(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 835 056**

(51) Int. CI.:

H04W 12/04 (2009.01)
H04W 12/00 (2009.01)
H04L 29/06 (2006.01)
H04W 4/00 (2008.01)
H04W 12/02 (2009.01)
H04W 4/02 (2008.01)
H04W 68/00 (2009.01)
H04W 40/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **13.06.2016 PCT/US2016/037279**

(87) Fecha y número de publicación internacional: **09.03.2017 WO17039777**

(96) Fecha de presentación y número de la solicitud europea: **13.06.2016 E 16819704 (4)**

(97) Fecha y número de publicación de la concesión europea: **02.09.2020 EP 3320710**

(54) Título: **Arquitectura y seguridad de red con contextos de dispositivo cliente cifrado**

(30) Prioridad:

12.07.2015 US 201562191457 P
09.04.2016 US 201662320506 P
20.05.2016 US 201615160198

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.06.2021

(73) Titular/es:

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

(72) Inventor/es:

LEE, SOO BUM;
HORN, GAVIN BERNARD;
PALANIGOUNDER, ANAND;
ESCOTT, ADRIAN EDWARD y
FACCIN, STEFANO

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Arquitectura y seguridad de red con contextos de dispositivo cliente cifrado

INTRODUCCIÓN

Campo de la divulgación

[0001] Los aspectos de la divulgación se relacionan en general con las comunicaciones de red y, más específicamente, pero no exclusivamente, con una arquitectura de red de Internet de las cosas (IoT).

Antecedentes

[0002] Las capacidades de los dispositivos electrónicos para recopilar, procesar e intercambiar datos continúan creciendo. Además, un número cada vez mayor de estos dispositivos electrónicos cuentan con conectividad de red. Estas capacidades y características permiten que muchos dispositivos electrónicos evolucionen hacia dispositivos de Internet de las cosas (IoT). Dado que el número de estos tipos de dispositivos electrónicos sigue aumentando rápidamente, es posible que las redes no tengan los recursos para soportar adecuadamente estos dispositivos electrónicos.

[0003] Por ejemplo, en un entorno de IoT, una red (por ejemplo, una red LTE) puede necesitar soportar una gran cantidad (por ejemplo, miles de millones) de dispositivos de IoT. Dado que la cantidad de recursos asignados por la red para fines de IoT puede ser limitada, es posible que la red no pueda mantener todos los contextos para este tipo de dispositivos. Además, dado que los dispositivos de IoT pueden estar activos con poca frecuencia y tener recursos limitados, es posible que estos dispositivos no puedan realizar la señalización compleja necesaria para la conectividad.

[0004] El documento US 2014/053241 divulga un sistema para la autentificación de un dispositivo en una red estableciendo un segundo contexto de seguridad entre el dispositivo y un nodo de red de servicio cuando se ha establecido previamente un primer contexto de seguridad, asistido por un servidor de autentificación, basado en un valor aleatorio y un secreto compartido entre un módulo de identidad asociado con el dispositivo y el servicio de autentificación.

[0005] El documento US 2002/184217 divulga sistemas y procedimientos para proporcionar inicio de sesión de usuario y auntentificación sin estado como se describen en un entorno de procesamiento distribuido.

[0006] El documento US 2013/305386 divulga un procedimiento y un terminal de comunicaciones para proteger la seguridad de los datos, una entidad del lado de la red y un terminal de comunicaciones, que pueden garantizar la transmisión segura de datos y mejorar la seguridad de las comunicaciones.

[0007] El documento EP2 804 441 divulga nodos de red, procedimientos y un producto de programa informático para mejorar el funcionamiento de la red de telecomunicaciones inalámbricas.

[0008] Un informe técnico del Proyecto de Asociación de Tercera Generación de fecha 26 de junio de 2014 (33868-C10, Versión 12, XP050917128) divulga un estudio sobre los aspectos de seguridad de las Comunicaciones Tipo Máquina (MTC) y otras mejoras de comunicaciones de aplicaciones de datos móviles.

[0009] El documento US 2013/301611 divulga un procedimiento y un sistema para la transmisión de paquetes de datos de enlace ascendente-descendente en una red celular inalámbrica, durante el estado inactivo del Equipo de Usuario (UE) utilizando la señalización de transmisión sin conexión necesaria para la conectividad.

BREVE EXPLICACIÓN

[0010] A continuación se presenta una breve explicación simplificada de algunos aspectos de la divulgación para proporcionar un entendimiento básico de dichos aspectos. Esta breve explicación no es una visión general exhaustiva de todas las características contempladas de la divulgación y no pretende identificar ni elementos clave ni críticos de todos los aspectos de la divulgación, ni delimitar el alcance de algunos o todos los aspectos de la divulgación. Su único propósito es presentar diversos conceptos de algunos aspectos de la divulgación en una forma simplificada como preludio de la descripción más detallada que se presenta más adelante.

[0011] En un aspecto, se proporciona un procedimiento para un nodo de acceso a la red. El nodo de acceso a la red obtiene una clave para un contexto de dispositivo cliente cifrado asociado con un dispositivo cliente, recibe un primer paquete de datos y el contexto de dispositivo cliente cifrado del dispositivo cliente, obtiene un contexto de seguridad para el dispositivo cliente a partir del contexto de dispositivo cliente cifrado utilizando la clave, descifra y/o verifica el primer paquete de datos basándose en el contexto de seguridad, y reenvía el primer paquete de datos a una red de servicio cuando el descifrado y la verificación son exitosos. En un aspecto, el nodo de acceso

a la red obtiene el contexto de seguridad descifrando el contexto de dispositivo cliente cifrado basándose en la clave, y en el que el contexto de seguridad incluye al menos una clave de cifrado del plano de usuario, una clave de protección de integridad del plano de usuario o combinaciones de las mismas. En un aspecto, el primer paquete de datos se verifica al menos con la clave de protección de integridad del plano de usuario o se descifra con la clave de cifrado del plano de usuario. En un aspecto, el contexto de seguridad incluye una clave de cifrado del plano de usuario y una clave de protección de integridad del plano de usuario. En tal aspecto, el nodo de acceso a la red puede recibir un segundo paquete de datos de un servidor o una pasarela de red de paquetes de datos, cifrar o proteger la integridad del segundo paquete de datos utilizando la clave de cifrado del plano de usuario o la clave de protección de integridad del plano de usuario, y reenviar el segundo paquete de datos al dispositivo cliente. El nodo de acceso a la red puede eliminar el al menos un contexto. El nodo de acceso a la red puede recibir un mensaje que incluye una petición de establecimiento de recursos y al menos uno de los uno o más contextos de dispositivo cliente cifrado desde el dispositivo cliente. El nodo de acceso a la red puede obtener una dirección de red para el dispositivo cliente en respuesta al mensaje. El nodo de acceso a la red puede transmitir una dirección de red al dispositivo cliente. En un aspecto, el nodo de acceso a la red puede recibir un mensaje de petición de liberación de recursos desde el dispositivo cliente y puede transmitir el mensaje de petición de liberación de recursos desde el dispositivo cliente a una pasarela, donde el mensaje de petición de liberación de recursos permite que la pasarela libere uno o más recursos. para el dispositivo cliente. En un aspecto, el uno o más recursos comprenden al menos la dirección de red o un portador para el dispositivo cliente. En otro aspecto, el nodo de acceso a la red puede transmitir un mensaje de petición de liberación de recursos a una pasarela cuando un temporizador expira antes de una transmisión desde el dispositivo cliente a la red o antes de una transmisión desde la red al dispositivo cliente, en el que el mensaje de petición de liberación de recursos permite que la pasarela libere uno o más recursos para el dispositivo cliente. En un aspecto, el uno o más recursos comprenden al menos la dirección de red o un portador para el dispositivo cliente. En un aspecto, el nodo de acceso a la red puede liberar uno o más recursos para el dispositivo cliente cuando un temporizador expira antes de una transmisión desde el dispositivo cliente a la red o antes de una transmisión desde la red al dispositivo cliente. En un aspecto, el uno o más recursos comprenden al menos la dirección de red o un portador para el dispositivo cliente. En otro aspecto, el nodo de acceso a la red puede recibir un mensaje de petición de liberación de recursos desde el dispositivo cliente. En tal aspecto, el nodo de acceso a la red puede liberar uno o más recursos para el dispositivo cliente en respuesta al mensaje de petición de liberación de recursos. En un aspecto, el uno o más recursos comprenden al menos la dirección de red o un portador para el dispositivo cliente.

[0012] En un aspecto, se proporciona un nodo de acceso a la red. El nodo de acceso a la red incluye medios para obtener una clave para un contexto de dispositivo cliente cifrado asociado con un dispositivo cliente, medios para recibir un primer paquete de datos y el contexto de dispositivo cliente cifrado desde el dispositivo cliente, medios para obtener un contexto de seguridad para el dispositivo cliente desde el contexto de dispositivo cliente cifrado que usa la clave, medios para descifrar y/o verificar el primer paquete de datos basándose en el contexto de seguridad, y medios para reenviar el primer paquete de datos a una red de servicios cuando el descifrado y la verificación son exitosos. En un aspecto, los medios para obtener el contexto de seguridad están configurados para descifrar el contexto de dispositivo cliente cifrado basándose en la clave, en el que el contexto de seguridad incluye al menos una clave de cifrado del plano de usuario, una clave de protección de integridad del plano de usuario o combinaciones de las mismas. En un aspecto, el primer paquete de datos se verifica al menos con la clave de protección de integridad del plano de usuario o se descifra con la clave de cifrado del plano de usuario. En un aspecto, el contexto de seguridad incluye una clave de cifrado del plano de usuario y una clave de protección de integridad del plano de usuario. En tal aspecto, el nodo de acceso a la red puede incluir medios para recibir un segundo paquete de datos de un servidor o una pasarela de red de paquetes de datos, medios para cifrar o proteger la integridad del segundo paquete de datos utilizando la clave de cifrado del plano de usuario o la clave de protección de integridad del plano de usuario. y medios para enviar el segundo paquete de datos al dispositivo cliente. En un aspecto, el nodo de acceso a la red incluye medios para eliminar el al menos un contexto. En un aspecto, el nodo de acceso a la red incluye medios para recibir un mensaje que incluye una petición de establecimiento de recursos y al menos uno de los uno o más contextos de dispositivo cliente cifrado desde el dispositivo cliente. En un aspecto, el nodo de acceso a la red incluye medios para obtener una dirección de red para el dispositivo cliente en respuesta al mensaje. En un aspecto, el nodo de acceso a la red incluye medios para transmitir una dirección de red al dispositivo cliente. En un aspecto, el nodo de acceso a la red incluye medios para recibir un mensaje de petición de liberación de recursos desde el dispositivo cliente y medios para transmitir el mensaje de petición de liberación de recursos desde el dispositivo cliente a una pasarela, donde el mensaje de petición de liberación de recursos permite que la pasarela libere uno o más recursos para el dispositivo cliente. En un aspecto, el uno o más recursos comprenden al menos la dirección de red o un portador para el dispositivo cliente. En otro aspecto, el nodo de acceso a la red incluye medios para transmitir un mensaje de petición de liberación de recursos a una pasarela cuando un temporizador expira antes de una transmisión desde el dispositivo cliente a la red o antes de una transmisión desde la red al dispositivo cliente, en el que el mensaje de petición de liberación de recursos permite que la pasarela libere uno o más recursos para el dispositivo cliente. En un aspecto, el uno o más recursos comprenden al menos la dirección de red o un portador para el dispositivo cliente. En un aspecto, el nodo de acceso a la red incluye medios para liberar uno o más recursos para el dispositivo cliente cuando un temporizador expira antes de una transmisión desde el dispositivo cliente a la red o antes de una transmisión desde la red al dispositivo cliente. En un aspecto, el uno o más recursos comprenden al menos la dirección de red o un portador para el dispositivo cliente. En otro aspecto, el nodo de acceso a la red incluye medios

para recibir un mensaje de petición de liberación de recursos desde el dispositivo cliente. En tal aspecto, el nodo de acceso a la red incluye medios para liberar uno o más recursos para el dispositivo cliente en respuesta al mensaje de petición de liberación de recursos. En un aspecto, el uno o más recursos comprenden al menos la dirección de red o un portador para el dispositivo cliente.

[0013] En un aspecto, se proporciona un procedimiento para un dispositivo cliente. El dispositivo cliente transmite una petición para comunicarse con una red, establece un contexto de seguridad para una conexión con la red, en el que el contexto de seguridad incluye al menos un algoritmo de cifrado, una clave de cifrado, un algoritmo de protección de integridad, una clave de protección de integridad o combinaciones. de los mismos, y recibe uno o más contextos de dispositivo cliente cifrado de la red en respuesta a la petición. El dispositivo cliente transmite un mensaje que incluye al menos uno de los uno o más contextos de dispositivo cliente cifrado a la red, en el que el uno o más contextos de dispositivo cliente cifrado permiten la reconstrucción de un contexto en la red para la comunicación con el dispositivo cliente, con el contexto que incluye la información de estado de la red asociada con el dispositivo cliente. En un aspecto, el contexto se elimina en la red. En un aspecto, el dispositivo cliente determina al menos uno de los uno o más contextos de dispositivo cliente cifrado para usar basándose en si el mensaje incluye datos o información de control. En un aspecto, el uno o más contextos de dispositivo cliente cifrado incluyen un primer contexto que se utilizará para la comunicación relacionada con los datos con el dispositivo cliente y un segundo contexto que se utilizará para la comunicación relacionada con el control con el dispositivo cliente. En un aspecto, el uno o más contextos de dispositivo cliente cifrado incluyen al menos uno de un contexto de seguridad, una calidad de servicio para un portador, un identificador de punto final de túnel o combinaciones de los mismos. En un aspecto, la petición comprende una indicación de que el dispositivo cliente está solicitando uno o más contextos de dispositivo cliente cifrado. En un aspecto, la petición comprende una indicación de un servicio que está solicitando el dispositivo cliente. En un aspecto, uno o más contextos de dispositivo cliente cifrado incluyen un contexto de dispositivo cliente cifrado en el plano de usuario y un contexto de dispositivo cliente cifrado en el plano de control. En tal aspecto, el mensaje incluye un primer paquete de datos con el contexto de dispositivo cliente cifrado en el plano de usuario, o un paquete de control con el contexto de dispositivo cliente cifrado en el plano de control. En un aspecto, la clave de cifrado es una clave de cifrado del plano de usuario y la clave de protección de integridad es una clave de protección de integridad del plano de usuario, en la que la clave de cifrado del plano de usuario y la clave de protección de integridad del plano de usuario se mantienen en el dispositivo cliente, y en la que el primer paquete de datos está al menos protegido en integridad con la clave de protección de integridad del plano de usuario o cifrado con la clave de cifrado del plano de usuario. En un aspecto, la transmisión del mensaje que incluye el primer paquete de datos no establece una conexión de control de recursos de radio con un nodo de acceso a la red de la red. En un aspecto, el dispositivo cliente entra en modo inactivo inmediatamente después de transmitir el mensaje que incluye el primer paquete de datos. En un aspecto, el dispositivo cliente recibe un segundo paquete de datos, en el que la recepción del segundo paquete de datos no establece una conexión de control de recursos de radio con un nodo de acceso a la red. En un aspecto, la clave de cifrado es una clave de cifrado del plano de usuario y la clave de protección de integridad es una clave de protección de integridad del plano de usuario, en la que la clave de cifrado del plano de usuario y la clave de protección de integridad del plano de usuario se mantienen en el dispositivo cliente, y en la que la recepción del segundo paquete de datos comprende al menos uno de verificar el segundo paquete de datos con la clave de protección de integridad del plano de usuario o descifrar el segundo paquete de datos con la clave de cifrado del plano de usuario. En un aspecto, el paquete de control es una actualización del área de seguimiento. En un aspecto, el dispositivo cliente recibe un mensaje de búsqueda de la red. En un aspecto, el dispositivo cliente transmite un paquete vacío con el contexto de dispositivo cliente cifrado en el plano de usuario a la red. En un aspecto, el contexto de dispositivo cliente cifrado se recibe de la red como resultado de una auntentificación exitosa con la red. En un aspecto, la auntentificación exitosa con la red no establece un contexto de seguridad de Estrato de Acceso. En un aspecto, el dispositivo cliente almacena uno o más contextos de dispositivo cliente cifrado en un almacenamiento local. En un aspecto, el uno o más contextos de dispositivo cliente cifrado no se descifran en el dispositivo cliente, y el uno o más contextos de dispositivo cliente cifrado se descifran solo mediante un dispositivo de red que generó el uno o más contextos de dispositivo cliente cifrado. En un aspecto, el mensaje incluye además una petición de establecimiento de recursos. En tal aspecto, el dispositivo cliente recibe una dirección de red para el dispositivo cliente en respuesta al mensaje y transmite una pluralidad de paquetes de datos que incluyen la dirección de red a la red. En un aspecto, el dispositivo cliente transmite un mensaje de petición de liberación de recursos a la red, en el que el mensaje de petición de liberación de recursos permite a la red liberar uno o más recursos para el dispositivo cliente. En un aspecto, el contexto se elimina en la red después de recibir uno o más contextos de dispositivo cliente cifrado de la red.

[0014] En un aspecto, se proporciona un dispositivo cliente. El dispositivo cliente incluye medios para transmitir una petición para comunicarse con una red, medio para establecer un contexto de seguridad para una conexión con la red, en el que el contexto de seguridad incluye al menos un algoritmo de cifrado, una clave de cifrado, un algoritmo de protección de integridad, una clave de protección de integridad, o combinaciones de los mismos, medios para recibir uno o más contextos de dispositivo cliente cifrado de la red en respuesta a la petición, y medios para transmitir un mensaje que incluye al menos uno de los uno o más contextos de dispositivo cliente cifrado a la red, en el que uno o más contextos de dispositivo cliente cifrado permiten la reconstrucción de un contexto en la red para la comunicación con el dispositivo cliente, incluyendo el contexto la información de estado de la red asociada con el dispositivo cliente. En un aspecto, el contexto se elimina en la red. En un aspecto, el dispositivo

cliente incluye medios para determinar al menos uno de los uno o más contextos de dispositivo cliente cifrado a utilizar basándose en si el mensaje incluye datos o información de control. En un aspecto, el uno o más contextos de dispositivo cliente cifrado incluyen un primer contexto que se utilizará para la comunicación relacionada con los datos con el dispositivo cliente y un segundo contexto que se utilizará para la comunicación relacionada con el control con el dispositivo cliente. En un aspecto, el uno o más contextos de dispositivo cliente cifrado incluyen al menos uno de un contexto de seguridad, una calidad de servicio para un portador, un identificador de punto final de túnel o combinaciones de los mismos. En un aspecto, la petición comprende una indicación de que el dispositivo cliente está solicitando uno o más contextos de dispositivo cliente cifrado. En un aspecto, la petición comprende una indicación de un servicio que está solicitando el dispositivo cliente. En un aspecto, uno o más contextos de dispositivo cliente cifrado incluyen un contexto de dispositivo cliente cifrado en el plano de usuario y un contexto de dispositivo cliente cifrado en el plano de control. En tal aspecto, el mensaje incluye un primer paquete de datos con el contexto de dispositivo cliente cifrado en el plano de usuario, o un paquete de control con el contexto de dispositivo cliente cifrado en el plano de control. En un aspecto, la clave de cifrado es una clave de cifrado del plano de usuario y la clave de protección de integridad es una clave de protección de integridad del plano de usuario, en la que la clave de cifrado del plano de usuario y la clave de protección de integridad del plano de usuario se mantienen en el dispositivo cliente, y en la que el primer paquete de datos está al menos protegido en integridad con la clave de protección de integridad del plano de usuario o cifrado con la clave de cifrado del plano de usuario. En un aspecto, la transmisión del mensaje que incluye el primer paquete de datos no establece una conexión de control de recursos de radio con un nodo de acceso a la red de la red. En un aspecto, el dispositivo cliente incluye medios para entrar en un modo inactivo inmediatamente después de transmitir el mensaje que incluye el primer paquete de datos. En un aspecto, el dispositivo cliente incluye medios para recibir un segundo paquete de datos, en el que recibir el segundo paquete de datos no establece una conexión de control de recursos de radio con un nodo de acceso a la red. En un aspecto, la clave de cifrado es una clave de cifrado del plano de usuario y la clave de protección de integridad es una clave de protección de integridad del plano de usuario, en la que la clave de cifrado del plano de usuario y la clave de protección de integridad del plano de usuario se mantienen en el dispositivo cliente, y en la que la recepción del segundo paquete de datos comprende al menos uno de verificar el segundo paquete de datos con la clave de protección de integridad del plano de usuario o descifrar el segundo paquete de datos con la clave de cifrado del plano de usuario. En un aspecto, el paquete de control es una actualización del área de seguimiento. En un aspecto, el dispositivo cliente incluye medios para recibir un mensaje de búsqueda desde la red. En un aspecto, el dispositivo cliente incluye medios para transmitir un paquete vacío con el contexto de dispositivo cliente cifrado en el plano de usuario a la red. En un aspecto, el contexto de dispositivo cliente cifrado se recibe de la red como resultado de una auntentificación exitosa con la red. En un aspecto, la auntentificación exitosa con la red no establece un contexto de seguridad de Estrato de Acceso. En un aspecto, el dispositivo cliente incluye medios para almacenar uno o más contextos de dispositivo cliente cifrado en un almacenamiento local. En un aspecto, el uno o más contextos de dispositivo cliente cifrado no se descifran en el dispositivo cliente, y en el que el uno o más contextos de dispositivo cliente cifrado se descifran solo mediante un dispositivo de red que generó el uno o más contextos de dispositivo cliente cifrado. En un aspecto, el mensaje incluye además una petición de establecimiento de recursos. En tal aspecto, el dispositivo cliente incluye medios para recibir una dirección de red para el dispositivo cliente en respuesta al mensaje, y medios para transmitir una pluralidad de paquetes de datos que incluyen la dirección de red a la red. En un aspecto, el dispositivo cliente incluye medios para transmitir un mensaje de petición de liberación de recursos a la red, en el que el mensaje de petición de liberación de recursos permite a la red liberar uno o más recursos para el dispositivo cliente. En un aspecto, el contexto se elimina en la red después de recibir uno o más contextos de dispositivo cliente cifrado de la red.

[0015] En un aspecto, se proporciona un procedimiento para un dispositivo cliente. El dispositivo cliente transmite una petición para comunicarse con una red, establece un contexto de seguridad para una conexión con la red, en el que el contexto de seguridad incluye al menos un algoritmo de cifrado, una clave de cifrado, un algoritmo de protección de integridad, una clave de protección de integridad o combinaciones. de los mismos, y recibe uno o más contextos de dispositivo cliente cifrado de la red en respuesta a la petición. El dispositivo cliente transmite un mensaje que incluye al menos uno de los uno o más contextos de dispositivo cliente cifrado a la red. En un aspecto, el uno o más contextos de dispositivo cliente cifrado permiten la reconstrucción de al menos una parte de un contexto en la red para la comunicación con el dispositivo cliente, incluyendo el contexto información de estado de la red asociada con el dispositivo cliente. En un aspecto, cada uno de los uno o más contextos de dispositivo cliente cifrado está asociado con uno de una pluralidad de servicios proporcionados por la red. En un aspecto, el dispositivo cliente obtiene el mensaje, en el que el mensaje está asociado con un servicio proporcionado por la red. En tal aspecto, el dispositivo cliente determina al menos uno de los uno o más contextos de dispositivo cliente cifrado que está asociado con el servicio, en el que al menos uno de los uno o más contextos de dispositivo cliente cifrado permite la reconstrucción de la parte del contexto de dispositivo cliente que soporta el servicio. Por ejemplo, la pluralidad de servicios puede incluir un servicio de banda ancha móvil, un servicio de comunicaciones de baja latencia ultra fiable (URLLC), un servicio de acceso de alta prioridad, un servicio de acceso tolerante al retardo y/o un servicio de comunicaciones de tipo máquina (MTC). El dispositivo cliente obtiene información de uso asociada con al menos uno de los uno o más contextos de dispositivo cliente cifrado. En un aspecto, la información de uso asociada con al menos uno de los uno o más contextos de dispositivo cliente cifrado indica si la transmisión del mensaje es una transmisión de datos reducida o una transmisión de datos por ráfagas. En un aspecto, la información de uso puede incluir un valor (por ejemplo, un número de índice u otro valor) asociado con el contexto

(o parte de un contexto) que será reconstruido por la red para un tipo de servicio proporcionado por la red. En un aspecto, la parte del contexto se mantiene en la red durante un período de tiempo que se determina basándose en si la transmisión del mensaje es la transmisión de datos reducida o la transmisión de datos por ráfagas. En un aspecto, el mensaje incluye la información de uso. En un aspecto, el uno o más contextos de dispositivo cliente cifrado incluyen un primer contexto de dispositivo cliente cifrado en el plano de usuario que permite la reconstrucción de un primer contexto para el dispositivo cliente en una primera entidad en la red, y un segundo contexto de dispositivo cliente cifrado en el plano de usuario que permite la reconstrucción de un segundo contexto para el dispositivo cliente en una segunda entidad en la red. En tal aspecto, el mensaje incluye al menos el contexto de dispositivo cliente cifrado del primer plano de usuario y el contexto de dispositivo cliente cifrado del segundo plano de usuario.

[0016] En un aspecto, se proporciona un dispositivo cliente. El dispositivo cliente incluye medios para transmitir una petición para comunicarse con una red, medios para establecer un contexto de seguridad para una conexión con la red, en el que el contexto de seguridad incluye al menos un algoritmo de cifrado, una clave de cifrado, un algoritmo de protección de integridad, una clave de protección de integridad, o combinaciones de las mismas, y recibe uno o más contextos de dispositivo cliente cifrado de la red en respuesta a la petición. El dispositivo cliente incluye además medios para transmitir un mensaje que incluye al menos uno de los uno o más contextos de dispositivo cliente cifrado a la red. En un aspecto, el uno o más contextos de dispositivo cliente cifrado permiten la reconstrucción de al menos una parte de un contexto en la red para la comunicación con el dispositivo cliente, incluyendo el contexto información de estado de la red asociada con el dispositivo cliente. En un aspecto, cada uno de los uno o más contextos de dispositivo cliente cifrado está asociado con uno de una pluralidad de servicios proporcionados por la red. En un aspecto, el dispositivo cliente incluye medios para obtener el mensaje, en el que el mensaje está asociado con un servicio proporcionado por la red. En tal aspecto, el dispositivo cliente incluye medios para determinar al menos uno de los uno o más contextos de dispositivo cliente cifrado que está asociado con el servicio, en el que el al menos uno de los uno o más contextos de dispositivo cliente cifrado permite la reconstrucción de la parte del contexto de dispositivo cliente que da soporte al servicio. Por ejemplo, la pluralidad de servicios puede incluir un servicio de banda ancha móvil, un servicio de comunicaciones de baja latencia ultra fiable (URLLC), un servicio de acceso de alta prioridad, un servicio de acceso tolerante al retardo y/o un servicio de comunicaciones de tipo máquina (MTC). En un aspecto, el dispositivo cliente incluye medios para obtener información de uso asociada con al menos uno de los uno o más contextos de dispositivo cliente cifrado. En un aspecto, la información de uso asociada con al menos uno de los uno o más contextos de dispositivo cliente cifrado indica si la transmisión del mensaje es una transmisión de datos reducida o una transmisión de datos por ráfagas. En un aspecto, la información de uso puede incluir un valor (por ejemplo, un número de índice u otro valor) asociado con el contexto (o parte de un contexto) que será reconstruido por la red para un tipo de servicio proporcionado por la red. En un aspecto, la parte del contexto se mantiene en la red durante un período de tiempo que se determina basándose en si la transmisión del mensaje es la transmisión de datos reducida o la transmisión de datos por ráfagas. En un aspecto, el mensaje incluye la información de uso. En un aspecto, el uno o más contextos de dispositivo cliente cifrado incluyen un primer contexto de dispositivo cliente cifrado en el plano de usuario que permite la reconstrucción de un primer contexto para el dispositivo cliente en una primera entidad en la red, y un segundo contexto de dispositivo cliente cifrado en el plano de usuario que permite la reconstrucción de un segundo contexto para el dispositivo cliente en una segunda entidad en la red. En tal aspecto, el mensaje incluye al menos el contexto de dispositivo cliente cifrado del primer plano de usuario y el contexto de dispositivo cliente cifrado del segundo plano de usuario.

[0017] En un aspecto, se proporciona un procedimiento para un dispositivo de red. El dispositivo de red recibe, de un dispositivo cliente, una petición para comunicarse con una red, establece al menos un contexto con el dispositivo cliente, incluyendo el al menos un contexto información de estado de la red asociada con una conexión entre el dispositivo cliente y la red, en el que la información de estado de la red incluye al menos un algoritmo de cifrado, una clave de cifrado, un algoritmo de protección de integridad, una clave de protección de integridad o combinaciones de los mismos, genera uno o más contextos de dispositivo cliente cifrado, en los que uno o más contextos de dispositivo cliente cifrado permiten la reconstrucción del al menos un contexto en la red para la comunicación con el dispositivo cliente, y transmite el uno o más contextos de dispositivo cliente cifrado al dispositivo cliente. En un aspecto, el dispositivo de red determina generar uno o más contextos de dispositivo cliente cifrado, en el que la determinación se basa en al menos uno de la información de uso del contexto de dispositivo cliente cifrado indicada en la petición, una suscripción del dispositivo cliente, una política, o combinaciones de los mismos. En un aspecto, el uno o más contextos de dispositivo cliente cifrado comprenden un primer contexto que se utilizará para la comunicación relacionada con los datos y un segundo contexto que se utilizará para la comunicación relacionada con el control. En un aspecto, el dispositivo de red solicita información de auntentificación de un servidor de abonado doméstico (HSS)/servidor de auntentificación, autorización y contabilidad (AAA), y realiza una auntentificación mutua con el dispositivo cliente. En un aspecto, el dispositivo de red recibe un paquete de control y un contexto de dispositivo cliente cifrado del dispositivo cliente, verifica el contexto de dispositivo cliente cifrado recibido del dispositivo cliente, reconstruye el al menos un contexto del contexto de dispositivo cliente cifrado, procesa el control paquete que usa el al menos un contexto, en el que el procesamiento comprende al menos uno de verificar, descifrar el paquete de control usando el contexto, o combinaciones de los mismos, almacena un identificador temporal para un paquete de enlace descendente para el dispositivo cliente, y reenvía una parte de carga útil del paquete de control a un servidor de aplicaciones o

pasarela de red de paquetes de datos. En un aspecto, la clave de cifrado incluye al menos una clave de cifrado del plano de control, una clave de cifrado del plano de usuario o combinaciones de las mismas, y la clave de protección de integridad incluye al menos una clave de protección de integridad del plano de usuario, una clave de protección de integridad del plano de control o combinaciones de las mismas. En un aspecto, verificar el contexto de dispositivo cliente cifrado incluye determinar si el contexto de dispositivo cliente cifrado ha expirado, generar uno o más contextos nuevos del dispositivo cliente cifrado cuando ha expirado un contexto de dispositivo cliente cifrado anterior y transmitir uno o más contextos de dispositivo cliente cifrado nuevos al dispositivo cliente cuando el contexto de dispositivo cliente cifrado anterior ha expirado. En un aspecto, el dispositivo de red recibe un paquete de control de un segundo dispositivo cliente, solicita un contexto para el segundo dispositivo cliente desde un segundo dispositivo de red, con la petición que incluye un contexto de dispositivo cliente cifrado en el plano de control, recibe el contexto para el segundo dispositivo cliente desde el segundo dispositivo de red, genera un nuevo contexto de dispositivo cliente cifrado y transmite el nuevo contexto de dispositivo cliente cifrado al segundo dispositivo cliente. En un aspecto, verificar el contexto de dispositivo cliente cifrado incluye determinar una clave para verificar el contexto de dispositivo cliente cifrado. En un aspecto, el dispositivo de red elimina el al menos un contexto, recibe un mensaje que incluye una petición de establecimiento de recursos y al menos uno de los uno o más contextos de dispositivo cliente cifrado del dispositivo cliente, obtiene una dirección de red para el dispositivo cliente en respuesta al mensaje y transmite la dirección de red al dispositivo cliente. En un aspecto, el dispositivo de red recibe un mensaje de petición de liberación de recursos desde el dispositivo cliente y transmite el mensaje de petición de liberación de recursos desde el dispositivo cliente a una pasarela, en el que el mensaje de petición de liberación de recursos permite que la pasarela libere uno o más recursos para el dispositivo cliente. En un aspecto, el dispositivo de red transmite un mensaje de petición de liberación de recursos a una pasarela cuando un temporizador expira antes de una transmisión desde el dispositivo cliente a la red o antes de una transmisión desde la red al dispositivo cliente, en el que el mensaje de petición de liberación de recursos permite que la pasarela libere uno o más recursos para el dispositivo cliente.

[0018] En un aspecto, se proporciona un dispositivo de red. El dispositivo de red incluye medios para recibir, desde un dispositivo cliente, una petición para comunicarse con una red, medios para establecer al menos un contexto con el dispositivo cliente, incluyendo el al menos un contexto información de estado de la red asociada con una conexión entre el dispositivo cliente y la red, en la que la información de estado de la red incluye al menos un algoritmo de cifrado, una clave de cifrado, un algoritmo de protección de integridad, una clave de protección de integridad o combinaciones de los mismos, medios para generar uno o más contextos de dispositivo cliente cifrado, en el que el uno o más contextos de dispositivo cliente cifrado permiten la reconstrucción de al menos un contexto en la red para la comunicación con el dispositivo cliente, y medios para transmitir el uno o más contextos de dispositivo cliente cifrado al dispositivo cliente. En un aspecto, el dispositivo de red incluye medios para determinar la generación de uno o más contextos de dispositivo cliente cifrado, en el que la determinación se basa en al menos una de la información de uso del contexto de dispositivo cliente cifrado indicada en la petición, una suscripción del dispositivo cliente, una póliza, o combinaciones de las mismas. En un aspecto, el uno o más contextos de dispositivo cliente cifrado comprenden un primer contexto que se utilizará para la comunicación relacionada con los datos y un segundo contexto que se utilizará para la comunicación relacionada con el control. En un aspecto, el dispositivo de red incluye medios para solicitar información de auntentificación de un servidor de abonado doméstico (HSS)/servidor de auntentificación, autorización y contabilidad (AAA), y medios para realizar la auntentificación mutua con el dispositivo cliente. En un aspecto, el dispositivo de red incluye medios para recibir un paquete de control y un contexto de dispositivo cliente cifrado desde el dispositivo cliente, medios para verificar el contexto de dispositivo cliente cifrado recibido desde el dispositivo cliente, medios para reconstruir el al menos un contexto a partir del contexto de dispositivo cliente cifrado, medios para procesar el paquete de control usando el al menos un contexto, en el que el procesamiento comprende al menos uno de verificar, descifrar el paquete de control usando el contexto, o combinaciones de los mismos, medios para almacenar un identificador temporal para un paquete de enlace descendente para el dispositivo cliente, y medios para enviar una parte de carga útil del paquete de control a un servidor de aplicaciones o pasarela de red de paquetes de datos. En un aspecto, la clave de cifrado incluye al menos una clave de cifrado del plano de control, una clave de cifrado del plano de usuario o combinaciones de las mismas, y la clave de protección de integridad incluye al menos una clave de protección de integridad del plano de usuario, una clave de protección de integridad del plano de control o combinaciones de las mismas. En un aspecto, los medios para verificar el dispositivo cliente cifrado están configurados para determinar si el contexto de dispositivo cliente cifrado ha expirado, generar uno o más contextos nuevos de dispositivos cliente cifrado cuando ha expirado un contexto de dispositivo cliente cifrado anterior y transmitir el uno o más nuevos contextos de dispositivo cliente cifrado al dispositivo cliente cuando el contexto de dispositivo cliente cifrado anterior ha expirado. En un aspecto, el dispositivo de red incluye medios para recibir un paquete de control desde un segundo dispositivo cliente, medios para solicitar un contexto para el segundo dispositivo cliente desde un segundo dispositivo de red, incluyendo la petición un contexto de dispositivo cliente cifrado en el plano de control, medios para recibir el contexto para el segundo dispositivo cliente desde el segundo dispositivo de red, medios para generar un nuevo contexto de dispositivo cliente cifrado, y medios para transmitir el nuevo contexto de dispositivo cliente cifrado al segundo dispositivo cliente. En un aspecto, los medios para verificar el contexto de dispositivo cliente cifrado están configurados para determinar una clave para verificar el contexto de dispositivo cliente cifrado. En un aspecto, el dispositivo de red incluye medios para eliminar el al menos un contexto, medios para recibir un mensaje que incluye una petición de establecimiento de recursos y al menos uno de los uno o más contextos de dispositivo cliente cifrado del dispositivo cliente, medios para obtener un dirección de red para el dispositivo cliente

en respuesta al mensaje, y medios para transmitir la dirección de red al dispositivo cliente. En un aspecto, el dispositivo de red incluye medios para recibir un mensaje de petición de liberación de recursos desde el dispositivo cliente, y medios para transmitir el mensaje de petición de liberación de recursos desde el dispositivo cliente a una pasarela, en el que el mensaje de petición de liberación de recursos permite que la pasarela libere uno o más recursos para el dispositivo cliente. En un aspecto, el dispositivo de red incluye medios para transmitir un mensaje de petición de liberación de recursos a una pasarela cuando un temporizador expira antes de una transmisión desde el dispositivo cliente a la red o antes de una transmisión desde la red al dispositivo cliente, en el que el mensaje de petición de liberación de recursos permite que la pasarela libere uno o más recursos para el dispositivo cliente.

