soportan el formato de filtro TFT extendido) se proporcionan a la PCRF por la GW PDN si se reciben en el mensaje anterior. La información de ubicación del usuario y la zona horaria del UE se utilizan para el cobro basado en la ubicación. Para los UE conectados de emergencia que no están autenticados, la GW PDN proporciona el IMEI como identidad del UE en lugar de la IMSI a la PCRF. Si la PCRF decide que la conexión PDN puede utilizar el formato de filtro TFT extendido, devolverá el indicador ETFTN a la GW PDN para su inclusión en las opciones de configuración del protocolo devueltas al UE.

La PCRF puede modificar el APN-AMBR y los parámetros QoS (QCI y ARP) asociados con la portadora predeterminada en la respuesta a la GW PDN como se define en TS 23.203 [6].

Si el PCC está configurado para soportar servicios de emergencia y si se despliega PCC dinámico, la PCRF, basada en el APN de emergencia, establece el ARP de las reglas de PCC a un valor reservado para servicios de emergencia y la autorización de reglas de PCC dinámicas como se describe en TS 23.203 [6]. Si no se despliega el PCC dinámico, la GW PDN utiliza el ARP de portadora EPS de emergencia predeterminada para cualquier portadora EPS de emergencia dedicada potencialmente iniciada. La P-GW determina que se solicitan servicios de emergencia basándose en el APN de emergencia recibido en el mensaje de solicitud de creación de sesión.

NOTA 10: Mientras que la GW PDN/PCEF se puede configurar para activar reglas PCC predefinidas para la portadora predeterminada; la interacción con la PCRF aún es necesaria para proporcionar, por ejemplo, la información de la dirección IP del UE a la PCRF.

NOTA 11: Si la dirección IP no está disponible cuando la GW PDN realiza el procedimiento de establecimiento de sesión IP-CAN con la PCRF, la GW PDN inicia un procedimiento de modificación de sesión IP-CAN para informar a la PCRF sobre una dirección IP asignada tan pronto como la dirección esté disponible. En esta versión de la especificación, esto se aplica únicamente a la asignación de direcciones IPv4.

Si se despliega el PCC dinámico y la indicación de traspaso está presente, la GW PDN ejecuta un procedimiento de modificación de sesión IP-CAN iniciada por PCEF con la PCRF como se especifica en TS 23.203 [6] para reportar el nuevo tipo de IP-CAN. Dependiendo de las reglas PCC activas, puede ser necesario el establecimiento de portadoras dedicadas para el UE. El establecimiento de esas portadoras se llevará a cabo en combinación con la activación de la portadora predeterminada como se describe en el anexo F. Este procedimiento puede continuar sin esperar una respuesta de PCRF. Si se requieren cambios en las reglas activas PCC, la PCRF puede proporcionarlos una vez finalizado el procedimiento de traspaso. En ambos casos (la indicación de traspaso está presente o no), si no se despliega el PCC dinámico, la GW PDN puede aplicar la política de QoS local. Esto puede conducir al establecimiento de una serie de portadoras dedicadas para el UE siguiendo los procedimientos definidos en la cláusula 5.4.1 en combinación con el establecimiento de la portadora predeterminada, que se describe en el anexo F.

Si los activadores de reportes de información CSG se reciben de la PCRF, por consiguiente, la GW PDN debería configurar el IE de acción de reporte de información CSG. El comportamiento adicional de PGW para los datos PS desactivados de 3GPP se define en TS 23.203.

15. La P-GW crea una nueva entrada en su tabla de contexto de portadora EPS y genera un ID de cobro para la portadora predeterminada. La nueva entrada permite a la P-GW enrutar las PDU del plano de usuario entre la S-GW y la red de paquetes de datos, y comenzar a cobrar. La forma en que la P-GW maneja las características de cobro que pueda haber recibido se define en TS 32.251. Si los parámetros SPEF están presentes, la función SPEF se invocará en la PDN-GW y comenzará a monitorizar las PDU del plano de usuario para este UE.

La GW PDN devuelve un mensaje de respuesta de creación de sesión (dirección GW PDN para el plano de usuario, TEID de GW PDN del plano de usuario, TEID de GW PDN del plano de control, tipo de PDN, dirección de PDN, identidad de portadora de EPS, QoS de portadora de EPS, opciones de configuración del protocolo, ID de cobro, compresión de carga útil prohibida, restricción de APN, causa, acción de reporte de cambio de información MS (inicio) (si la GW PDN decide recibir información de ubicación del UE durante la sesión), acción de reporte de información de CSG (Inicio) (si la GW PDN decide para recibir información de CSG del usuario del UE durante la sesión), acción del área de informe de presencia (si la GW PDN decide recibir notificaciones sobre un cambio de presencia del UE en el área de reporte de presencia), indicación habilitada de pausa de cobro de PDN (si la GW PDN ha elegido habilitar el función), APN-AMBR, conexión tolerante al retardo) a la GW de servicio.

La GW PDN tiene en cuenta el tipo de PDN recibido, el indicador de portadora de dirección dual y las políticas del operador cuando la GW PDN selecciona el tipo de PDN que se ha de utilizar de la siguiente manera. Si el tipo de PDN recibido es IPv4v6 y es posible tanto el direccionamiento IPv4 como IPv6 en la PDN pero el indicador de portadora de dirección dual no está configurado, o solamente es posible el direccionamiento de versión IP única para este APN en la PDN, la GW PDN selecciona una única versión IP (ya sea IPv4 o IPv6). Si el tipo de PDN recibido es IPv4 o IPv6 o "No IP", la GW PDN utiliza el tipo de PDN recibido si es compatible con la PDN, de lo contrario, se devolverá una causa de error adecuada. Para IPv4, IPv6 e IPv4v6, la GW PDN asigna una dirección PDN según el tipo de PDN seleccionado. Si la GW PDN ha seleccionado un tipo de PDN diferente del tipo de PDN recibido, la GW PDN indica junto con el IE del tipo de PDN un motivo al UE por el cual se ha modificado el tipo de PDN, como se describe en la cláusula 5.3.1.1. La GW PDN aceptará o rechazará (pero no modificará) el tipo de PDN si el tipo de PDN se establece a "No IP". La dirección PDN puede contener una dirección IPv4 para IPv4 y/o un prefijo IPv6 y un identificador de interfaz, o puede omitirse para el tipo PDN "No IP". Si el operador ha configurado la PDN, de manera que las direcciones de PDN para el APN solicitado se asignarán mediante el uso de DHCPv4 únicamente, o si la GW PDN permite que el UE utilice DHCPv4 para la asignación de direcciones según la preferencia de asignación de direcciones recibida del UE, la dirección PDN se establecerá en 0.0.0.0, lo que indica que la dirección de PDN IPv4 será negociada por el UE con DHCPv4 después de completar el procedimiento de activación de portadora predeterminada. Para el direccionamiento de PDN externo para IPv6, la GW PDN obtiene el prefijo IPv6 de la PDN externa utilizando, bien la función de cliente RADIUS, o bien diámetro. En el campo dirección de PDN de la respuesta de creación de sesión, la GW PDN incluye el identificador de interfaz y el prefijo IPv6. La GW PDN envía un anuncio de enrutador al UE después del establecimiento de portadora predeterminada con la información del prefijo IPv6 para todos los casos. Si la dirección de PDN está contenida en la solicitud de creación de sesión, la GW PDN asignará la dirección IPv4 y/o el prefijo IPv6 contenido en la dirección de PDN al UE. Los detalles de asignación de direcciones IP se describen en la cláusula 5.3.1 sobre "Asignación de direcciones IP". La GW PDN deriva el BCM basándose en la NRSU y la política del operador. La GW PDN determina si se ha de utilizar el formato de filtro TFT extendido basándose en la ETFTU, la ETFTN recibida de la PCRF y la política del operador. Las opciones de configuración del protocolo contienen BCM, ETFTN y parámetros de PDN opcionales que la P-GW puede transferir al UE. Estos parámetros de PDN opcionales pueden ser solicitados por el UE o pueden ser enviados sin ser solicitados por la

P-GW. Las opciones de configuración del protocolo se envían de forma transparente a través de la MME. La GW PDN incluye una indicación de conexión tolerante al retardo si la GW PDN soporta la recepción de una causa de rechazo de la SGW que indica que el UE no está accesible temporalmente debido al ahorro de energía y a la retención de procedimientos terminados en móvil, hasta que la GW PDN reciba un mensaje que indique que el UE está disponible para señalización de extremo a extremo.

Cuando la indicación de traspaso está presente, la GW PDN no envía todavía paquetes de enlace descendente a la S-GW; la ruta de enlace descendente ha de cambiarse en la etapa 23a. Si la GW PDN es una L-GW, no reenvía paquetes de enlace descendente a la S-GW. Los paquetes sólo se reenviarán al HeNB en la etapa 20 mediante la ruta directa del plano de usuario.

16. La GW de servicio devuelve un mensaje de respuesta de creación de sesión (tipo de PDN, dirección de PDN, dirección de GW de servicio para el plano de usuario, TEID de GW de servicio para el plano de usuario S1-U, TEID de GW de servicio para el plano de control, identidad de portadora de EPS, QoS de portadora de EPS, direcciones de GW de PDN y TEID (S5/S8 basado en GTP) o claves GRE (S5/S8 basado en PMIP) en las GW PDN para tráfico de enlace ascendente, opciones de configuración de protocolo, compresión de carga útil prohibida, restricción de APN, causa, acción de reporte de cambio de información de MS (inicio), acción de área de reporte de presencia, acción de reporte de información CSG (inicio), APN-AMBR, Conexión tolerante al retardo) a la nueva MME. Para la optimización de EPS CIoT del plano de control, la MME utiliza la dirección de GW de servicio para el plano de usuario S11-U y el TEID de GW de servicio para reenviar datos de UL a la SGW. Si el estado de UE de datos PS desactivados de 3GPP ha estado presente en la solicitud de creación de sesión PCO y la PGW soporta la función de desactivación de datos PS de 3GPP, la PGW incluirá la indicación de soporte de desactivación de datos PS 3GPP en la respuesta de creación de sesión PCO.

**** FIN DE LOS CAMBIOS ****

APÉNDICE E - Cambios en Desconexión TR 23.401

Este CR añade un mensaje de desconexión enviado a la MME desde la SPEF en la GW-PDN que indica que el tráfico observado desde un UE está fuera del rango esperado.

Los cambios propuestos se basan en el procedimiento de desconexión iniciado por MME de la sección 5.3.8.3 de 23.401.

**** PRIMER CAMBIO****

[Las etapas que no son relevantes para el cambio se eliminan para mayor claridad]

[Añadir una nueva sección después de la sección 5.3.8.3 Desconexión iniciada por MME]

5.3.8.4 La GW PDN con procedimiento de desconexión iniciado por SPEF

El procedimiento de desconexión iniciado por la MME cuando lo inicia la MME se ilustra en la fig. 5.3.8.3-1.