[0019] En un aspecto, se proporciona un procedimiento para un dispositivo de red. El dispositivo de red recibe, de un dispositivo cliente, una petición para comunicarse con una red. El dispositivo de red establece al menos un contexto con el dispositivo cliente, con el al menos un contexto que incluye información de estado de la red asociada con una conexión entre el dispositivo cliente y la red, en el que la información de estado de la red incluye al menos un algoritmo de cifrado, una clave de cifrado, un algoritmo de protección de integridad, una clave de protección de integridad o combinaciones de los mismos. El dispositivo de red puede generar uno o más contextos de dispositivo cliente cifrado. En un aspecto, el uno o más contextos de dispositivo cliente cifrado permiten la reconstrucción de al menos un contexto en la red para la comunicación con el dispositivo cliente. El dispositivo de red puede transmitir uno o más contextos de dispositivo cliente cifrado al dispositivo cliente. El dispositivo de red elimina el al menos un contexto. El dispositivo de red recibe un mensaje del dispositivo cliente, el mensaje incluye al menos uno de los uno o más contextos de dispositivo cliente cifrado e información de uso asociada con el uno o más contextos de dispositivo cliente cifrado. En un aspecto, la información de uso indica si la transmisión del mensaje es una transmisión de datos reducida o una transmisión de datos por ráfagas. En un aspecto, el dispositivo de red puede reconstruir al menos una parte de un contexto basándose en al menos uno de los uno o más contextos de dispositivo cliente cifrado y la información de uso. En un aspecto, el dispositivo de red mantiene al menos una parte de un contexto durante un primer período de tiempo umbral cuando la información de uso indica una transmisión de datos reducida, o un segundo período de tiempo umbral cuando la información de uso indica una transmisión de datos en ráfaga, siendo el segundo período de tiempo umbral mayor que el primer período de tiempo umbral.

[0020] En un aspecto, se proporciona un dispositivo de red. El dispositivo de red incluye medios para recibir, desde un dispositivo cliente, una petición para comunicarse con una red. El dispositivo de red incluye además medios para establecer al menos un contexto con el dispositivo cliente, incluyendo el al menos un contexto información de estado de la red asociada con una conexión entre el dispositivo cliente y la red, en el que la información de estado de la red incluye al menos un algoritmo de cifrado, una clave de cifrado, un algoritmo de protección de integridad, una clave de protección de integridad o combinaciones de los mismos. En un aspecto, el dispositivo de red incluye medios para generar uno o más contextos de dispositivo cliente cifrado. En un aspecto, el uno o más contextos de dispositivo cliente cifrado permiten la reconstrucción de al menos un contexto en la red para la comunicación con el dispositivo cliente. En un aspecto, el dispositivo de red incluye medios para transmitir uno o más contextos de dispositivo cliente cifrado al dispositivo cliente. En un aspecto, el dispositivo de red incluye medios para eliminar el al menos un contexto. En un aspecto, el dispositivo de red incluye medios para recibir un mensaje del dispositivo cliente, incluyendo el mensaje al menos uno de los uno o más contextos de dispositivo cliente cifrado e información de uso asociada con el uno o más contextos de dispositivo cliente cifrado. En un aspecto, la información de uso indica si la transmisión del mensaje es una transmisión de datos reducida o una transmisión de datos por ráfagas. En un aspecto, el dispositivo de red incluye medios para reconstruir al menos una parte de un contexto basándose en al menos uno de los uno o más contextos de dispositivo cliente cifrado y la información de uso. En un aspecto, el dispositivo de red incluye un medio para mantener al menos una parte de un contexto durante un primer período de tiempo umbral cuando la información de uso indica una transmisión de datos reducida, o un segundo período de tiempo umbral cuando la información de uso indica una ráfaga. transmisión de datos, siendo el segundo período de tiempo umbral mayor que el primer período de tiempo umbral.

[0021] En un aspecto, se proporciona un procedimiento para un dispositivo de red. El dispositivo de red obtiene una clave para un contexto de dispositivo cliente cifrado asociado con un dispositivo cliente, recibe un primer paquete de datos y el contexto de dispositivo cliente cifrado del dispositivo cliente, obtiene un contexto de seguridad para el dispositivo cliente a partir del contexto de dispositivo cliente cifrado utilizando el clave, descifra y verifica el primer paquete de datos basándose en el contexto de seguridad, y reenvía el primer paquete de datos a una red de servicio cuando el descifrado y la verificación son exitosos. En un aspecto, el dispositivo de red obtiene el contexto de seguridad descifrando el contexto de dispositivo cliente cifrado basándose en la clave, y en el que el contexto de seguridad incluye al menos una clave de cifrado del plano de usuario, una clave de protección de integridad del plano de usuario o combinaciones de las mismas. En un aspecto, el primer paquete de datos se verifica al menos con la clave de protección de integridad del plano de usuario o se descifra con la clave de cifrado del plano de usuario. En un aspecto, el contexto de seguridad incluye una clave de cifrado del plano de usuario y una clave de protección de integridad del plano de usuario. En tal aspecto, el dispositivo de red recibe un segundo paquete de datos de un servidor o una pasarela de red de paquetes de datos, determina un nodo de acceso a la red al que se reenvía el segundo paquete de datos, agrega un identificador temporal al segundo paquete de datos que permite al nodo de acceso a la red determinar el dispositivo cliente, cifra o protege con integridad el segundo

paquete de datos usando la clave de cifrado del plano de usuario o la clave de protección de integridad del plano de usuario, y reenvía el segundo paquete de datos al dispositivo cliente.

[0022] En un aspecto, se proporciona un dispositivo de red. El dispositivo de red incluye medios para obtener una clave para un contexto de dispositivo cliente cifrado asociado con un dispositivo cliente, medios para recibir un primer paquete de datos y el contexto de dispositivo cliente cifrado desde el dispositivo cliente, medios para obtener un contexto de seguridad para el dispositivo cliente desde el contexto de dispositivo cliente cifrado que utiliza la clave, medios para descifrar y verificar el primer paquete de datos basándose en el contexto de seguridad, y reenvía el primer paquete de datos a una red de servicios cuando el descifrado y la verificación son satisfactorios. En un aspecto, los medios para obtener el contexto de seguridad están configurados para descifrar el contexto de dispositivo cliente cifrado basándose en la clave, y en el que el contexto de seguridad incluye al menos una clave de cifrado del plano de usuario, una clave de protección de integridad del plano de usuario o combinaciones de las mismas. En un aspecto, el primer paquete de datos se verifica al menos con la clave de protección de integridad del plano de usuario o se descifra con la clave de cifrado del plano de usuario. En un aspecto, el contexto de seguridad incluye una clave de cifrado del plano de usuario y una clave de protección de integridad del plano de usuario. En tal aspecto, el dispositivo de red incluye medios para recibir un segundo paquete de datos de un servidor o una pasarela de red de paquetes de datos, medios para determinar un nodo de acceso a la red al que se reenvía el segundo paquete de datos, medios para agregar un identificador temporal al segundo paquete de datos que permite al nodo de acceso a la red determinar el dispositivo cliente, medios para cifrar o proteger la integridad del segundo paquete de datos utilizando la clave de cifrado del plano de usuario o la clave de protección de integridad del plano de usuario, y medios para reenviar el segundo paquete de datos al dispositivo cliente.

[0023] En un aspecto, se proporciona un procedimiento para un nodo de acceso a la red. El nodo de acceso a la red recibe, desde un dispositivo cliente, un primer paquete de datos con una petición para comunicarse con una red, determina un nodo de red al que está destinado el primer paquete de datos, recibe un segundo paquete de datos de una función de red implementada en el nodo de red y determina el dispositivo cliente al que se reenviará el segundo paquete de datos. En un aspecto, el nodo de acceso a la red almacena un identificador temporal para el dispositivo cliente, en el que el identificador temporal es un identificador temporal de la red de radio celular (C-RNTI) y en el que el identificador temporal se almacena durante un período de tiempo predeterminado. En un aspecto, el nodo de acceso a la red agrega el identificador temporal al primer paquete de datos. En un aspecto, el nodo de acceso a la red determina la función de red a la que se reenviará la petición, en el que la determinación está preconfigurada en el nodo de acceso a la red, y reenvía el primer paquete de datos a la función de red. En un aspecto, el nodo de acceso a la red elimina el identificador temporal en el segundo paquete de datos y reenvía el segundo paquete de datos al dispositivo cliente. En un aspecto, el nodo de acceso a la red determina el dispositivo cliente al que se va a enviar el segundo paquete de datos identificando el dispositivo cliente a partir de un identificador temporal en el segundo paquete de datos.

[0024] En un aspecto, se proporciona un nodo de acceso a la red. El nodo de acceso a la red incluye medios para recibir, desde un dispositivo cliente, un primer paquete de datos con una petición para comunicarse con una red, medios para determinar un nodo de red al que está destinado el primer paquete de datos, medios para recibir un segundo paquete de datos desde una función de red implementada en el nodo de red, y medios para determinar el dispositivo cliente al que se enviará el segundo paquete de datos. En un aspecto, el nodo de acceso a la red incluye medios para almacenar un identificador temporal para el dispositivo cliente, en el que el identificador temporal es un identificador temporal de la red de radio celular (C-RNTI), y en el que el identificador temporal se almacena durante un período de tiempo predeterminado. En un aspecto, el nodo de acceso a la red incluye medios para agregar el identificador temporal al primer paquete de datos. En un aspecto, el nodo de acceso a la red incluye medios para determinar la función de red a la que se reenviará la petición, en el que la determinación está preconfigurada en el nodo de acceso a la red, y medios para reenviar el primer paquete de datos a la función de red. En un aspecto, el nodo de acceso a la red incluye medios para eliminar el identificador temporal en el segundo paquete de datos y medios para enviar el segundo paquete de datos al dispositivo cliente. En un aspecto, los medios para determinar el dispositivo cliente al que se reenviará el segundo paquete de datos están configurados para identificar el dispositivo cliente a partir de un identificador temporal en el segundo paquete de datos.

[0025] Estos y otros aspectos de la divulgación se entenderán más completamente tras una revisión de la descripción detallada, que se adjunta a continuación. Otros aspectos, rasgos característicos e implementaciones de la divulgación serán evidentes para los expertos en la técnica tras revisar la siguiente descripción de implementaciones específicas de la divulgación junto con las figuras adjuntas. Si bien los rasgos característicos de la divulgación se pueden analizar en relación con determinadas implementaciones y las figuras siguientes, todas las implementaciones de la divulgación pueden incluir uno o más de los rasgos característicos ventajosos analizados en el presente documento. En otras palabras, si bien se pueden analizar que una o más implementaciones tienen determinados rasgos característicos ventajosos, también se pueden usar uno o más de dichos rasgos característicos de acuerdo con las diversas implementaciones de la divulgación analizadas en el presente documento. De manera similar, si bien determinadas implementaciones se pueden analizar a continuación como implementaciones de dispositivo, sistema o procedimiento, se debe entender que dichas implementaciones se pueden implementar en diversos dispositivos, sistemas y procedimientos.

BREVE DESCRIPCIÓN DE LAS FIGURAS

[0026]

La FIG. 1 es un diagrama de bloques de una arquitectura de red de Internet de las cosas (IoT), de acuerdo con diversos aspectos de la presente divulgación.

La FIG. 2 es un diagrama que ilustra una jerarquía de claves para una arquitectura de red de Internet de IoT, de acuerdo con diversos aspectos de la presente divulgación.

La FIG. 3 es un diagrama que ilustra una jerarquía de claves para cifrar contextos en una arquitectura de red de IoT, de acuerdo con diversos aspectos de la presente divulgación.

La FIG. 4 es un diagrama que ilustra varios contextos (por ejemplo, información de estado de la red) para un dispositivo cliente en una red.

La FIG. 5 es un diagrama de bloques que ilustra un procedimiento de conexión inicial mediante un dispositivo cliente en una arquitectura de red de IoT, de acuerdo con diversos aspectos de la presente divulgación.

La FIG. 6 es un diagrama de flujo de señales de un procedimiento de conexión mediante un dispositivo cliente en una arquitectura de red de IoT de acuerdo con diversos aspectos de la presente divulgación.

La FIG. 7 es un diagrama de bloques que ilustra una transmisión de datos iniciada por un dispositivo cliente en una arquitectura de red de IoT de acuerdo con diversos aspectos de la presente divulgación.

La FIG. 8 es un diagrama de flujo de señales que ilustra una transmisión de datos iniciada por un dispositivo cliente en una arquitectura de red de IoT, de acuerdo con diversos aspectos de la presente divulgación.

la FIG. 9 es un diagrama de flujo de señales de una transmisión de datos terminada en un dispositivo cliente en una arquitectura de red de IoT de acuerdo con varios aspectos de la presente divulgación.

La FIG. 10 es un diagrama de flujo de señales de un establecimiento y liberación de recursos a modo de ejemplo en una arquitectura de red de IoT de acuerdo con varios aspectos de la presente divulgación.

La FIG. 11 es un diagrama de flujo de señales de un procedimiento de conexión a modo de ejemplo mediante un dispositivo cliente en una arquitectura de red de IoT de acuerdo con varios aspectos de la presente divulgación.

La FIG. 12 es un diagrama de flujo de señales de un establecimiento y liberación de recursos a modo de ejemplo en una arquitectura de red de IoT de acuerdo con varios aspectos de la presente divulgación.

La FIG. 13 una pila de protocolos de plano de control para la transmisión de datos de IoT de acuerdo con varios aspectos de la presente divulgación.

La FIG. 14 es un diagrama que ilustra una pila de protocolos de plano de usuario para transmisión de datos de IoT de acuerdo con diversos aspectos de la presente divulgación.

La FIG. 15 es un diagrama de un formato de paquetes de acuerdo con diversos aspectos de la presente divulgación.

La FIG. 16 es un diagrama de flujo de señales de un procedimiento de actualización del área de seguimiento (TAU) en una arquitectura de red de IoT de acuerdo con varios aspectos de la presente divulgación.

La FIG. 17 es una ilustración de un aparato configurado para soportar operaciones relacionadas con la comunicación en una arquitectura de red de IoT de acuerdo con varios aspectos de la presente divulgación.

La FIG. 18 (incluidas las FIG. 18A y 18B) ilustra un procedimiento para comunicarse en una arquitectura de red de IoT de acuerdo con varios aspectos de la presente divulgación.

La FIG. 19 ilustra un procedimiento para comunicarse con una red de acuerdo con varios aspectos de la divulgación.

La FIG. 20 ilustra un procedimiento para comunicarse con una red de acuerdo con varios aspectos de la divulgación.

La FIG. 21 es una ilustración de un aparato configurado para soportar operaciones relacionadas con la comunicación en una arquitectura de red de IoT de acuerdo con varios aspectos de la presente divulgación.

La FIG. 22 (incluidas las FIG. 22A y 22B) ilustra un procedimiento para comunicarse en una arquitectura de red de IoT de acuerdo con varios aspectos de la presente divulgación.

La FIG. 23 (incluidas las FIG. 23A y 23B) ilustra un procedimiento para comunicarse en una arquitectura de red de IoT de acuerdo con varios aspectos de la divulgación.

La FIG. 24 ilustra un procedimiento operativo en un aparato para la comunicación en una arquitectura de red de IoT de acuerdo con varios aspectos de la presente divulgación.

La FIG. 25 (incluidas las FIG. 25A y 25B) ilustra un procedimiento para comunicarse en una arquitectura de red de IoT de acuerdo con varios aspectos de la presente divulgación.

La FIG. 26 (incluidas las FIG. 26A y 26B) ilustra un procedimiento para comunicarse en una arquitectura de red de IoT de acuerdo con varios aspectos de la divulgación.

La FIG. 27 es una ilustración de un aparato configurado para soportar operaciones relacionadas con la comunicación en una arquitectura de red de IoT de acuerdo con varios aspectos de la presente divulgación.

La FIG. 28 ilustra un procedimiento para comunicarse en una arquitectura de red de IoT de acuerdo con diversos aspectos de la presente divulgación.

La FIG. 29 (incluidas las FIG. 29A y 29B) ilustra un procedimiento para comunicarse en una arquitectura de red de IoT de acuerdo con varios aspectos de la divulgación.

DESCRIPCIÓN DETALLADA

[0027] La descripción detallada expuesta a continuación en relación con las figuras adjuntas pretende ser una descripción de diversas configuraciones y no pretende representar las únicas configuraciones en las que se pueden llevar a la práctica los conceptos descritos en el presente documento. La descripción detallada incluye detalles específicos con el propósito de proporcionar un entendimiento exhaustivo de diversos conceptos. Sin embargo, resultará evidente para los expertos en la técnica que estos conceptos se pueden llevar a la práctica sin estos detalles específicos. En algunos casos, se muestran estructuras y componentes bien conocidos en forma de diagrama de bloques para evitar complicar dichos conceptos.

[0028] Como se mencionó anteriormente, en un entorno de IoT, una red (por ejemplo, una red LTE) puede necesitar soportar una gran cantidad (por ejemplo, miles de millones) de dispositivos cliente (también conocidos como dispositivos de Internet de las cosas (IoT)). Un dispositivo cliente puede ser un teléfono celular (por ejemplo, un teléfono inteligente), un ordenador personal (por ejemplo, un ordenador portátil), un dispositivo de videojuegos, un equipo de usuario (UE) o cualquier otro dispositivo adecuado que esté configurado para comunicarse con una red (por ejemplo, una red LTE). Los dispositivos cliente pueden tener diferentes requisitos para la transmisión de datos y la seguridad. Por ejemplo, el tráfico de dispositivos cliente (también conocido como tráfico de IoT) puede tolerar retardos o no requerir una transmisión fiable. En otro ejemplo, el tráfico de dispositivos cliente puede no requerir seguridad de estrato de acceso (AS) para reducir la sobrecarga.

[0029] Convencionalmente, cuando un dispositivo cliente pasa de un modo inactivo a un modo conectado, se puede incurrir en gastos generales de señalización. Por ejemplo, un dispositivo cliente puede establecer una conexión con un nodo de acceso a la red (por ejemplo, Nodo B evolucionado (eNB), estación base o punto de acceso a la red) y el nodo de acceso a la red puede generar un contexto para el dispositivo cliente. Cuando el dispositivo cliente entra posteriormente en un modo inactivo, es posible que el nodo de acceso a la red ya no mantenga el contexto de dispositivo cliente.

[0030] Cuando un dispositivo cliente se conecta a la red, el contexto de dispositivo cliente en la red puede permitir que el dispositivo realice menos señalización para transmitir datos. Por ejemplo, es posible que no se requiera que un dispositivo cliente que esté registrado realice un procedimiento de auntentificación completo. Sin embargo, para lograr tal eficiencia, la red puede usar una cantidad sustancial de recursos para mantener uno o más contextos para cada uno de la gran cantidad de dispositivos cliente conectados.

[0031] Como se usa en el presente documento, el "contexto" de un dispositivo cliente puede referirse a la información de estado de la red asociada con el dispositivo cliente. Por ejemplo, el contexto puede referirse al contexto de seguridad del dispositivo cliente, un contexto asociado con un portador de acceso de radio E-UTRAN (eRAB) y/o un contexto asociado con el portador de radio y el portador S1.

[0032] Dado que la cantidad de recursos (por ejemplo, equipos que implementan funciones de red) asignados por la red para propósitos de IoT puede ser limitada, las funciones de red pueden no ser capaces de mantener todos los contextos (por ejemplo, información de estado de la red) para dispositivos cliente que están activos con poca frecuencia. Por ejemplo, algunos dispositivos cliente pueden activarse cada 10 minutos o más, enviar tráfico (por ejemplo, transmitir datos) a un servidor y entrar inmediatamente en modo de suspensión. Como otro ejemplo, algunos dispositivos cliente pueden enviar una alerta a un servidor cuando ocurre un evento inesperado. Además, algunos dispositivos cliente pueden tener recursos limitados (por ejemplo, memoria, procesador, batería) y pueden no ser adecuados para manejar pilas de protocolos complejos y/o procedimientos de señalización.

[0033] La gestión de la movilidad y la gestión de sesiones de Evolución a largo plazo (LTE) implican demasiados gastos generales para escalar potencialmente miles de millones de dispositivos cliente. Específicamente, la gestión del contexto y el almacenamiento en los nodos de la red pueden plantear desafíos.

[0034] Por ejemplo, cuando el dispositivo cliente se despierta del modo inactivo y entra en un modo conectado, el nodo de acceso a la red establece un nuevo contexto de dispositivo cliente mediante una petición de servicio a una entidad de gestión de movilidad (MME). El contexto de dispositivo cliente puede mantenerse en un MME y una pasarela de servicio (S-GW) mientras el dispositivo cliente está en el estado registrado de Gestión de movilidad del sistema de paquetes evolucionado (EMM). Por consiguiente, para soportar muchos dispositivos cliente, el MME y el S-GW deben estar equipados con una gran cantidad de almacenamiento para mantener contextos para los dispositivos cliente que pueden permanecer en modo inactivo la mayor parte del tiempo.

[0035] Los aspectos divulgados en el presente documento incluyen arquitecturas de red para dispositivos cliente (también denominados dispositivos de Internet de las cosas (IoT)), desde una perspectiva de capa superior, para lograr un consumo de energía de dispositivo cliente ultrabajo, una gran cantidad de dispositivos cliente por célula, un espectro pequeño y/o un área de cobertura aumentada en una célula. Se introducen funciones de red dedicadas para permitir la implementación independiente y eliminar los requisitos de escalabilidad/interfuncionamiento. La seguridad está anclada en una función de red de IoT (también conocida como función de IoT (IoTF)).

[0036] De acuerdo con varios aspectos, la arquitectura puede no permitir ningún contexto de seguridad en un nodo de acceso a la red (por ejemplo, eNB, estación base, punto de acceso a la red) para la transferencia de datos hacia o desde dispositivos cliente. Para evitar afectar la conexión/tráfico PDN de los dispositivos cliente normales, se asignan recursos de red central dedicados para pequeñas transferencias de datos. La red puede asignar recursos de la capa física dedicada (PHY) para el control de acceso para limitar también el tráfico de datos pequeños. El contexto de dispositivo cliente se utiliza para la transferencia de datos pequeños a fin de eliminar el contexto semipersistente del dispositivo cliente en el IoTF durante el estado inactivo. Para lograr una transmisión de datos eficiente para los dispositivos de IoT, las arquitecturas de red divulgadas pueden incluir un IoTF implementado en un dispositivo de red. Dicho IoTF puede incluir un IoTF de plano de control (IoTF-C) y un IoTF de plano de usuario (IoTF-U). En un aspecto, el IoTF-C puede tener funciones similares a una entidad de gestión de movilidad. En un aspecto, el IoTF-U puede ser el ancla de movilidad y seguridad para el tráfico de datos en el plano de usuario. En un aspecto, el IoTF-U puede tener funciones similares a una pasarela de servicio (S-GW) y/o un nodo de acceso a la red (por ejemplo, Nodo B evolucionado (eNB), estación base o punto de acceso a la red).

[0037] Para permitir que las funciones de red (por ejemplo, IoTF-C, IoTF-U) optimicen el uso de recursos para los dispositivos cliente, varios aspectos de las arquitecturas de red de IoT divulgadas pueden implementar un protocolo de diseño en el que el contexto de dispositivo cliente se transporta en un paquete (por ejemplo, paquete IP) y el IoTF (por ejemplo, un IoTF que incluye un IoTF-C y un IoTF-U) crean un contexto de dispositivo cliente de manera oportunista. Esto permite que las funciones de red mantengan una información mínima o nula sobre el estado de la red para el dispositivo cliente y una sobrecarga de señalización mínima o nula. Un dispositivo cliente, por ejemplo, puede ser un teléfono celular (por ejemplo, un teléfono inteligente), un ordenador personal (por ejemplo, un ordenador portátil), un dispositivo de juego, un automóvil, un aparato o cualquier otro dispositivo adecuado que esté configurado para comunicarse con la red. En algunos aspectos, el dispositivo cliente puede denominarse equipo de usuario (UE) o terminal de acceso (AT). En algunos aspectos, un dispositivo cliente como se menciona en el presente documento puede ser un dispositivo móvil o un dispositivo estático. Debe entenderse que las arquitecturas de red de IoT divulgadas y las funciones incluidas en ellas pueden usarse para pequeñas transferencias de datos con dispositivos distintos a los dispositivos cliente. En un aspecto, un dispositivo cliente puede tener un modo nominal en el que establece una conexión y transfiere datos, pero también usa procedimientos como se describe en el presente documento para transferir datos utilizando un contexto de dispositivo cliente.

Arquitectura de red de IoT

[0038] La FIG. 1 es un diagrama de bloques de una arquitectura de red de IoT 100 de acuerdo con diversos aspectos de la presente divulgación. Como se muestra en la FIG. 1, la arquitectura de red de IoT 100 incluye un dispositivo cliente 102 (también denominado dispositivo de IoT), un nodo de acceso a la red 104, un dispositivo de red 105, una red de servicio 110 y un servidor de abonado doméstico (HSS)/auntentificación, autorización y

servidor de contabilidad (AAA) 112. En un aspecto, el nodo de acceso a la red 104 puede ser un eNB, una estación base o un punto de acceso a la red.

[0039] En un aspecto, el dispositivo de red 105 puede incluir uno o más circuitos de procesamiento y/u otro hardware apropiado configurado para implementar un IoTF. En un aspecto de la presente divulgación, un IoTF puede incluir una función de IoT de plano de control (IoTF-C) 106 y una función de IoT de plano de usuario (IoTF-U) 108. Por ejemplo, el IoTF-C 106 puede implementarse en un primer nodo de red 107 y el IoTF-U 108 puede implementarse en un segundo nodo de red 109. De acuerdo con los diversos aspectos divulgados en el presente documento, el término "nodo" puede representar una entidad física, tal como un circuito de procesamiento, un dispositivo, un servidor o una entidad de red, incluida en el dispositivo de red 105. En consecuencia, por ejemplo, un nodo de red puede denominarse dispositivo de nodo de red.

[0040] En un aspecto, el IoTF-C 106 y el IoTF-U 108 pueden implementarse en la misma plataforma de hardware (por ejemplo, un circuito de procesamiento y otros componentes de hardware asociados, como la memoria). En tal aspecto, por ejemplo, el IoTF-C 106 puede implementarse en una primera máquina virtual (por ejemplo, un primer sistema operativo) proporcionada en una plataforma de hardware (por ejemplo, el dispositivo de red 105), y el IoTF-U 108 puede ser implementado en una segunda máquina virtual (por ejemplo, un segundo sistema operativo) proporcionada en la plataforma de hardware.

[0041] Como se muestra en la FIG. 1, el IoTF-C 106 está en comunicación con el nodo de acceso a la red 104 a través de una primera conexión 116 S1, y el IoTF-U 108 está en comunicación con el nodo de acceso a la red 104 a través de una segunda conexión 114 S1. En un aspecto, la red de servicios 110 puede incluir varias entidades, funciones, pasarelas y/o servidores configurados para proporcionar varios tipos de servicios. Por ejemplo, la red de servicio 110 puede incluir una entidad de mensajes cortos (SME) 118, una función de interfuncionamiento de comunicaciones de tipo máquina (MTC-IWF) 120, un servidor IoT122 y/o una pasarela de red de datos de paquetes (PDN) (P-GW) 124. Debe entenderse que la red de servicio 110 descrita en la FIG. 1 sirve como un ejemplo y que, en otros aspectos, la red de servicio 110 puede incluir diferentes tipos de entidades, funciones y/o servidores que los descritos en la FIG. 1.

[0042] En un aspecto de la presente divulgación, el IoTF implementado en el dispositivo de red 105 puede proporcionar funcionalidad de plano de control y plano de usuario. En un aspecto, el IoTF-C 106 maneja la señalización del plano de control (por ejemplo, paquetes que transportan información de control, denominados aquí "paquetes de control") para dispositivos cliente. Por ejemplo, el IoTF-C 106 puede realizar la gestión de la movilidad y la sesión para los dispositivos cliente, realizar la auntentificación y el acuerdo de claves (también denominado procedimiento AKA) con los dispositivos cliente y/o puede crear contextos de seguridad para los dispositivos cliente. En un aspecto, el IoTF-C 106 puede obtener clave(s) del plano de control (CP) 126 para el tráfico del plano de control asociado con el dispositivo cliente 102, clave(s) del plano de usuario (UP) 128 para el tráfico del plano de usuario asociado con el dispositivo cliente 102, y/o una clave de contexto 130 para generar un contexto cifrado para el dispositivo cliente 102. En un aspecto, el IoTF-C 106 puede proporcionar la(s) clave(s) del plano de usuario 128 y/o al menos una de las claves de contexto 130 al IoTF-U 108. En consecuencia, en algunos aspectos, el IoTF-U 108 puede incluir la(s) clave(s) del plano de usuario 128 y/o la(s) clave(s) de contexto 131 proporcionadas por el IoTF-C 106.

[0043] En un aspecto, el IoTF-U 108 puede manejar el tráfico del plano de usuario para los dispositivos cliente. Por ejemplo, el IoTF-U 108 puede obtener una clave de cifrado y una clave de integridad (por ejemplo, un cifrado de cifrado auntentificado con datos asociados (AEAD) utilizando la clave UP128), crear un contexto de dispositivo cliente sobre la marcha, autentificar y descifrar los paquetes de enlace ascendente enviados por dispositivos cliente y reenviar los paquetes de enlace ascendente a un PDN o P-GW (por ejemplo, P-GW 124), cifrar y auntentificar paquetes de enlace descendente para dispositivos cliente conectados y reenviar los paquetes de enlace descendente al nodo de acceso a la red del siguiente salto (por ejemplo, eNB) y/o paquetes de enlace descendente en búfer para dispositivos cliente inactivos durante la búsqueda. En un aspecto, el IoTF-U 108 puede considerarse el ancla de movilidad y seguridad para el tráfico de datos.

Jerarquía de claves a modo de ejemplo para una red de IoT

[0044] La FIG. 2 es un diagrama que ilustra una jerarquía de claves 200 para una arquitectura de red de IoT (por ejemplo, arquitectura de red de IoT 100) de acuerdo con varios aspectos de la presente divulgación. En la FIG. 2, la clave K_{IoT} 202 puede ser una clave secreta almacenada permanentemente en un Módulo de Identidad de Suscriptor (USIM) del Sistema Universal de Telecomunicaciones Móviles (UMTS) de un dispositivo cliente (por ejemplo, el dispositivo cliente 102) y un Centro de auntentificación (AuC) de la red. La clave de integridad (IK) y la clave de cifrado (CK) (mostradas como IK, CK 204 en la FIG. 2) son un par de claves obtenidas en AuC y USIM durante un procedimiento AKA. Con referencia a la FIG. 1, durante el procedimiento AKA, el IoTF-C 106 puede recibir vectores de auntentificación (AV) del servidor HSS/AAA 112 que contienen una clave (mostrada en la FIG.2 como la clave K_{ASME} 206) de una entidad de gestión de seguridad de acceso (ASME). El IoTF-C 106 puede obtener una clave de plano de control (K_{CP}) 208 y una clave de plano de usuario (K_{UP}) 214 a partir de la clave K_{ASME} 206. El IoTF-C 106 puede proporcionar la clave K_{UP} 214 al IoTF-U 108. El IoTF-C 106 puede obtener una clave de

cifrado $K_{IoT-CPenc}$ 210 y una clave de protección de integridad $K_{IoT-CPint}$ 212 a partir de la clave K_{CP} 208. El IoTF-U 108 puede obtener una clave de cifrado $K_{IoT-UPenc}$ 216 y una clave de protección de integridad $K_{IoT-UPint}$ 218 a partir de la clave K_{UP} 214.

[0045] La figura 3 es un diagrama que ilustra una jerarquía de claves 300 para cifrar contextos en una arquitectura de red de IoT (por ejemplo, arquitectura de red de IoT 100) de acuerdo con varios aspectos de la presente divulgación. En un aspecto de la presente divulgación, con referencia a la FIG. 1, el IoTF-C 106 puede generar aleatoriamente una clave de cifrado del contexto de dispositivo cliente del plano de control ($K_{CDC-IoTF-C}$) 304 y una clave de cifrado del contexto de dispositivo cliente del plano de usuario ($K_{CDC-IoTF-U}$) 306 para un dispositivo cliente (por ejemplo, dispositivo cliente 102) basado en una clave de contexto $K_{ODC-IoTF}$ 302 para un dispositivo cliente.

Estados de red a modo de ejemplo de un dispositivo cliente

[0046] En un sistema de comunicación inalámbrica (por ejemplo, una red LTE), los estados de la red se definen para un dispositivo cliente para la gestión de movilidad (por ejemplo, Gestión de movilidad del sistema de paquetes evolucionado (EMM)). Tales estados de red permiten una comunicación eficiente entre un dispositivo cliente y otras entidades de la red.

[0047] En un aspecto de la presente divulgación, un dispositivo cliente (por ejemplo, el dispositivo cliente 102 en la FIG. 1) puede estar en un estado anulado o registrado. Por ejemplo, cuando el dispositivo cliente se encuentra en un estado anulado, el contexto de dispositivo cliente puede almacenarse en el HSS. La red no contiene información de enrutamiento o ubicación válida para el dispositivo cliente, y el dispositivo cliente no es accesible.

[0048] Como otro ejemplo, el dispositivo cliente puede entrar en un estado registrado mediante un registro exitoso en la red. En un aspecto de la presente divulgación, el dispositivo cliente puede realizar tal registro realizando un procedimiento de conexión con la red. En el estado registrado, el dispositivo cliente tiene al menos una conexión PDN activa. El dispositivo cliente también tiene configurado un contexto de seguridad de Sistema de paquetes evolucionado (EPS). Cabe señalar que los estados registrados y eliminados asumen que el dispositivo cliente tiene credenciales (por ejemplo, hay una suscripción disponible en el HSS) para la red.

[0049] Una red de comunicación inalámbrica (por ejemplo, una red LTE) puede incluir además estados de red definidos para un dispositivo cliente para la Gestión de Conexión del Sistema de paquetes evolucionado (ECM). En consecuencia, un dispositivo cliente (por ejemplo, el dispositivo cliente 102 en la FIG. 1) en un estado registrado puede estar en uno de dos estados (también denominados subestados del estado registrado), como un estado inactivo o un estado conectado. En el estado inactivo, no existe ninguna conexión de señalización sin estrato de acceso (NAS) entre el dispositivo cliente y las otras entidades de la red. Además, el dispositivo cliente puede realizar selección/reselección de célula y selección de red móvil terrestre pública (PLMN), y puede que no haya contexto para el dispositivo cliente en la RAN (por ejemplo, nodo de acceso a la red). Además, puede que no haya conexión S1-MME ni S1-U para el dispositivo cliente en estado inactivo.

[0050] En el estado conectado, la ubicación del dispositivo cliente se conoce en el MME con una precisión de un identificador de red de acceso de servicio (por ejemplo, identificador (ID) eNB, ID de estación base o ID de punto de acceso a la red). La movilidad del dispositivo cliente se gestiona mediante un procedimiento de traspaso. En el estado conectado, existe una conexión de señalización entre el dispositivo cliente y el MME. La conexión de señalización puede constar de dos partes: una conexión de control de recursos de radio (RRC) y una conexión S1-MME.

[0051] La FIG. 4 es un diagrama que ilustra estados de red de ejemplo de un dispositivo cliente mantenido en varias entidades en una red 400. Como se muestra en la FIG. 4, la red 400 incluye un dispositivo cliente 402, un nodo de acceso a la red 404 y un núcleo de paquete evolucionado (EPC) 406. Como se muestra además en la FIG. 4, el EPC406 incluye un servidor de abonado doméstico (HSS) 412, una entidad de gestión de movilidad (MME) 408 y una pasarela de red de paquetes de datos (P-GW)/pasarela de servicio (S-GW) 410. En un aspecto de la presente divulgación, la red 400 puede ser una red 4G. En otros aspectos, la red 400 puede ser una red 3G, una red LTE, una red 5G u otra red apropiada.

[0052] Por ejemplo, con referencia a la FIG. 4, el nodo de acceso a la red 404 puede mantener un contexto 414 (también denominado información de estado de la red) para el dispositivo cliente 402 cuando el dispositivo cliente 402 está en un estado conectado. El MME 408 puede mantener un contexto 416 para el dispositivo cliente 402 cuando el dispositivo cliente 402 está en un estado conectado, y un contexto 418 para el dispositivo cliente 402 cuando el dispositivo cliente 402 está en un estado inactivo. El P-GW/S-GW 410 puede mantener un contexto 426 para el dispositivo cliente 402 cuando el dispositivo cliente 402 está en un estado conectado, y un contexto 428 para el dispositivo cliente 402 cuando el dispositivo cliente 402 está en un estado inactivo. El HSS 412 puede mantener un contexto 420 para el dispositivo cliente 402 cuando el dispositivo cliente 402 está en un estado conectado, un contexto 422 para el dispositivo cliente 402 cuando el dispositivo cliente 402 está en un estado inactivo, y un contexto 424 para el dispositivo cliente 402 cuando el dispositivo cliente 402 está en un estado anulado. En un aspecto de la presente divulgación, si la red 400 se implementa como una red 3G, el P-GW/S-GW

410 puede no mantener un contexto para el dispositivo cliente 402 cuando el dispositivo cliente 402 está en estado inactivo.

[0053] En un aspecto de la presente divulgación, se puede generar un contexto de dispositivo cliente cifrado para funciones de red, tales como IoTF-C 106 y IoTF-U 108 en la FIG. 1, para permitir la reconstrucción oportunista de un contexto para un dispositivo cliente (también denominado contexto de dispositivo cliente). Por ejemplo, un contexto de dispositivo cliente cifrado puede permitir que una entidad de red reconstruya el contexto de un dispositivo cliente mientras mantiene mínima o ninguna información de estado de la red para el dispositivo cliente. Por consiguiente, el contexto de dispositivo cliente cifrado puede permitir que una entidad de red reconstruya un contexto de dispositivo cliente sin almacenar o almacenar en memoria caché ninguna información de estado de la red.

[0054] Cabe señalar que en presencia de miles de millones de dispositivos cliente que transmiten tráfico con poca frecuencia, no es deseable que las funciones de red (por ejemplo, el MME 408, el P-GW/S-GW 410) mantengan contextos (incluidos los contextos de seguridad) para dispositivos cliente. Además, el contexto de dispositivo cliente cifrado puede eliminar la sobrecarga de señalización en el nodo de acceso a la red (por ejemplo, eNB, estación base o punto de acceso a la red) durante un traspaso o durante la transición del modo inactivo al modo conectado. El contexto de dispositivo cliente cifrado puede usarse para reducir sustancialmente o eliminar la sobrecarga de señalización, ya que se puede evitar la comunicación con un controlador/MME.

Contexto de dispositivo cliente cifrado del plano de usuario

[0055] En un aspecto de la presente divulgación, se puede generar un contexto de dispositivo cliente cifrado en el plano de usuario (UP) para un dispositivo cliente. Por ejemplo, con referencia a la FIG. 1, el contexto de dispositivo cliente cifrado en el plano de usuario puede usarse en el IoTF-U 108 para transmisiones de datos de enlace ascendente (UL). En un aspecto de la presente divulgación, el contexto de dispositivo cliente cifrado en el plano de usuario puede incluir ID de portador, calidad de servicio (QoS) de portador del sistema de paquetes evolucionado (EPS), un identificador de punto final de túnel S5 (TEID) para un protocolo de tunelización del servicio de radio por paquetes general (GPRS) (GTP-U), una dirección de Protocolo de Internet (IP) P-GW (o información equivalente) a la que IoTF-U 108 reenvía los datos UL, un contexto de seguridad (por ejemplo, un algoritmo de cifrado seleccionado y una tecla de plano de usuario (UP) 128), y cualquier otro parámetro, valor, configuración o característica que pueda necesitar la red para proporcionar un servicio al dispositivo cliente. Por ejemplo, la clave UP 128 puede ser la clave K_{UP} 214, a partir de la cual se puede obtener la clave $K_{IoT\text{-}UPenc}$ 216 y la clave $K_{IoT\text{-}UPint}$ 218. El contexto de dispositivo cliente cifrado en el plano de usuario puede generarse cifrando un contexto del plano de usuario para el dispositivo cliente utilizando una clave secreta del IoTF-U 108, tal como la clave $K_{CDC\text{-}IoTF\text{-}U}$ 306 mostrada en la FIG. 3. En un aspecto de la presente divulgación, la clave secreta de IoTF-U 108, como la clave $K_{CDC\text{-}IoTF\text{-}U}$ 306, puede ser proporcionada por IoTF-C 106. El contexto de dispositivo cliente cifrado en el plano de usuario puede ser descifrado por un IoTF que tiene la clave secreta (por ejemplo, la clave $K_{CDC\text{-}IoTF\text{-}U}$ 306). Por consiguiente, un contexto de dispositivo cliente cifrado en el plano de usuario puede ser descifrado por el IoTF que generó el contexto de dispositivo cliente cifrado en el plano de usuario.

Contexto de dispositivo cliente cifrado del plano de control

[0056] Se puede generar un contexto de dispositivo cliente cifrado en el plano de control (CP) cifrando un contexto de dispositivo cliente en el plano de control para mensajes de control (por ejemplo, paquetes de control o mensajes que incluyen paquetes de control). En un aspecto, el contexto de dispositivo cliente cifrado del plano de control puede incluir un identificador de dispositivo cliente, el contexto de seguridad del dispositivo cliente (por ejemplo, claves del plano de control, como la clave K_{IoT} (equivalente a K_{ASME}), la clave $K_{IoT\text{-}CPenc}$ 210, la clave $K_{IoT\text{-}CPint}$ 212), las capacidades de seguridad del dispositivo cliente (por ejemplo, el algoritmo de cifrado del sistema de paquetes evolucionado (EEA), el algoritmo de integridad del sistema de paquetes evolucionado (EIA)) y/o la información de configuración del siguiente salto (S5/S8). Por ejemplo, la información de configuración del próximo salto puede incluir una dirección de servidor IoT, una dirección P-GW y/o TEID. Por ejemplo, con referencia a la FIG. 1, el contexto de dispositivo cliente del plano de control para los mensajes de control se puede cifrar con una clave secreta del IoTF-C 106, como la clave $K_{CDC\text{-}IoTF\text{-}C}$ 304 mostrada en la FIG. 3. El contexto de dispositivo cliente cifrado en el plano de control puede ser descifrado por un IoTF que tiene la clave secreta (por ejemplo, la clave $K_{CDC\text{-}IoTF\text{-}C}$ 304). Por consiguiente, un contexto de dispositivo cliente cifrado en el plano de control puede ser descifrado por el IoTF que generó el contexto de dispositivo cliente cifrado en el plano de control.

Procedimiento de conexión inicial

[0057] La FIG. 5 es un diagrama de bloques que ilustra un procedimiento de conexión inicial mediante un dispositivo cliente en una arquitectura de red de IoT 500 de acuerdo con diversos aspectos de la presente divulgación. En algunos aspectos, un procedimiento de conexión como se describe en el presente documento también se denomina procedimiento de conexión a la red o procedimiento de registro.

[0058] Como se muestra en la FIG. 5, la arquitectura de red de IoT500 incluye un dispositivo cliente 502 (también denominado dispositivo de IoT), un nodo de acceso a la red 504 (por ejemplo, eNB, estación base, punto de acceso a la red), un dispositivo de red 505, una red de servicio 510, y un servidor de abonado doméstico (HSS)/servidor de auntentificación, autorización y contabilidad (AAA) 512.

[0059] En un aspecto, el dispositivo de red 505 puede incluir uno o más circuitos de procesamiento y/u otro hardware apropiado configurado para implementar un IoTF. Por ejemplo, una IoTF puede incluir una función de IoT en el plano de control (IoTF-C) 506 y una función de IoT en el plano de usuario (IoTF-U) 508. En tal aspecto, el IoTF-C506 puede implementarse en un nodo de red 507 y el IoTF-U508 puede implementarse en un nodo de red 509. En un aspecto, el IoTF-C506 y el IoTF-U508 pueden implementarse en la misma plataforma de hardware, de manera que el IoTF-C506 y el IoTF-U508 representan cada uno un nodo independiente en la arquitectura 500. En tal aspecto, por ejemplo, el IoTF-C506 puede implementarse en una primera máquina virtual (por ejemplo, un primer sistema operativo) proporcionada en una plataforma de hardware (por ejemplo, el dispositivo de red 505) y el IoTF-U508 puede implementarse en una segunda máquina virtual (por ejemplo, un segundo sistema operativo) proporcionada en la plataforma de hardware.

[0060] Como se muestra en la FIG. 5, el IoTF-C506 está en comunicación con el nodo de acceso a la red 504 a través de una primera conexión S1 516, y el IoTF-U508 está en comunicación con el nodo de acceso a la red 504 a través de una segunda conexión S1 514. En un aspecto de la presente divulgación, la red de servicio 510 puede incluir varias entidades, funciones, pasarelas y/o servidores configurados para proporcionar varios tipos de servicios. Por ejemplo, la red de servicio 510 puede incluir una entidad de mensajes cortos (SME) 518, una función de interfuncionamiento de comunicaciones de tipo máquina (MTC-IWF) 520, un servidor IoT522 y/o una pasarela de red de paquetes de datos (PDN) (P- GW) 524. Debe entenderse que la red de servicio 510 descrita en la FIG. 5 sirve como un ejemplo y que, en otros aspectos, la red de servicio 510 puede incluir diferentes tipos de entidades, funciones y/o servidores que los descritos en la FIG. 5.

[0061] Como se muestra en la FIG. 5, el dispositivo cliente 502 puede transmitir una petición de conexión 532 a la red, que puede ser recibida por el nodo de acceso a la red 504. En un aspecto de la presente divulgación, la petición de adjuntar 532 puede proporcionar una o más indicaciones. Por ejemplo, la petición de adjuntar 532 puede indicar que: 1) el dispositivo cliente 502 debe conectarse como un dispositivo IoT, 2) la petición de conexión 532 es una petición para realizar una transferencia de datos pequeña (reducida) y/o 3) el dispositivo cliente 502 está operando en un modo de bajo consumo de energía. La petición de adjuntar 532 puede indicar además el dominio de origen (por ejemplo, ID de HPLMN o nombre de dominio completamente calificado (FQDN)) del cual se debe recuperar la información de auntentificación. El nodo de acceso a la red 504 puede reenviar la petición al IoTF-C506 al que pertenece.

[0062] El IoTF-C506 puede determinar la dirección del servidor HSS/AAA512 a partir de la información del dominio doméstico proporcionada por el dispositivo cliente 502 y puede transmitir una petición 534 de información de auntentificación para el dispositivo cliente 502 al servidor HSS/AAA512. El IoTF-C506 puede recibir la información de auntentificación 535 desde el servidor HSS/AAA512.

[0063] El IoTF-C506 puede realizar una auntentificación mutua (por ejemplo, un procedimiento AKA) con el dispositivo cliente 502. Durante el procedimiento de AKA, el IoTF-C506 puede recibir AV del servidor 512 HSS/AAA a través de la información 535 de auntentificación. Por ejemplo, los AV pueden contener una clave (mostrada en la FIG. 2 como la clave K_{ASME} 206) de una Entidad de gestión de seguridad de acceso (ASME). Por ejemplo, el IoTF-C506 puede proporcionar la clave K_{ASME} 206 al dispositivo cliente 502 a través de la señal 536. Cuando se completa el procedimiento AKA, el IoTF-C506 y el dispositivo cliente 502 pueden obtener la(s) clave(s) CP526, como la clave K_{CP} 208, la clave $K_{IoT\text{-}CPenc}$ 210 y/o la clave $K_{IoT\text{-}CPint}$ 212, y puede obtener la(s) clave(s) UP528, como la clave K_{UP} 214, la clave $K_{IoT\text{-}UPenc}$ 216 y/o la clave $K_{IoT\text{-}UPint}$ 218, a partir de la clave K_{ASME} 206 o de la clave K_{IoT} 202.

[0064] En algunos aspectos, el IoTF-C506 puede transferir la clave K_{UP} 214 y las claves de protección de integridad y cifrado del plano de usuario, como la clave $K_{IoT\text{-}UPenc}$ 216 y la clave $K_{IoT\text{-}UPint}$ 218, al IoTF-U508 a través del mensaje 538.

[0065] En un aspecto de la presente divulgación, el IoTF-C506 puede generar uno o más contextos de dispositivo cliente cifrado para el dispositivo cliente 502 utilizando la clave de contexto 530 para cifrar un contexto de dispositivo cliente. A continuación, el IoTF-C506 puede transmitir el uno o más contextos de dispositivo cliente cifrado al dispositivo cliente 502. Por ejemplo, el IoTF-C506 puede generar un contexto de dispositivo cliente cifrado para el plano de control y un contexto de dispositivo cliente cifrado para el plano de usuario. En tal ejemplo, la clave de contexto 530 puede incluir una primera clave de contexto (por ejemplo, la clave $K_{CDC\text{-}IoTF\text{-}C}$ 304) para generar un contexto de dispositivo cliente cifrado para el plano de control y una segunda clave de contexto (por ejemplo, la clave $K_{CDC\ \text{-}IoTF\text{-}U}$ 306) para generar un contexto de dispositivo cliente cifrado para el plano de usuario. En un aspecto de la presente divulgación, el IoTF-C506 puede proporcionar una o más de las claves de contexto 530 para el IoTF-U508. Por ejemplo, el IoTF-C506 puede transmitir la segunda clave de contexto (por ejemplo, la clave $K_{CDC\text{-}IoTF\text{-}U}$ 306) para generar el contexto de dispositivo cliente cifrado para el plano de usuario al IoTF-U508

a través del mensaje 538. En consecuencia, en algunos aspectos, el IoTF-U508 puede incluir clave(s) de contexto 531 proporcionadas por el IoTF-C506.

[0066] La FIG. 6 es un diagrama de flujo de señales 600 de un procedimiento de conexión a modo de ejemplo mediante un dispositivo cliente en una arquitectura de red de IoT (por ejemplo, arquitectura de red de IoT 100, 500) de acuerdo con varios aspectos de la presente divulgación. Como se muestra en la FIG. 6, el diagrama de flujo de señales 600 incluye un dispositivo cliente 602 (también denominado dispositivo IoT), un nodo de acceso a la red 604 (por ejemplo, eNB, estación base o punto de acceso a la red), un IoTF-C606 implementado en una nodo de red 605, un IoTF-U608 implementado en un nodo de red 607, una red de servicio 609 y un servidor de abonado doméstico (HSS) 610.

[0067] Como se muestra en la FIG. 6, el dispositivo cliente 602 puede transmitir una petición 612 (por ejemplo, una petición de conexión RRC) al nodo de acceso a la red 604 para comunicarse con la red. El dispositivo cliente 602 puede recibir un mensaje de establecimiento de conexión RRC 614, que puede incluir una configuración de portador de radio de señalización (SRB) (por ejemplo, una configuración SRB1 para transmitir mensajes NAS sobre un canal de control dedicado (DCCH)). El dispositivo cliente 602 puede transmitir un mensaje de configuración de conexión RRC completa 616 al nodo de acceso a la red 604. Por ejemplo, el mensaje 616 de establecimiento de conexión RRC completo puede indicar una petición de adjuntar.

[0068] El nodo de acceso a la red 604 puede transmitir un mensaje de dispositivo cliente inicial 618 al IoTF-C606. El IoTF-C606 puede determinar la dirección del servidor HSS610 a partir de la información del dominio doméstico proporcionada por el dispositivo cliente 602, y puede comunicarse 621 con el HSS610. Por ejemplo, el IoTF-C606 puede transmitir una petición de información de auntentificación para el dispositivo cliente 602 al servidor HSS610 y puede recibir la información de auntentificación desde el servidor HSS610.

[0069] Como se muestra en la FIG. 6, el IoTF-C606 puede realizar una auntentificación mutua, tal como un procedimiento AKA620, con el dispositivo cliente 602. Cuando se completa el procedimiento de AKA620, IoTF-C606 y el dispositivo cliente 602 pueden obtener claves del plano de control, como la clave $K_{IoT\text{-}CPenc}$ 210 y/o la clave $K_{IoT\text{-}CPint}$ 212, a partir de la clave K_{ASME} 206 o a partir de la clave K_{IoT} 202. El IoTF-C606 y el dispositivo cliente 602 pueden obtener además claves del plano de usuario, como la clave $K_{IoT\text{-}UPenc}$ 216 y/o la clave $K_{IoT\text{-}UPint}$ 218, a partir de la clave K_{ASME} 206 o de la clave K_{IoT} 202.

[0070] En un aspecto de la presente divulgación, el IoTF-C606 puede generar un contexto de dispositivo cliente cifrado en el plano de control cifrando un contexto del plano de control para el dispositivo cliente 602 utilizando la clave $K_{CDC\text{-}IoTF\text{-}C}$ 304 y/o puede generar un usuario plano de contexto de dispositivo cliente cifrado cifrando un contexto de plano de usuario para el dispositivo cliente 602 utilizando la clave $K_{CDC\text{-}IoTF\text{-}U}$ 306. El IoTF-C606 puede transferir una o más claves (por ejemplo, claves del plano de usuario, como la clave $K_{IoT\text{-}UPenc}$ 216 y/o la clave $K_{IoT\text{-}UPint}$ 218, y/o la clave $K_{CDC\text{-}IoTF\text{-}U}$ 306) al IoTF-U608 mediante el mensaje 622.

[0071] El IoTF-C606 puede transmitir un mensaje 623 de petición de configuración de contexto inicial con un contexto de dispositivo cliente cifrado (por ejemplo, un contexto de dispositivo cliente cifrado en el plano de control y/o un contexto de dispositivo cliente cifrado en el plano de usuario) al dispositivo cliente 602. Por consiguiente, el contexto de dispositivo cliente cifrado puede incluir un contexto de dispositivo cliente asociado con IoTF-C606 y/o IoTF-U608, donde el contexto de dispositivo cliente puede usarse para la transmisión de datos de enlace ascendente mediante el dispositivo cliente 602.

[0072] En un aspecto de la presente divulgación, la clave de cifrado solo es conocida por un IoTF (por ejemplo, el contexto de seguridad del dispositivo cliente puede ser recuperado exclusivamente por el IoTF-C606 y/o IoTF-U608). Por consiguiente, en tal aspecto, la clave de cifrado puede ser la K_{CDC}-IoTF-U 306, que puede ser desconocida para las entidades de red fuera de una IoTF, como un nodo de acceso a la red 604 o un dispositivo cliente 602. En un aspecto de la presente divulgación, cada contexto de dispositivo cliente cifrado corresponde a un portador de radio de datos (DRB).

[0073] El nodo de acceso a la red 604 puede transmitir un mensaje de reconfiguración de la conexión RRC 626 al dispositivo cliente 602. En un aspecto de la presente divulgación, el mensaje de reconfiguración de la conexión RRC 626 puede incluir el contexto de dispositivo cliente cifrado. El dispositivo cliente 602 puede transmitir un mensaje completo de reconfiguración de la conexión RRC 628 al nodo de acceso a la red 604.

[0074] El dispositivo cliente 602 puede transmitir un primer mensaje 630 que incluye un paquete de datos (por ejemplo, un paquete de datos UL) al nodo de acceso a la red 604. El nodo de acceso a la red 604 puede reenviar el paquete de datos a la red de servicio 609 a través del segundo mensaje 632. Por ejemplo, y como se muestra en la FIG. 6, el segundo mensaje 632 puede ser enviado a la red de servicios 609 por el nodo de acceso a la red 604 y el IoTF-U608.

[0075] La red de servicios 609 puede transmitir un tercer mensaje 634 que incluye un paquete de datos (por ejemplo, un paquete de datos DL) al dispositivo cliente 602. Por ejemplo, y como se muestra en la FIG. 6, el tercer

mensaje 634 puede ser reenviado al dispositivo cliente 602 por el IoTF-U608 y el nodo de acceso a la red 604. A continuación, el dispositivo cliente 602 puede hacer la transición 636 al modo inactivo. El nodo de acceso a la red 604, el IoTF-C606 y el IoTF-U608 pueden proceder a eliminar 638 el contexto de dispositivo cliente.

Transferencia de datos de enlace ascendente (UL) de IoT

[0076] La FIG. 7 es un diagrama de bloques que ilustra una transmisión de datos iniciada por un dispositivo cliente en una arquitectura de red de IoT 700, de acuerdo con diversos aspectos de la presente divulgación. Como se muestra en la FIG. 7, la arquitectura de red de IoT700 incluye un dispositivo cliente 702 (también denominado dispositivo de IoT), un nodo de acceso a la red 704 (por ejemplo, eNB, estación base, punto de acceso a la red), un dispositivo de red 705, una red de servicio 710, y un servidor de abonado doméstico (HSS)/servidor de auntentificación, autorización y contabilidad (AAA) 712.

[0077] En un aspecto, el dispositivo de red 705 puede incluir uno o más circuitos de procesamiento y/u otro hardware apropiado configurado para implementar un IoTF. Por ejemplo, una IoTF puede incluir una función de IoT en el plano de control (IoTF-C) 706 y una función de IoT en el plano de usuario (IoTF-U) 708. En tal aspecto, el IoTF-C706 puede implementarse en un nodo de red 707 y el IoTF-U708 puede implementarse en un nodo de red 709. En un aspecto, el IoTF-C706 y el IoTF-U708 pueden implementarse en la misma plataforma de hardware, de modo que cada uno del IoTF-C706 y el IoTF-U708 representa un nodo independiente en la arquitectura 700. En tal aspecto, por ejemplo, el IoTF-C706 puede implementarse en una primera máquina virtual (por ejemplo, un primer sistema operativo) proporcionada en una plataforma de hardware (por ejemplo, el dispositivo de red 705) y el IoTF-U708 puede implementarse en una segunda máquina virtual (por ejemplo, un segundo sistema operativo) proporcionada en la plataforma de hardware.

[0078] En un aspecto de la presente divulgación, la red de servicio 710 puede incluir varias entidades, funciones, pasarelas y/o servidores configurados para proporcionar varios tipos de servicios. Por ejemplo, la red de servicio 710 puede incluir una entidad de mensajes cortos (SME) 718, una función de interfuncionamiento de comunicaciones de tipo máquina (MTC-IWF) 720, un servidor IoT722 y/o una pasarela de red de paquetes de datos (PDN) (P- GW) 724. Debe entenderse que la red de servicio 710 descrita en la FIG. 7 sirve como un ejemplo y que, en otros aspectos, la red de servicio 710 puede incluir diferentes tipos de entidades, funciones y/o servidores que los descritos en la FIG. 7.

[0079] En el aspecto de la FIG. 7, el IoTF-C706 puede haber generado un contexto de dispositivo cliente cifrado para el plano de control y un contexto de dispositivo cliente cifrado para el plano de usuario. En tal aspecto, la(s) clave(s) de contexto 730 pueden incluir una primera clave de contexto (por ejemplo, la clave $K_{CDC\text{-}IoTF\text{-}C}$ 304) para generar un contexto de dispositivo cliente cifrado para el plano de control y una segunda clave de contexto (por ejemplo, la clave $K_{CDC\text{-}IoTF\text{-}U}$ 306) para generar un contexto de dispositivo cliente cifrado para el plano de usuario. Por ejemplo, el IoTF-C706 puede haber transmitido la segunda clave de contexto (por ejemplo, la clave $K_{CDC\text{-}IoTF\text{-}U}$ 306) para generar el contexto de dispositivo cliente cifrado para el plano de usuario al IoTF-U708. Por consiguiente, en tal ejemplo, el IoTF-U708 puede incluir la(s) clave(s) de contexto 731 proporcionadas por el IoTF-C706 como se muestra en la FIG. 7. En el aspecto de la FIG. 7, el dispositivo cliente 702 ha obtenido la(s) clave(s) de CP 726 y la(s) clave(s) UP 728 de la manera descrita anteriormente.

[0080] Como se muestra en la FIG. 7, el dispositivo cliente 702 puede transmitir un primer mensaje 732 que incluye un paquete de datos y un contexto de dispositivo cliente cifrado proporcionado por el IoTF-C706 al nodo de acceso a la red 704. El nodo de acceso a la red 704 puede determinar la dirección del IoTF-U708 a partir del identificador de IoTF-U en el paquete de datos y puede reenviar el paquete de datos al IoTF-U708 mediante un segundo mensaje 734. En un aspecto, el nodo de acceso a la red 704 puede reenviar el paquete de datos al nodo del siguiente salto (por ejemplo, el IoTF-U708) indicado por el dispositivo cliente 702 sin verificar el paquete. El IoTF-U708 puede verificar el contexto de dispositivo cliente cifrado y puede descifrar el contexto de dispositivo cliente cifrado utilizando la clave de contexto 731 (por ejemplo, la clave $K_{CDC\text{-}IoTF\text{-}U}$ 306 para generar el contexto de dispositivo cliente cifrado para el plano de usuario). A continuación, el IoTF-U708 puede reconstruir el contexto de dispositivo cliente basándose en la información descifrada. A continuación, el IoTF-U708 puede descifrar y verificar el paquete de datos con las claves de cifrado e integridad (por ejemplo, clave(s) UP 728).

[0081] La FIG. 8 es un diagrama de flujo de señales 800 que ilustra una transmisión de datos a modo de ejemplo iniciada por un dispositivo cliente en una arquitectura de red de IoT (por ejemplo, arquitectura de red 700 de IoT) de acuerdo con varios aspectos de la presente divulgación. Como se muestra en la FIG. 8, el diagrama de flujo de señal 800 incluye un dispositivo cliente 802 (también denominado dispositivo IoT), un nodo de acceso a la red 804 (por ejemplo, eNB, estación base o punto de acceso a la red), un IoTF-U 806 implementado en un nodo de red 805 y una red de servicio 808. El dispositivo cliente 802 puede transmitir un mensaje de petición de transferencia de datos 810 que incluye un contexto de dispositivo cliente cifrado y un paquete de datos (por ejemplo, un paquete de datos UL) al nodo 804 de acceso a la red. En un aspecto, el mensaje 810 de petición de transferencia de datos puede ser enviado por el dispositivo 802 cliente sin establecer una conexión RRC con el nodo 804 de acceso a la red.

[0082] El nodo 804 de acceso a la red, al recibir el mensaje 810 de petición de transferencia de datos, puede asignar 812 un identificador temporal (TID) para el dispositivo 802 cliente para tráfico potencial de enlace descendente (DL). Por ejemplo, el TID puede ser un identificador temporal de red de radio celular (C-RNTI). El nodo de acceso a la red 804 puede determinar el identificador de IoTF-U incluido en la cabecera del paquete de datos. Un formato de ejemplo del paquete de datos que incluye tal cabecera se analiza aquí con referencia a la FIG. 12.

[0083] El nodo 804 de acceso a la red puede determinar la dirección IP del IoTF-U 806 y puede reenviar el paquete de datos al IoTF-U 806 mediante un primer mensaje 814. Por ejemplo, como parte de los procedimientos de Operaciones y Mantenimiento (OAM), el nodo de acceso a la red 804 puede configurarse con un conjunto de identificadores de IoTF-U y la dirección IP correspondiente, o de forma alternativa, el nodo de acceso a la red 804 puede usar una consulta del sistema de nombre de dominio (DNS) basada en la ID de IoTF-U para determinar la dirección IP de IoTF-U 806. En un aspecto de la presente divulgación, y como se muestra en la FIG. 8, el nodo 804 de acceso a la red puede incluir el TID y el contexto de dispositivo cliente cifrado junto con el paquete de datos en el primer mensaje 814. En un aspecto de la presente divulgación, el TID se almacena en el nodo de acceso a la red 804 durante un intervalo de tiempo predefinido. En tal aspecto, el nodo 804 de acceso a la red puede transmitir el tiempo de expiración del TID a IoTF-U 806 junto con el TID en el primer mensaje 814. El IoTF-U 806 puede descifrar el contexto de dispositivo cliente cifrado y puede reconstruir 816 el contexto de dispositivo cliente (por ejemplo, portador S5). El IoTF-U 806 puede reenviar el paquete de datos a la red de servicio 808 (por ejemplo, el P-GW en la red de servicio 808 u otra entidad en la red de servicio 808) a través de un segundo mensaje 818.

[0084] En respuesta a los datos de enlace ascendente (por ejemplo, el paquete de datos UL en el segundo mensaje 818), el IoTF-U 806 puede recibir un paquete de datos (por ejemplo, un paquete de datos DL) de la red de servicio 808 (por ejemplo, el P-GW en la red de servicios 808 o una entidad correspondiente en la red de servicios 808) a través del tercer mensaje 820. El IoTF-U 806 puede transmitir el paquete de datos recibido al nodo 804 de acceso a la red con el TID en un cuarto mensaje 822. El nodo 804 de acceso a la red puede identificar el dispositivo 802 cliente usando el TID y puede transmitir el paquete de datos al dispositivo 802 cliente en un quinto mensaje 824. El dispositivo cliente 802 puede pasar 826 al modo inactivo basándose en un temporizador preconfigurado. El nodo de acceso a la red 804 y el IoTF-U 806 pueden proceder a eliminar 828 el contexto de dispositivo cliente que se creó sobre la marcha del contexto de dispositivo cliente cifrado.

Transferencia de datos terminada por dispositivo cliente (búsqueda)

[0085] La FIG. 9 es un diagrama de flujo de señales 900 de una transmisión de datos terminada en un dispositivo cliente a modo de ejemplo en una arquitectura de red de IoT (por ejemplo, arquitectura de red de IoT 100) de acuerdo con varios aspectos de la presente divulgación. Como se muestra en la FIG. 9, el diagrama de flujo de señal 900 incluye un dispositivo cliente 902 (también denominado dispositivo IoT), un nodo de acceso a la red 904 (por ejemplo, eNB, estación base, punto de acceso a la red), un IoTF-C906 implementado en un nodo de red 905 y un IoTF-U 908 implementados en un nodo de red 907, un P-GW 910 y un servidor IoT 912. El servidor de IoT 912 puede transmitir un mensaje de enlace descendente (DL) 914 que incluye un paquete de datos DL y un identificador global de IoTF (GIOTFI) al P-GW 910. El P-GW 910 puede localizar el IoTF-U 908 basándose en el GIOTFI y puede reenviar el paquete de datos DL al IoTF-U 908 en un mensaje de reenvío 916. El IoTF-U 908 puede transmitir un mensaje 918 de notificación de datos DL al IoTF-C906. En un aspecto de la presente divulgación, el mensaje 918 de notificación de datos DL puede incluir el paquete de datos DL si el paquete de datos DL es lo suficientemente pequeño para ser transportado en un mensaje de búsqueda. El IoTF-C906 puede transmitir un mensaje de búsqueda 920 a uno o más nodos de acceso a la red (por ejemplo, el nodo de acceso a la red 904). A continuación, el nodo de acceso a la red 904 puede localizar el dispositivo cliente 902 transmitiendo el mensaje de localización 922.

[0086] El dispositivo cliente 902 puede transmitir un mensaje de petición de conexión RRC 924 que incluye un paquete de datos UL al IoTF-U 908. En un aspecto de la presente divulgación, el paquete de datos UL transmitido por el dispositivo cliente 902 puede estar vacío. El nodo de acceso a la red 904 puede asignar 926 un identificador temporal (TID) para el dispositivo cliente 902 para posible tráfico de enlace descendente (DL). Por ejemplo, el TID puede ser un identificador temporal de red de radio celular (C-RNTI). A continuación, el nodo de acceso a la red 904 puede reenviar el paquete de datos UL con el TID y el contexto de dispositivo cliente cifrado al IoTF-U 908 en un mensaje de reenvío 928. El IoTF-U 908 puede almacenar 930 el TID y el ID del nodo de acceso a la red 904.

[0087] El IoTF-U 908 puede transmitir un mensaje de notificación de respuesta del dispositivo cliente 932 al IoTF-C906. En un aspecto de la presente divulgación, el IoTF-U 908 puede transmitir, al dispositivo cliente 902, un mensaje 934 que incluye un paquete de datos DL y el TID para el dispositivo cliente 902 si el IoTF-U 908 no pudo incluir el paquete de datos DL en el mensaje de notificación de datos DL918. El nodo de acceso a la red 904 puede reenviar el paquete de datos DL al dispositivo cliente 902 en un mensaje 936 de reenvío. A continuación, el dispositivo cliente 902 puede hacer la transición 938 al modo inactivo. El nodo de acceso a la red 904 e IoTF-C906 pueden eliminar 940 el contexto de dispositivo cliente.