La fig. 5.3.8.4-1: GW PDN con procedimiento de desconexión iniciado por SPEF [VÉASE FIGURA 17]

1. La SPEF de GW PDN envía una notificación de desconexión a la MME para la sesión en la que se ha observado un comportamiento del tráfico fuera de un rango esperado.

2. A la conclusión del procedimiento de desconexión definido en 5.8.3.1 procedimiento de desconexión iniciado por la MME, la MME envía un acuse de recibo de desconexión final a la SPEF de GW PDN.

**** FIN DE LOS CAMBIOS ****

REIVINDICACIONES

1.- Un método en un equipo de usuario, comprendiendo el método:

el envío, desde el equipo de usuario a un elemento de red, de un conjunto de características y un rango de valores para cada uno del conjunto de características para el tráfico del plano de usuario entre el equipo de usuario y el elemento de red;

la transmisión del tráfico del plano de usuario al elemento de red;

cuando al menos una característica del tráfico del plano de usuario cae fuera del rango de valores, la recepción de una acción de red y la realización de al menos una de las siguientes:

recepción de un mensaje seguro desde el elemento de red que contiene información asociada con una infracción de característica basada en al menos una característica de tráfico del plano de usuario que cae fuera del rango de valores;

realización de un restablecimiento de conexión habiendo realizado un procedimiento en el equipo de usuario que promueve que el equipo de usuario realice un nuevo procedimiento de registro de red, y además realizando el nuevo procedimiento de registro de red desde el equipo de usuario;

activación de un procedimiento de autenticación en el equipo de usuario; y

activación de al menos uno de cifrado o protección de integridad;

en donde el envío se realiza durante el nuevo procedimiento de registro de red entre el equipo de usuario y el elemento de red.

2.- El método según la reivindicación 1, en el que el tráfico en el plano de usuario se transmite sin al menos una protección de integridad y cifrado.

3. El método según la reivindicación 1, en donde el conjunto de características incluye al menos una característica seleccionada del grupo que comprende: la ubicación del equipo de usuario; volumen de tráfico hacia o desde el equipo de usuario, hora del día de tráfico para el equipo de usuario; número de conexiones al equipo de usuario; duración de una sesión en el equipo de usuario; un número máximo de paquetes de datos enviados durante un período de tiempo desde el equipo de usuario; un tipo de datos para paquetes procedentes del equipo de usuario; una dirección de destino para paquetes procedentes del equipo de usuario; y un uso de suscripción permitido para el equipo de usuario.

4.- El método según la reivindicación 1, en donde la acción y ejecución de la red comprende la recepción de un mensaje seguro en el equipo de usuario que contiene información asociada con la infracción de la característica.

5.- El método de la reivindicación 1, en donde la acción y ejecución de la red activa un procedimiento de autenticación en el equipo de usuario.

6.- El método de la reivindicación 2, en donde la acción y ejecución de la red comprende la activación de al menos uno de cifrado o protección de integridad.

7.- Un equipo de usuario que comprende:

un procesador;

un subsistema de comunicación;

un memoria;

en donde el procesador, el subsistema de comunicación y la memoria cooperan para llevar a cabo las etapas de cualquiera de las reivindicaciones 1 a 6.

8. Un medio no transitorio legible por ordenador para almacenar instrucciones de programa, que cuando se ejecuta por un procesador de un equipo de usuario hace que el equipo de usuario realice cualquiera de los métodos de las reivindicaciones 1 a 6.

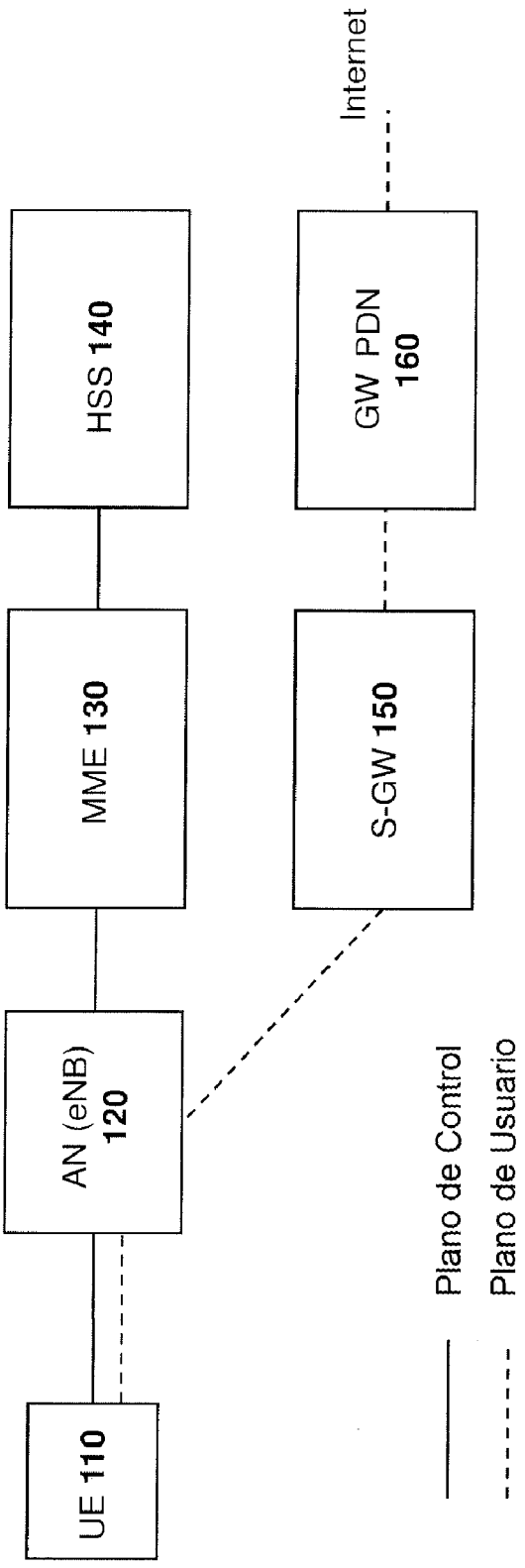
Internet
HSS 140
GW PDN 160
MME 130
S-GW 150
AN (eNB) 120
UE 110
Plano de Control
Plano de Usuario

FIG. 1

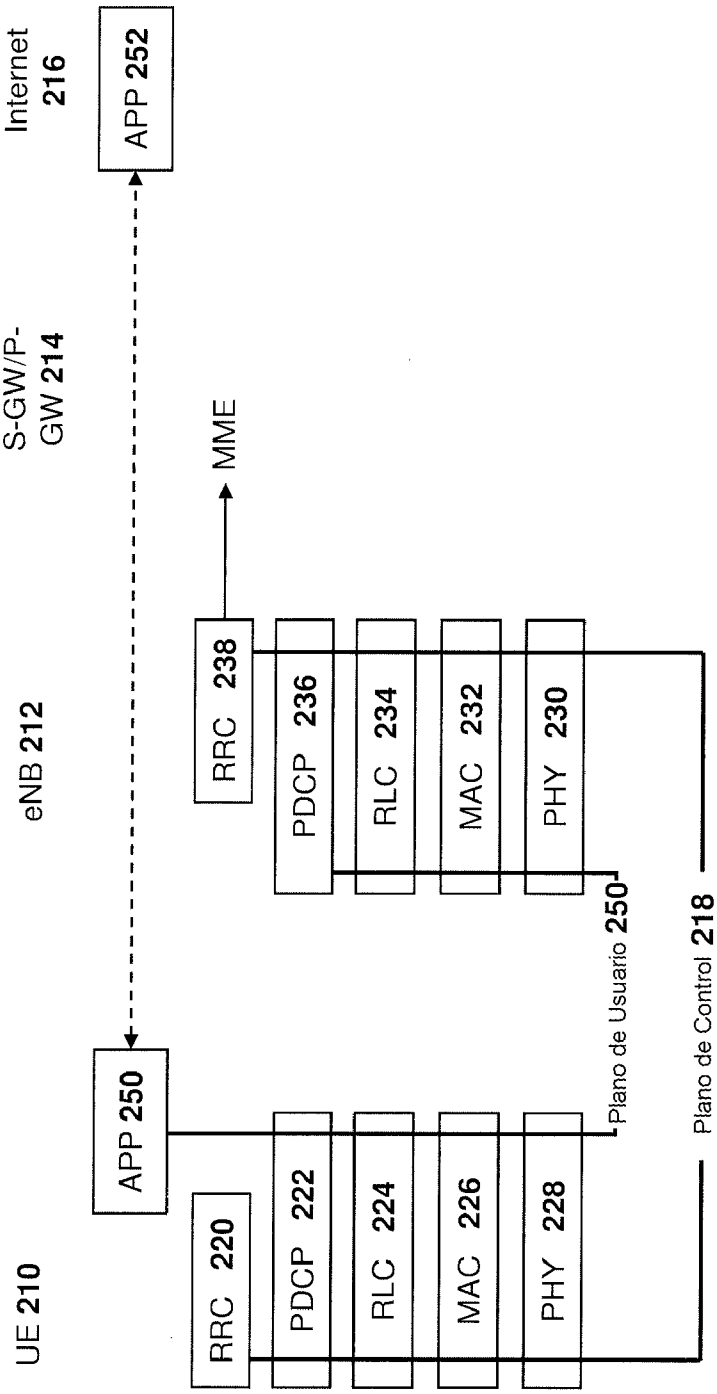
UE 210
eNB 212
S-GW/P-GW 214
Internet 216
APP 250
RRC 220
PDCP 222
RLC 224
MAC 226
PHY 228
RRC 238
PDCP 236
RLC 234
MAC 232
PHY 230
MME
APP 252
Plano de Usuario 250
Plano de Control 218