Establecimiento y liberación de recursos

[0088] La FIG. 10 es un diagrama de flujo de señales 1000 de un establecimiento y liberación de recursos a modo de ejemplo en una arquitectura de red de IoT (por ejemplo, arquitectura de red de IoT 100) de acuerdo con varios aspectos de la presente divulgación. Como se muestra en la FIG. 10, el diagrama de flujo de señal 1000 incluye un dispositivo cliente 1002 (también denominado dispositivo IoT), un IoTF-C 1004 implementado en un nodo de red 1006, un IoTF-U 1008 implementado en un nodo de red 1010 y un P- GW 1012.

[0089] Como se muestra en la FIG. 10, IoTF-C 1004, IoTF-U 1008 y/o P-GW 1012 pueden eliminar 1014 un contexto para el dispositivo cliente 1002. En un aspecto, el IoTF-C 1004 y/o el IoTF-U 1008 pueden eliminar el contexto de dispositivo cliente 1002 después de que el IoTF-C 1006 haya proporcionado un contexto de dispositivo cliente cifrado al dispositivo cliente 1002. Como se muestra en la FIG. 10, el dispositivo cliente 1002 puede transmitir un mensaje de petición de establecimiento de recursos 1016 al IoTF-C 1004. Por ejemplo, el dispositivo cliente 1002 puede transmitir el mensaje de petición de establecimiento de recursos 1016 cuando el dispositivo cliente 1002 debe transmitir transmisiones de datos en ráfagas infrecuentes a la red (por ejemplo, al P-GW 1012). Por ejemplo, una transmisión de datos en ráfaga puede incluir una secuencia de unidades de datos de protocolo (PDU), como paquetes IP. En un aspecto, el mensaje de petición de establecimiento de recursos 1016 puede incluir un contexto de dispositivo cliente cifrado (por ejemplo, un contexto de dispositivo cliente para el plano de control).

[0090] Durante la operación de establecimiento de recursos 1018, el IoTF-C 1004 puede verificar el contexto de dispositivo cliente cifrado desde el dispositivo cliente 1002 y, tras la verificación exitosa, el IoTF-C 1004 puede descifrar el contexto de dispositivo cliente cifrado. A continuación, el IoTF-C 1004 puede reconstruir el contexto para el dispositivo cliente 1002. En un aspecto, el IoTF-U 1008 y el P-GW 1012 también pueden reconstruir el contexto para el dispositivo cliente 1002. En un aspecto, el IoTF-C 1004 puede obtener una dirección de red (por ejemplo, una dirección IP) para el dispositivo cliente 1002 y puede proporcionar la dirección de red al dispositivo cliente 1002 durante la operación de establecimiento de recursos 1018. Como se muestra en la FIG. 10, el dispositivo cliente 1002 puede transmitir datos de enlace ascendente (UL) 1020 al P-GW 1012 a través del IoTF-U 1008. En un aspecto, el dispositivo cliente 1002 puede transmitir los datos UL1020 en una o más PDU que incluyen la dirección de red del dispositivo cliente 1002.

[0091] En un aspecto, el dispositivo cliente 1002 puede determinar que no hay más transmisiones de datos que realizar a la red. En tal aspecto, el dispositivo cliente 1002 puede transmitir opcionalmente un mensaje 1 1022 de petición de liberación de recursos al IoTF-C 1004. A continuación, el dispositivo cliente 1002 puede entrar en el modo inactivo 1024. El IoTF-C 1004 puede transmitir el mensaje de petición de liberación de recursos 1 1022 al P-GW 1012. En un aspecto, el mensaje de petición de liberación de recursos 1 1022 permite que la P-GW 1012 liberar uno o más recursos para el dispositivo cliente 1002. Por ejemplo, el uno o más recursos pueden incluir la dirección de red asignada al dispositivo cliente 1002 (por ejemplo, para permitir la reasignación de esa dirección de red), un portador para el dispositivo cliente 1002 y/u otros recursos para el dispositivo cliente 1002. A continuación, el IoTF-C 1004 y el IoTF-U 1008 pueden eliminar 1030 el contexto de dispositivo cliente 1002. En otro aspecto, el IoTF-C 1004 y/o el IoTF-U 1008 pueden iniciar un temporizador 1026 después de que se reciban los datos UL1020 en el IoTF-U 1008. Si el temporizador 1026 expira antes de recibir nuevos datos UL (por ejemplo, datos UL adicionales posteriores a los datos UL1020) desde el dispositivo cliente 1002 y/o antes de transmitir cualquier dato de enlace descendente (DL) al dispositivo cliente 1002, el IoTF -C 1004 y/o IoTF-U 1008 pueden determinar que el dispositivo cliente 1002 está en el modo inactivo 1024. En tal escenario, el IoTF-C 1004 puede transmitir un mensaje de petición de liberación de recursos 2 1028 al P-GW 1012. En un aspecto, el mensaje de petición de liberación de recursos 2 1028 permite que la P-GW 1012 liberar uno o más recursos para el dispositivo cliente 1002. Por ejemplo, el uno o más recursos pueden incluir la dirección de red asignada al dispositivo cliente 1002 (por ejemplo, para permitir la reasignación de esa dirección de red), un portador para el dispositivo cliente 1002 y/u otros recursos para el dispositivo cliente 1002. A continuación, el IoTF-C 1004 y el IoTF-U 1008 pueden eliminar 1030 el contexto de dispositivo cliente 1002. En un aspecto, el temporizador 1026 puede ser reiniciado por el IoTF-C 1004 y/o el IoTF-U 1008 cuando se recibe una nueva transmisión de datos UL (por ejemplo, datos UL adicionales posteriores a los datos UL1020) en el IoTF-U 1008 desde el dispositivo cliente 1002 antes de la expiración del temporizador 1026.

[0092] La FIG. 11 es un diagrama de flujo de señales 1100 de un procedimiento de conexión a modo de ejemplo por un dispositivo cliente en una arquitectura de red de IoT de acuerdo con varios aspectos de la presente divulgación. Como se muestra en la FIG. 11, el diagrama de flujo de señal 1100 incluye un dispositivo cliente 1102 (también denominado dispositivo IoT), una función de plano de usuario 1112 implementada en un nodo de acceso a la red 1104 (por ejemplo, eNB, estación base o punto de acceso a la red), un control función de plano 1114 implementada en un nodo de red 1106, una red de servicio 1108 y un servidor de abonado doméstico (HSS) 1110.

[0093] Como se muestra en la FIG. 11, el dispositivo cliente 1102 puede transmitir una petición 1116 (por ejemplo, una petición de conexión RRC) al nodo de acceso a la red 1104 para comunicarse con la red. El dispositivo cliente 1102 puede recibir un mensaje de establecimiento de conexión RRC 1118, que puede incluir una configuración de portador de radio de señalización (SRB) (por ejemplo, una configuración SRB1 para transmitir mensajes NAS sobre un canal de control dedicado (DCCH)). El dispositivo cliente 1102 puede transmitir un mensaje de configuración

de conexión RRC completa 1120 al nodo de acceso a la red 1104. Por ejemplo, el mensaje 1120 de establecimiento de conexión RRC completo puede indicar una petición de adjuntar.

[0094] El nodo de acceso a la red 1104 puede transmitir un mensaje 1122 del dispositivo cliente inicial al nodo de red 1106. La función de plano de control 1114 puede determinar la dirección del servidor HSS1110 a partir de la información del dominio doméstico proporcionada por el dispositivo cliente 1102, y puede comunicarse 1126 con el HSS1110. Por ejemplo, la función de plano de control 1114 puede transmitir una petición de información de auntentificación para el dispositivo cliente 1102 al servidor HSS1110 y puede recibir la información de auntentificación desde el servidor HSS1110.

[0095] Como se muestra en la FIG. 11, la función de plano de control 1114 puede realizar una auntentificación mutua, tal como un procedimiento AKA1124, con el dispositivo cliente 1102. Cuando se completa el procedimiento AKA 1124, la función del plano de control 1114 y el dispositivo cliente 1102 pueden obtener claves del plano de control, como la clave $K_{IoT\text{-}CPenc}$ 210 y/o la clave $K_{IoT\text{-}CPint}$ 212, a partir de la clave K_{ASME} 206 o a partir de la clave K_{IoT} 202. La función del plano de control 1114 y el dispositivo cliente 1102 pueden obtener además claves del plano de usuario, como la clave $K_{IoT\text{-}UPenc}$ 216 y/o la clave $K_{IoT\text{-}UPint}$ 218, a partir de la clave K_{ASME} 206 o de la clave K_{IoT} 202.

[0096] En un aspecto de la presente divulgación, la función de plano de control 1114 puede generar un contexto de dispositivo cliente cifrado en el plano de control cifrando un contexto de plano de control para el dispositivo cliente 1102 utilizando la clave $K_{CDC\text{-}IoTF\text{-}C}$ 304 y/o puede generar un contexto de dispositivo cliente cifrado de plano de usuario cifrando un contexto de plano de usuario para el dispositivo cliente 1102 usando la clave $K_{CDC\text{-}IoTF\text{-}U}$ 306.

[0097] La función de plano de control 1114 puede transmitir un mensaje 1128 de petición de configuración de contexto inicial con un contexto de dispositivo cliente cifrado (por ejemplo, un contexto de dispositivo cliente cifrado de plano de control y/o un contexto de dispositivo cliente cifrado de plano de usuario) al dispositivo cliente 1102. Por consiguiente, el contexto de dispositivo cliente cifrado puede incluir un contexto de dispositivo cliente asociado con la función de plano de control 1114 y/o la función de plano de usuario 1112, donde el contexto de dispositivo cliente puede usarse para la transmisión de datos de enlace ascendente mediante el dispositivo cliente 1102. En un aspecto, la función del plano de control 1114 puede transferir una o más claves (por ejemplo, claves del plano de usuario, como la clave $K_{IoT\text{-}UPenc}$ 216 y/o la clave $K_{IoT\text{-}UPint}$ 218, y/o la clave $K_{CDC\text{-}IoTF\text{-}U}$ 306) a la función del plano de usuario 1112 a través del mensaje 1128.

[0098] En un aspecto de la presente divulgación, la clave de cifrado solo es conocida por la función del plano de usuario 1112 y/o la función del plano de control 1114 (por ejemplo, el contexto de seguridad del dispositivo cliente puede ser recuperado exclusivamente mediante la función del plano de usuario 1112 y/o el función de plano de control 1114). En tal aspecto, por ejemplo, la clave de cifrado puede ser la K_{CDC} -IoTF-U 306. En un aspecto de la presente divulgación, cada contexto de dispositivo cliente cifrado corresponde a un portador de radio de datos (DRB).

[0099] El nodo de acceso a la red 1104 puede transmitir un mensaje de reconfiguración de la conexión RRC 1130 al dispositivo cliente 1102. En un aspecto de la presente divulgación, el mensaje de reconfiguración de la conexión RRC 1130 puede incluir el contexto de dispositivo cliente cifrado. El dispositivo cliente 1102 puede transmitir un mensaje completo de reconfiguración de la conexión RRC 1132 al nodo de acceso a la red 1104.

[0100] El dispositivo cliente 1102 puede transmitir un primer mensaje 1134 que incluye un paquete de datos (por ejemplo, un paquete de datos UL) al nodo de acceso a la red 1104. La función del plano de usuario 1112 implementada en el nodo de acceso a la red 1104 puede reenviar el paquete de datos a la red de servicios 1108. La red de servicios 1108 puede transmitir un segundo mensaje 1136 que incluye un paquete de datos (por ejemplo, un paquete de datos DL) al dispositivo cliente 1102. Por ejemplo, y como se muestra en la FIG. 11, el segundo mensaje 1136 puede ser enviado al dispositivo cliente 1102 mediante la función de plano de usuario 1112 en el nodo de acceso a la red 1104. A continuación, el dispositivo cliente 1102 puede hacer la transición 1138 al modo inactivo. El nodo de acceso a la red 1104 y el nodo de red 1106 pueden proceder a eliminar 1140 el contexto de dispositivo cliente.

[0101] La FIG. 12 es un diagrama de flujo de señal 1200 de un establecimiento y liberación de recursos a modo de ejemplo en una arquitectura de red de IoT de acuerdo con diversos aspectos de la presente divulgación. Como se muestra en la FIG. 12, el diagrama de flujo de señales 1200 incluye un dispositivo cliente 1202 (también denominado dispositivo IoT), una función de plano de usuario 1210 implementada en un nodo de acceso a la red 1204, una función de plano de control 1212 implementada en un nodo de red 1206, y un P-GW 1208. En un aspecto, el nodo de acceso a la red 1204, la función del plano de usuario 1210, el nodo de red 1206 y la función del plano de control 1212 de la FIG. 12 pueden corresponder respectivamente al nodo de acceso a la red 1104, la función del plano de usuario 1112, el nodo de red 1106 y la función del plano de control 1114 de la FIG. 11.

[0102] Como se muestra en la FIG. 12, el nodo de acceso a la red 1204, el nodo de red 1206 y/o el P-GW 1208 pueden eliminar 1214 un contexto para el dispositivo cliente 1202. En un aspecto, el nodo de acceso a la red 1204

y/o el nodo de red 1206 pueden eliminar el contexto de dispositivo cliente 1202 después de que la función de plano de control 1212 haya proporcionado un contexto de dispositivo cliente cifrado al dispositivo cliente 1202. Como se muestra en la FIG. 12, el dispositivo cliente 1202 puede transmitir una petición de establecimiento de recursos 1216 al nodo de acceso a la red 1204. Por ejemplo, el dispositivo cliente 1202 puede transmitir la petición de establecimiento de recursos 1216 cuando el dispositivo cliente 1202 debe transmitir transmisiones de datos en ráfagas infrecuentes a la red (por ejemplo, al P-GW 1208). Por ejemplo, una transmisión de datos en ráfaga puede incluir una secuencia de unidades de datos de protocolo (PDU), como paquetes IP. En un aspecto, la petición de establecimiento de recursos 1216 puede incluir un contexto de dispositivo cliente cifrado (por ejemplo, un contexto de dispositivo cliente para el plano de control).

[0103] Durante la operación de establecimiento de recursos 1218, la función del plano de control 1212 puede verificar el contexto de dispositivo cliente cifrado desde el dispositivo cliente 1202 y, tras la verificación satisfactoria, la función del plano de control 1212 puede descifrar el contexto de dispositivo cliente cifrado. A continuación, la función de plano de control 1212 puede reconstruir el contexto para el dispositivo cliente 1202. En un aspecto, la función del plano de usuario 1210 y el P-GW 1208 también pueden reconstruir el contexto para el dispositivo cliente 1202. En un aspecto, la función de plano de control 1212 puede obtener una dirección de red (por ejemplo, una dirección IP) para el dispositivo cliente 1202 y puede proporcionar la dirección de red al dispositivo cliente 1202 durante la operación de establecimiento de recursos 1218. Como se muestra en la FIG. 12, el dispositivo cliente 1202 puede transmitir datos de enlace ascendente (UL) 1220 al P-GW 1208 a través del nodo de acceso a la red 1204. En un aspecto, el dispositivo cliente 1202 puede transmitir los datos UL1220 en una o más PDU que incluyen la dirección de red del dispositivo cliente 1202.

[0104] En un aspecto, el dispositivo cliente 1202 puede determinar que no hay más transmisiones de datos que realizar a la red. En tal aspecto, el dispositivo cliente 1202 puede transmitir opcionalmente un mensaje 1 1222 de petición de liberación de recursos al nodo de acceso a la red 1204. A continuación, el dispositivo cliente 1202 puede entrar en el modo inactivo 1224. Como se muestra en la FIG. 12, el nodo de acceso a la red 1204 puede transmitir el mensaje de petición de liberación de recursos 1 1222 al P-GW 1208 a través del nodo de red 1206. En un aspecto, el mensaje de petición de liberación de recursos 1 1222 permite que la P-GW 1208 liberar uno o más recursos para el dispositivo cliente 1202. Por ejemplo, el uno o más recursos pueden incluir la dirección de red asignada al dispositivo cliente 1202 (por ejemplo, para permitir la reasignación de esa dirección de red), un portador para el dispositivo cliente 1202 y/u otros recursos para el dispositivo cliente 1202. A continuación, la función de plano de control 1212 y la función de plano de usuario 1210 pueden eliminar 1232 el contexto para el dispositivo cliente 1202. En otro aspecto, la función de plano de usuario 1210 y/o la función de plano de control 1212 pueden iniciar un temporizador 1226 después de que se reciben los datos UL1220. Si el temporizador 1226 expira antes de recibir nuevos datos UL (por ejemplo, datos UL adicionales posteriores a los datos UL1220) desde el dispositivo cliente 1202 y/o antes de transmitir cualquier dato de enlace descendente (DL) al dispositivo cliente 1202, la función de plano de control 1212 y/o la función de plano de usuario 1210 pueden determinar que el dispositivo cliente 1202 está en el modo inactivo 1224. En tal escenario, de acuerdo con un aspecto, la función de plano de usuario 1210 puede transmitir un mensaje de petición de liberación de recursos 2 1228 a la P-GW 1208 a través del nodo de red 1206. De forma alternativa, de acuerdo con otro aspecto, la función de plano de control 1212 puede transmitir un mensaje de petición de liberación de recursos 3 1230 al P-GW 1208. En un aspecto, el mensaje 2 1228 de petición de liberación de recursos o el mensaje 3 1230 de petición de liberación de recursos habilita al P-GW 1208 para liberar uno o más recursos para el dispositivo cliente 1202. Por ejemplo, el uno o más recursos pueden incluir la dirección de red asignada al dispositivo cliente 1202 (por ejemplo, para permitir la reasignación de esa dirección de red), un portador para el dispositivo cliente 1202 y/u otros recursos para el dispositivo cliente 1202. A continuación, la función de plano de control 1212 y la función de plano de usuario 1210 pueden eliminar 1232 el contexto para el dispositivo cliente 1202. En un aspecto, el temporizador 1226 puede reiniciarse mediante la función de plano de control 1212 y/o la función de plano de usuario 1210 cuando se recibe una nueva transmisión de datos UL (por ejemplo, datos UL adicionales posteriores a los datos UL1220) en la función del plano de usuario. 1210 desde el dispositivo cliente 1202 antes de la expiración del temporizador 1226.

Pila de protocolos de plano de control

[0105] La FIG. 13 es un diagrama que ilustra una pila 1300 de protocolos del plano de control para la transmisión de datos de IoT de acuerdo con varios aspectos de la presente divulgación. Como se muestra en la FIG. 13, la pila de protocolos 1300 puede incluir una pila de protocolos de dispositivo cliente 1302 (también denominada pila de protocolos de dispositivos de IoT), una pila de protocolos de nodo de acceso a la red 1304, una pila de protocolos de IoTF 1306 implementada en un nodo de red 1305 y una red de servicio pila de protocolos 1308. Por ejemplo, la pila de protocolos de nodo de acceso a la red 1304 puede implementarse en un eNB, estación base o punto de acceso a la red. Como otro ejemplo, la pila de protocolos de red de servicio 1308 puede implementarse en un P-GW. Como se muestra en la FIG. 13, la pila de protocolos de dispositivo cliente 1302 puede incluir una capa física (PHY) 1310, una capa de control de acceso a medios (MAC) 1312, una capa de control de enlace de radio (RLC) 1314, una capa de protocolo de convergencia de datos por paquetes (PDCP) 1316, y una capa de control (Ctrl) 1320. Como se muestra además en la FIG. 13, la pila de protocolos de dispositivo cliente 1302 puede implementar una capa de protocolo de contexto 1318 para comunicar un contexto de dispositivo cliente cifrado en el plano de control (abreviado como "CDC_{CP}" en la FIG. 13). La capa de protocolo de contexto 1318 puede permitir además la

comunicación de un ID de IoTF (IID) y/o una cabecera de seguridad (abreviado como "Sec" en la FIG. 13) que indica la presencia de un contexto de dispositivo cliente cifrado.

[0106] Como se muestra en la FIG. 13, la pila de protocolos de nodo de acceso a la red 1304 puede incluir una capa PHY1322, una capa MAC 1324, una capa RLC 1326 y una capa PDCP1328 que interactúan respectivamente con la capa PHY1310, la capa MAC 1312, la capa RLC 1314 y la capa 1316 de PDCP de la pila 1302 de protocolos del dispositivo cliente. La pila de protocolos de nodo de acceso a la red 1304 puede incluir además una capa de Ethernet 1330, una capa de MAC 1332, una capa de protocolo de Internet (IP) 1334, una capa de protocolo de datagrama de usuario (UDP) 1336 y una capa de plano de control de protocolo de túnel GPRS (GTP-C) 1338.

[0107] Como se muestra en la FIG. 13, la pila de protocolos de IoTF 1306 puede incluir una capa Ethernet 1340, una capa MAC 1342, una capa IP1344, una capa UDP1346, una capa GTP-C 1348 y una capa de control (Ctrl) 1352. Como se muestra además en la FIG. 13, la pila de protocolos de IoTF 1306 puede implementar una capa de protocolo de contexto 1350 para comunicar un contexto de dispositivo cliente cifrado en el plano de control (abreviado como "CDC_{CP} " en la FIG. 13). La capa de protocolo de contexto 1350 también puede permitir la comunicación de un ID de IoTF (IID) y/o una cabecera de seguridad (abreviado como "Sec" en la FIG. 13) que indica la presencia de un contexto de dispositivo cliente cifrado. Como se muestra en la FIG. 13, la capa de protocolo de contexto 1318 de la pila de protocolos de dispositivo cliente 1302 está en comunicación con la capa de protocolo de contexto 1350 de la pila de protocolos de IoTF 1306. En un aspecto, un contexto de dispositivo cliente cifrado puede transportarse en una cabecera de paquete fuera de un mensaje del plano de usuario de acuerdo con el formato de paquete de IoT a modo de ejemplo descrito con respecto a la FIG. 15.

[0108] La pila de protocolos de red de servicio 1308 puede incluir una capa IP1354, una capa UDP1356, una capa GTP-C 1358 y una capa Ctrl 1360 que interactúan respectivamente con la capa IP1344, la capa UDP1346, la capa GTP-C 1348 y la capa Ctrl 1352 de la pila de protocolos IoTF 1306. En un aspecto de la presente divulgación, si se implementa una arquitectura de red como una red de acceso de radio GSM EDGE (GERAN), se pueden usar protocolos diferentes a los protocolos IP1364. En un aspecto de la presente divulgación, los protocolos GTP-C y UDP indicados por las regiones 1362 y 1366 pueden omitirse.

Pilas de protocolos de plano de usuario

[0109] La FIG. 14 es un diagrama que ilustra una pila de protocolos de plano de usuario 1400 para la transmisión de datos de IoT de acuerdo con varios aspectos de la presente divulgación. Como se muestra en la FIG. 14, la pila de protocolos 1400 puede incluir una pila de protocolos de dispositivo cliente 1402 (también denominada pila de protocolos de dispositivos de IoT), una pila de protocolos de nodo de acceso a la red 1404, una pila de protocolos de IoTF 1406 implementada en un nodo de red 1405 y una red de servicio pila de protocolos 1408. Por ejemplo, la pila de protocolos de nodo de acceso a la red 1404 puede implementarse en un eNB, estación base o punto de acceso a la red. Como otro ejemplo, la pila de protocolos de red de servicios 1408 puede implementarse en un P-GW. Como se muestra en la FIG. 14, la pila de protocolo de dispositivo cliente 1402 puede incluir una capa física (PHY) 1410, una capa de control de acceso a medios (MAC) 1412, una capa de control de enlace de radio (RLC) 1414, una capa de protocolo de convergencia de datos por paquetes (PDCP) 1416, y una capa de plano de usuario (ARRIBA) 1420. Como se muestra además en la FIG. 14, la pila de protocolos de dispositivo cliente 1402 puede implementar una capa 1418 de protocolo de contexto para comunicar un contexto de dispositivo cliente cifrado en el plano de usuario (abreviado como "CDC_{UP} " en la FIG. 14). La capa de protocolo de contexto 1418 puede permitir además la comunicación de un ID de IoTF (IID) y/o una cabecera de seguridad (abreviado como "Sec" en la FIG. 14) que indica la presencia de un contexto de dispositivo cliente cifrado.

[0110] Como se muestra en la FIG. 14, la pila de protocolos de nodo de acceso a la red 1404 puede incluir una capa PHY1422, una capa MAC 1424, una capa RLC 1426 y una capa PDCP1428 que interactúan respectivamente con la capa PHY1410, la capa MAC 1412, la capa RLC 1414, y la capa 1416 de PDCP de la pila de protocolos del dispositivo cliente 1402. La pila de protocolos de nodo de acceso a la red 1404 puede incluir además una capa de Ethernet 1430, una capa de MAC 1432, una capa de protocolo de Internet (IP) 1434, una capa de protocolo de datagramas de usuario (UDP) 1436 y un protocolo de túnel GPRS de plano de usuario (GTP-U) capa 1438.

[0111] Como se muestra en la FIG. 14, la pila de protocolos de IoTF 1406 puede incluir una capa Ethernet 1440, una capa MAC 1442, una capa IP1444, una capa UDP1446 y una capa GTP-U1448. Como se muestra además en la FIG. 14, la pila de protocolos de IoTF 1406 puede implementar una capa 1450 de protocolo de contexto para comunicar un contexto de dispositivo cliente cifrado en el plano de usuario (abreviado como "CDC_{UP} " en la FIG. 14). La capa de protocolo de contexto 1450 también puede permitir la comunicación de un ID de IoTF (IID) y/o una cabecera de seguridad (abreviado como "Sec" en la FIG. 14) que indica la presencia de un contexto de dispositivo cliente cifrado. Como se muestra en la FIG. 14, la capa de protocolo de contexto 1418 de la pila de protocolos de dispositivo cliente 1402 está en comunicación con la capa de protocolo de contexto 1450 de la pila de protocolos de IoTF 1406. En un aspecto, un contexto de dispositivo cliente cifrado en el plano de usuario puede transportarse en una cabecera de paquete fuera de un mensaje UP de acuerdo con el formato de paquete de IoT a modo de ejemplo descrito con respecto a la FIG. 15.

[0112] La pila de protocolos de red de servicio 1408 puede incluir una capa IP1454, una capa UDP1456, una capa GTP-U1458 y una capa UP1460 que interactúan respectivamente con la capa IP1444, la capa UDP1446, la capa GTP-U1448, y la capa UP1452 de la pila de protocolos IoTF 1406. En un aspecto de la presente divulgación, si se implementa una arquitectura de red como una Red de Acceso de Radio GSM EDGE (GERAN), se pueden usar protocolos diferentes a los protocolos IP1464. En un aspecto de la presente divulgación, los protocolos GTP-U y UDP indicados por las regiones 1462 y 1466 pueden omitirse. En un aspecto de la presente divulgación, si se usa el protocolo IP para la entrega de mensajes UP, el contexto de accesibilidad de la red cifrada en el plano de usuario puede llevarse en el campo de opciones de IP (IPv4) o la cabecera de extensión de IP (IPv6).

Formato de paquete IoT

[0113] La FIG. 15 es un diagrama de un formato de paquete 1500 para transmisiones en una arquitectura de red de IoT, de acuerdo con diversos aspectos de la presente divulgación. Con referencia a la FIG. 15, el campo de identificador temporal (TID) 1502 puede ser utilizado por un nodo de acceso a la red (por ejemplo, eNB, estación base o punto de acceso a la red) para identificar un dispositivo cliente (también denominado dispositivo IoT) localmente. Por ejemplo, el valor asignado por un nodo de acceso a la red al campo TID1502 para identificar un dispositivo cliente puede ser un C-RNTI o equivalente.

[0114] En un aspecto de la presente divulgación, el campo 1504 ID de IoTF (IID) puede incluir un identificador temporal único global (GUTI). Por ejemplo, el GUTI puede incluir un identificador asociado con un IoTF y un identificador (por ejemplo, un identificador temporal, como una entidad de gestión de movilidad (MME) identidad de abonado móvil temporal (M-TMSI)) asociado con el dispositivo cliente. Por ejemplo, el GUTI puede ser utilizado por un nodo de acceso a la red para identificar un IoTF, y el GUTI puede ser utilizado por un IoTF para identificar un dispositivo cliente. En otro aspecto, el campo IID1504 puede incluir un identificador de IoTF global (GIOTFI) y un identificador (por ejemplo, un identificador temporal, tal como un M-TMSI) asociado con el dispositivo cliente. Por ejemplo, GIOTFI puede ser un equivalente de un identificador de entidad de gestión de movilidad único a nivel mundial (GUMMEI) para un IoTF. En un aspecto de la presente divulgación, la M-TMSI puede estar cifrada para la privacidad del dispositivo cliente. Cabe señalar que el uso de la dirección IP de IoTF puede divulgar la topología de la red.

[0115] El campo de cabecera de seguridad 1506 puede indicar la presencia de un contexto de dispositivo cliente cifrado, una indicación de plano de control (CP)/plano de usuario (UP), un número de secuencia, un valor de sello de tiempo y/o un valor aleatorio. Por ejemplo, el valor del sello de tiempo puede basarse en un tiempo y un contador, donde el tiempo es el tiempo del nodo de acceso a la red o el tiempo de IoTF. El campo de contexto de dispositivo cliente 1508 puede incluir un contexto de dispositivo cliente cifrado. Cabe señalar que si se utiliza una marca de tiempo para el cifrado en lugar del número de secuencia, es posible que IoTF no necesite mantener ningún estado de red del dispositivo cliente. Un valor aleatorio puede basarse en el número aleatorio y un contador. El valor aleatorio lo genera el nodo de acceso a la red o el dispositivo cliente, o una combinación de los mismos. El contador puede incrementarse en un cierto valor (por ejemplo, uno) para cada paquete. Si se utiliza un valor aleatorio para el cifrado en lugar del número de secuencia, el dispositivo cliente puede generar una nueva clave de cifrado basada en la clave de cifrado en el contexto de seguridad y el número aleatorio. Si se utiliza un valor aleatorio para la protección de integridad en lugar del número de secuencia, el dispositivo cliente puede generar una nueva clave de protección de integridad basada en la clave de protección de integridad en el contexto de seguridad y el número aleatorio, y puede proteger un mensaje utilizando la nueva clave de protección de integridad. El campo de carga útil 1510 puede incluir datos o información de control (por ejemplo, un paquete de datos o un paquete de control).

[0116] El campo 1512 del código de auntentificación de mensajes (MAC) se puede utilizar para la protección de integridad. Por ejemplo, el campo MAC 1512 puede incluir un código de auntentificación de mensaje generado por una entidad o dispositivo transmisor. A continuación, el código de auntentificación de mensaje en el campo MAC 1512 puede ser utilizado por un dispositivo o entidad de recepción para verificar que la integridad del mensaje no ha sido comprometida (por ejemplo, que el contenido del mensaje no ha sido alterado o manipulado). En un aspecto, el código de auntentificación de mensaje en el campo MAC 1512 se puede generar en un dispositivo o entidad transmisora aplicando un algoritmo de generación de código de auntentificación de mensaje (por ejemplo, un código AEAD), donde un mensaje (por ejemplo, un paquete) y la clave de plano de usuario o una clave de plano de control se utilizan como entradas para el algoritmo de generación de código de auntentificación de mensajes. La salida del algoritmo de generación del código de auntentificación de mensajes puede ser el código de auntentificación de mensajes incluido en el campo MAC 1512. Un dispositivo o entidad de recepción puede verificar la integridad del mensaje recibido aplicando el algoritmo de generación del código de auntentificación del mensaje (por ejemplo, el código AEAD) al mensaje. Por ejemplo, el mensaje recibido (por ejemplo, el paquete) y la clave del plano de usuario o la clave del plano de control pueden usarse como entradas para el algoritmo de generación del código de auntentificación de mensajes. A continuación, el dispositivo o entidad de recepción puede comparar la salida del algoritmo de generación del código de auntentificación de mensajes con el código de auntentificación de mensajes incluido en el campo MAC 1512. En tal ejemplo, cuando la salida del algoritmo de generación del código de auntentificación de mensajes coincide con el código de auntentificación de mensajes incluido en el campo MAC 1512, el dispositivo o entidad de recepción puede determinar que el mensaje se ha verificado con éxito.

Diseño y generación de contexto de dispositivo cliente cifrado

[0117] De acuerdo con los aspectos divulgados en el presente documento, el contexto de dispositivo cliente cifrado puede contener información que la red puede necesitar para proporcionar un servicio al dispositivo cliente. Por ejemplo, el contexto de dispositivo cliente puede incluir un contexto de seguridad, un ID de portador, calidad de servicio (QoS) de portador del sistema de paquetes evolucionado (EPS) y S5-TEID (s), y/u otros servicios, parámetros, valores, configuraciones o funciones que la red pueda necesitar para brindar un servicio al dispositivo cliente. En algunos aspectos, el contexto de dispositivo cliente puede establecerse durante un procedimiento AKA.

[0118] En algunos aspectos, el contexto de dispositivo cliente cifrado puede incluir uno o más elementos de información además del contexto de dispositivo cliente. Por ejemplo, el contexto de dispositivo cliente cifrado puede incluir un tiempo de caducidad establecido por IoTF-C 106 (o indicado en el contexto de dispositivo cliente), que limita la vida útil del contexto de dispositivo cliente cifrado (por ejemplo, para evitar la reutilización permanente). Como otro ejemplo, el contexto de dispositivo cliente cifrado puede tener un índice de clave que identifica la clave utilizada para generar el contexto de dispositivo cliente cifrado.

[0119] En algunos aspectos, el contexto de dispositivo cliente cifrado puede generarse utilizando una clave secreta que solo es conocida por una entidad en la red y, por consiguiente, no puede ser interpretada y/o modificada por los dispositivos cliente. Por ejemplo, el contexto de dispositivo cliente cifrado puede generarse cifrando un contexto de dispositivo cliente utilizando la clave secreta de IoTF-U (por ejemplo, IoTF-U 108). En algunos aspectos, el contexto de dispositivo cliente cifrado puede estar protegido por integridad con la clave secreta de IoTF-U (por ejemplo, IoTF-U 108) y, por consiguiente, no puede ser manipulado/modificado por dispositivos cliente.