FIG. 2

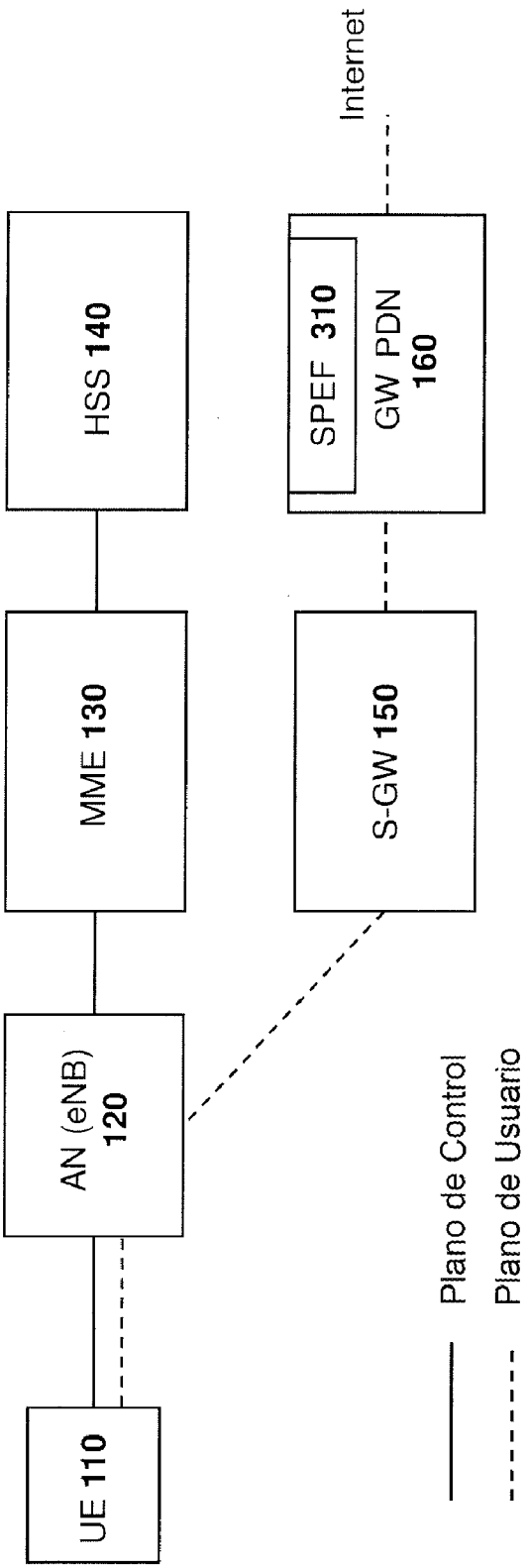
Internet
HSS 140
SPEF 310
GW PDN 160
MME 130
S-GW 150
AN (eNB) 120
UE 110
Plano de Control
Plano de Usuario

FIG. 3

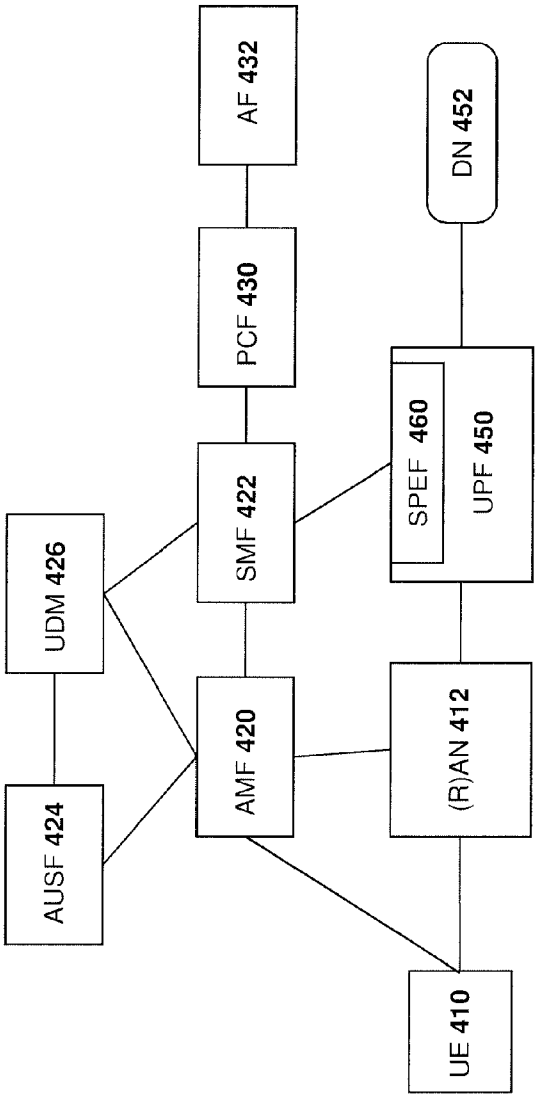
AF 432
DN 452
PCF 430
SPEF 460
UPF 450
SMF 422
UDM 426
AMF 420
(R)AN 412
AUSF 424
UE 410

FIG. 4

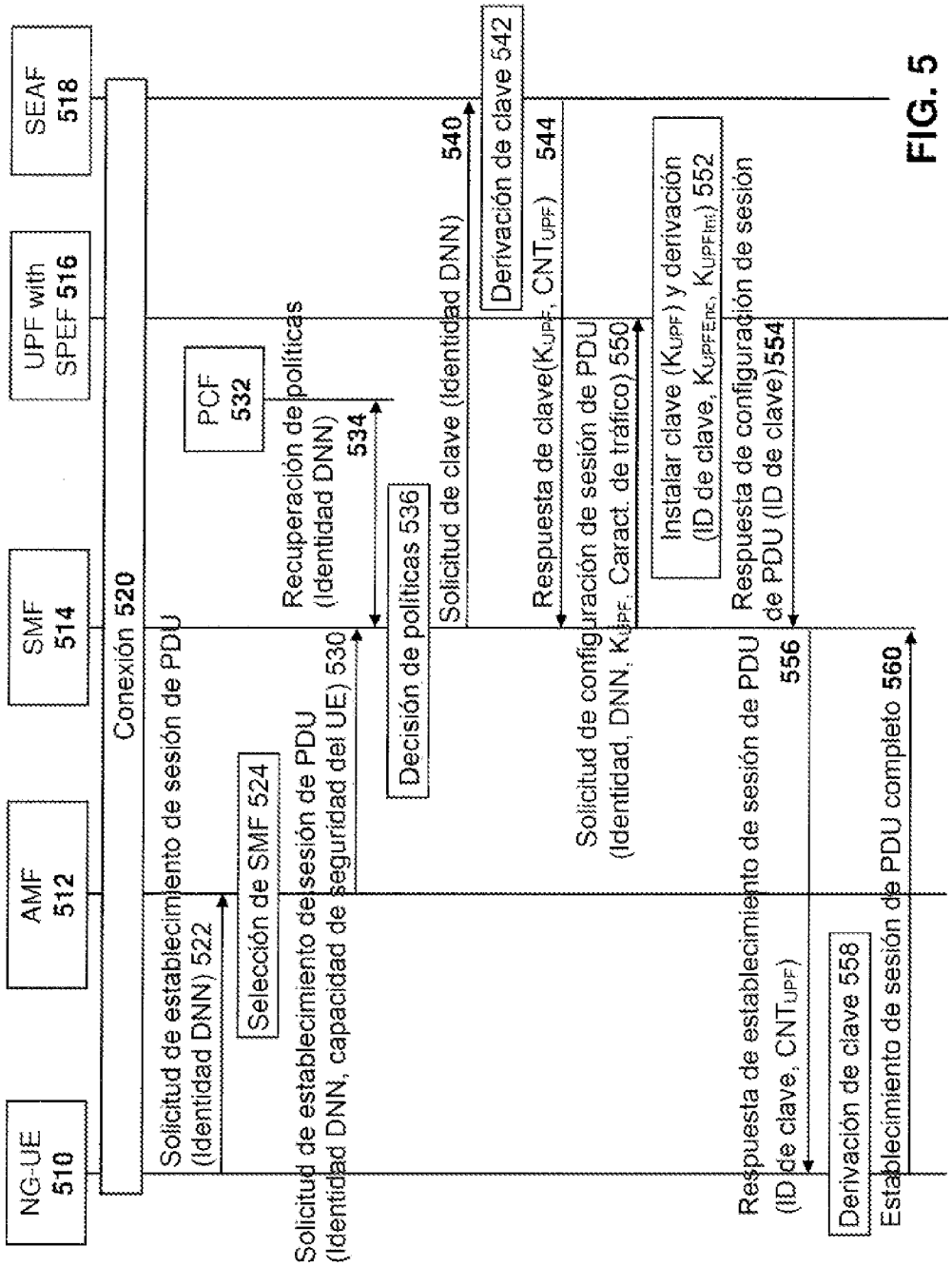
NG-UE 510
AMF 512
SMF 514
UPF with SPEF 516
SEAF 518
Conexión 520
Solicitud de establecimiento de sesión de PDU (Identidad DNN) 522
Selección de SMF 524
Solicitud de establecimiento de sesión de PDU (Identidad DNN, capacidad de seguridad del UE) 530
PCF 532
Recuperación de políticas (Identidad DNN) 534
Decisión de políticas 536
Solicitud de clave (Identidad DNN) 540
Derivación de clave 542
Respuesta de clave(K_{UPF}, CNT_{UPF}) 544
Solicitud de configuración de sesión de PDU (Identidad, DNN, K_{UPF}, Caract. de tráfico) 550
Instalar clave (K_{UPF}) y derivación (ID de clave, K_{UPFEnc}, K_{UPFInt}) 552
Respuesta de configuración de sesión de PDU (ID de clave) 554
Respuesta de establecimiento de sesión de PDU (ID de clave, CNT_{UPF}) 556
Derivación de clave 558
Establecimiento de sesión de PDU completo 560