[0120] En un aspecto, el contexto de dispositivo cliente cifrado puede ser proporcionado a un dispositivo cliente (por ejemplo, el dispositivo cliente 102) por el IoTF-C (por ejemplo, IoTF-C 106) como una finalización exitosa de la configuración de auntentificación y contexto (por ejemplo, portador). En un aspecto, un dispositivo cliente puede incluir el contexto de dispositivo cliente cifrado en uno o más paquetes del plano de usuario (por ejemplo, paquetes de datos UL) para permitir que IoTF-U (por ejemplo, IoTF-U 108) reconstruya el contexto de dispositivo cliente sobre la marcha. Por ejemplo, si un dispositivo cliente necesita transmitir múltiples paquetes en serie, el dispositivo cliente puede incluir el contexto de dispositivo cliente cifrado en el primer paquete sin incluir el contexto de dispositivo cliente cifrado en los paquetes posteriores. En algunos aspectos, el contexto de dispositivo cliente cifrado puede ser específico de un dispositivo cliente y, por consiguiente, un contexto de dispositivo cliente cifrado emitido a un dispositivo cliente puede no ser utilizado por ningún otro dispositivo cliente.

a) Contexto de dispositivo cliente cifrado del plano de control

[0121] En un aspecto de la presente divulgación, un IoTF (por ejemplo, el IoTF-C 106 en la FIG. 1) puede generar un contexto de dispositivo cliente cifrado concatenando uno o más elementos de información. Por ejemplo, se puede generar un contexto de dispositivo cliente cifrado en el plano de control (CP) (CDC_{CP}) basándose en la expresión KeyID ‖ Enc_$K_{CDC\text{-}IoTF\text{-}C}$ (CDC_{CP}) ‖ MAC. En un aspecto de la presente divulgación, la clave $K_{CDC\text{-}IoTF\text{-}C}$ (por ejemplo, la clave $K_{CDC\text{-}IoTF\text{-}C}$ 304 en la FIG. 3) puede ser la misma que la clave $K_{CDC\text{-}IoTF}$ (por ejemplo, la clave $K_{CDC\text{-}IoTF}$ 302 en la FIG. 3) u obtenerse a partir de la clave $K_{CDC\text{-}IoTF}$. El término KeyID puede representar el índice de claves (utilizado para generar el contexto de dispositivo cliente cifrado). El término CDC_{CP} puede representar el contexto de dispositivo cliente del plano de control. Por ejemplo, el contexto de dispositivo cliente del plano de control puede incluir un identificador de dispositivo cliente, el contexto de seguridad del dispositivo cliente (por ejemplo, claves del plano de control, como la clave K_{IoT} (equivalente a K_{ASME}), la clave $K_{IoT\text{-}CPenc}$ 210, la clave $K_{IoT\text{-}CPint}$ 212), las capacidades de seguridad del dispositivo cliente (por ejemplo, el algoritmo de cifrado del sistema de paquetes evolucionado (EEA), el algoritmo de integridad del sistema de paquetes evolucionado (EIA)) y/o la información de configuración del siguiente salto (S5/S8). Por ejemplo, la información de configuración del próximo salto puede incluir una dirección de servidor IoT, una dirección P-GW y/o TEID. El término MAC puede indicar el modo de cifrado y/o un algoritmo de generación de código de auntentificación de mensajes (también denominado algoritmo MAC), que puede ser elegido por un operador de red móvil (MNO) y configurado para IoTF. Por consiguiente, el término Enc_$K_{CDC\text{-}IoTF\text{-}C}$ (CDC_{CP}) puede representar el resultado de una operación de cifrado realizada en el contexto de dispositivo cliente del plano de control utilizando la clave $K_{CDC\text{-}IoTF\text{-}C}$.

b) Contexto de dispositivo cliente cifrado del plano de usuario

[0122] Como otro ejemplo, se puede generar un contexto de dispositivo cliente cifrado en el plano de usuario (UP) (CDC_{UP}) basándose en la expresión KeyID ‖ Enc_$K_{CDC\text{-}IoTF\text{-}U}$ (CDC_{UP}) ‖ MAC. El término CDC_{UP} puede representar el contexto de dispositivo cliente del plano de usuario. Por ejemplo, el contexto de dispositivo cliente del plano de usuario puede incluir un identificador de dispositivo cliente, ID de portador, calidad de servicio(s) (QoS) de portador del sistema de paquetes evolucionado (EPS), un identificador de punto final del túnel S5 (TEID) para un protocolo de tunelización de paquete general del plano de usuario del servicio de radio (GPRS) (GTP-U), una dirección de protocolo de Internet (IP) P-GW (o información equivalente) a la que IoTF-U 108 reenvía los datos UL,

un contexto de seguridad del dispositivo cliente (por ejemplo, un cifrado seleccionado algoritmo y claves del plano de usuario, como la clave $K_{IoT-UPenc}$ 216, la clave $K_{IoT-UPint}$ 218), las capacidades de seguridad del dispositivo cliente (por ejemplo, el algoritmo de cifrado del sistema de paquetes evolucionado (EEA), el algoritmo de integridad del sistema de paquetes evolucionado (EIA)) y/o la información de configuración del siguiente salto (S5/S8). Por ejemplo, la información de configuración del próximo salto puede incluir una dirección de servidor IoT, una dirección P-GW y/o TEID. Por consiguiente, el término Enc_$K_{CDC-IoTF-U}$ (CDC_{UP}) puede representar el resultado de una operación de cifrado realizada en el contexto de dispositivo cliente del plano de usuario utilizando la clave $K_{CDC-IoTF-U}$. En un aspecto de la presente divulgación, el contexto de dispositivo cliente cifrado solo puede ser descifrado por el IoTF (por ejemplo, IoTF-C 106 y/o IoTF-U 108) al que está conectado/asociado el dispositivo cliente. En un aspecto de la presente divulgación, el contexto de un dispositivo cliente puede comprimirse antes de cifrarse.

[0123] El contexto de dispositivo cliente cifrado puede tener una o más características. Por ejemplo, un contexto de dispositivo cliente cifrado puede contener la información de estado de la red asociada con un dispositivo cliente particular y, por consiguiente, puede no ser transferible a otros dispositivos cliente. Un IoTF-C/U (por ejemplo, el IoTF-C 106 y/o el IoTF-U 108) no mantiene los contextos (por ejemplo, información de estado de la red) de un dispositivo cliente. En consecuencia, tal IoTF-C/U puede recuperar un contexto de dispositivo cliente a partir de un contexto de dispositivo cliente cifrado utilizando su propia clave secreta y, por consiguiente, IoTF-C/U no necesita almacenar ninguna información adicional para recuperar un contexto de dispositivo cliente. El IoTF-C/U puede eliminar el contexto de un dispositivo cliente bajo ciertas condiciones (por ejemplo, gestión de conexión del sistema de paquetes evolucionado (ECM)-inactivo o inmediatamente después de una pequeña transferencia de datos) y restaurarlo cuando sea necesario (por ejemplo, para la transferencia de datos).

[0124] Un dispositivo cliente puede almacenar contextos de dispositivo cliente cifrado proporcionados por un IoTF-C para una transferencia rápida de datos UL/transferencia rápida de mensajes en el plano de control. El dispositivo cliente puede entrar en modo de suspensión inmediatamente después de transmitir uno o más paquetes de datos. Dado que puede no haber una sobrecarga de intercambio de mensajes para que un IoTF-U reconstruya el contexto de un dispositivo cliente, no se puede experimentar ningún retardo para la transmisión de pequeños paquetes de datos. En un aspecto de la presente divulgación, no se puede utilizar ningún mensaje del plano de control para la transmisión de datos del plano de usuario cuando el dispositivo cliente está en el modo inactivo.

Actualización de área de seguimiento

[0125] Un dispositivo cliente puede realizar un procedimiento de actualización del área de seguimiento (TAU) cuando el dispositivo cliente entra en una nueva área de seguimiento durante el modo inactivo. El mensaje TAU puede incluir el ID de área de seguimiento actual (TAI) y el GIOTFI o equivalente (por ejemplo, un identificador de entidad de gestión móvil globalmente único (GUMMEI)) del IoTF-C de origen. El IoTF-C objetivo puede actualizar la ubicación del dispositivo cliente y el ancla de movilidad (por ejemplo, Id. De IoTF-U) a una o más entidades de red (por ejemplo, un P-GW) junto con un contexto de accesibilidad de red cifrado. En un aspecto de la presente divulgación, el contexto de accesibilidad de la red cifrada puede permitir que IoTF-U verifique el paquete de enlace descendente. En un aspecto de la presente divulgación, un servidor de aplicaciones (por ejemplo, un servidor de IoT) y/o un P-GW pueden transmitir un paquete de enlace descendente (DL) con el contexto de accesibilidad de red cifrado al IoTF-U/C (identificado por el GIOTFI).

[0126] La FIG. 16 es un diagrama de flujo de señales 1600 de un procedimiento TAU en una arquitectura de red de IoT (por ejemplo, arquitectura de red de IoT 100) de acuerdo con varios aspectos de la presente divulgación. Como se muestra en la FIG. 16, el diagrama de flujo de señal 1600 incluye un dispositivo cliente 1602 (también denominado dispositivo IoT), un nodo de acceso a la red 1604 (por ejemplo, eNB, estación base, punto de acceso a la red), un IoTF-C 1606 de destino implementado en un destino dispositivo de red 1605, un IoTF-C 1608 de origen implementado en un dispositivo de red de origen 1607, un P-GW1610 y un servidor de IoT1612 (también denominado servidor de aplicaciones). El dispositivo cliente 1602 puede transmitir un mensaje de petición de transferencia de datos 1614 que incluye un contexto de dispositivo cliente cifrado (por ejemplo, un contexto de cliente cifrado del plano de control (CP)) y una petición TAU al nodo de acceso a la red 1604. En un aspecto de la presente divulgación, el dispositivo cliente 1602 puede enviar el mensaje de petición de transferencia de datos 1614 sin establecer una conexión RRC.

[0127] El nodo de acceso a la red 1604 puede determinar 1616 el identificador de IoTF-C objetivo incluido en la petición de TAU. A continuación, el nodo de acceso a la red 1604 puede determinar la dirección IP del IoTF-C 1606 de destino, y puede transmitir un mensaje 1618 que incluye el TID asociado con el dispositivo cliente 1602, el contexto de dispositivo cliente cifrado y la petición de TAU al IoTF-C de destino 1606. El IoTF-C 1606 de destino puede transmitir un mensaje 1620 que incluye una petición del contexto de dispositivo cliente y el contexto de dispositivo cliente cifrado al IoTF-C 1608 de origen.

[0128] El IoTF-C 1608 de origen puede transmitir un mensaje 1622 que incluye el contexto de dispositivo cliente al IoTF-C 1606 de destino. El IoTF-C 1606 de destino puede almacenar 1624 el TID para el dispositivo cliente y una ID para el nodo de acceso a la red 1604, y puede generar 1624 un nuevo GUTI y un nuevo contexto de dispositivo cliente cifrado para el dispositivo cliente 1602 basado en el contexto de dispositivo cliente recibido. En

un aspecto de la presente divulgación, el IoTF-C 1606 de destino puede generar claves de plano de usuario (UP) y claves de generación de contexto y puede proporcionar las claves para un IoTF-U.

[0129] El IoTF-C 1606 de destino puede transmitir un mensaje 1626 que incluye el ID de área de seguimiento (TAI) y el ID del IoTF-C 1606 de destino (por ejemplo, GIOTFI) al servidor 1612 de IoT (o P-GW1610). El IoTF-C 1606 de destino puede transmitir un mensaje 1628 que incluye el TID, el nuevo GUTI, el nuevo contexto de dispositivo cliente cifrado y la respuesta TAU al dispositivo cliente 1602. El nodo de acceso a la red 1604 puede reenviar el nuevo GUTI, el nuevo contexto de dispositivo cliente cifrado y la respuesta TAU al dispositivo cliente 1602 en un mensaje 1630 basado en el TID.

[0130] Los aspectos divulgados en el presente documento proporcionan una arquitectura con nuevas funciones de red dedicadas que permiten un despliegue independiente y que evitan los requisitos de escalabilidad/interfuncionamiento. Los aspectos divulgados en el presente documento pueden permitir que un nodo de acceso a la red (por ejemplo, una estación base) transfiera datos hacia o desde los dispositivos cliente sin almacenar ni mantener contextos de seguridad para los dispositivos cliente, evitando así el consumo de una cantidad sustancial de recursos en el nodo de acceso a la red. (u otra entidad de la red). Las características de seguridad pueden estar ancladas en una nueva función de red (denominada función IoT (IoTF)). Los recursos dedicados se asignan para la transferencia de datos de IoT a fin de evitar afectar la conexión/tráfico PDN de los dispositivos cliente normales. Puede usarse un contexto de UE cifrado para la transferencia de datos para eliminar el contexto semipersistente del UE en el IoTF cuando el UE está en el estado inactivo. El MME/S-GW no debe mantener estados grandes (es decir, contextos) de dispositivos IoT que no transmiten tráfico con frecuencia. Es posible que los dispositivos de IoT solo requieran una entrega de datos rentable sin agotar los costosos recursos de la red central.

Información de uso del contexto de dispositivo cliente cifrado

[0131] De acuerdo con los diversos aspectos de la presente divulgación, un dispositivo cliente (por ejemplo, el dispositivo cliente 702 en la FIG. 7) puede transmitir información de uso asociada con un contexto de dispositivo cliente cifrado (también denominado información de uso de contexto de dispositivo cliente cifrado) cuando el dispositivo cliente transmite un contexto de dispositivo cliente cifrado a la red.

[0132] En un aspecto, la información de uso del contexto de dispositivo cliente cifrado puede indicar una cantidad de datos a transmitir desde el dispositivo cliente. Por ejemplo, la cantidad de datos puede indicarse como una transmisión de datos reducida (por ejemplo, una transmisión que incluye un solo paquete de datos) o una transmisión de datos en ráfagas (por ejemplo, una o más transmisiones que incluyen varios paquetes de datos). En un aspecto, la cantidad de datos a transmitir desde el dispositivo cliente puede indicarse usando un solo bit (por ejemplo, como parte de un elemento de información (IE) en una cabecera de un paquete). En tal aspecto, por ejemplo, el dispositivo cliente puede habilitar el bit (por ejemplo, establecer el bit en "1") para indicar que la cantidad de datos que se transmitirán desde el dispositivo cliente es una transmisión de datos reducida o puede deshabilitar el bit (por ejemplo, establecer el bit en "0") para indicar que la cantidad de datos a transmitir desde el dispositivo cliente es una transmisión de datos en ráfagas.

[0133] En un aspecto, cuando el dispositivo cliente indica que la cantidad de datos a transmitir es una transmisión de datos reducida, la red (por ejemplo, un nodo de red, como el nodo de red 707, 709, y/o un nodo de acceso a la red, como como el nodo de acceso a la red 704) puede eliminar el contexto para el dispositivo cliente inmediatamente después de que se reciba la transmisión de datos reducida desde el dispositivo cliente. En otro aspecto, cuando el dispositivo cliente indica que la cantidad de datos a transmitir es una transmisión de datos reducida, la red puede mantener el contexto para el dispositivo cliente durante un primer período de tiempo umbral. Por ejemplo, la red puede implementar un primer temporizador configurado para medir el primer período de tiempo umbral. En este aspecto, la red puede eliminar el contexto de dispositivo cliente al expirar el primer temporizador. En un aspecto, si la red recibe una transmisión de datos (por ejemplo, un paquete) del dispositivo cliente antes de que expire el primer temporizador, la red puede reiniciar el primer temporizador y puede mantener el contexto para el dispositivo cliente hasta que expire el primer temporizador.

[0134] En otro aspecto, cuando el dispositivo cliente indica que la cantidad de datos a transmitir es una transmisión de datos en ráfaga, la red puede mantener el contexto para el dispositivo cliente durante un segundo período de tiempo umbral. Por ejemplo, la red puede implementar un segundo temporizador configurado para medir el segundo período de tiempo umbral. En este aspecto, la red puede eliminar el contexto de dispositivo cliente al expirar el segundo temporizador. En un aspecto, si la red recibe una transmisión de datos (por ejemplo, un paquete) del dispositivo cliente antes de que expire el segundo temporizador, la red puede reiniciar el segundo temporizador y puede mantener el contexto para el dispositivo cliente hasta que expire el segundo temporizador. Por ejemplo, el segundo período de tiempo umbral puede ser menor que el primer período de tiempo umbral.

[0135] En un aspecto, la información de uso del contexto de dispositivo cliente cifrado puede incluirse en una cabecera de un paquete transmitido a la red. En otro aspecto, el dispositivo cliente puede proporcionar la

información de uso del contexto de dispositivo cliente cifrado a la red durante un procedimiento de señalización RRC.

[0136] En un aspecto, la red (por ejemplo, el nodo de red 605 en la FIG. 6) puede proporcionar múltiples tipos de contextos de dispositivo cliente cifrado a un dispositivo cliente (por ejemplo, el dispositivo cliente 602 en la FIG. 6). En tal aspecto, cada tipo de contexto de dispositivo cliente cifrado puede ser utilizado por la red (por ejemplo, el nodo de red 907 en la FIG. 9) para reconstruir una parte de un contexto para el dispositivo cliente (por ejemplo, un subconjunto de un contexto para el dispositivo cliente). Por ejemplo, un primer tipo de contexto de dispositivo cliente cifrado puede asociarse con un primer servicio (por ejemplo, un servicio de banda ancha móvil) proporcionado por la red, donde el primer tipo de contexto de dispositivo cliente cifrado permite a la red reconstruir una primera parte del contexto de dispositivo cliente que se necesita para soportar el primer servicio. En tal ejemplo, un segundo tipo de contexto de dispositivo cliente cifrado puede asociarse con un segundo servicio (por ejemplo, comunicaciones de baja latencia ultra fiables (URLLC)) proporcionado por la red, donde el segundo tipo de contexto de dispositivo cliente cifrado habilita la red para reconstruir una segunda parte del contexto de dispositivo cliente que se necesita para soportar el segundo servicio. En un aspecto, la primera parte del contexto de dispositivo cliente y la segunda parte del contexto de dispositivo cliente pueden incluir menos información de contexto que el contexto de dispositivo cliente generado originalmente por la red para el dispositivo cliente.

[0137] En un aspecto, el dispositivo cliente puede determinar uno o más de los múltiples tipos de contextos de dispositivo cliente cifrado para usar basándose en el tipo de transmisión que se enviará a (o se recibirá de) la red. Por ejemplo, y con referencia a los ejemplos proporcionados anteriormente, si el dispositivo cliente va a transmitir datos asociados con un servicio de banda ancha móvil, el dispositivo cliente puede transmitir el primer tipo de contexto de dispositivo cliente cifrado a la red. Como otro ejemplo, si el dispositivo cliente va a transmitir datos asociados con un servicio URLLC, el dispositivo cliente puede transmitir el segundo tipo de contexto de dispositivo cliente cifrado a la red. Debe entenderse que la red puede proporcionar otros tipos de servicios además o en lugar de los ejemplos proporcionados anteriormente, como un servicio de acceso de alta prioridad, un servicio de acceso tolerante al retardo o un servicio de comunicaciones de tipo máquina (MTC).

[0138] De acuerdo con los diversos aspectos de la presente divulgación, un dispositivo cliente puede indicar el tipo de contexto de dispositivo cliente cifrado en la información de uso descrita anteriormente cuando el dispositivo cliente transmite un contexto de dispositivo cliente cifrado a la red. En un aspecto, la información de uso del contexto de dispositivo cliente cifrado puede indicar el tipo de información que se transmite desde el dispositivo cliente. Por ejemplo, la información de uso del contexto de dispositivo cliente cifrado puede indicar que la información que se transmite desde el dispositivo cliente está asociada con el plano de usuario (por ejemplo, datos) o el plano de control (por ejemplo, información de control). Se puede apreciar que dado que cada uno de los diferentes tipos de contextos de dispositivo cliente cifrado analizados anteriormente puede ser utilizado por la red para reconstruir una parte de un contexto para el dispositivo cliente (por ejemplo, un subconjunto de un contexto para el dispositivo cliente), tales diferentes tipos de contextos de dispositivo cliente cifrado pueden reducirse en tamaño en comparación con un contexto de dispositivo cliente cifrado que permite la reconstrucción de todo el contexto de dispositivo cliente (por ejemplo, completo).

[0139] En un aspecto, el contexto (o parte de un contexto) que será reconstruido por la red (por ejemplo, en el nodo de red 907 en la FIG. 9) para un tipo de servicio proporcionado por la red (por ejemplo, en el servidor IoT 912 en FIG. 9) puede asociarse con un valor (por ejemplo, un número de índice u otro valor). En tal aspecto, el dispositivo cliente (por ejemplo, el dispositivo cliente 902 en la FIG. 9) puede transmitir el número de índice junto con el contexto de dispositivo cliente cifrado para facilitar la reconstrucción de un contexto en la red para un servicio particular (u otro uso específico o petición). Por ejemplo, un número de índice "1" puede indicar una calidad de servicio (QoS) particular para un servicio de banda ancha móvil y la información necesaria para reconstruir un contexto para soportar esa QoS. En tal ejemplo, el dispositivo cliente puede transmitir un contexto de dispositivo cliente cifrado asociado con un servicio de banda ancha móvil y el número de índice "1" para facilitar la reconstrucción de una parte del contexto de dispositivo cliente que soporta el servicio de banda ancha móvil.

Funciones de red de múltiples planos de usuario

[0140] En un aspecto de la presente divulgación, una red puede incluir, entre otras cosas, un dispositivo cliente, un nodo de acceso a la red (por ejemplo, eNB, estación base, punto de acceso a la red) y una entidad de red (por ejemplo, una pasarela de servicio (S -GW), una pasarela de red de paquetes de datos (P-GW)). En tal aspecto, el nodo de acceso a la red puede implementar una función de red del primer plano de usuario y la entidad de red puede implementar una función de red del segundo plano de usuario. Por consiguiente, el nodo de acceso a la red puede obtener y transmitir un contexto de dispositivo cliente cifrado en el primer plano de usuario al dispositivo cliente y la entidad de red puede obtener y transmitir un contexto de dispositivo cliente cifrado en el segundo plano de usuario al dispositivo cliente. En un aspecto, el contexto de dispositivo cliente cifrado del primer plano de usuario puede permitir que la función de red del primer plano de usuario reconstruya un primer contexto (por ejemplo, un primer contexto de seguridad) para el dispositivo cliente para su procesamiento (por ejemplo, para verificar y/o descifrar datos de usuario paquetes) del tráfico de datos del usuario para el dispositivo cliente, y el contexto de dispositivo cliente cifrado del segundo plano de usuario puede permitir que la función de red del segundo plano de

usuario reconstruya un segundo contexto (por ejemplo, un segundo contexto de seguridad) para el dispositivo cliente para su procesamiento (por ejemplo, para verificar y/o descifrar paquetes de datos de usuario) del tráfico de datos de usuario para el dispositivo cliente. En un aspecto, el dispositivo cliente puede transmitir múltiples contextos de dispositivo cliente cifrado a la red junto con el tráfico de datos UL. Por ejemplo, el dispositivo cliente puede transmitir tanto el contexto de dispositivo cliente cifrado del primer plano de usuario como el contexto de dispositivo cliente cifrado del segundo plano de usuario junto con el tráfico de datos UL. En un aspecto, los contextos de dispositivo cliente cifrado del primer y segundo plano de usuario pueden transmitirse simultáneamente (por ejemplo, en el mismo paquete transmitido desde el dispositivo cliente). Por consiguiente, se puede apreciar que, en algunos aspectos, los múltiples contextos de dispositivo cliente cifrado transmitidos desde el dispositivo cliente pueden permitir la reconstrucción de contextos de dispositivo cliente independientes que están asociados con diferentes entidades (por ejemplo, nodo de acceso a la red, S-GW) en la red.

Aparato a modo de ejemplo (por ejemplo, dispositivo cliente) y procedimiento al respecto

[0141] La FIG. 17 es una ilustración de un aparato 1700 configurado para comunicarse con una red basada en una arquitectura de red de IoT de acuerdo con uno o más aspectos de la divulgación (por ejemplo, aspectos relacionados con los procedimientos de las FIGS. 18-20 descritos a continuación). El aparato 1700 incluye una interfaz de comunicación (por ejemplo, al menos un transceptor) 1702, un medio de almacenamiento 1704, una interfaz de usuario 1706, un dispositivo de memoria 1708 y un circuito de procesamiento 1710.

[0142] Estos componentes se pueden acoplar a y/o colocar en comunicación eléctrica entre sí por medio de un bus de señalización u otro componente adecuado, representado de forma genérica por las líneas de conexión en la FIG. 17. El bus de señalización puede incluir un número cualquiera de buses y puentes de interconexión, dependiendo de la aplicación específica del circuito de procesamiento 1710 y de las restricciones de diseño globales. El bus de señalización enlaza conjuntamente diversos circuitos de modo que cada uno de la interfaz de comunicación 1702, el medio de almacenamiento 1704, la interfaz de usuario 1706 y el dispositivo de memoria 1708 están acoplados a y/o en comunicación eléctrica con el circuito de procesamiento 1710. El bus de señalización también puede enlazar otros circuitos diversos (no mostrados) tales como fuentes de temporización, dispositivos periféricos, reguladores de voltaje y circuitos de gestión de potencia, que son bien conocidos en la técnica y, por consiguiente, no se describirán en mayor detalle.

[0143] La interfaz de comunicación 1702 se puede adaptar para facilitar la comunicación inalámbrica del aparato 1700. Por ejemplo, la interfaz de comunicación 1702 puede incluir circuitos y/o código (por ejemplo, instrucciones) adaptados para facilitar la comunicación de información bidireccionalmente con respecto a uno o más dispositivos de comunicación en una red. La interfaz de comunicación 1702 puede estar acoplada a una o más antenas 1712 para la comunicación inalámbrica dentro de un sistema de comunicación inalámbrica. La interfaz de comunicación 1702 se puede configurar con uno o más receptores y/o transmisores independientes, así como uno o más transceptores. En el ejemplo ilustrado, la interfaz de comunicación 1702 incluye un transmisor 1714 y un receptor 1716.

[0144] El dispositivo de memoria 1708 puede representar uno o más dispositivos de memoria. Como se indica, el dispositivo de memoria 1708 puede mantener información relacionada con la red / junto con otra información usada por el aparato 1700. En algunas implementaciones, el dispositivo de memoria 1708 y el medio de almacenamiento 1704 se implementan como un componente de memoria común. El dispositivo de memoria 1708 también se puede usar para almacenar datos que se manipulan por el circuito de procesamiento 1710 o algún otro componente del aparato 1700.

[0145] El medio de almacenamiento 1704 puede representar uno o más dispositivos legibles por ordenador, legibles por máquina y/o legibles por procesador para almacenar código, tales como código o instrucciones ejecutables por procesador (por ejemplo, software, firmware), datos electrónicos, bases de datos u otra información digital. El medio de almacenamiento 1704 también se puede usar para almacenar datos manipulados por el circuito de procesamiento 1710 cuando se ejecuta el código. El medio de almacenamiento 1704 puede ser cualquier medio disponible al que se pueda acceder mediante un procesador de propósito general o de propósito especial, incluidos dispositivos de almacenamiento portátiles o fijos, dispositivos de almacenamiento ópticos y otros medios diversos que puedan almacenar, contener o transportar código.

[0146] A modo de ejemplo y sin limitación, el medio de almacenamiento 1704 puede incluir un dispositivo de almacenamiento magnético (por ejemplo, disco duro, disco flexible, banda magnética), un disco óptico (por ejemplo, un disco compacto (CD) o un disco versátil digital (DVD)), una tarjeta inteligente, un dispositivo de memoria flash (por ejemplo, una tarjeta, una memoria USB o un lápiz USB), una memoria de acceso aleatorio (RAM), una memoria de solo lectura (ROM), una ROM programable (PROM), una PROM borrable (EPROM), una PROM borrable eléctricamente (EEPROM), un registro, un disco extraíble y cualquier otro medio adecuado para almacenar código al que se pueda acceder y que se pueda leer mediante un ordenador. El medio de almacenamiento 1704 puede estar incorporado en un artículo de fabricación (por ejemplo, un producto de programa informático). A modo de ejemplo, un producto de programa informático puede incluir un medio legible por ordenador

en materiales de embalaje. En vista de lo anterior, en algunas implementaciones, el medio de almacenamiento 1704 puede ser un medio de almacenamiento no transitorio (por ejemplo, tangible).

[0147] El medio de almacenamiento 1704 puede estar acoplado al circuito de procesamiento 1710 de modo que el circuito de procesamiento 1710 pueda leer información de, y escribir información en, el medio de almacenamiento 1704. Es decir, el medio de almacenamiento 1704 se puede acoplar al circuito de procesamiento 1710 de modo que el medio de almacenamiento 1704 sea al menos accesible por el circuito de procesamiento 1710, incluidos ejemplos donde al menos un medio de almacenamiento está integrado en el circuito de procesamiento 1710 y/o ejemplos donde al menos un medio de almacenamiento está separado del circuito de procesamiento 1710 (por ejemplo, residente en el aparato 1700, externo al aparato 1700, distribuido a través de múltiples entidades, etc.).

[0148] El código y/o las instrucciones almacenados por el medio de almacenamiento 1704, cuando son ejecutados por el circuito de procesamiento 1710, hacen que el circuito de procesamiento 1710 realice una o más de las diversas funciones y/u operaciones de proceso descritas en el presente documento. Por ejemplo, el medio de almacenamiento 1704 puede incluir operaciones configuradas para regular operaciones en uno o más bloques de hardware del circuito de procesamiento 1710, así como para utilizar la interfaz de comunicación 1702 para la comunicación inalámbrica utilizando sus respectivos protocolos de comunicación.

[0149] El circuito de procesamiento 1710 está adaptado, en general, para el procesamiento, incluida la ejecución de dicho código/instrucciones almacenados en el medio de almacenamiento 1704. Como se usa en el presente documento, el término "código" o "instrucciones" se debe interpretar en un sentido amplio para incluir, sin limitación, instrucciones, conjuntos de instrucciones, datos, código, segmentos de código, código de programa, programas, programas, subprogramas, módulos de software, aplicaciones, aplicaciones de software, paquetes de software, rutinas, subrutinas, objetos, ejecutables, hilos de ejecución, procedimientos, funciones, etc., independientemente de que se denominen software, firmware, middleware, microcódigo, lenguaje de descripción de hardware o de otro modo.

[0150] El circuito de procesamiento 1710 está dispuesto para obtener, procesar y/o enviar datos, controlar el acceso y el almacenamiento de datos, emitir comandos y controlar otras operaciones deseadas. El circuito de procesamiento 1710 puede incluir circuitos configurados para implementar el código deseado proporcionado por medios apropiados en al menos un ejemplo. Por ejemplo, el circuito de procesamiento 1710 puede implementarse como uno o más procesadores, uno o más controladores y/u otra estructura configurada para ejecutar código ejecutable. Ejemplos del circuito de procesamiento 1710 pueden incluir un procesador de propósito general, un procesador de señales digitales (DSP), un circuito integrado específico de la aplicación (ASIC), una matriz de puertas programables *in situ* (FPGA) u otro componente de lógica programable, lógica de transistor o de puertas discretas, componentes de hardware discretos o cualquier combinación de los mismos diseñada para realizar las funciones descritas en el presente documento. Un procesador de propósito general puede incluir un microprocesador, así como cualquier procesador, controlador, microcontrolador o máquina de estados convencional. El circuito de procesamiento 1710 también puede implementarse como una combinación de componentes informáticos, tal como una combinación de un DSP y un microprocesador, una pluralidad de microprocesadores, uno o más microprocesadores junto con un núcleo de DSP, un ASIC y un microprocesador o cualquier otra pluralidad de configuraciones variables. Estos ejemplos del circuito de procesamiento 1710 tienen fines ilustrativos y también se contemplan otras configuraciones adecuadas dentro del alcance de la divulgación.

[0151] De acuerdo con uno o más aspectos de la divulgación, el circuito de procesamiento 1710 se puede adaptar para realizar cualquiera o todas las características, procesos, funciones, operaciones y/o rutinas para cualquiera o todos los aparatos descritos en el presente documento. Como se usa en el presente documento, el término "adaptado" en relación con el circuito de procesamiento 1710 se puede referir a que el circuito de procesamiento 1710 está configurado, es utilizado, está implementado y/o está programado para realizar un proceso, función, operación y/o rutina particular de acuerdo con diversas características descritas en el presente documento.

[0152] De acuerdo con al menos un ejemplo del aparato 1700, el circuito de procesamiento 1710 puede incluir uno o más de un circuito/módulo de transmisión 1720, un circuito/módulo de recepción 1722, un circuito/módulo de almacenamiento de contexto de dispositivo cliente cifrado 1724, un circuito/módulo de determinación de contexto de dispositivo cliente 1726, un circuito/módulo de entrada en modo inactivo 1728, un circuito/módulo de establecimiento de contexto de seguridad 1730, un circuito/módulo de obtención de mensajes 1732 y un circuito/módulo de obtención de información de uso 1733 que están adaptados para realizar cualquiera o todos de las características, procesos, funciones, operaciones y/o rutinas descritas en el presente documento (por ejemplo, características, procesos, funciones, operaciones y/o rutinas descritos con respecto a las FIGS. 18-20).

[0153] El circuito/módulo de transmisión 1720 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones de transmisión 1734 almacenadas en el medio de almacenamiento 1704) adaptadas para realizar varias funciones relacionadas con, por ejemplo, transmitir una petición para comunicarse con una red, transmitir un mensaje que incluye al menos uno de los uno o más contextos de dispositivo cliente cifrado a la red, transmitir un paquete vacío con el contexto de dispositivo cliente cifrado UP a la red, transmitir una pluralidad de paquetes de datos que

incluyen una dirección de red a la red y transmitir un mensaje de petición de liberación de recursos a la red, en el que el mensaje de petición de liberación de recursos permite a la red liberar uno o más recursos para el dispositivo cliente.

[0154] El circuito/módulo de recepción 1722 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones recepción 1736 almacenadas en el medio de almacenamiento 1704) adaptadas para realizar varias funciones relacionadas con, por ejemplo, recibir uno o más contextos de dispositivo cliente cifrado de la red en respuesta a la petición, recibir un segundo paquete de datos, en el que recibir el segundo paquete de datos no establece una conexión de control de recursos de radio (RRC) con un nodo de acceso a la red, recibir un mensaje de búsqueda de la red y recibir una dirección de red para el dispositivo cliente en respuesta al mensaje.

[0155] El circuito/módulo de almacenamiento de contexto de dispositivo cliente cifrado 1724 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones 1738 de almacenamiento de contexto de dispositivo cliente cifrado almacenadas en el medio de almacenamiento 1704) adaptadas para realizar varias funciones relacionadas, por ejemplo, con el almacenamiento de uno o más contextos de dispositivo cliente cifrado en un almacenamiento local.

[0156] El circuito/módulo de determinación del contexto de dispositivo cliente cifrado 1726 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones 1740 de determinación del contexto de dispositivo cliente cifrado almacenadas en el medio de almacenamiento 1704) adaptadas para realizar varias funciones relacionadas, por ejemplo, con la determinación de al menos una del uno o más contextos de dispositivo cliente cifrado que se utilizarán basándose en si la comunicación comprende datos o información de control, y la determinación del al menos uno de los uno o más contextos de dispositivo cliente cifrado que está asociado con un servicio, en el que el al menos uno del uno o más contextos de dispositivo cliente cifrado permiten la reconstrucción de la parte del contexto de dispositivo cliente que soporta el servicio.

[0157] El circuito/módulo de entrada en modo inactivo 1728 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones de entrada en modo inactivo 1742 almacenadas en el medio de almacenamiento 1704) adaptadas para realizar varias funciones relacionadas con, por ejemplo, entrar en un modo inactivo inmediatamente después de transmitir el mensaje. que incluye el primer paquete de datos.

[0158] El circuito/módulo de establecimiento de contexto de seguridad 1730 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones 1744 de establecimiento de contexto de seguridad almacenadas en el medio de almacenamiento 1704) adaptadas para realizar varias funciones relacionadas, por ejemplo, con el establecimiento de un contexto de seguridad para una conexión con la red, en la que el contexto de seguridad incluye al menos un algoritmo de cifrado, una clave de cifrado, un algoritmo de protección de integridad, una clave de protección de integridad o combinaciones de los mismos.

[0159] El circuito/módulo de obtención de mensajes 1732 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones 1746 de obtención de mensajes almacenadas en el medio de almacenamiento 1704) adaptadas para realizar varias funciones relacionadas con, por ejemplo, la obtención de un mensaje, donde el mensaje está asociado servicio proporcionado por la red.

[0160] El circuito/módulo de obtención de información de uso 1733 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones de obtención de información de uso 1747 almacenadas en el medio de almacenamiento 1704) adaptadas para realizar varias funciones relacionadas con, por ejemplo, obtener información de uso asociada con el al menos uno de uno o más contextos de dispositivo cliente cifrado.

[0161] Como se ha mencionado anteriormente, las instrucciones almacenadas por el medio de almacenamiento 1704, cuando son ejecutados por el circuito de procesamiento 1710, hacen que el circuito de procesamiento 1710 realice una o más de las diversas funciones y/u operaciones de proceso descritas en el presente documento. Por ejemplo, el medio de almacenamiento 1704 puede incluir una o más de las instrucciones de transmisión 1734, instrucciones de recepción 1736, instrucciones de almacenamiento de contexto de dispositivo cliente cifrado 1738, instrucciones de determinación de contexto de dispositivo cliente cifrado 1740, instrucciones de entrada en modo inactivo 1742, instrucciones de establecimiento de contexto de seguridad 1744, instrucciones de obtención de mensajes 1746 e instrucciones de obtención de información de uso 1747.

[0162] La FIG. 18 (que incluye las FIGS. 18A y 18B) es un diagrama de flujo 1800 que ilustra un procedimiento para comunicarse con una red de acuerdo con varios aspectos de la divulgación. El procedimiento puede ser realizado por un aparato como un dispositivo cliente (por ejemplo, el dispositivo cliente 102, 502 o el aparato 1700). Debe entenderse que las operaciones indicadas por líneas discontinuas en la FIG. 18 representan operaciones opcionales.

[0163] El dispositivo cliente transmite una petición para comunicarse con una red 1802. En un ejemplo, la petición puede ser la petición 612 descrita previamente con respecto a la FIG. 6. En un aspecto, la petición puede incluir una indicación de que el dispositivo cliente está solicitando un contexto de dispositivo cliente cifrado y/o una

indicación de un servicio que está solicitando el dispositivo cliente. El dispositivo cliente establece un contexto de seguridad para una conexión con la red, en el que el contexto de seguridad incluye al menos un algoritmo de cifrado, una clave de cifrado, un algoritmo de protección de integridad y/o una clave de protección de integridad 1803. En un aspecto, la clave de cifrado es una clave de cifrado del plano de usuario y la clave de protección de integridad es una clave de protección de integridad del plano de usuario, la clave de cifrado del plano de usuario y la clave de protección de integridad del plano de usuario se mantienen en el dispositivo cliente y el primer paquete de datos tiene al menos protección de integridad con la clave de protección de integridad del plano de usuario o está cifrada con la clave de cifrado del plano de usuario.

[0164] El dispositivo cliente recibe uno o más contextos de dispositivo cliente cifrado de la red en respuesta a la petición 1804. En un ejemplo, uno o más contextos de dispositivo cliente cifrado pueden ser el contexto de dispositivo cliente cifrado en el mensaje de reconfiguración de la conexión RRC 626 recibido por el dispositivo cliente 602 en la FIG. 6. En un aspecto, el contexto de dispositivo cliente cifrado puede recibirse de la red como resultado de una auntentificación exitosa con la red. En tal aspecto, la auntentificación exitosa con la red no establece un contexto de seguridad de estrato de acceso (AS). Por ejemplo, el uno o más contextos de dispositivo cliente cifrado pueden incluir al menos uno de un contexto de seguridad, una calidad de servicio (QoS) para un portador y/o un identificador de punto final de túnel (TEID). En un aspecto, el uno o más contextos de dispositivo cliente cifrado pueden incluir un primer contexto que se utilizará para la comunicación relacionada con los datos con el dispositivo cliente y un segundo contexto que se utilizará para la comunicación relacionada con el control con el dispositivo cliente. En un aspecto, el uno o más contextos de dispositivo cliente cifrado pueden no descifrarse en el dispositivo cliente. En tal aspecto, el uno o más contextos de dispositivo cliente cifrado pueden ser descifrados solo por un dispositivo de red que generó el uno o más contextos de dispositivo cliente cifrado.

[0165] El dispositivo cliente almacena uno o más contextos de dispositivo cliente cifrado en un almacenamiento local 1806. El dispositivo cliente determina al menos uno de los uno o más contextos de dispositivo cliente cifrado que se utilizarán basándose en si un mensaje (por ejemplo, un paquete) que se va a transmitir desde el dispositivo cliente incluye datos o información de control 1808. Por ejemplo, uno o más contextos de dispositivo cliente cifrado pueden incluir un contexto de dispositivo cliente cifrado en el plano de usuario (UP) y un contexto de dispositivo cliente cifrado en el plano de control (CP). En tal ejemplo, el dispositivo cliente puede transmitir un primer paquete de datos con el contexto de dispositivo cliente cifrado UP, o un paquete de control con el contexto de dispositivo cliente cifrado CP. Por ejemplo, el paquete de control puede ser un paquete de actualización del área de seguimiento (TAU).

[0166] El dispositivo cliente transmite un mensaje que incluye al menos uno de los uno o más contextos de dispositivo cliente cifrado a la red 1810. En un ejemplo, el mensaje puede ser el mensaje de petición de transferencia de datos 810 que incluye un contexto de dispositivo cliente cifrado y un paquete de datos transmitido por el dispositivo 802 cliente al nodo 804 de acceso a la red en la FIG. 8. En un aspecto, el uno o más contextos de dispositivo cliente cifrado permiten la reconstrucción de un contexto en la red para la comunicación con el dispositivo cliente, incluyendo el contexto la información de estado de la red asociada con el dispositivo cliente. En un aspecto, el contexto se elimina (por ejemplo, se elimina o ya no se mantiene) en la red. En un aspecto, el dispositivo cliente puede transmitir el mensaje que incluye el primer paquete de datos sin establecer una conexión de control de recursos de radio (RRC) con un nodo de acceso a la red de la red. El dispositivo cliente entra en modo inactivo inmediatamente después de transmitir el mensaje que incluye el primer paquete de datos 1812.

[0167] El dispositivo cliente recibe un segundo paquete de datos, en el que la recepción del segundo paquete de datos no establece una conexión RRC con un nodo de acceso a la red 1814. En un ejemplo, el segundo paquete de datos puede ser el paquete de datos del quinto mensaje 824 transmitido al dispositivo cliente 802 desde el nodo de acceso a la red 804 en la FIG. 8. En un aspecto, la clave de cifrado es una clave de cifrado del plano de usuario y la clave de protección de integridad es una clave de protección de integridad del plano de usuario, donde la clave de cifrado del plano de usuario y la clave de protección de integridad del plano de usuario se mantienen en el dispositivo cliente. En tal aspecto, al recibir el segundo paquete de datos, el dispositivo cliente verifica el segundo paquete de datos con la clave de protección de integridad del plano de usuario y/o descifra el segundo paquete de datos con la clave de cifrado del plano de usuario. El dispositivo cliente recibe un mensaje de búsqueda de la red 1816. El dispositivo cliente transmite un paquete vacío con el contexto de dispositivo cliente cifrado UP a la red 1818.

[0168] La FIG. 19 muestra un diagrama de flujo 1900 que ilustra un procedimiento para la comunicación con una red de acuerdo con diversos aspectos de la presente divulgación. El procedimiento puede ser realizado por un aparato como un dispositivo cliente (por ejemplo, el dispositivo cliente 102, 502 o el aparato 1700). Debe entenderse que las operaciones indicadas por líneas discontinuas en la FIG. 19 representan operaciones opcionales.

[0169] El dispositivo cliente transmite una petición para comunicarse con una red 1902. En un ejemplo, la petición puede ser la petición 612 descrita previamente con respecto a la FIG. 6. En un aspecto, la petición puede incluir una indicación de que el dispositivo cliente está solicitando un contexto de dispositivo cliente cifrado y/o una indicación de un servicio que está solicitando el dispositivo cliente. El dispositivo cliente establece un contexto de

seguridad para una conexión con la red, en el que el contexto de seguridad incluye al menos un algoritmo de cifrado, una clave de cifrado, un algoritmo de protección de integridad y/o una clave de protección de integridad 1904. En un aspecto, la clave de cifrado es una clave de cifrado del plano de usuario y la clave de protección de integridad es una clave de protección de integridad del plano de usuario, la clave de cifrado del plano de usuario y la clave de protección de integridad del plano de usuario se mantienen en el dispositivo cliente y el primer paquete de datos tiene al menos protección de integridad con la clave de protección de integridad del plano de usuario o está cifrada con la clave de cifrado del plano de usuario.

[0170] El dispositivo cliente recibe uno o más contextos de dispositivo cliente cifrado de la red en respuesta a la petición 1906. En un ejemplo, uno o más contextos de dispositivo cliente cifrado pueden ser el contexto de dispositivo cliente cifrado en el mensaje de reconfiguración de la conexión RRC 626 recibido por el dispositivo cliente 602 en la FIG. 6. En un aspecto, el contexto de dispositivo cliente cifrado puede recibirse de la red como resultado de una auntentificación exitosa con la red. En tal aspecto, la auntentificación exitosa con la red no establece un contexto de seguridad de estrato de acceso (AS). Por ejemplo, el uno o más contextos de dispositivo cliente cifrado pueden incluir al menos uno de un contexto de seguridad, una calidad de servicio (QoS) para un portador y/o un identificador de punto final de túnel (TEID). En un aspecto, el uno o más contextos de dispositivo cliente cifrado pueden incluir un primer contexto que se utilizará para la comunicación relacionada con los datos con el dispositivo cliente y un segundo contexto que se utilizará para la comunicación relacionada con el control con el dispositivo cliente. En un aspecto, el uno o más contextos de dispositivo cliente cifrado pueden no descifrarse en el dispositivo cliente. En tal aspecto, el uno o más contextos de dispositivo cliente cifrado pueden ser descifrados solo por un dispositivo de red que generó el uno o más contextos de dispositivo cliente cifrado. En un aspecto, el contexto se elimina en la red después de que el dispositivo cliente recibe uno o más contextos de dispositivo cliente cifrado de la red. El dispositivo cliente transmite un mensaje que incluye al menos uno de los uno o más contextos de dispositivo cliente cifrado a la red 1908. En un aspecto, el uno o más contextos de dispositivo cliente cifrado permiten la reconstrucción de un contexto en la red para la comunicación con el dispositivo cliente, incluyendo el contexto la información de estado de la red asociada con el dispositivo cliente. En un aspecto, el mensaje incluye además una petición de establecimiento de recursos y al menos uno de los uno o más contextos de dispositivo cliente cifrado. Por ejemplo, el mensaje puede ser el mensaje de petición de establecimiento de recursos 1016. El dispositivo cliente recibe una dirección de red para el dispositivo cliente en respuesta al mensaje 1910. El dispositivo cliente transmite una pluralidad de paquetes de datos que incluyen la dirección de red a la red 1912. El dispositivo cliente transmite un mensaje de petición de liberación de recursos a la red, en el que el mensaje de petición de liberación de recursos permite a la red liberar uno o más recursos para el dispositivo cliente 1914.

[0171] La FIG. 20 muestra un diagrama de flujo 2000 que ilustra un procedimiento para la comunicación con una red de acuerdo con diversos aspectos de la presente divulgación. El procedimiento puede ser realizado por un aparato como un dispositivo cliente (por ejemplo, el dispositivo cliente 102, 502 o el aparato 1700). Debe entenderse que las operaciones indicadas por líneas discontinuas en la FIG. 20 representan operaciones opcionales.

[0172] En un aspecto, se proporciona un procedimiento para un dispositivo cliente. El dispositivo cliente transmite una petición para comunicarse con una red 2002. El dispositivo cliente establece un contexto de seguridad para una conexión con la red, en el que el contexto de seguridad incluye al menos un algoritmo de cifrado, una clave de cifrado, un algoritmo de protección de integridad, una clave de protección de integridad o combinaciones de los mismos 2004. El dispositivo cliente recibe uno o más contextos de dispositivo cliente cifrado de la red en respuesta a la petición 2006.

[0173] El dispositivo cliente obtiene un mensaje, donde el mensaje está asociado con un servicio proporcionado por la red 2008. En un aspecto, cada uno de los uno o más contextos de dispositivo cliente cifrado está asociado con uno de una pluralidad de servicios proporcionados por la red. En tal aspecto, el dispositivo cliente determina al menos uno de los uno o más contextos de dispositivo cliente cifrado que está asociado con el servicio, en el que al menos uno de los uno o más contextos de dispositivo cliente cifrado permite la reconstrucción de la parte del contexto de dispositivo cliente que soporta el servicio 2010. Por ejemplo, la pluralidad de servicios puede incluir un servicio de banda ancha móvil, un servicio de comunicaciones de baja latencia ultra fiable (URLLC), un servicio de acceso de alta prioridad, un servicio de acceso tolerante al retardo y/o un servicio de comunicaciones de tipo máquina (MTC).

[0174] El dispositivo cliente obtiene información de uso asociada con al menos uno de los uno o más contextos de dispositivo cliente cifrado 2012. En un aspecto, la información de uso asociada con al menos uno de los uno o más contextos de dispositivo cliente cifrado indica si la transmisión del mensaje es una transmisión de datos reducida o una transmisión de datos por ráfagas. En un aspecto, la información de uso puede incluir un valor (por ejemplo, un número de índice u otro valor) asociado con el contexto (o parte de un contexto) que será reconstruido por la red para un tipo de servicio proporcionado por la red.

[0175] El dispositivo cliente transmite un mensaje que incluye al menos uno de los uno o más contextos de dispositivo cliente cifrado a la red 2014. En un aspecto, el mensaje incluye la información de uso. En un aspecto, el uno o más contextos de dispositivo cliente cifrado permiten la reconstrucción de al menos una parte de un

contexto en la red para la comunicación con el dispositivo cliente, incluyendo el contexto información de estado de la red asociada con el dispositivo cliente. En un aspecto, la parte del contexto se mantiene en la red durante un período de tiempo que se determina basándose en si la transmisión del mensaje es la transmisión de datos reducida o la transmisión de datos por ráfagas. En un aspecto, el uno o más contextos de dispositivo cliente cifrado incluyen un primer contexto de dispositivo cliente cifrado en el plano de usuario que permite la reconstrucción de un primer contexto para el dispositivo cliente en una primera entidad en la red, y un segundo contexto de dispositivo cliente cifrado en el plano de usuario que permite la reconstrucción de un segundo contexto para el dispositivo cliente en una segunda entidad en la red. En tal aspecto, el mensaje incluye al menos el contexto de dispositivo cliente cifrado del primer plano de usuario y el contexto de dispositivo cliente cifrado del segundo plano de usuario.

Aparato a modo de ejemplo (por ejemplo, dispositivo de red) y procedimiento al respecto

[0176] La FIG. 21 es una ilustración de un aparato 2100 de acuerdo con uno o más aspectos de la divulgación (por ejemplo, aspectos relacionados con los procedimientos de las FIGS. 22-26 descritos a continuación). El aparato 2100 incluye una interfaz de comunicación de red (por ejemplo, al menos un transceptor) 2102, un medio de almacenamiento 2104, una interfaz de usuario 2106, un dispositivo de memoria 2108 y un circuito de procesamiento 2110. En un aspecto, el aparato 2100 puede ser un dispositivo de red (por ejemplo, un dispositivo de red 105, 505, 705) que implementa una función de Internet de las cosas (IoT). Por ejemplo, el aparato 2100 puede implementar una función de IoT en el plano de control (por ejemplo, IoTF-C 106, 506, 606, 706, 906, 1406) y/o una función de IoT en el plano de usuario (por ejemplo, IoTF-U 108, 508, 608, 708, 806, 908). Debe entenderse que dicho dispositivo de red puede implementarse como una única entidad de red o como múltiples entidades de red.

[0177] Estos componentes se pueden acoplar a y/o colocar en comunicación eléctrica entre sí por medio de un bus de señalización u otro componente adecuado, representado de forma genérica por las líneas de conexión en la FIG. 21. El bus de señalización puede incluir un número cualquiera de buses y puentes de interconexión, dependiendo de la aplicación específica del circuito de procesamiento 2110 y de las restricciones de diseño globales. El bus de señalización enlaza conjuntamente diversos circuitos de modo que cada uno de la interfaz de comunicación de red 2102, el medio de almacenamiento 2104, la interfaz de usuario 2106 y el dispositivo de memoria 2108 están acoplados a y/o en comunicación eléctrica con el circuito de procesamiento 2110. El bus de señalización también puede enlazar otros circuitos diversos (no mostrados) tales como fuentes de temporización, dispositivos periféricos, reguladores de voltaje y circuitos de gestión de potencia, que son bien conocidos en la técnica y, por consiguiente, no se describirán en mayor detalle.

[0178] La interfaz de comunicación de red 2102 se puede adaptar para facilitar la comunicación inalámbrica del aparato 2100. Por ejemplo, la interfaz de comunicación de red 2102 puede incluir circuitos y/o código (por ejemplo, instrucciones) adaptados para facilitar la comunicación de información bidireccionalmente con respecto a una o más entidades de red en una red. La interfaz de comunicación de red 2102 se puede configurar con uno o más receptores y/o transmisores independientes, así como uno o más transceptores.

[0179] El dispositivo de memoria 2108 puede representar uno o más dispositivos de memoria. Como se indica, el dispositivo de memoria 2108 puede mantener información relacionada con la red junto con otra información utilizada por el aparato 2100. En algunas implementaciones, el dispositivo de memoria 2108 y el medio de almacenamiento 2104 se implementan como un componente de memoria común. El dispositivo de memoria 2108 también se puede usar para almacenar datos que se manipulan por el circuito de procesamiento 2110 o algún otro componente del aparato 2100.

[0180] El medio de almacenamiento 2104 puede representar uno o más dispositivos legibles por ordenador, legibles por máquina y/o legibles por procesador para almacenar código, tales como código o instrucciones ejecutables por procesador (por ejemplo, software, firmware), datos electrónicos, bases de datos u otra información digital. El medio de almacenamiento 2104 también se puede usar para almacenar datos manipulados por el circuito de procesamiento 2110 cuando se ejecuta el código. El medio de almacenamiento 2104 puede ser cualquier medio disponible al que se pueda acceder mediante un procesador de propósito general o de propósito especial, incluidos dispositivos de almacenamiento portátiles o fijos, dispositivos de almacenamiento ópticos y otros medios diversos que puedan almacenar, contener o transportar código.

[0181] A modo de ejemplo y sin limitación, el medio de almacenamiento 2104 puede incluir un dispositivo de almacenamiento magnético (por ejemplo, disco duro, disco flexible, banda magnética), un disco óptico (por ejemplo, un disco compacto (CD) o un disco versátil digital (DVD)), una tarjeta inteligente, un dispositivo de memoria flash (por ejemplo, una tarjeta, una memoria USB o un lápiz USB), una memoria de acceso aleatorio (RAM), una memoria de solo lectura (ROM), una ROM programable (PROM), una PROM borrable (EPROM), una PROM borrable eléctricamente (EEPROM), un registro, un disco extraíble y cualquier otro medio adecuado para almacenar código al que se pueda acceder y que se pueda leer mediante un ordenador. El medio de almacenamiento 2104 puede estar incorporado en un artículo de fabricación (por ejemplo, un producto de programa informático). A modo de ejemplo, un producto de programa informático puede incluir un medio legible por ordenador

en materiales de embalaje. En vista de lo anterior, en algunas implementaciones, el medio de almacenamiento 2104 puede ser un medio de almacenamiento no transitorio (por ejemplo, tangible).

[0182] El medio de almacenamiento 2104 puede estar acoplado al circuito de procesamiento 2110 de modo que el circuito de procesamiento 2110 pueda leer información de, y escribir información en, el medio de almacenamiento 2104. Es decir, el medio de almacenamiento 2104 se puede acoplar al circuito de procesamiento 2110 de modo que el medio de almacenamiento 2104 sea al menos accesible por el circuito de procesamiento 2110, incluidos ejemplos donde al menos un medio de almacenamiento está integrado en el circuito de procesamiento 2110 y/o ejemplos donde al menos un medio de almacenamiento está separado del circuito de procesamiento 2110 (por ejemplo, residente en el aparato 2100, externo al aparato 2100, distribuido a través de múltiples entidades, etc.).

[0183] El código y/o las instrucciones almacenados por el medio de almacenamiento 2104, cuando son ejecutados por el circuito de procesamiento 2110, hacen que el circuito de procesamiento 2110 realice una o más de las diversas funciones y/u operaciones de proceso descritas en el presente documento. Por ejemplo, el medio de almacenamiento 2104 puede incluir operaciones configuradas para regular operaciones en uno o más bloques de hardware del circuito de procesamiento 2110, así como para utilizar la interfaz de comunicación de red 2102 para la comunicación de red utilizando sus respectivos protocolos de comunicación.

[0184] El circuito de procesamiento 2110 está adaptado, en general, para el procesamiento, incluida la ejecución de dicho código/instrucciones almacenados en el medio de almacenamiento 2104. Como se usa en el presente documento, el término "código" o "instrucciones" se debe interpretar en un sentido amplio para incluir, sin limitación, instrucciones, conjuntos de instrucciones, datos, código, segmentos de código, código de programa, programas, programas, subprogramas, módulos de software, aplicaciones, aplicaciones de software, paquetes de software, rutinas, subrutinas, objetos, ejecutables, hilos de ejecución, procedimientos, funciones, etc., independientemente de que se denominen software, firmware, middleware, microcódigo, lenguaje de descripción de hardware o de otro modo.

[0185] El circuito de procesamiento 2110 está dispuesto para obtener, procesar y/o enviar datos, controlar el acceso y el almacenamiento de datos, emitir comandos y controlar otras operaciones deseadas. El circuito de procesamiento 2110 puede incluir circuitos configurados para implementar el código deseado proporcionado por medios apropiados en al menos un ejemplo. Por ejemplo, el circuito de procesamiento 2110 puede implementarse como uno o más procesadores, uno o más controladores y/u otra estructura configurada para ejecutar código ejecutable. Ejemplos del circuito de procesamiento 2110 pueden incluir un procesador de propósito general, un procesador de señales digitales (DSP), un circuito integrado específico de la aplicación (ASIC), una matriz de puertas programables *in situ* (FPGA) u otro componente de lógica programable, lógica de transistor o de puertas discretas, componentes de hardware discretos o cualquier combinación de los mismos diseñada para realizar las funciones descritas en el presente documento. Un procesador de propósito general puede incluir un microprocesador, así como cualquier procesador, controlador, microcontrolador o máquina de estados convencional. El circuito de procesamiento 2110 también puede implementarse como una combinación de componentes informáticos, tal como una combinación de un DSP y un microprocesador, una pluralidad de microprocesadores, uno o más microprocesadores junto con un núcleo de DSP, un ASIC y un microprocesador o cualquier otra pluralidad de configuraciones variables. Estos ejemplos del circuito de procesamiento 2110 tienen fines ilustrativos y también se contemplan otras configuraciones adecuadas dentro del alcance de la divulgación.

[0186] De acuerdo con uno o más aspectos de la divulgación, el circuito de procesamiento 2110 se puede adaptar para realizar cualquiera o todas las características, procesos, funciones, operaciones y/o rutinas para cualquiera o todos los aparatos descritos en el presente documento. Como se usa en el presente documento, el término "adaptado" en relación con el circuito de procesamiento 2110 se puede referir a que el circuito de procesamiento 2110 está configurado, es utilizado, está implementado y/o está programado para realizar un proceso, función, operación y/o rutina particular de acuerdo con diversas características descritas en el presente documento.

[0187] De acuerdo con al menos un ejemplo del aparato 2100, el circuito de procesamiento 2110 puede incluir uno o más de un circuito/módulo de transmisión 2120, un circuito/módulo de recepción 2122, un circuito/módulo de auntentificación y verificación 2124, un circuito/módulo de generación de contexto de dispositivo cliente cifrado 2126, circuito/módulo de reconstrucción/eliminación de contexto 2128, circuito/módulo de procesamiento de paquetes 2130, circuito/módulo de almacenamiento 2132, circuito/módulo de determinación de nodo de acceso a la red 2134, circuito/módulo de adición de identificador temporal 2136, un circuito/módulo de obtención/liberación de dirección de red 2137, un circuito/módulo de cifrado y protección de paquetes 2138, y un circuito/módulo de establecimiento de contexto de seguridad 2139 que están adaptados para realizar cualquiera o todas las características, procesos, funciones, operaciones y/o rutinas descritas en el presente documento (por ejemplo, características, procesos, funciones, operaciones y/o rutinas descritas con respecto a las FIGS. 22-26).

[0188] El circuito/módulo de transmisión 2120 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones de transmisión 2140 almacenadas en el medio de almacenamiento 2104) adaptadas para realizar varias funciones relacionadas, por ejemplo, con transmitir uno o más contextos de dispositivo cliente cifrado al dispositivo cliente,

transmitir un nuevo contexto de dispositivo cliente cifrado a un segundo dispositivo cliente, reenviar una parte de carga útil del paquete de control a un servidor de aplicaciones o pasarela de red de paquetes de datos (P-GW), reenviar el paquete de control al dispositivo cliente, reenviar el primer paquete de datos a la red de servicio, reenviar el segundo paquete de datos al dispositivo cliente y/o transmitir la dirección de red al dispositivo cliente.

[0189] El circuito/módulo de recepción 2122 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones de recepción 2142 almacenadas en el medio de almacenamiento 2104) adaptadas para realizar varias funciones relacionadas con, por ejemplo, recibir, desde un dispositivo cliente, una petición para comunicarse con un red, recibir un paquete de control y un contexto de dispositivo cliente cifrado desde el dispositivo cliente, recibir un primer paquete de datos y un contexto de dispositivo cliente cifrado desde el dispositivo cliente, recibir un segundo paquete de datos de un servidor o una pasarela de red de paquetes de datos (P- GW), recibir un paquete de control de un segundo dispositivo cliente, recibir el contexto de un segundo dispositivo cliente de un segundo dispositivo de red, recibir un mensaje que incluye una petición de establecimiento de recursos y al menos uno de los uno o más contextos de dispositivo cliente cifrado del dispositivo cliente, que recibe un mensaje del dispositivo cliente, el mensaje incluye al menos uno de los uno o más contextos de dispositivo cliente cifrado e información de uso como asociado con uno o más contextos de dispositivo cliente cifrado, y/o recibir un mensaje de petición de liberación de recursos desde el dispositivo cliente.

[0190] El circuito/módulo de auntentificación y verificación 2124 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones de auntentificación y verificación 2144 almacenadas en el medio de almacenamiento 2104) adaptadas para realizar varias funciones relacionadas, por ejemplo, con la petición de información de auntentificación de un servidor de abonado doméstico (HSS)/servidor de auntentificación, autorización y contabilidad (AAA), que realiza la auntentificación mutua con el dispositivo cliente y verifica el contexto de dispositivo cliente cifrado recibido del dispositivo cliente.

[0191] El circuito/módulo de generación de contexto de dispositivo cliente cifrado 2126 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones de generación de contexto de dispositivo cliente cifrado 2146 almacenadas en el medio de almacenamiento 2104) adaptadas para realizar varias funciones relacionadas con, por ejemplo, generar una o más contextos de dispositivo cliente, en los que uno o más contextos de dispositivo cliente cifrado permiten la reconstrucción de al menos un contexto en la red para la comunicación con el dispositivo cliente, determinar si el contexto de dispositivo cliente cifrado ha expirado, generar un nuevo contexto de dispositivo cliente cifrado, determinar para generar uno o más contextos de dispositivo cliente cifrado, donde la determinación se basa en al menos una de la información de uso del contexto de dispositivo cliente cifrado indicada en la petición, una suscripción del dispositivo o una política, y pedir a un dispositivo cliente contexto para un segundo dispositivo cliente de un segundo dispositivo de red, con la petición que incluye un contexto de dispositivo cliente cifrado de plano de control (CP). Por ejemplo, el uno o más contextos de dispositivo cliente cifrado pueden incluir un primer contexto que se utilizará para la comunicación relacionada con datos y un segundo contexto que se utilizará para la comunicación relacionada con el control.

[0192] El circuito/módulo de reconstrucción/eliminación de contexto 2128 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones de reconstrucción/eliminación de contexto 2148 almacenadas en el medio de almacenamiento 2104) adaptadas para realizar varias funciones relacionadas con, por ejemplo, obtener una clave (por ejemplo, la clave $K_{CDC\text{-}IoTF\text{-}U}$) para un contexto de dispositivo cliente cifrado asociado con un dispositivo cliente, obtener un contexto de seguridad para el dispositivo cliente a partir del contexto de dispositivo cliente cifrado basado en la clave, reconstruir el al menos un contexto de dispositivo cliente cifrado contexto, reconstruir al menos una parte de un contexto basado en al menos uno de los uno o más contextos de dispositivo cliente cifrado y la información de uso, eliminar al menos un contexto y/o mantener al menos una parte de un contexto para un primer período de tiempo umbral cuando la información de uso indica una transmisión de datos reducida, o un segundo período de tiempo umbral cuando la información de uso indica una transmisión de datos en ráfaga, siendo el segundo período de tiempo umbral mayor que el primer período de tiempo umbral.

[0193] El circuito/módulo de procesamiento de paquetes 2130 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones de procesamiento de paquetes 2150 almacenadas en el medio de almacenamiento 2104) adaptadas para realizar varias funciones relacionadas, por ejemplo, con el procesamiento del paquete de control usando el al menos un contexto, en el que el procesamiento incluye al menos uno de verificar o descifrar el paquete de control usando el contexto.

[0194] El circuito/módulo de almacenamiento 2132 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones de almacenamiento 2152 almacenadas en el medio de almacenamiento 2104) adaptadas para realizar varias funciones relacionadas con, por ejemplo, almacenar un identificador temporal (ID) para un paquete de enlace descendente para el dispositivo cliente.

[0195] El circuito/módulo de determinación del nodo de acceso a la red 2134 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones de determinación del nodo de acceso a la red 2154 almacenadas en el medio de almacenamiento 2104) adaptadas para realizar varias funciones relacionadas, por ejemplo, con la determinación de un nodo de acceso a la red al que se reenvía el segundo paquete de datos.

[0196] El circuito/módulo de adición de identificador temporal 2136 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones de adición de identificador temporal 2156 almacenadas en el medio de almacenamiento 2104) adaptadas para realizar varias funciones relacionadas, por ejemplo, con la adición de un identificador temporal al segundo paquete de datos. que permite al nodo de acceso a la red determinar el dispositivo cliente.

[0197] El circuito/módulo de obtención/liberación de direcciones de red 2137 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones de obtención/liberación de direcciones de red 2157 almacenadas en el medio de almacenamiento 2104) adaptadas para realizar varias funciones relacionadas con, por ejemplo, obtener una dirección de red para el dispositivo cliente en respuesta al mensaje, transmitir un mensaje de petición de liberación de recursos desde el dispositivo cliente a una pasarela, en el que el mensaje de petición de liberación de recursos hace que la pasarela libere la dirección de red para el dispositivo cliente y/o transmitir una petición de liberación de recursos mensaje a una pasarela cuando un temporizador expira antes de una transmisión desde el dispositivo cliente a la red o antes de una transmisión desde la red al dispositivo cliente, en el que el mensaje de petición de liberación de recursos permite que la pasarela libere uno o más recursos para el dispositivo cliente.

[0198] El circuito/módulo de cifrado y protección de paquetes 2138 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones de cifrado y protección de paquetes 2158 almacenadas en el medio de almacenamiento 2104) adaptadas para realizar varias funciones relacionadas con, por ejemplo, cifrado o protección de integridad del paquete utilizando una clave de dispositivo cliente de plano de usuario (UP), que descifra y verifica el primer paquete de datos basándose en el contexto de seguridad, y/o cifra o protege la integridad del segundo paquete de datos utilizando la clave de cifrado de plano de usuario o la clave de protección de integridad de plano de usuario.

[0199] El circuito/módulo de establecimiento de contexto de seguridad 2139 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones de establecimiento de contexto de seguridad 2159 almacenadas en el medio de almacenamiento 2104) adaptadas para realizar varias funciones relacionadas con, por ejemplo, establecer al menos un contexto con el dispositivo cliente, con el al menos un contexto que incluye información de estado de la red asociada con una conexión entre el dispositivo cliente y la red, en el que la información de estado de la red incluye al menos un algoritmo de cifrado, una clave de cifrado, un algoritmo de protección de integridad, una clave de protección de integridad o combinaciones de los mismos.

[0200] Como se ha mencionado anteriormente, las instrucciones almacenadas por el medio de almacenamiento 2104, cuando son ejecutados por el circuito de procesamiento 2110, hacen que el circuito de procesamiento 2110 realice una o más de las diversas funciones y/u operaciones de proceso descritas en el presente documento. Por ejemplo, el medio de almacenamiento 2104 puede incluir una o más de las instrucciones de transmisión 2140, instrucciones de recepción 2142, instrucciones de auntentificación y verificación 2144, instrucciones de generación de contexto de dispositivo cliente cifrado 2146, instrucciones de reconstrucción/eliminación de contexto 2148, instrucciones de procesamiento de paquetes 2150, instrucciones de almacenamiento 2152, instrucciones de determinación de nodo de acceso a la red 2154, instrucciones de adición de identificador temporal 2156, instrucciones de obtención/liberación de direcciones de red 2157, instrucciones de cifrado y protección de paquetes 2158 e instrucciones de establecimiento de contexto de seguridad 2159.

[0201] La FIG. 22 (que incluye las FIGS. 22A y 22B) es un diagrama de flujo 2200 que ilustra un procedimiento para comunicarse en una arquitectura de red de IoT de acuerdo con varios aspectos de la divulgación. El procedimiento puede ser realizado por un aparato como un dispositivo de red (por ejemplo, el dispositivo de red 105 de la FIG. 1 o el aparato 2100 de la FIG. 21) que implementa una función de IoT (por ejemplo, un plano de control de IoTF, como el plano de control IoTF 106 de la FIG. 1). Se debe entender que las operaciones indicadas con líneas discontinuas en la FIG. 22 representan operaciones opcionales.

[0202] El aparato recibe, desde un dispositivo cliente, una petición para comunicarse con una red 2202. El aparato solicita información de auntentificación de un servidor de abonado doméstico (HSS)/servidor 2204 de auntentificación, autorización y contabilidad (AAA). El aparato realiza una auntentificación mutua con el dispositivo cliente 2206.

[0203] El aparato establece al menos un contexto con el dispositivo cliente, incluyendo el al menos un contexto información de estado de la red asociada con una conexión entre el dispositivo cliente y la red 2207. En un aspecto, la información de estado de la red incluye al menos un algoritmo de cifrado, una clave de cifrado, un algoritmo de protección de integridad y/o una clave de protección de integridad. El aparato determina generar uno o más contextos de dispositivo cliente cifrado, en los que la determinación se basa en al menos una de la información de uso del contexto de dispositivo cliente cifrado indicada en la petición, una suscripción del dispositivo cliente y/o una política 2208.

[0204] El aparato genera uno o más contextos 2210 de dispositivo cliente cifrado. En un aspecto, el uno o más contextos de dispositivo cliente cifrado permiten la reconstrucción de un contexto en la red para la comunicación con el dispositivo cliente. En un aspecto, el uno o más contextos de dispositivo cliente cifrado incluyen un primer contexto que se utilizará para la comunicación relacionada con los datos y un segundo contexto que se utilizará

para la comunicación relacionada con el control. El aparato transmite uno o más contextos de dispositivo cliente cifrado al dispositivo cliente 2212.