FIG. 5

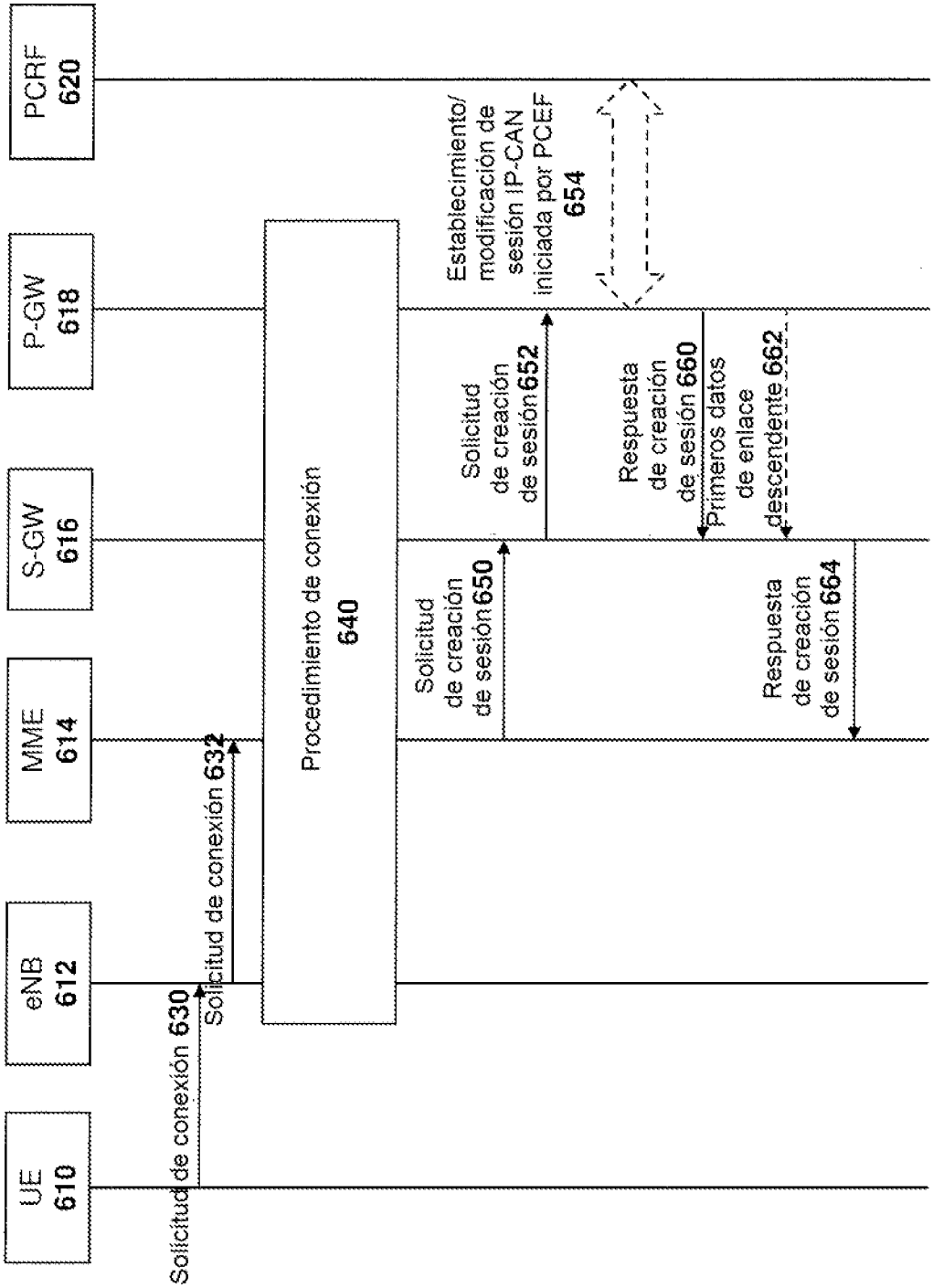
UE 610
eNB 612
MME 614
S-GW 616
P-GW 618
PCRF 620
Solicitud de conexión 630
Solicitud de conexión 632
Procedimiento de conexión 640
Solicitud de creación de sesión 650
Solicitud de creación de sesión 652
Establecimiento/ modificación de sesión IP-CAN iniciada por PCEF 654
Respuesta de creación de sesión 660
Primeros datos de enlace descendente 662
Respuesta de creación de sesión 664

FIG. 6

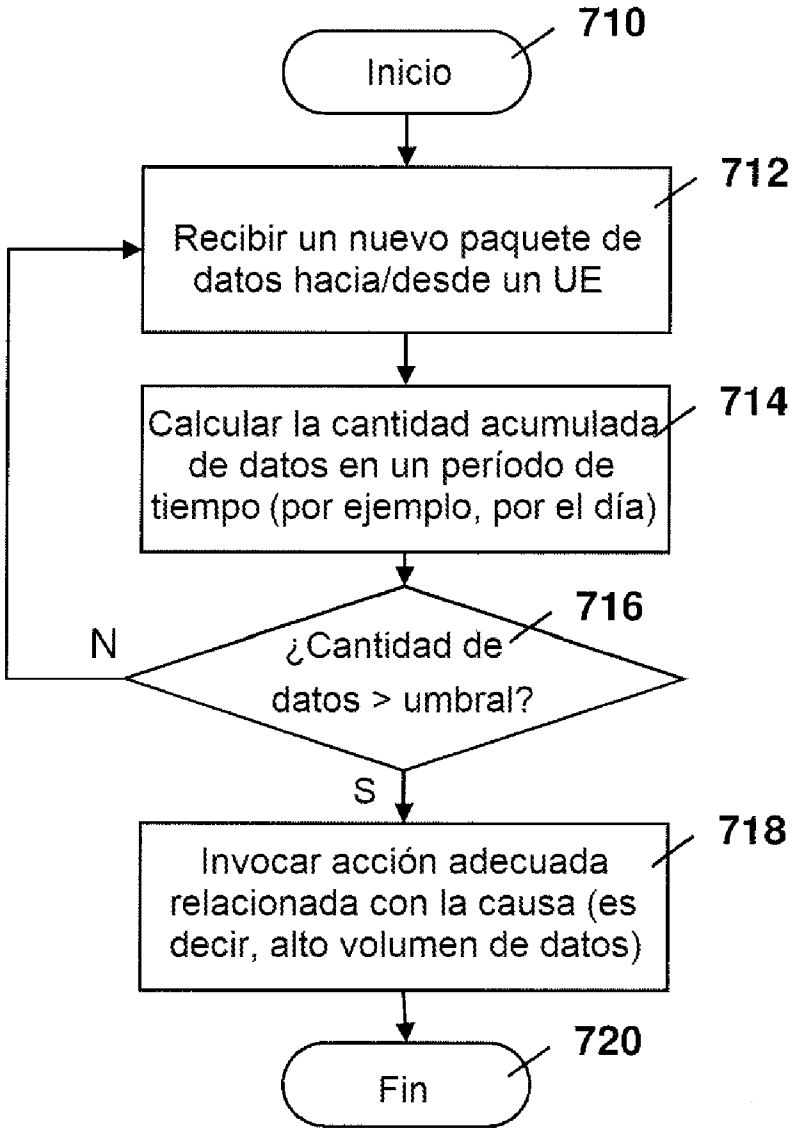
710
Inicio
712
Recibir un nuevo paquete de datos hacia/desde un UE
714
Calcular la cantidad acumulada de datos en un período de tiempo (por ejemplo, por el día)
716
¿Cantidad de datos > umbral?
N
S
718
Invocar acción adecuada relacionada con la causa (es decir, alto volumen de datos)
720
Fin

FIG. 7

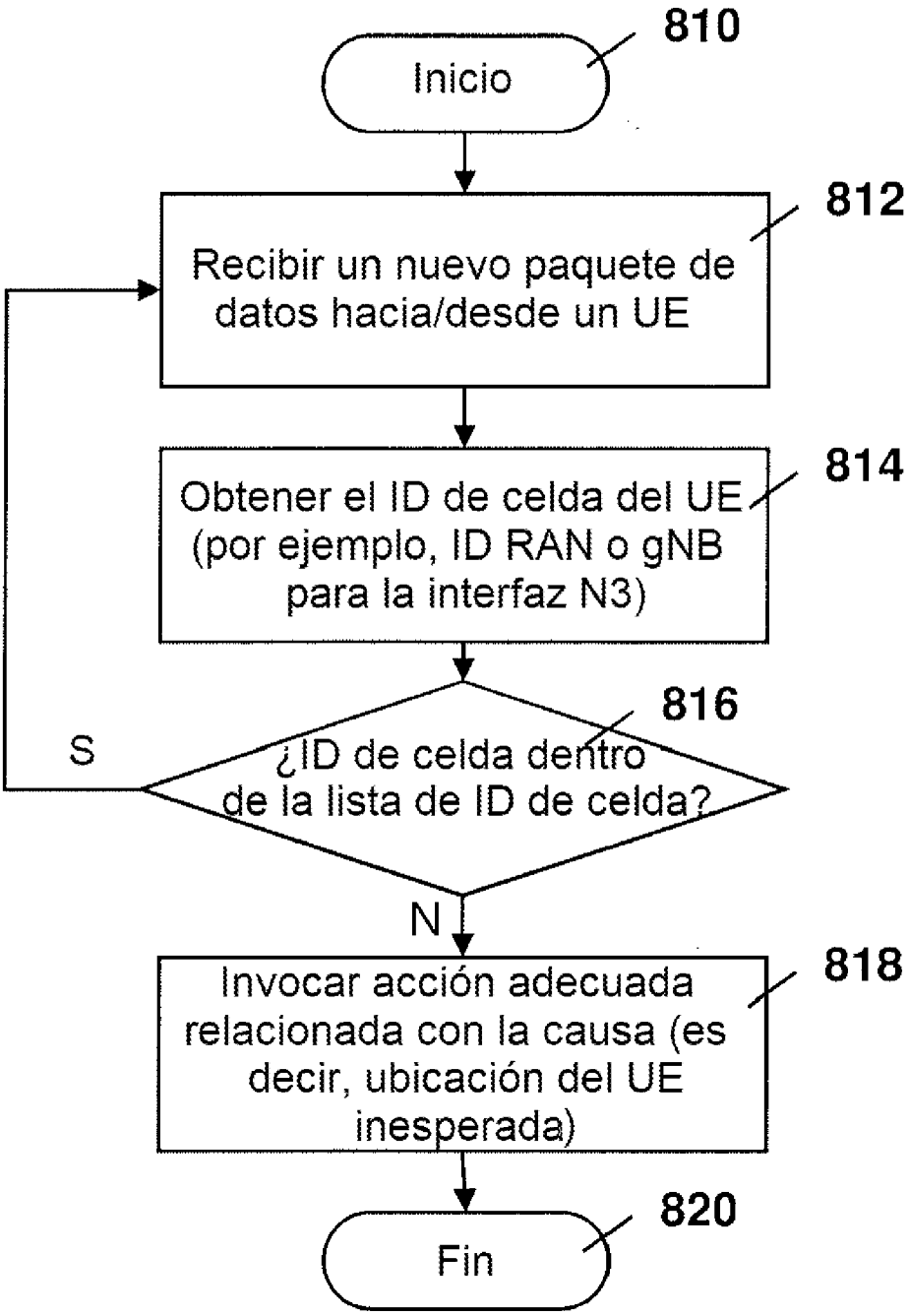
810
Inicio
812
Recibir un nuevo paquete de datos hacia/desde un UE
814
Obtener el ID de celda del UE (por ejemplo, ID RAN o gNB para la interfaz N3)
816
¿ID de celda dentro de la lista de ID de celda?
S
N
818
Invocar acción adecuada relacionada con la causa (es decir, ubicación del UE inesperada)
820
Fin

FIG. 8

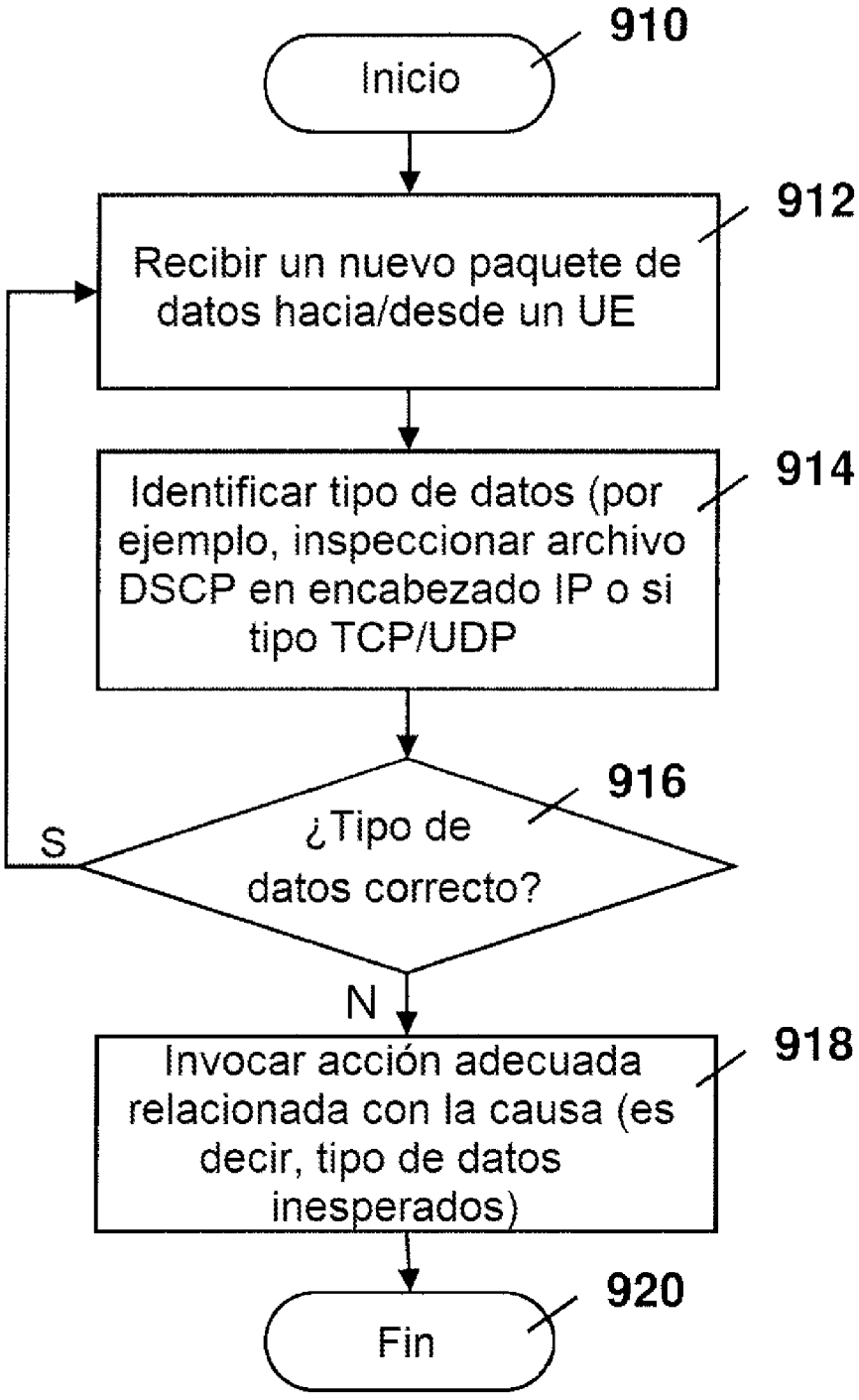
910
Inicio
912
Recibir un nuevo paquete de datos hacia/desde un UE
914
Identificar tipo de datos (por ejemplo, inspeccionar archivo DSCP en encabezado IP o si tipo TCP/UDP
916
¿Tipo de datos correcto?
S
N
918
Invocar acción adecuada relacionada con la causa (es decir, tipo de datos inesperados)
920
Fin

FIG. 9

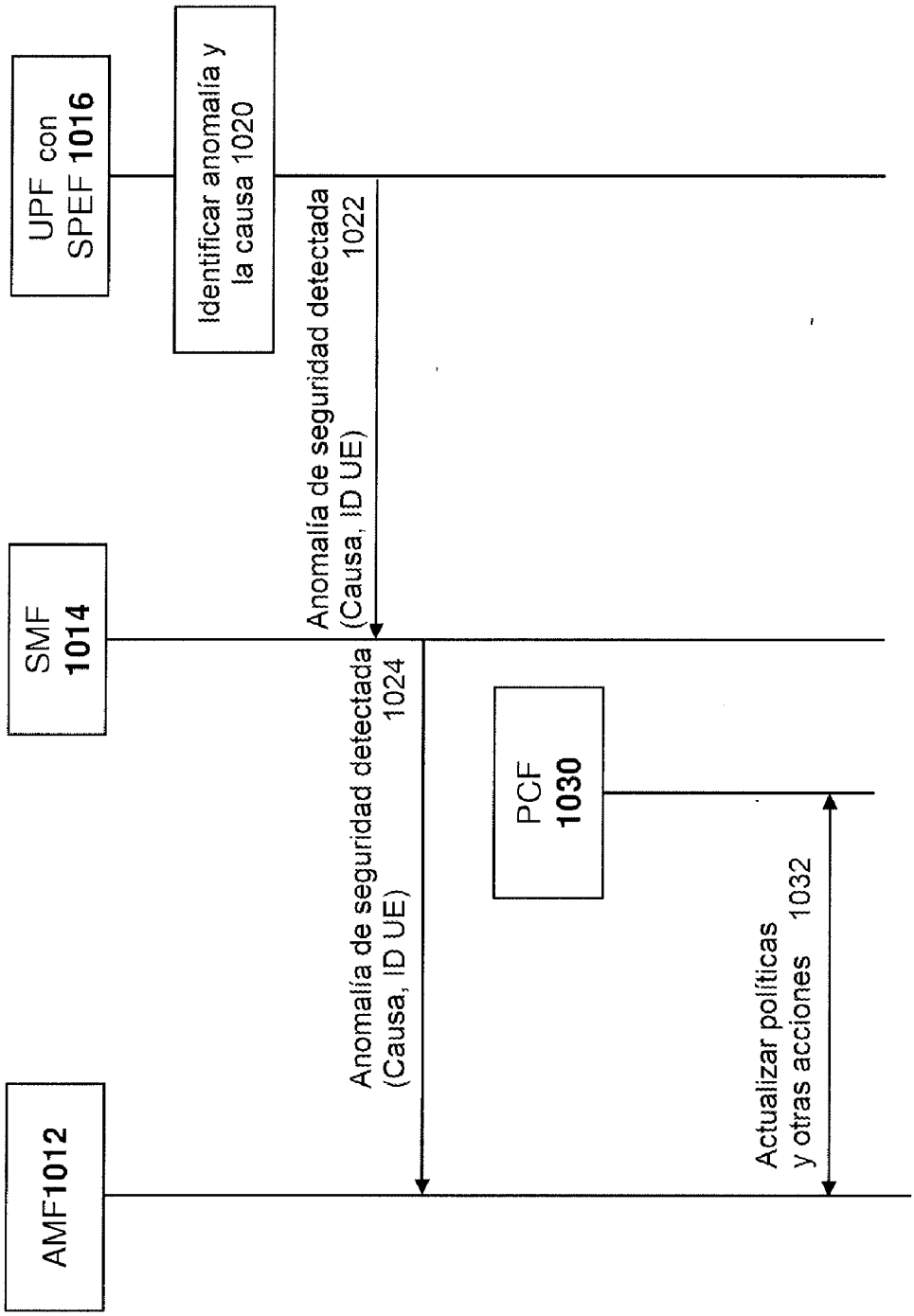
UPF con SPEF 1016
Identificar anomalía y la causa 1020
SMF 1014
Anomalía de seguridad detectada (Causa, ID UE) 1022
Anomalía de seguridad detectada (Causa, ID UE) 1024
PCF 1030
Actualizar políticas y otras acciones 1032
AMF1012

FIG. 10

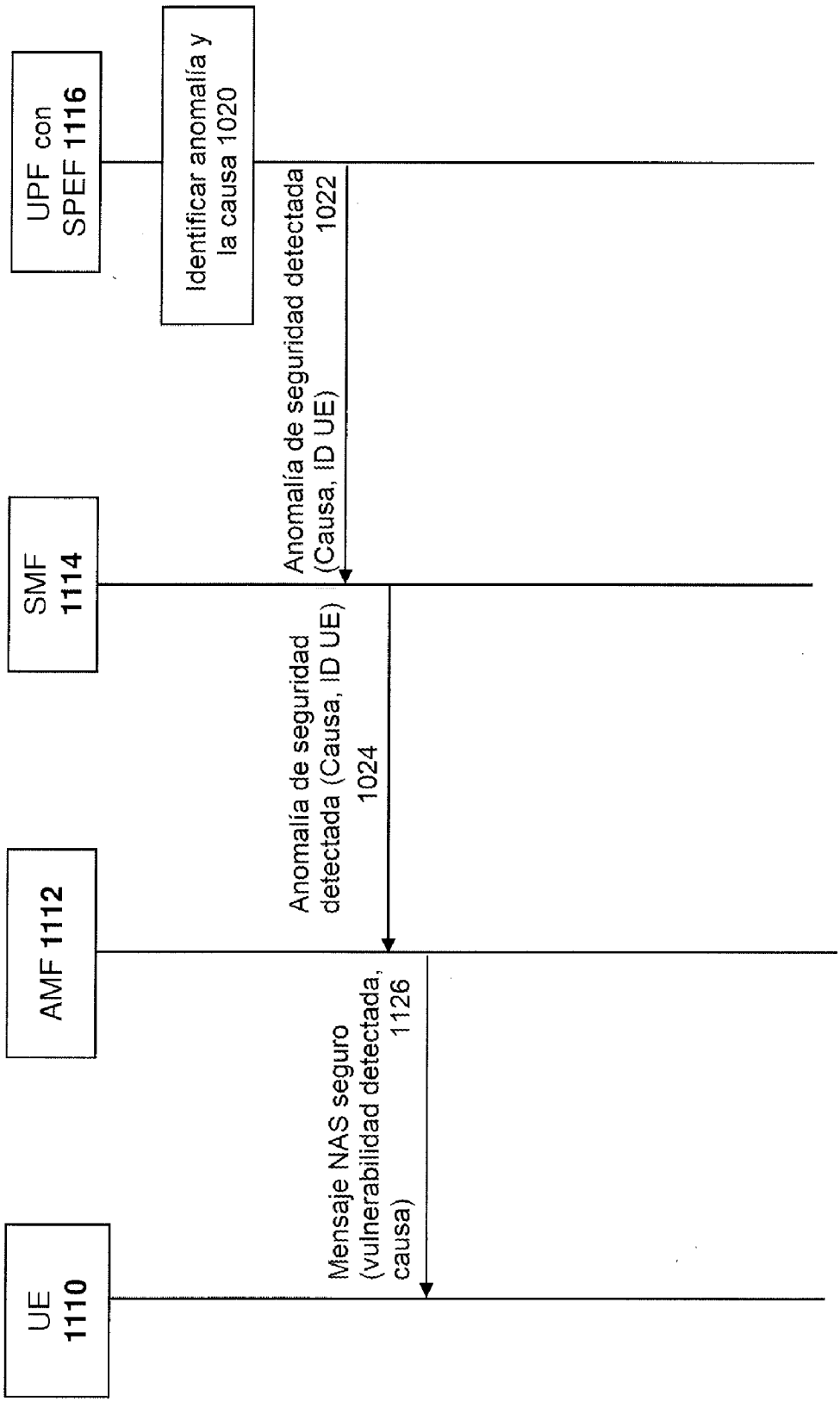
UPF con SPEF 1116
Identificar anomalía y la causa 1020
SMF 1114
Anomalía de seguridad detectada (Causa, ID UE) 1022
AMF 1112
Anomalía de seguridad detectada (Causa, ID UE) 1024
UE 1110
Mensaje NAS seguro (vulnerabilidad detectada, causa) 1126