[0205] El aparato recibe un paquete de control y un contexto de dispositivo cliente cifrado desde el dispositivo cliente 2214. El aparato verifica el contexto de dispositivo cliente cifrado recibido desde el dispositivo cliente 2216. En un aspecto, el aparato verifica el contexto de dispositivo cliente cifrado recibido del dispositivo cliente determinando si el contexto de dispositivo cliente cifrado ha expirado, genera uno o más contextos nuevos del dispositivo cliente cifrado cuando el contexto de dispositivo cliente cifrado anterior ha expirado, y transmite el uno o más contextos de dispositivo cliente cifrado nuevos para el dispositivo cliente cuando el contexto de dispositivo cliente cifrado anterior ha expirado. En un aspecto, verificar el contexto de dispositivo cliente cifrado incluye determinar una clave para verificar el contexto de dispositivo cliente cifrado.

[0206] El aparato reconstruye el al menos un contexto a partir del contexto 2218 del dispositivo cliente cifrado. El aparato procesa el paquete de control usando el al menos un contexto, donde el procesamiento incluye al menos uno de verificar o descifrar el paquete de control usando el al menos un contexto 2220. El aparato almacena un identificador (ID) temporal para un paquete de enlace descendente para el dispositivo cliente 2222. El aparato reenvía una parte de carga útil del paquete de control a un servidor de aplicaciones o pasarela de red de paquetes de datos (P-GW) 2224.

[0207] La FIG. 23 (que incluye las FIGS. 23A y 23B) es un diagrama de flujo 2300 que ilustra un procedimiento para comunicarse en una arquitectura de red de IoT de acuerdo con varios aspectos de la divulgación. El procedimiento puede ser realizado por un aparato como un dispositivo de red (por ejemplo, el dispositivo de red 105 de la FIG. 1 o el aparato 2100 de la FIG. 21) que implementa una función de IoT (por ejemplo, un plano de control de IoTF, como el plano de control IoTF 106 de la FIG. 1). Se debe entender que las operaciones indicadas con líneas discontinuas en la FIG. 23 representan operaciones opcionales.

[0208] El aparato recibe, desde un dispositivo cliente, una petición para comunicarse con una red 2302. El aparato establece al menos un contexto con el dispositivo cliente, incluyendo el al menos un contexto información de estado de la red asociada con una conexión entre el dispositivo cliente y la red, donde la información de estado de la red incluye al menos un algoritmo de cifrado, una clave de cifrado, una algoritmo de protección de integridad y/o una clave de protección de integridad 2304. El aparato genera uno o más contextos 2306 de dispositivo cliente cifrado. En un aspecto, el uno o más contextos de dispositivo cliente cifrado permiten la reconstrucción de al menos un contexto en la red para la comunicación con el dispositivo cliente. El aparato transmite uno o más contextos de dispositivo cliente cifrado al dispositivo cliente 2308. El aparato elimina el al menos un contexto 2310. El aparato recibe un mensaje del dispositivo cliente, incluyendo el mensaje al menos uno de los uno o más contextos de dispositivo cliente cifrado e información de uso asociada con uno o más contextos 2312 de dispositivo cliente cifrado. En un aspecto, la información de uso indica si la transmisión del mensaje es una transmisión de datos reducida o una transmisión de datos por ráfagas. En un aspecto, el dispositivo de red puede reconstruir al menos una parte de un contexto basándose en al menos uno de los uno o más contextos de dispositivo cliente cifrado y la información de uso. En un aspecto, el mensaje del dispositivo cliente incluye una petición de establecimiento de recursos y al menos uno de los uno o más contextos de dispositivo cliente cifrado. Por ejemplo, el mensaje puede ser el mensaje de petición de establecimiento de recursos 1016 en la FIG. 10. El aparato obtiene una dirección de red para el dispositivo cliente en respuesta al mensaje 2314. El aparato transmite la dirección de red al dispositivo cliente 2316. En un aspecto, el aparato mantiene al menos una parte de un contexto durante un primer período de tiempo umbral cuando la información de uso indica una transmisión de datos reducida, o un segundo período de tiempo umbral cuando la información de uso indica una transmisión de datos en ráfaga, siendo el segundo período de tiempo umbral mayor que el primer período de tiempo umbral. En un aspecto, el aparato transmite un mensaje de petición de liberación de recursos a una pasarela cuando un temporizador expira antes de una transmisión desde el dispositivo cliente a la red o antes de una transmisión desde la red al dispositivo cliente 2318. En un aspecto, el mensaje de petición de liberación de recursos permite que la pasarela libere uno o más recursos para el dispositivo cliente. En otro aspecto, el aparato recibe un mensaje de petición de liberación de recursos desde el dispositivo cliente 2320. En tal aspecto, el aparato transmite el mensaje de petición de liberación de recursos desde el dispositivo cliente a una pasarela 2322. En un aspecto, el mensaje de petición de liberación de recursos permite que la pasarela libere uno o más recursos para el dispositivo cliente. En algunos aspectos, la operación 2318 y las operaciones 2320 y 2322 pueden realizarse de forma alternativa. Por ejemplo, si se realiza la operación 2318, es posible que no se realicen las operaciones 2320 y 2322. Como otro ejemplo, si se realizan las operaciones 2320 y 2322, es posible que no se realice la operación 2318.

[0209] La FIG. 24 es un diagrama de flujo 2400 que ilustra un procedimiento para comunicación en una arquitectura de red de IoT de acuerdo con diversos aspectos de la divulgación. El procedimiento puede ser realizado por un aparato como un dispositivo de red (por ejemplo, el dispositivo de red 105 de la FIG. 1 o el aparato 2100 de la FIG. 21) que implementa una función de IoT (por ejemplo, un plano de control de IoTF, como el plano de control IoTF 106 de la FIG. 1).

[0210] El aparato recibe un paquete del plano de control de un segundo dispositivo cliente 2402. En un aspecto, el segundo dispositivo cliente es diferente del dispositivo cliente desde el que se recibe inicialmente la petición

para comunicarse con la red. El aparato solicita un contexto para el segundo dispositivo cliente desde un segundo dispositivo de red, incluyendo la petición un contexto 2404 de dispositivo cliente cifrado en el plano de control (CP). El aparato recibe el contexto para el segundo dispositivo cliente desde el segundo dispositivo de red 2406. El aparato genera un nuevo contexto 2408 de dispositivo cliente cifrado. El aparato transmite el nuevo contexto de dispositivo cliente cifrado al segundo dispositivo cliente 2410.

[0211] La FIG. 25 (que incluye las FIGS. 25A y 25B) es un diagrama de flujo 2500 que ilustra un procedimiento para comunicarse en una arquitectura de red de IoT de acuerdo con varios aspectos de la divulgación. El procedimiento puede ser realizado por un aparato como un dispositivo de red (por ejemplo, el dispositivo de red 105 de la FIG. 1 o el aparato 2100 de la FIG. 21) que implementa una función de IoT (por ejemplo, un plano de usuario IoTF, como el usuario plano IoTF 108 de la FIG. 1). Se debe entender que las operaciones indicadas con líneas discontinuas en la FIG. 25 representan operaciones opcionales.

[0212] El aparato obtiene una clave (por ejemplo, la clave $K_{CDC\text{-}IoTF\text{-}U}$) para un contexto de dispositivo cliente cifrado asociado con un dispositivo cliente 2502. El aparato recibe un primer paquete de datos (por ejemplo, paquete de datos UL) y el contexto de dispositivo cliente cifrado desde el dispositivo cliente 2504. El aparato obtiene un contexto de seguridad para el dispositivo cliente a partir del contexto de dispositivo cliente cifrado utilizando la clave 2506. El aparato descifra y verifica el primer paquete de datos basándose en el contexto de seguridad 2508. El aparato envía el primer paquete de datos a una red de servicios cuando el descifrado y la verificación son exitosos 2510.

[0213] En un aspecto, el aparato recibe un segundo paquete de datos (por ejemplo, el paquete de datos DL en el mensaje 914 de la FIG. 9) desde un servidor o una pasarela de red de paquetes de datos 2512. El aparato determina un nodo de acceso a la red al que se reenvía el segundo paquete de datos 2514. El aparato añade un identificador temporal al segundo paquete de datos que permite al nodo de acceso a la red determinar el dispositivo cliente 2516. El aparato cifra o protege la integridad del segundo paquete de datos usando la clave de cifrado del plano de usuario o la clave 2518 de protección de integridad del plano de usuario. El aparato reenvía (por ejemplo, a través del mensaje 934 en la FIG. 9) el segundo paquete de datos al dispositivo cliente 2520.

[0214] La FIG. 26 (que incluye las FIGS. 26A y 26B) es un diagrama de flujo 2600 que ilustra un procedimiento para comunicarse en una arquitectura de red de IoT de acuerdo con varios aspectos de la divulgación. El procedimiento puede ser realizado por un aparato como un dispositivo de red (por ejemplo, el dispositivo de red 105 de la FIG. 1 o el aparato 2100 de la FIG. 21) que implementa una función de IoT (por ejemplo, un plano de control de IoTF, como el plano de control IoTF 106 de la FIG. 1). Se debe entender que las operaciones indicadas con líneas discontinuas en la FIG. 26 representan operaciones opcionales.

[0215] El aparato recibe, desde un dispositivo cliente, una petición para comunicarse con una red 2602. El aparato solicita información de auntentificación de un servidor de abonado doméstico (HSS)/servidor 2604 de auntentificación, autorización y contabilidad (AAA). El aparato realiza una auntentificación mutua con el dispositivo cliente 2606.

[0216] El aparato establece al menos un contexto con el dispositivo cliente, incluyendo el al menos un contexto información de estado de la red asociada con una conexión entre el dispositivo cliente y la red 2608. En un aspecto, la información de estado de la red incluye al menos un algoritmo de cifrado, una clave de cifrado, un algoritmo de protección de integridad y/o una clave de protección de integridad. El aparato determina generar uno o más contextos de dispositivo cliente cifrado, en los que la determinación se basa en al menos una de la información de uso del contexto de dispositivo cliente cifrado indicada en la petición, una suscripción del dispositivo cliente y/o una política 2610.

[0217] El aparato genera uno o más contextos 2612 de dispositivo cliente cifrado. En un aspecto, el uno o más contextos de dispositivo cliente cifrado permiten la reconstrucción de un contexto en la red para la comunicación con el dispositivo cliente. En un aspecto, el uno o más contextos de dispositivo cliente cifrado incluyen un primer contexto que se utilizará para la comunicación relacionada con los datos y un segundo contexto que se utilizará para la comunicación relacionada con el control. El aparato transmite uno o más contextos de dispositivo cliente cifrado al dispositivo cliente 2614. El aparato elimina el al menos un contexto 2616. El aparato recibe un mensaje del dispositivo cliente, incluyendo el mensaje al menos uno de los uno o más contextos de dispositivo cliente cifrado e información de uso asociada con uno o más contextos 2618 de dispositivo cliente cifrado. El aparato reconstruye al menos una parte de un contexto basándose en al menos uno de los uno o más contextos de dispositivo cliente cifrado y la información de uso 2620. El aparato mantiene al menos una parte de un contexto durante un primer período de tiempo umbral cuando la información de uso indica una transmisión de datos reducida, o un segundo período de tiempo umbral cuando la información de uso indica una transmisión de datos en ráfaga, siendo el segundo período de tiempo umbral mayor que el primer período de tiempo umbral 2622.

Aparato a modo de ejemplo (por ejemplo, nodo de acceso a la red) y procedimiento al respecto

[0218] La FIG. 27 es una ilustración de un aparato 2700 de acuerdo con uno o más aspectos de la divulgación (por ejemplo, aspectos relacionados con los procedimientos de las FIGs. 28 y 29 descritos a continuación). El aparato 2700 incluye una interfaz de comunicación (por ejemplo, al menos un transceptor) 2702, una interfaz de comunicación de red 2703, un medio de almacenamiento 2704, una interfaz de usuario 2706, un dispositivo de memoria 2708 y un circuito de procesamiento 2710.

[0219] Estos componentes se pueden acoplar a y/o colocar en comunicación eléctrica entre sí por medio de un bus de señalización u otro componente adecuado, representado de forma genérica por las líneas de conexión en la FIG. 27. El bus de señalización puede incluir un número cualquiera de buses y puentes de interconexión, dependiendo de la aplicación específica del circuito de procesamiento 2710 y de las restricciones de diseño globales. El bus de señalización enlaza conjuntamente diversos circuitos de modo que cada uno de la interfaz de comunicación 2702, la interfaz de comunicación de red 2703, el medio de almacenamiento 2704, la interfaz de usuario 2706 y el dispositivo de memoria 2708 están acoplados a y/o en comunicación eléctrica con el circuito de procesamiento 2710. El bus de señalización también puede enlazar otros circuitos diversos (no mostrados) tales como fuentes de temporización, dispositivos periféricos, reguladores de voltaje y circuitos de gestión de potencia, que son bien conocidos en la técnica y, por consiguiente, no se describirán en mayor detalle.

[0220] La interfaz de comunicación 2702 se puede adaptar para facilitar la comunicación inalámbrica del aparato 2700. Por ejemplo, la interfaz de comunicación 2702 puede incluir circuitos y/o código (por ejemplo, instrucciones) adaptados para facilitar la comunicación de información bidireccionalmente con respecto a uno o más dispositivos de comunicación en una red. La interfaz de comunicación 2702 puede estar acoplada a una o más antenas 2712 para la comunicación inalámbrica dentro de un sistema de comunicación inalámbrica. La interfaz de comunicación 2702 se puede configurar con uno o más receptores y/o transmisores independientes, así como uno o más transceptores. En el ejemplo ilustrado, la interfaz de comunicación 2702 incluye un transmisor 2714 y un receptor 2716.

[0221] La interfaz de comunicación de red 2703 se puede adaptar para facilitar la comunicación inalámbrica del aparato 2700. Por ejemplo, la interfaz de comunicación de red 2703 puede incluir circuitos y/o código (por ejemplo, instrucciones) adaptados para facilitar la comunicación de información bidireccionalmente con respecto a una o más entidades de red en una red. La interfaz de comunicación de red 2703 se puede configurar con uno o más receptores y/o transmisores independientes, así como uno o más transceptores.

[0222] El dispositivo de memoria 2708 puede representar uno o más dispositivos de memoria. Como se indica, el dispositivo de memoria 2708 puede mantener información relacionada con la red / junto con otra información usada por el aparato 2700. En algunas implementaciones, el dispositivo de memoria 2708 y el medio de almacenamiento 2704 se implementan como un componente de memoria común. El dispositivo de memoria 2708 también se puede usar para almacenar datos que se manipulan por el circuito de procesamiento 2710 o algún otro componente del aparato 2700.

[0223] El medio de almacenamiento 2704 puede representar uno o más dispositivos legibles por ordenador, legibles por máquina y/o legibles por procesador para almacenar código, tales como código o instrucciones ejecutables por procesador (por ejemplo, software, firmware), datos electrónicos, bases de datos u otra información digital. El medio de almacenamiento 2704 también se puede usar para almacenar datos manipulados por el circuito de procesamiento 2710 cuando se ejecuta el código. El medio de almacenamiento 2704 puede ser cualquier medio disponible al que se pueda acceder mediante un procesador de propósito general o de propósito especial, incluidos dispositivos de almacenamiento portátiles o fijos, dispositivos de almacenamiento ópticos y otros medios diversos que puedan almacenar, contener o transportar código.

[0224] A modo de ejemplo y sin limitación, el medio de almacenamiento 2704 puede incluir un dispositivo de almacenamiento magnético (por ejemplo, disco duro, disco flexible, banda magnética), un disco óptico (por ejemplo, un disco compacto (CD) o un disco versátil digital (DVD)), una tarjeta inteligente, un dispositivo de memoria flash (por ejemplo, una tarjeta, una memoria USB o un lápiz USB), una memoria de acceso aleatorio (RAM), una memoria de solo lectura (ROM), una ROM programable (PROM), una PROM borrable (EPROM), una PROM borrable eléctricamente (EEPROM), un registro, un disco extraíble y cualquier otro medio adecuado para almacenar código al que se pueda acceder y que se pueda leer mediante un ordenador. El medio de almacenamiento 2704 puede estar incorporado en un artículo de fabricación (por ejemplo, un producto de programa informático). A modo de ejemplo, un producto de programa informático puede incluir un medio legible por ordenador en materiales de embalaje. En vista de lo anterior, en algunas implementaciones, el medio de almacenamiento 2704 puede ser un medio de almacenamiento no transitorio (por ejemplo, tangible).

[0225] El medio de almacenamiento 2704 puede estar acoplado al circuito de procesamiento 2710 de modo que el circuito de procesamiento 2710 pueda leer información de, y escribir información en, el medio de almacenamiento 2704. Es decir, el medio de almacenamiento 2704 se puede acoplar al circuito de procesamiento 2710 de modo que el medio de almacenamiento 2704 sea al menos accesible por el circuito de procesamiento 2710, incluidos ejemplos donde al menos un medio de almacenamiento está integrado en el circuito de procesamiento 2710 y/o ejemplos donde al menos un medio de almacenamiento está separado del circuito de

procesamiento 2710 (por ejemplo, residente en el aparato 2700, externo al aparato 2700, distribuido a través de múltiples entidades, etc.).

[0226] El código y/o las instrucciones almacenados por el medio de almacenamiento 2704, cuando son ejecutados por el circuito de procesamiento 2710, hacen que el circuito de procesamiento 2710 realice una o más de las diversas funciones y/u operaciones de proceso descritas en el presente documento. Por ejemplo, el medio de almacenamiento 2704 puede incluir operaciones configuradas para regular operaciones en uno o más bloques de hardware del circuito de procesamiento 2710, así como para utilizar la interfaz de comunicación 2702 para la comunicación inalámbrica utilizando sus respectivos protocolos de comunicación.

[0227] El circuito de procesamiento 2710 está adaptado, en general, para el procesamiento, incluida la ejecución de dicho código/instrucciones almacenados en el medio de almacenamiento 2704. Como se usa en el presente documento, el término "código" o "instrucciones" se debe interpretar en un sentido amplio para incluir, sin limitación, instrucciones, conjuntos de instrucciones, datos, código, segmentos de código, código de programa, programas, programas, subprogramas, módulos de software, aplicaciones, aplicaciones de software, paquetes de software, rutinas, subrutinas, objetos, ejecutables, hilos de ejecución, procedimientos, funciones, etc., independientemente de que se denominen software, firmware, middleware, microcódigo, lenguaje de descripción de hardware o de otro modo.

[0228] El circuito de procesamiento 2710 está dispuesto para obtener, procesar y/o enviar datos, controlar el acceso y el almacenamiento de datos, emitir comandos y controlar otras operaciones deseadas. El circuito de procesamiento 2710 puede incluir circuitos configurados para implementar el código deseado proporcionado por medios apropiados en al menos un ejemplo. Por ejemplo, el circuito de procesamiento 2710 puede implementarse como uno o más procesadores, uno o más controladores y/u otra estructura configurada para ejecutar código ejecutable. Ejemplos del circuito de procesamiento 2710 pueden incluir un procesador de propósito general, un procesador de señales digitales (DSP), un circuito integrado específico de la aplicación (ASIC), una matriz de puertas programables *in situ* (FPGA) u otro componente de lógica programable, lógica de transistor o de puertas discretas, componentes de hardware discretos o cualquier combinación de los mismos diseñada para realizar las funciones descritas en el presente documento. Un procesador de propósito general puede incluir un microprocesador, así como cualquier procesador, controlador, microcontrolador o máquina de estados convencional. El circuito de procesamiento 2710 también puede implementarse como una combinación de componentes informáticos, tal como una combinación de un DSP y un microprocesador, una pluralidad de microprocesadores, uno o más microprocesadores junto con un núcleo de DSP, un ASIC y un microprocesador o cualquier otra pluralidad de configuraciones variables. Estos ejemplos del circuito de procesamiento 2710 tienen fines ilustrativos y también se contemplan otras configuraciones adecuadas dentro del alcance de la divulgación.

[0229] De acuerdo con uno o más aspectos de la divulgación, el circuito de procesamiento 2710 se puede adaptar para realizar cualquiera o todas las características, procesos, funciones, operaciones y/o rutinas para cualquiera o todos los aparatos descritos en el presente documento. Como se usa en el presente documento, el término "adaptado" en relación con el circuito de procesamiento 2710 se puede referir a que el circuito de procesamiento 2710 está configurado, es utilizado, está implementado y/o está programado para realizar un proceso, función, operación y/o rutina particular de acuerdo con diversas características descritas en el presente documento.

[0230] De acuerdo con al menos un ejemplo del aparato 2700, el circuito de procesamiento 2710 puede incluir uno o más de un circuito/módulo de recepción 2722, un circuito/módulo de adición de identificador temporal 2724, un circuito/módulo de almacenamiento 2726, un circuito/módulo de eliminación de identificador temporal módulo 2728, un circuito/módulo de envío de paquetes de datos 2730, un circuito/módulo de procesamiento de paquetes 2732, un circuito/módulo de cifrado y protección de paquetes 2734, un circuito/módulo de reconstrucción/eliminación de contexto 2738 y un circuito/módulo de obtención/liberación de direcciones de red 2740 que están adaptados para realizar cualquiera o todas las características, procesos, funciones, operaciones y/o rutinas descritas en el presente documento (por ejemplo, características, procesos, funciones, operaciones y/o rutinas descritas con respecto a las FIGS. 28 y 29).

[0231] El circuito/módulo de recepción 2722 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones de recepción 2742 almacenadas en el medio de almacenamiento 2704) adaptadas para realizar varias funciones relacionadas con, por ejemplo, recibir, desde un dispositivo cliente, un primer paquete de datos con un petición para comunicarse con una red, recibir un primer paquete de datos y el contexto de dispositivo cliente cifrado desde el dispositivo cliente, recibir un segundo paquete de datos de una función de red implementada en el nodo de red y recibir un mensaje que incluye una petición de establecimiento de recursos y en al menos uno de los uno o más contextos de dispositivo cliente cifrado del dispositivo cliente.

[0232] El circuito/módulo de adición de identificador temporal 2724 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones de adición de identificador temporal 2744 almacenadas en el medio de almacenamiento 2704) adaptadas para realizar varias funciones relacionadas, por ejemplo, con la adición de un identificador temporal al primer paquete de datos.

[0233] El circuito/módulo de almacenamiento 2726 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones de almacenamiento 2746 almacenadas en el medio de almacenamiento 2704) adaptados para realizar varias funciones relacionadas, por ejemplo, con el almacenamiento de un identificador temporal para el dispositivo cliente. Por ejemplo, el identificador temporal puede ser un identificador temporal de la red de radio celular (C-RNTI). En un aspecto, el identificador temporal se almacena durante un período de tiempo predeterminado.

[0234] El circuito/módulo de eliminación de identificador temporal 2728 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones de eliminación de identificador temporal 2748 almacenadas en el medio de almacenamiento 2704) adaptadas para realizar varias funciones relacionadas, por ejemplo, con la eliminación del identificador temporal en el segundo paquete de datos.

[0235] El circuito/módulo de reenvío de paquetes de datos 2730 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones de reenvío de paquetes de datos 2750 almacenadas en el medio de almacenamiento 2704) adaptadas para realizar varias funciones relacionadas, por ejemplo, con la determinación de un primer nodo de red al que el paquete de datos está destinado, reenviar un primer paquete de datos a una red de servicio cuando el descifrado y la verificación son exitosos, determinar una función de red a la que se enviará una petición, donde la determinación está preconfigurada en el nodo de acceso a la red, determinar el dispositivo cliente al que se va a reenviar el segundo paquete de datos, y reenviar el segundo paquete de datos al dispositivo cliente.

[0236] El circuito/módulo de procesamiento de paquetes 2732 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones de procesamiento de paquetes 2752 almacenadas en el medio de almacenamiento 2704) adaptadas para realizar varias funciones relacionadas con, por ejemplo, descifrar y verificar el primer paquete de datos basándose en el contexto de seguridad.

[0237] El circuito/módulo de cifrado y protección de paquetes 2734 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones de cifrado y protección de paquetes 2754 almacenadas en el medio de almacenamiento 2704) adaptadas para realizar varias funciones relacionadas, por ejemplo, con el cifrado o la protección de integridad de un paquete utilizando claves de dispositivo cliente de plano de usuario (UP), el descifrado y la verificación del primer paquete de datos basándose en el contexto de seguridad, y/o el cifrado o la protección de integridad del segundo paquete de datos utilizando la clave de cifrado de plano de usuario o la clave de protección de integridad de plano de usuario.

[0238] El circuito/módulo de reconstrucción/eliminación de contexto 2738 puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones de reconstrucción/eliminación de contexto 2758 almacenadas en el medio de almacenamiento 2704) adaptadas para realizar varias funciones relacionadas con, por ejemplo, la obtención de una clave (por ejemplo, la clave $K_{CDC\text{-}IoTF\text{-}U}$) para un contexto de dispositivo cliente cifrado asociado con un dispositivo cliente, obtener un contexto de seguridad para el dispositivo cliente a partir del contexto de dispositivo cliente cifrado utilizando la clave, reconstruir al menos un contexto del contexto de dispositivo cliente cifrado, reconstruir al menos una parte de un contexto basándose en al menos uno de los uno o más contextos de dispositivo cliente cifrado y la información de uso, eliminar al menos un contexto y/o mantener al menos una parte de un contexto para un primer umbral período de tiempo en el que la información de uso indica una transmisión de datos reducida, o un segundo período de tiempo umbral en el que la información de uso indica una transmisión de datos en ráfaga, siendo el segundo un período de tiempo umbral superior al primer período de tiempo umbral.

[0239] El circuito/módulo 2740 de obtención/liberación de direcciones de red puede incluir circuitos y/o instrucciones (por ejemplo, instrucciones 2760 de obtención/liberación de direcciones de red almacenadas en el medio de almacenamiento 2704) adaptadas para realizar varias funciones relacionadas con, por ejemplo, obtener una dirección de red para el dispositivo cliente en respuesta al mensaje, transmitir la dirección de red al dispositivo cliente, transmitir un mensaje de petición de liberación de recursos desde el dispositivo cliente a una pasarela, donde el mensaje de petición de liberación de recursos permite que la pasarela libere uno o más recursos para el dispositivo cliente, y/o transmitir un mensaje de petición de liberación de recursos a una pasarela cuando un temporizador expira antes de una transmisión desde el dispositivo cliente a la red o antes de una transmisión desde la red al dispositivo cliente, en el que el mensaje de petición de liberación de recursos habilita la pasarela para liberar uno o más recursos para el dispositivo cliente.

[0240] Como se ha mencionado anteriormente, las instrucciones almacenadas por el medio de almacenamiento 2704, cuando son ejecutados por el circuito de procesamiento 2710, hacen que el circuito de procesamiento 2710 realice una o más de las diversas funciones y/u operaciones de proceso descritas en el presente documento. Por ejemplo, el medio de almacenamiento 2704 puede incluir una o más de las instrucciones de recepción 2742, instrucciones de adición de un identificador 2744, instrucciones de almacenamiento 2746, instrucciones de eliminación de identificador temporal 2748, instrucciones de envío de paquetes de datos 2750, instrucciones de procesamiento de paquetes 2752, instrucciones de cifrado y protección de paquetes 2754, instrucciones de reconstrucción/eliminación de contexto 2758 e instrucciones de obtención/liberación de direcciones de red 2760.

[0241] La FIG. 28 es un diagrama de flujo 2800 que ilustra un procedimiento para comunicación en una arquitectura de red de IoT de acuerdo con diversos aspectos de la divulgación. El procedimiento puede ser realizado por un aparato tal como un nodo de acceso a la red (por ejemplo, el nodo de acceso a la red 104 de la FIG. 1 o el aparato 2700 de la FIG. 27).

[0242] El aparato recibe, desde un dispositivo cliente, un primer paquete de datos con una petición para comunicarse con una red 2802. El aparato almacena un identificador temporal para el dispositivo cliente 2804. Por ejemplo, el identificador temporal puede ser un identificador temporal de la red de radio celular (C-RNTI), y el identificador temporal puede almacenarse durante un período de tiempo predeterminado. El aparato agrega el identificador temporal al primer paquete 2806 de datos.

[0243] El aparato determina un primer nodo de red al que está destinado el primer paquete de datos 2808. El aparato determina una función de red a la que se enviará la petición, donde la determinación está preconfigurada en el nodo de acceso a la red 2810. El aparato envía el primer paquete de datos a la función de red 2812.

[0244] El aparato recibe un segundo paquete de datos de una función de red implementada en el nodo de red 2814. El aparato determina el dispositivo cliente al que se enviará el segundo paquete de datos 2816. En un aspecto, el aparato determina el dispositivo cliente al que se reenviará el segundo paquete de datos identificando el dispositivo cliente a partir de un identificador temporal en el segundo paquete de datos. El aparato elimina el identificador temporal en el segundo paquete de datos 2818. El aparato envía el segundo paquete de datos al dispositivo cliente 2820.

[0245] La FIG. 29 (incluidas las FIGS. 29A y 29B) es un diagrama de flujo 2900 que ilustra un procedimiento para comunicarse en una red de acuerdo con varios aspectos de la divulgación. El procedimiento puede ser realizado por un aparato tal como un nodo de acceso a la red (por ejemplo, el nodo de acceso a la red 1204 de la FIG. 12 o el aparato 2700 de la FIG. 27). Se debe entender que las operaciones indicadas con líneas discontinuas en la FIG. 27 representan operaciones opcionales.

[0246] El aparato obtiene una clave (por ejemplo, la clave $K_{CDC\text{-}IoTF\text{-}U}$) para un contexto de dispositivo cliente cifrado asociado con un dispositivo cliente 2902. El aparato recibe un primer paquete de datos (por ejemplo, paquete de datos UL) y el contexto de dispositivo cliente cifrado desde el dispositivo cliente 2904. El aparato obtiene un contexto de seguridad para el dispositivo cliente a partir del contexto de dispositivo cliente cifrado utilizando la clave 2906. El aparato descifra y/o verifica el primer paquete de datos basándose en el contexto de seguridad 2908. El aparato envía el primer paquete de datos a una red de servicios cuando el descifrado y la verificación son exitosos 2910. El aparato recibe un segundo paquete de datos (por ejemplo, un paquete de datos DL) desde un servidor o una pasarela de red de paquetes de datos 2912. El aparato cifra o protege la integridad del segundo paquete de datos usando la clave de cifrado del plano de usuario o la clave 2914 de protección de integridad del plano de usuario. El aparato envía el segundo paquete de datos al dispositivo cliente 2916. El aparato elimina el al menos un contexto 2918. El aparato recibe un mensaje que incluye una petición de establecimiento de recursos y al menos uno de los uno o más contextos de dispositivo cliente cifrado desde el dispositivo cliente 2920. El aparato obtiene una dirección de red para el dispositivo cliente en respuesta al mensaje 2922. El aparato transmite la dirección de red al dispositivo cliente 2924. En un aspecto, el aparato transmite un mensaje de petición de liberación de recursos a una pasarela cuando un temporizador expira antes de una transmisión desde el dispositivo cliente a la red o antes de una transmisión desde la red al dispositivo cliente 2926. En un aspecto, el mensaje de petición de liberación de recursos permite que la pasarela libere uno o más recursos para el dispositivo cliente. En otro aspecto, el aparato recibe un mensaje de petición de liberación de recursos desde el dispositivo cliente 2928. En tal aspecto, el aparato transmite el mensaje de petición de liberación de recursos desde el dispositivo cliente a una pasarela 2930. En un aspecto, el mensaje de petición de liberación de recursos permite que la pasarela libere uno o más recursos para el dispositivo cliente. En algunos aspectos, la operación 2926 y las operaciones 2928 y 2930 pueden realizarse de forma alternativa. Por ejemplo, si se realiza la operación 2926, es posible que no se realicen las operaciones 2928 y 2930. Como otro ejemplo, si se realizan las operaciones 2928 y 2930, es posible que no se realice la operación 2926.

[0247] Uno o más de los componentes, pasos, características y/o funciones ilustrados en las figuras se pueden reorganizar y/o combinar en un solo componente, paso, característica o función o incorporarse en diversos componentes, pasos o funciones. También se pueden añadir elementos, componentes, pasos y/o funciones adicionales sin apartarse de los rasgos característicos novedosos divulgados en el presente documento. Los aparatos, dispositivos y/o componentes ilustrados en las figuras se pueden configurar para realizar uno o más de los procedimientos, características o pasos descritos en el presente documento. Los algoritmos novedosos descritos en el presente documento también pueden implementarse eficazmente en software y/o realizarse en hardware.

[0248] Se entenderá que el orden o jerarquía específicos de los pasos en los procedimientos divulgados es una ilustración de procesos a modo de ejemplo. Basándose en las preferencias de diseño, se entiende que se puede reorganizar el orden o jerarquía específicos de los pasos en los procedimientos. Las reivindicaciones adjuntas del procedimiento presentan elementos de los diversos pasos en un orden de muestra y no prevén limitarse al orden

o jerarquía específico presentado a menos que se mencione específicamente en las mismas. Elementos, componentes, pasos y/o funciones adicionales también pueden añadirse o no usarse sin apartarse de la divulgación.

[0249] Si bien los rasgos característicos de la divulgación se pueden haber analizado en relación con determinadas implementaciones y figuras, todas las implementaciones de la divulgación pueden incluir uno o más de los rasgos característicos ventajosos analizados en el presente documento. En otras palabras, aunque una o más implementaciones se pueden haber analizado como presentando determinados rasgos característicos ventajosos, también se pueden usar uno o más de dichos rasgos característicos de acuerdo con cualquiera de las diversas implementaciones analizadas en el presente documento. De forma similar, aunque las implementaciones a modo de ejemplo se pueden haber analizado en el presente documento como implementaciones de dispositivo, sistema o procedimiento, se debe entender que dichas implementaciones a modo de ejemplo se pueden implementar en diversos dispositivos, sistemas y procedimientos.

[0250] Asimismo, cabe destacar que al menos algunas implementaciones se han descrito como un proceso que se representa como un organigrama, un diagrama de flujo, un diagrama estructural o un diagrama de bloques. Aunque un organigrama puede describir las operaciones como un proceso secuencial, muchas de las operaciones pueden realizarse en paralelo o simultáneamente. Además, el orden de las operaciones puede redisponerse. Un proceso se termina cuando se acaban sus operaciones. En algunos aspectos, un proceso puede corresponder a un procedimiento, una función, un procedimiento, una subrutina, un subprograma, etc. Cuando un proceso corresponde a una función, su finalización corresponde al retorno de la función a la función de llamada o a la función principal. Uno o más de los diversos procedimientos descritos en el presente documento pueden implementarse parcial o totalmente mediante programas (por ejemplo, instrucciones y/o datos) que pueden almacenarse en un medio de almacenamiento legible por máquina, legible por ordenador y/o legible por procesador, y ejecutarse por uno o más procesadores, máquinas y/o dispositivos.

[0251] Los expertos en la técnica apreciarán además que los diversos bloques lógicos, módulos, circuitos y pasos de algoritmo ilustrativos descritos en relación con las implementaciones divulgadas en el presente documento pueden implementarse como hardware, software, firmware, middleware, microcódigo o cualquier combinación de los mismos. Para ilustrar claramente esta intercambiabilidad, anteriormente se han descrito, en general, diversos componentes, bloques, módulos, circuitos y pasos ilustrativos, en términos de su funcionalidad. Que dicha funcionalidad se implemente como hardware o software depende de las restricciones de aplicación y diseño particulares impuestas al sistema global.