FIG. 11

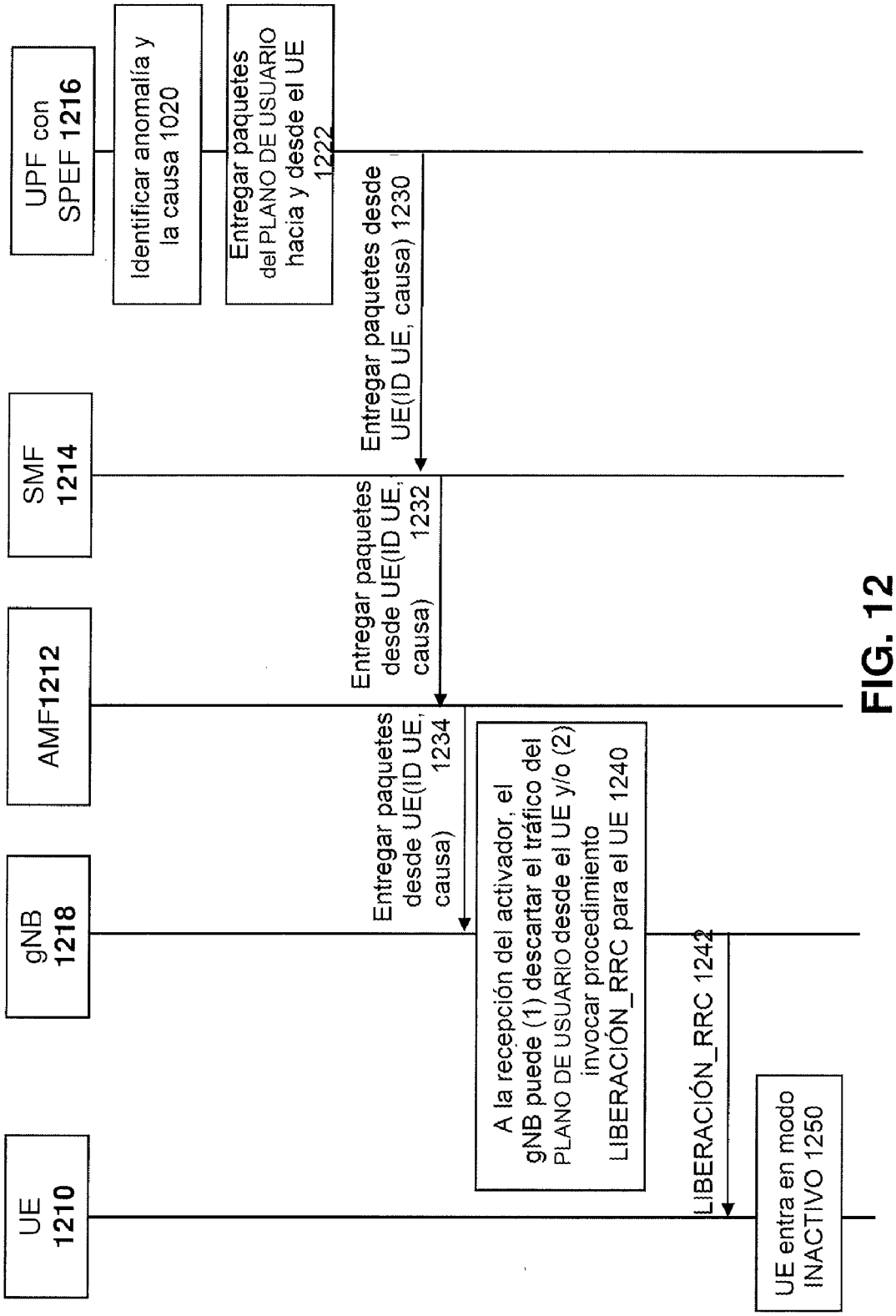
UE 1210
gNB 1218
AMF1212
SMF 1214
UPF con SPEF 1216
Identificar anomalía y la causa 1020
Entregar paquetes del PLANO DE USUARIO hacia y desde el UE 1222
Entregar paquetes desde UE(ID UE, causa) 1230
Entregar paquetes desde UE(ID UE, causa) 1232
Entregar paquetes desde UE(ID UE, causa) 1234
A la recepción del activador, el gNB puede (1) descartar el tráfico del PLANO DE USUARIO desde el UE y/o (2) invocar procedimiento LIBERACIÓN_RRC para el UE 1240
LIBERACIÓN_RRC 1242
UE entra en modo INACTIVO 1250

FIG. 12

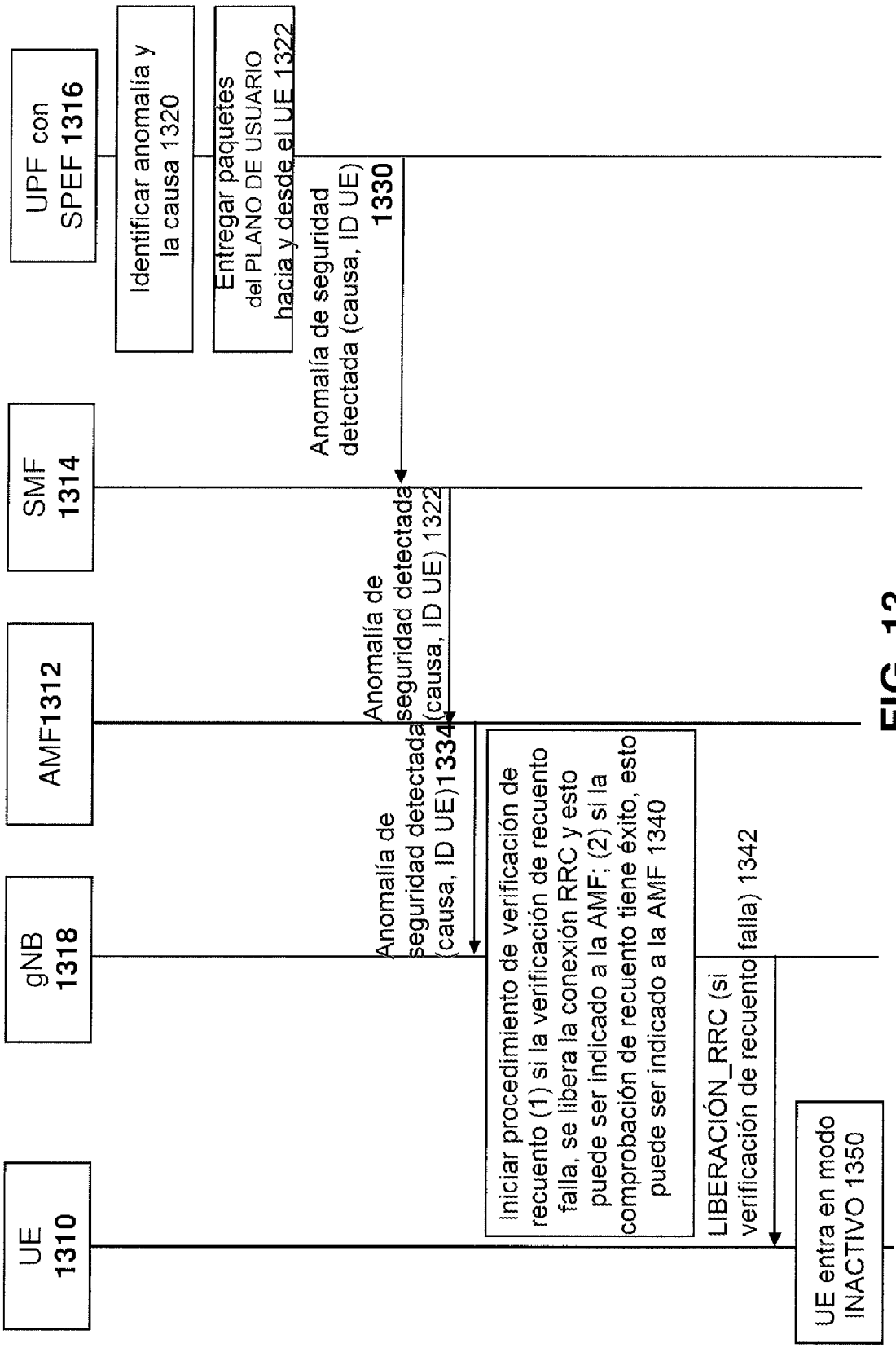
UE 1310
gNB 1318
AMF1312
SMF 1314
UPF con SPEF 1316
Identificar anomalía y la causa 1320
Entregar paquetes del PLANO DE USUARIO hacia y desde el UE 1322
Anomalía de seguridad detectada (causa, ID UE) 1330
Anomalía de seguridad detectada (causa, ID UE) 1322
Anomalía de seguridad detectada (causa, ID UE)1334
Iniciar procedimiento de verificación de recuento (1) si la verificación de recuento falla, se libera la conexión RRC y esto puede ser indicado a la AMF; (2) si la comprobación de recuento tiene éxito, esto puede ser indicado a la AMF 1340
LIBERACIÓN_RRC (si verificación de recuento falla) 1342
UE entra en modo INACTIVO 1350

FIG. 13

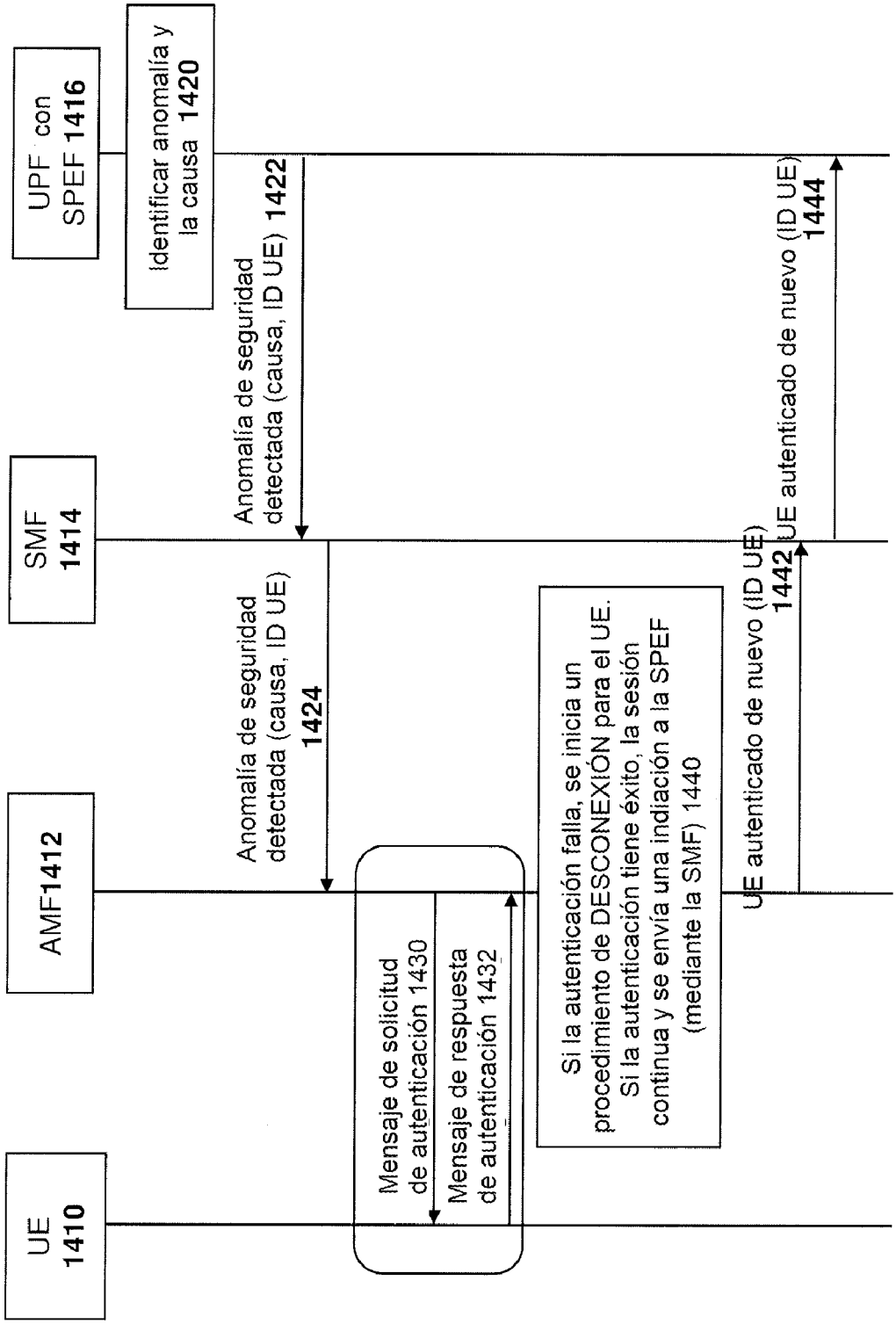
UE 1410
AMF1412
SMF 1414
UPF con SPEF 1416
Identificar anomalía y la causa 1420
Anomalía de seguridad detectada (causa, ID UE) 1422
Anomalía de seguridad detectada (causa, ID UE) 1424
Mensaje de solicitud de autenticación 1430
Mensaje de respuesta de autenticación 1432
Si la autenticación falla, se inicia un procedimiento de DESCONEXIÓN para el UE. Si la autenticación tiene éxito, la sesión continua y se envía una indiación a la SPEF (mediante la SMF) 1440
UE autenticado de nuevo (ID UE) 1442
UE autenticado de nuevo (ID UE) 1444

FIG. 14

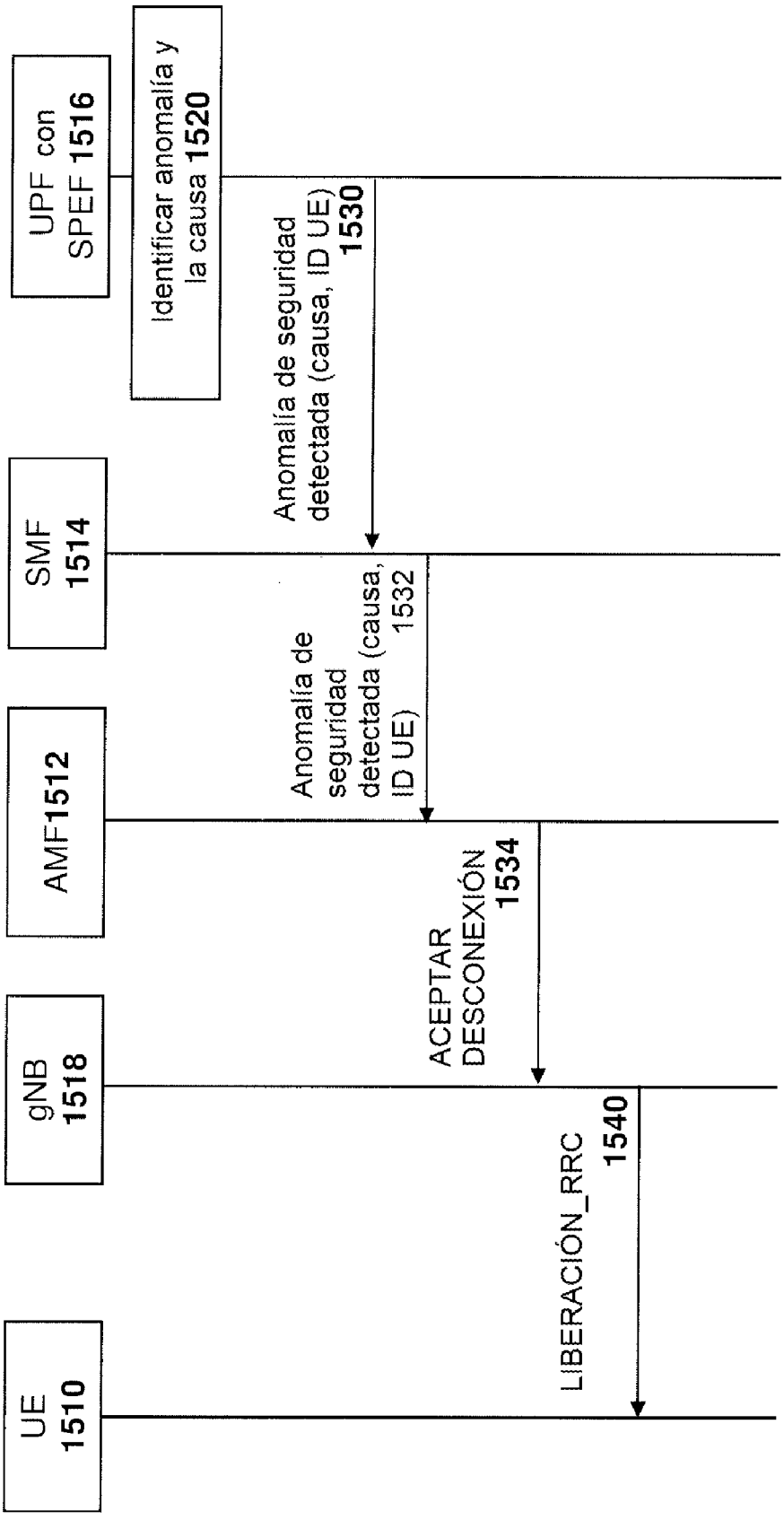
UE 1510
gNB 1518
AMF1512
SMF 1514
UPF con SPEF 1516
Identificar anomalía y la causa 1520
Anomalía de seguridad detectada (causa, ID UE) 1530
Anomalía de seguridad detectada (causa, ID UE) 1532
ACEPTAR DESCONEXIÓN 1534
LIBERACIÓN_RRC 1540

FIG. 15

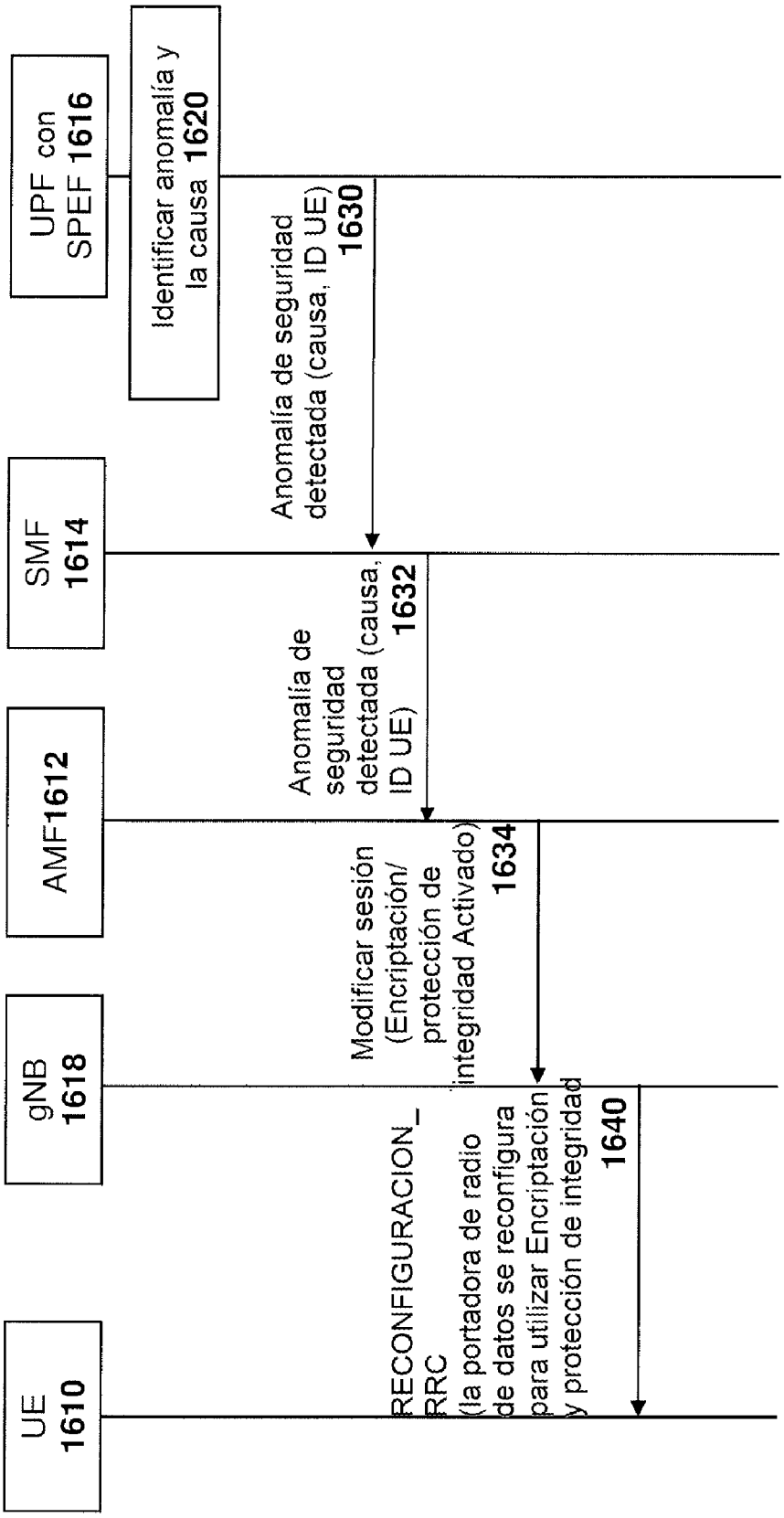
UE 1610
gNB 1618
AMF1612
SMF 1614
UPF con SPEF 1616
Identificar anomalía y la causa 1620
Anomalía de seguridad detectada (causa, ID UE) 1630
Anomalía de seguridad detectada (causa, ID UE) 1632
Modificar sesión (Encriptación/ protección de integridad Activado) 1634
RECONFIGURACION_ RRC (la portadora de radio de datos se reconfigura para utilizar Encriptación y protección de integridad 1640

FIG. 16

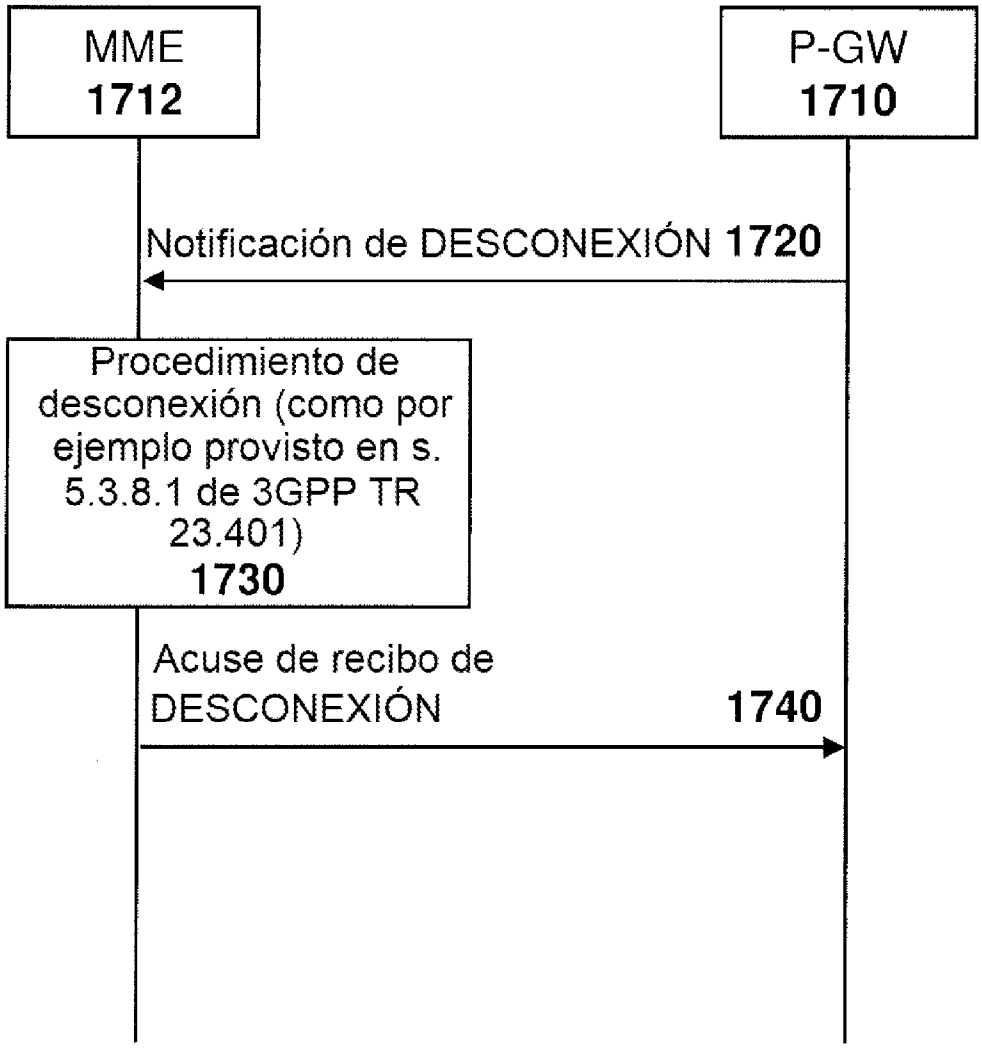
MME
1712
P-GW
1710
Notificación de DESCONEXIÓN 1720
Procedimiento de desconexión (como por ejemplo provisto en s. 5.3.8.1 de 3GPP TR 23.401)
1730
Acuse de recibo de DESCONEXIÓN
1740

FIG. 17

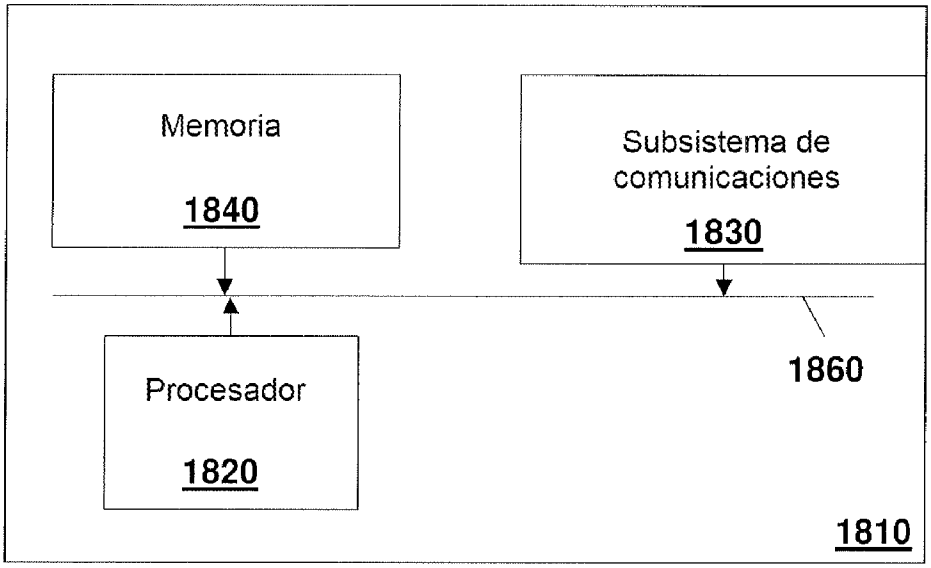
Memoria
1840
Subsistema de comunicaciones
1830
1860
Procesador
1820
1810

FIG. 18

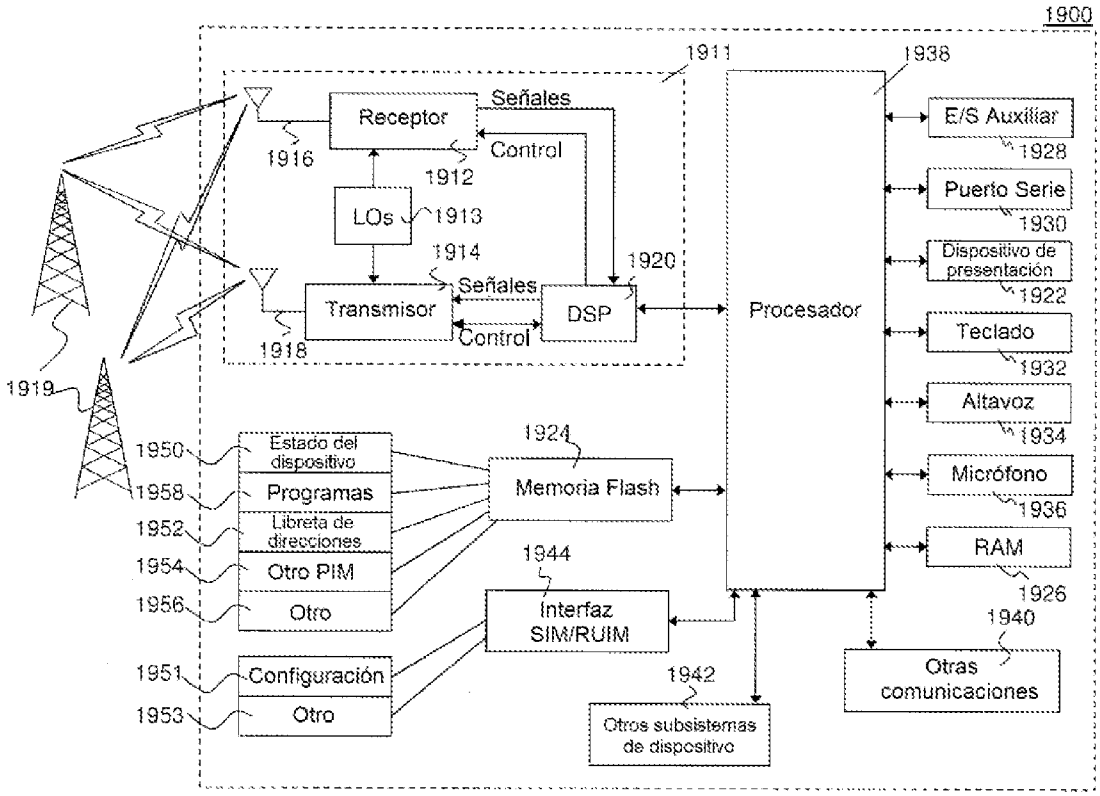
1900
1911
1938
Señales
Receptor
Control
1916
1912
LOs
1913
1914
1920
Señales
Transmisor
DSP
Control
1918
1919
Procesador
E/S Auxiliar
1928
Puerto Serie
1930
Dispositivo de presentación
1922
Teclado
1932
Altavoz
1934
Micrófono
1936
RAM
1926
1940
Otras comunicaciones
1924
Memoria Flash
1944
Interfaz SIM/RUIM
1942
Otros subsistemas de dispositivo
1950
Estado del dispositivo
1958
Programas
1952
Libreta de direcciones
1954
Otro PIM
1956
Otro
1951
Configuración
1953
Otro

FIG. 19