[0252] En la divulgación, el término "a modo de ejemplo" se usa para significar que "sirve de ejemplo, caso o ilustración". Cualquier implementación o aspecto descrito en el presente documento como "a modo de ejemplo" no se debe interpretar necesariamente como preferente o ventajoso con respecto a otros aspectos de la divulgación. Asimismo, el término "aspectos" no requiere que todos los aspectos de la divulgación incluyan la característica, ventaja o modo de funcionamiento analizados. El término "acoplado" se usa en el presente documento para referirse a la conexión directa o indirecta entre dos objetos. Por ejemplo, si el objeto A toca físicamente el objeto B, y el objeto B toca el objeto C, entonces los objetos A y C se pueden seguir considerando acoplados el uno al otro, incluso si no se tocan físicamente de forma directa entre sí. Por ejemplo, un primer chip se puede acoplar a un segundo chip en un encapsulado incluso aunque el primer chip nunca esté físicamente en contacto directo con el segundo chip. Los términos "circuito" y "circuitos" se usan de forma genérica y pretenden incluir implementaciones en hardware de dispositivos eléctricos y conductores que, cuando se conectan y configuran, posibilitan el cumplimiento de las funciones descritas en la presente divulgación, sin limitación en cuanto al tipo de circuitos electrónicos, así como implementaciones en software de información e instrucciones que, cuando son ejecutadas por un procesador, posibilitan el cumplimiento de las funciones descritas en la divulgación.

[0253] Como se usa en el presente documento, el término "determinar" engloba una amplia variedad de acciones. Por ejemplo, "determinar" puede incluir calcular, computar, procesar, obtener, investigar, consultar (por ejemplo, consultar una tabla, una base de datos u otra estructura de datos), averiguar y similares. Además, "determinar" puede incluir recibir (por ejemplo, recibir información), acceder (por ejemplo, acceder a datos de una memoria) y similares. Además, "determinar" puede incluir resolver, seleccionar, elegir, establecer y similares. Como se usa en el presente documento, el término "obtener" puede incluir una o más acciones que incluyen, pero no se limitan a, recibir, generar, determinar o cualquier combinación de los mismos.

[0254] La descripción previa se proporciona para permitir que cualquier experto en la técnica lleve a la práctica los diversos aspectos descritos en el presente documento. Diversas modificaciones de estos aspectos resultarán fácilmente evidentes a los expertos en la técnica, y los principios genéricos definidos en el presente documento se pueden aplicar a otros aspectos. Por tanto, las reivindicaciones no contemplan limitarse a los aspectos mostrados en el presente documento, sino que se les ha de conceder el alcance total compatible con el lenguaje de las reivindicaciones, en el que la referencia a un elemento en singular no está prevista para significar "uno y solo uno", a no ser que así se indique de forma específica, sino más bien "uno o más". A menos que se exprese de otro modo específicamente, el término "alguno/a" se refiere a uno/a o más. Una frase que hace referencia a "al menos uno de" una lista de elementos se refiere a cualquier combinación de esos elementos, incluyendo elementos

individuales. Como ejemplo, “al menos uno de: a, b o c” está previsto para abarcar: a; b; c; a y b; a y c; b y c; y a, b y c. Todos los equivalentes estructurales y funcionales de los elementos de los diversos aspectos descritos a lo largo de esta divulgación, que sean conocidos o que lleguen a ser conocidos posteriormente por los expertos en la técnica, están previstos para abarcarse por las reivindicaciones. Por otro lado, no se pretende que nada de lo divulgado en el presente documento esté dedicado al público, independientemente de si dicha divulgación se cita de forma explícita en las reivindicaciones. Ningún elemento de reivindicación debe interpretarse conforme a lo dispuesto en el título 35 U.S.C. § 112, párrafo seis, a no ser que el elemento se mencione expresamente con la expresión "medios para" o, en el caso de una reivindicación de procedimiento, el elemento se mencione con la expresión "paso para".

[0255] Por consiguiente, las diversas características asociadas a los ejemplos descritos en el presente documento y mostradas en las figuras adjuntas pueden implementarse en diferentes ejemplos e implementaciones sin apartarse del alcance de la divulgación. Por consiguiente, aunque determinadas estructuras y disposiciones específicas se han descrito y mostrado en las figuras adjuntas, dichas implementaciones son meramente ilustrativas y no limitan el alcance de la divulgación, puesto que otras diversas adiciones y modificaciones a, y omisiones de, las implementaciones descritas resultarán evidentes para los expertos en la técnica. Por tanto, el alcance de la divulgación solo está determinado por el lenguaje literal, y equivalencias legales, de las siguientes reivindicaciones.

REIVINDICACIONES

1. Un procedimiento para un dispositivo cliente (102, 502, 702, 1700) que comprende:

transmitir una petición para comunicarse con una red (110, 510, 710);
establecer un contexto de seguridad para una conexión con la red, en el que el contexto de seguridad incluye al menos un algoritmo de cifrado, una clave de cifrado, un algoritmo de protección de integridad, una clave de protección de integridad o combinaciones de los mismos;
recibir uno o más contextos de dispositivo cliente cifrado de la red en respuesta a la petición, en el que el uno o más contextos de dispositivo cliente cifrado incluyen información de estado de la red asociada con el dispositivo cliente, incluyendo la información de estado de la red al menos el contexto de seguridad y la información asociada con uno o más portadores del dispositivo cliente;
y transmitir un mensaje que incluye al menos uno de los uno o más contextos de dispositivo cliente cifrado a la red, en el que el uno o más contextos de dispositivo cliente cifrado permiten la reconstrucción de un contexto en la red para la comunicación con el dispositivo cliente, con el contexto que incluye la información de estado de la red.

2. El procedimiento según la reivindicación 1, en el que el contexto se elimina en la red, opcionalmente después de recibir uno o más contextos de dispositivo cliente cifrado de la red.

3. El procedimiento según la reivindicación 1, que comprende además:
determinar al menos uno de los uno o más contextos de dispositivo cliente cifrado para usar basándose en si el mensaje incluye datos o información de control.

4. El procedimiento según la reivindicación 1, en el que el uno o más contextos de dispositivo cliente cifrado incluyen:

un primer contexto que se utilizará para la comunicación relacionada con los datos con el dispositivo cliente y un segundo contexto que se utilizará para la comunicación relacionada con el control con el dispositivo cliente; o
al menos uno de un contexto de seguridad, una calidad de servicio para un portador, un identificador de punto final de túnel o combinaciones de los mismos.

5. El procedimiento según la reivindicación 1, en el que la petición comprende una indicación de que el dispositivo cliente está solicitando uno o más contextos de dispositivo cliente cifrado o una indicación de un servicio que el dispositivo cliente está solicitando.

6. El procedimiento según la reivindicación 1, en el que uno o más contextos de dispositivo cliente cifrado incluyen un contexto de dispositivo cliente cifrado en el plano de usuario y un contexto de dispositivo cliente cifrado en el plano de control, y en el que el mensaje incluye:

un primer paquete de datos con el contexto de dispositivo cliente cifrado en el plano de usuario, o
un paquete de control con el contexto de dispositivo cliente cifrado del plano de control.

7. El procedimiento según la reivindicación 6, en el que la clave de cifrado es una clave de cifrado del plano de usuario y la clave de protección de integridad es una clave de protección de integridad del plano de usuario, en el que la clave de cifrado del plano de usuario y la clave de protección de integridad del plano de usuario se mantienen en el dispositivo cliente, y en el que el primer paquete de datos está al menos protegido por integridad con la clave de protección de integridad del plano de usuario o cifrado con la clave de cifrado del plano de usuario.

8. El procedimiento según la reivindicación 6, en el que la transmisión del mensaje incluye el primer paquete de datos dispuesto para omitir el establecimiento de una conexión de control de recursos de radio con un nodo de acceso a la red de la red.

9. El procedimiento según la reivindicación 6, que comprende además entrar en un modo inactivo inmediatamente después de transmitir el mensaje que incluye el primer paquete de datos.

10. El procedimiento según la reivindicación 6, que comprende además:
recibir un segundo paquete de datos, en el que recibir el segundo paquete de datos dispuesto para omitir el establecimiento de una conexión de control de recursos de radio con un nodo de acceso a la red.

11. El procedimiento según la reivindicación 10, en el que recibir el segundo paquete de datos comprende al menos uno de verificar el segundo paquete de datos con la clave de protección de integridad del plano de usuario o descifrar el segundo paquete de datos con la clave de cifrado del plano de usuario.

12. El procedimiento según la reivindicación 6, en el que el paquete de control es una actualización del área de seguimiento.

13. El procedimiento según la reivindicación 1, que comprende además:
recibir un mensaje de búsqueda desde la red.

14. El procedimiento según la reivindicación 1, que comprende además:
transmitir un paquete vacío y el contexto de dispositivo cliente cifrado en el plano de usuario a la red.

15. El procedimiento según la reivindicación 1, en el que el contexto de dispositivo cliente cifrado se recibe desde la red como resultado de una auntentificación exitosa con la red.

16. El procedimiento según la reivindicación 15, en el que la auntentificación exitosa con la red no establece un contexto de seguridad de estrato de acceso.

17. El procedimiento según la reivindicación 1, que comprende además almacenar uno o más contextos de dispositivo cliente cifrado en un almacenamiento local.

18. El procedimiento según la reivindicación 1, en el que uno o más contextos de dispositivo cliente cifrado no se descifran en el dispositivo cliente, y en el que uno o más contextos de dispositivo cliente cifrado se descifran solo mediante un dispositivo de red que generó uno o más contextos de dispositivo cliente cifrado.

19. El procedimiento según la reivindicación 1, en el que el mensaje incluye además una petición de establecimiento de recursos, que comprende además:

recibir una dirección de red para el dispositivo cliente en respuesta al mensaje; y
transmitir una pluralidad de paquetes de datos que incluyen la dirección de red a la red.

20. El procedimiento según la reivindicación 1, que comprende además:
transmitir un mensaje de petición de liberación de recursos a la red, en el que el mensaje de petición de liberación de recursos permite a la red liberar uno o más recursos para el dispositivo cliente.

21. Un dispositivo cliente (102, 502, 702, 1700) que comprende:

un circuito de comunicación inalámbrica (1702) configurado para comunicarse con un nodo de acceso a la red; y
un circuito de procesamiento (1710) acoplado al circuito de comunicación inalámbrica, con el circuito de procesamiento configurado para
transmitir una petición para comunicarse con una red (110, 510, 710);
establecer un contexto de seguridad para una conexión con la red, en el que el contexto de seguridad incluye al menos un algoritmo de cifrado, una clave de cifrado, un algoritmo de protección de integridad, una clave de protección de integridad o combinaciones de los mismos;
recibir uno o más contextos de dispositivo cliente cifrado de la red en respuesta a la petición, en el que uno o más contextos de dispositivo cliente cifrado incluyen información de estado de la red asociada con el dispositivo cliente, incluyendo la información de estado de la red al menos el contexto de seguridad y la información asociada con uno o más portadores del dispositivo cliente; y
transmitir un mensaje que incluye al menos uno de los uno o más contextos de dispositivo cliente cifrado a la red, en el que uno o más contextos de dispositivo cliente cifrado permiten la reconstrucción de un contexto en la red para la comunicación con el dispositivo cliente, con el contexto que incluye la información de estado de la red.

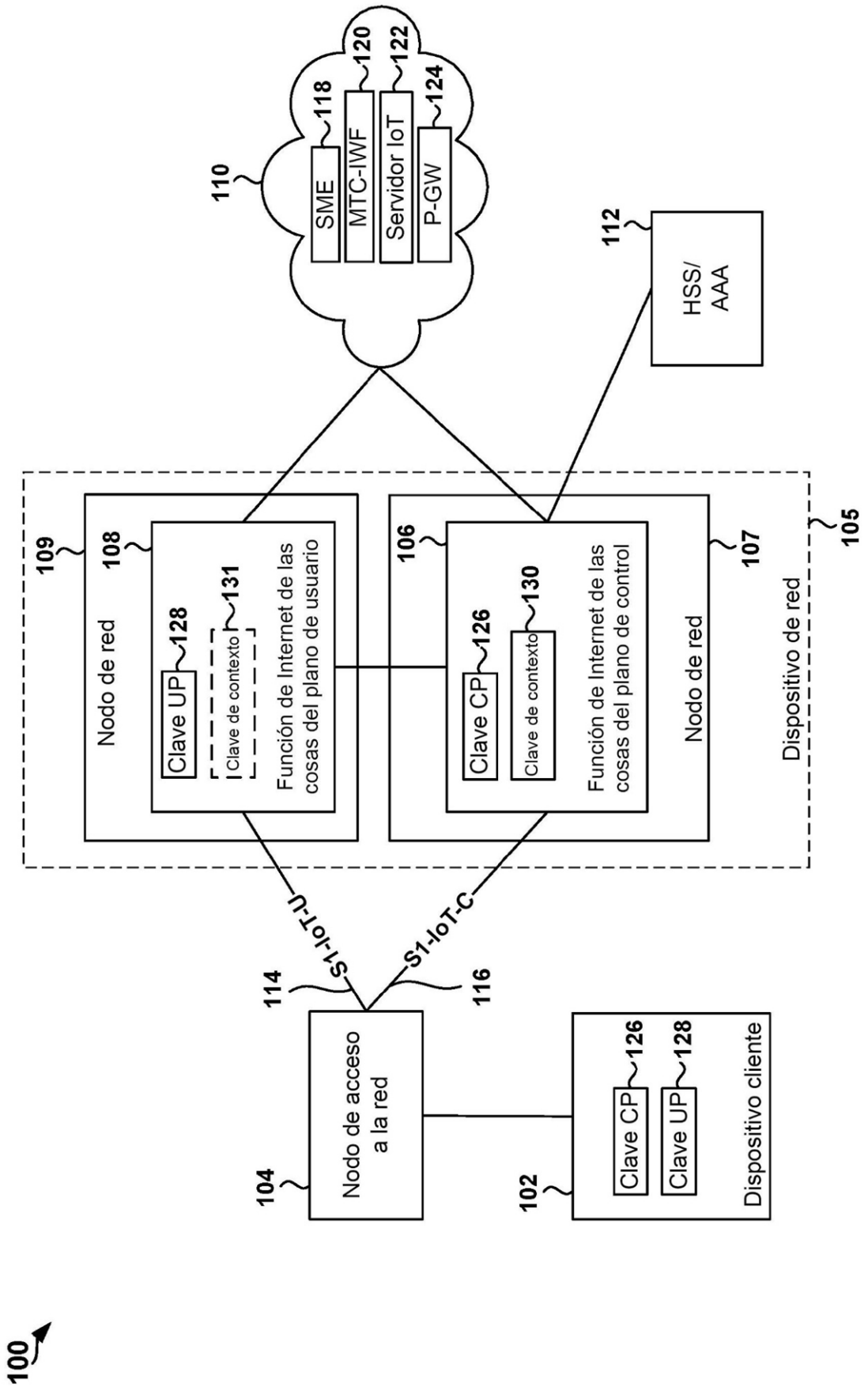
100
110
SME
118
MTC-IWF
120
Servidor IoT
122
P-GW
124
112
HSS/
AAA
109
Nodo de red
108
Clave UP
128
Clave de contexto
131
Función de Internet de las cosas del plano de usuario
106
Clave CP
126
Clave de contexto
130
Función de Internet de las cosas del plano de control
107
Nodo de red
105
Dispositivo de red
S1-IoT-U
S1-IoT-C
114
116
104
Nodo de acceso a la red
102
Clave CP
126
Clave UP
128
Dispositivo cliente

FIG. 1

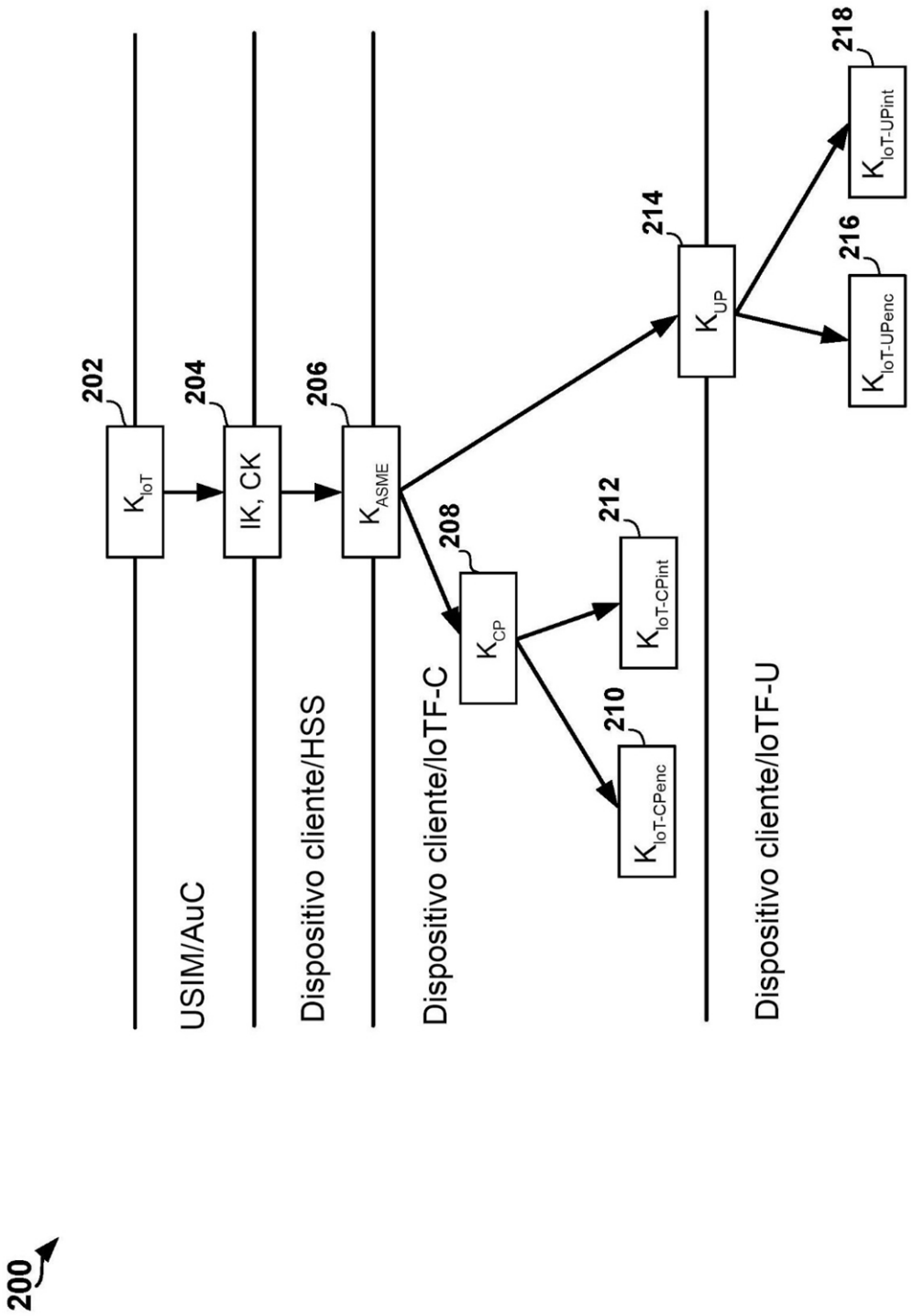
200
USIM/AuC
Dispositivo cliente/HSS
Dispositivo cliente/IoTF-C
Dispositivo cliente/IoTF-U
202
204
206
208
210
212
214
216
218
K_{IoT}
IK, CK
K_{ASME}
K_{CP}
$K_{IoT-CPenc}$
$K_{IoT-CPint}$
K_{UP}
$K_{IoT-UPenc}$
$K_{IoT-UPint}$

FIG. 2

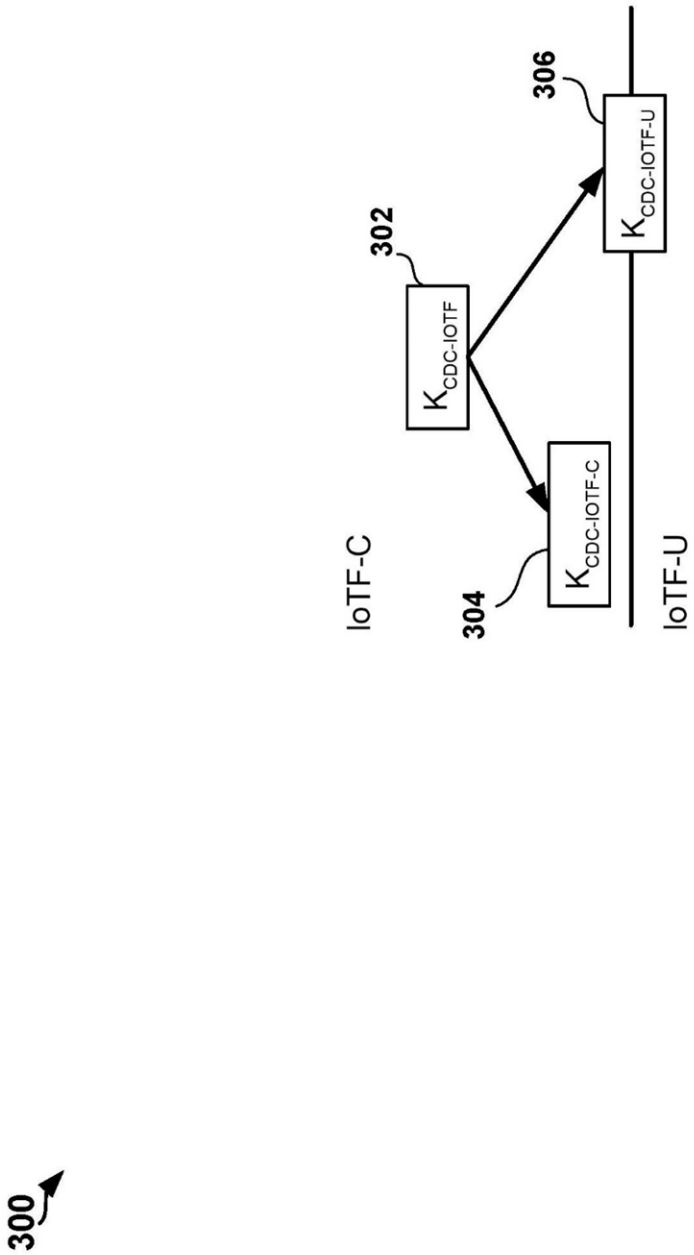

FIG. 3

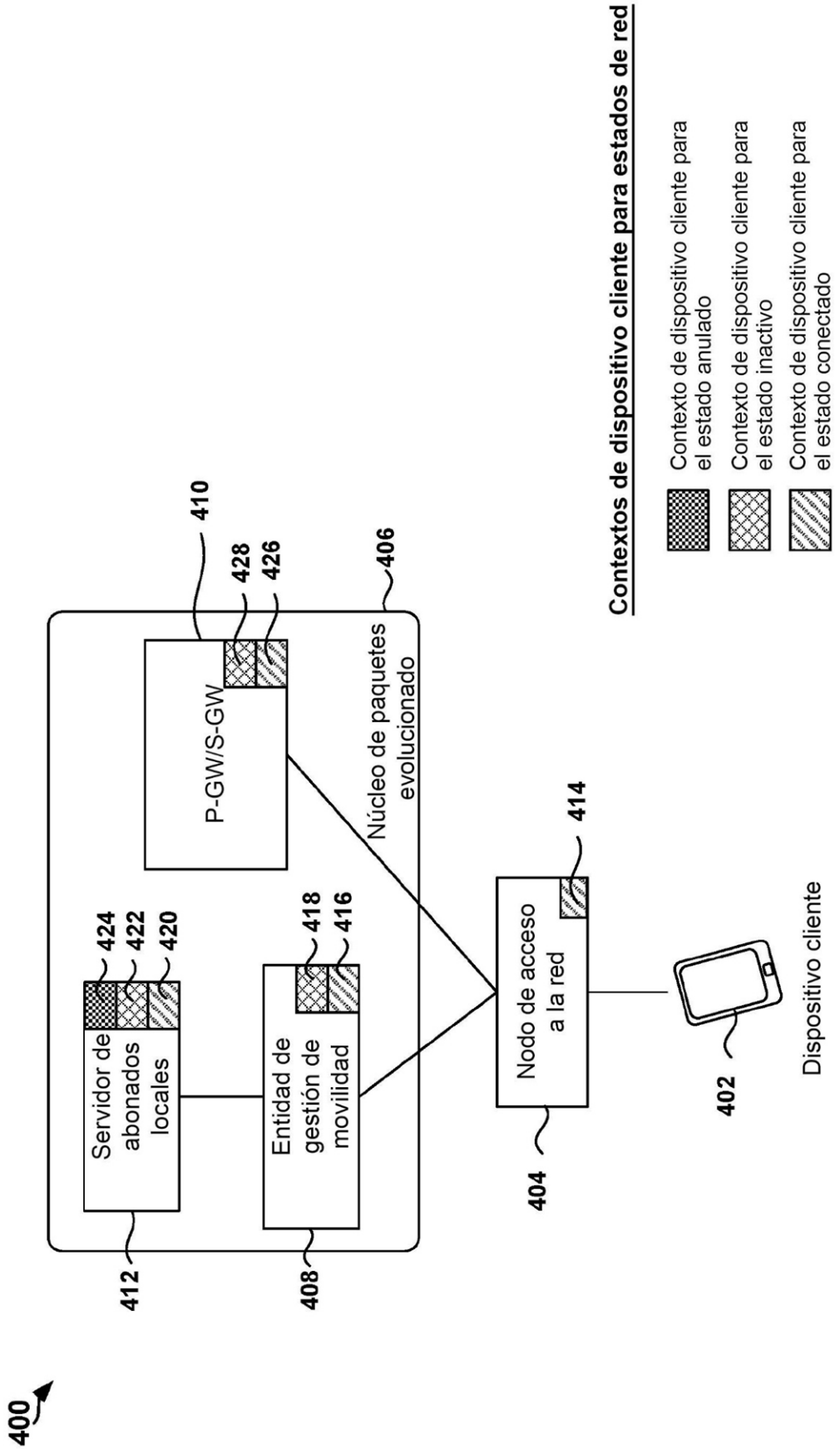
400
410
428
426
406
P-GW/S-GW
Núcleo de paquetes evolucionado
424
422
420
418
416
Servidor de abonados locales
Entidad de gestión de movilidad
414
Nodo de acceso a la red
412
408
404
402
Dispositivo cliente
Contextos de dispositivo cliente para estados de red
Contexto de dispositivo cliente para el estado anulado
Contexto de dispositivo cliente para el estado inactivo
Contexto de dispositivo cliente para el estado conectado

FIG. 4

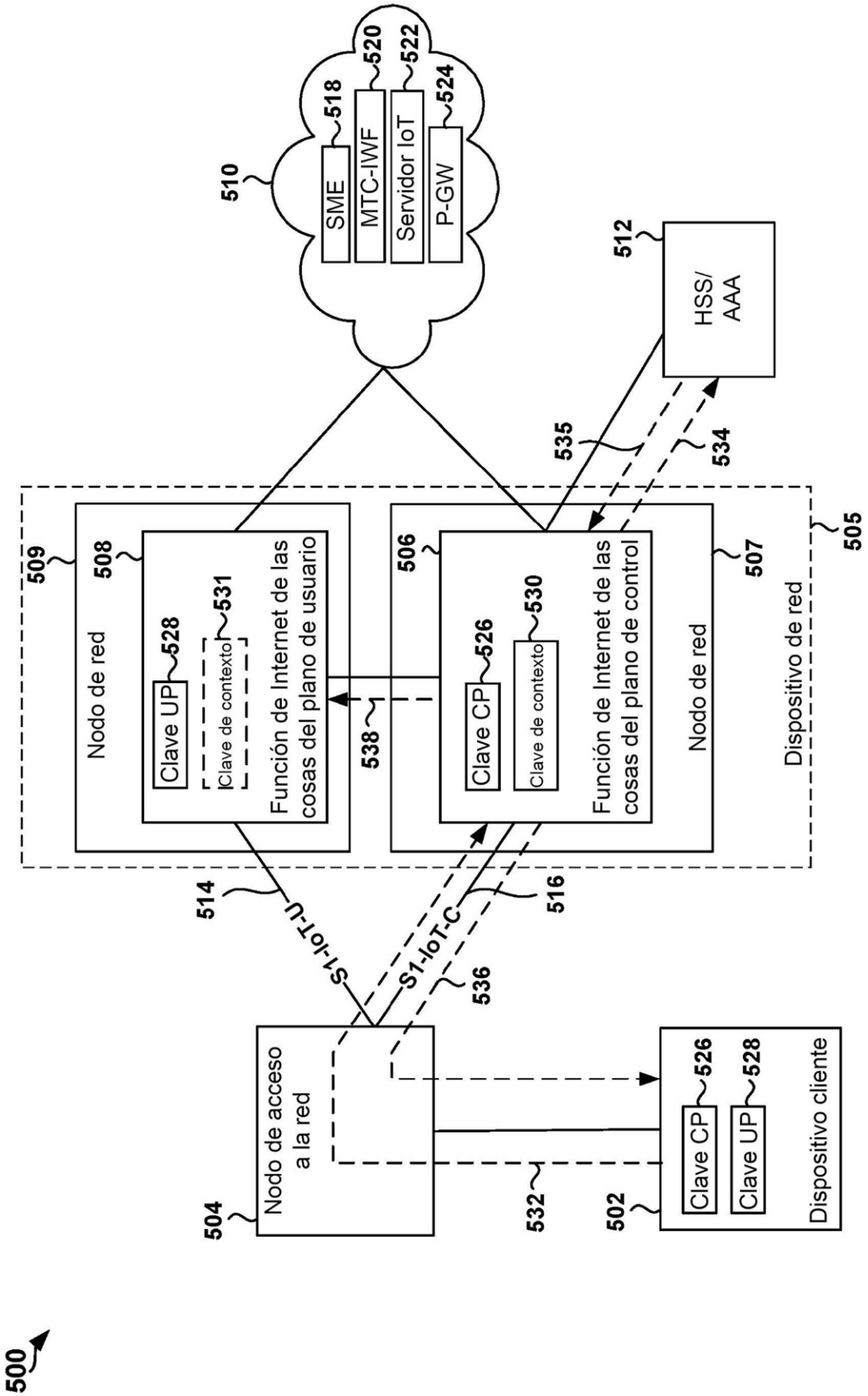
500
504
Nodo de acceso a la red
532
502
Clave CP
526
Clave UP
528
Dispositivo cliente
514
S1-IoT-U
S1-IoT-C
516
536
509
508
Nodo de red
Clave UP
528
Clave de contexto
531
Función de Internet de las cosas del plano de usuario
538
506
Clave CP
526
Clave de contexto
530
Función de Internet de las cosas del plano de control
507
Nodo de red
505
Dispositivo de red
510
SME
518
MTC-IWF
520
Servidor IoT
522
P-GW
524
512
HSS/ AAA
535
534

FIG. 5

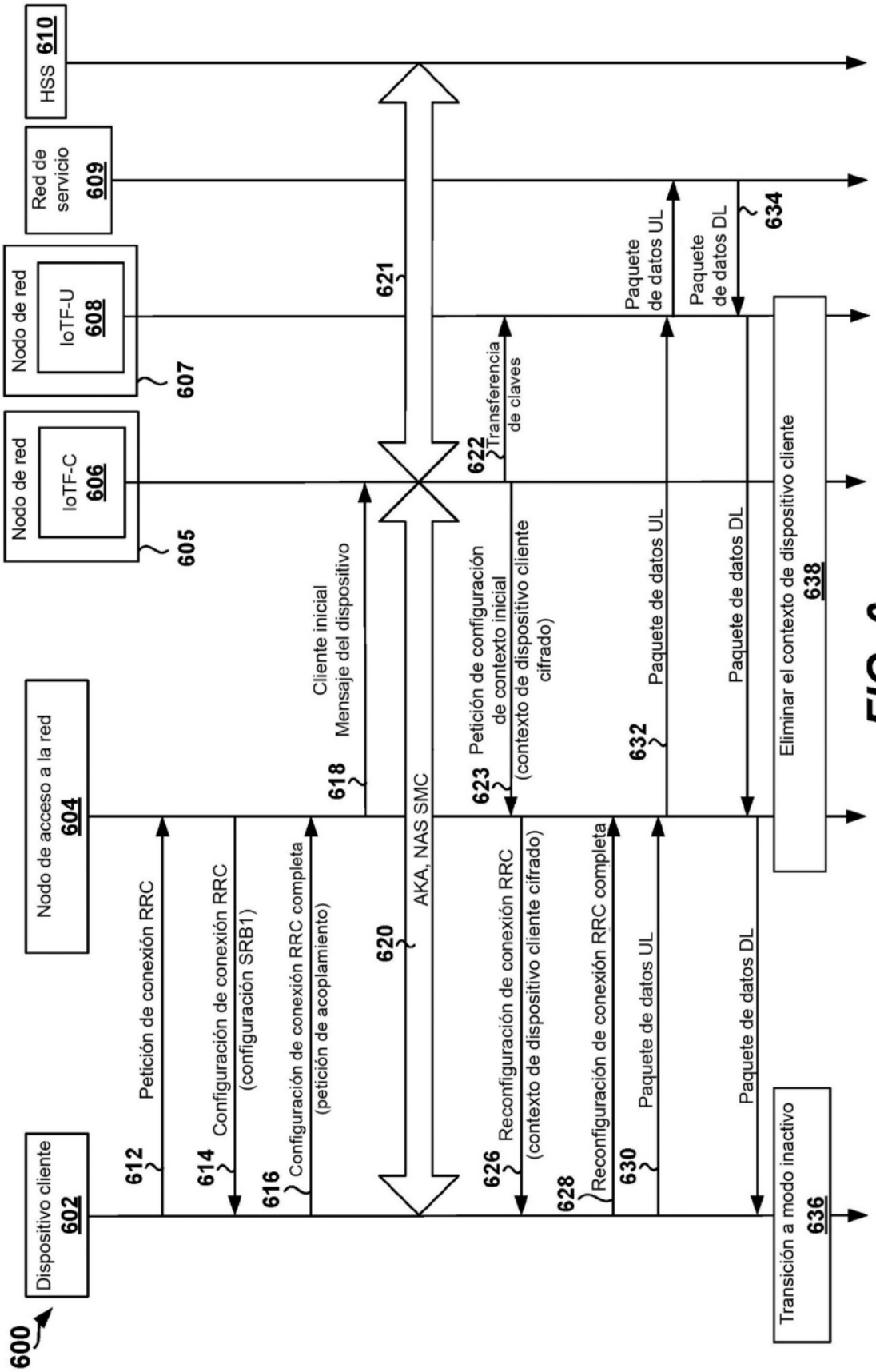
600
Dispositivo cliente 602
Nodo de acceso a la red 604
Nodo de red
IoTF-C 606
605
Nodo de red
IoTF-U 608
607
Red de servicio 609
HSS 610
612 Petición de conexión RRC
614 Configuración de conexión RRC (configuración SRB1)
616 Configuración de conexión RRC completa (petición de acoplamiento)
618 Cliente inicial Mensaje del dispositivo
620 AKA, NAS SMC
621
622 Transferencia de claves
623 Petición de configuración de contexto inicial (contexto de dispositivo cliente cifrado)
626 Reconfiguración de conexión RRC (contexto de dispositivo cliente cifrado)
628 Reconfiguración de conexión RRC completa
630 Paquete de datos UL
632 Paquete de datos UL
634 Paquete de datos DL
Paquete de datos DL
Paquete de datos DL
Eliminar el contexto de dispositivo cliente 638
Transición a modo inactivo 636

FIG. 6

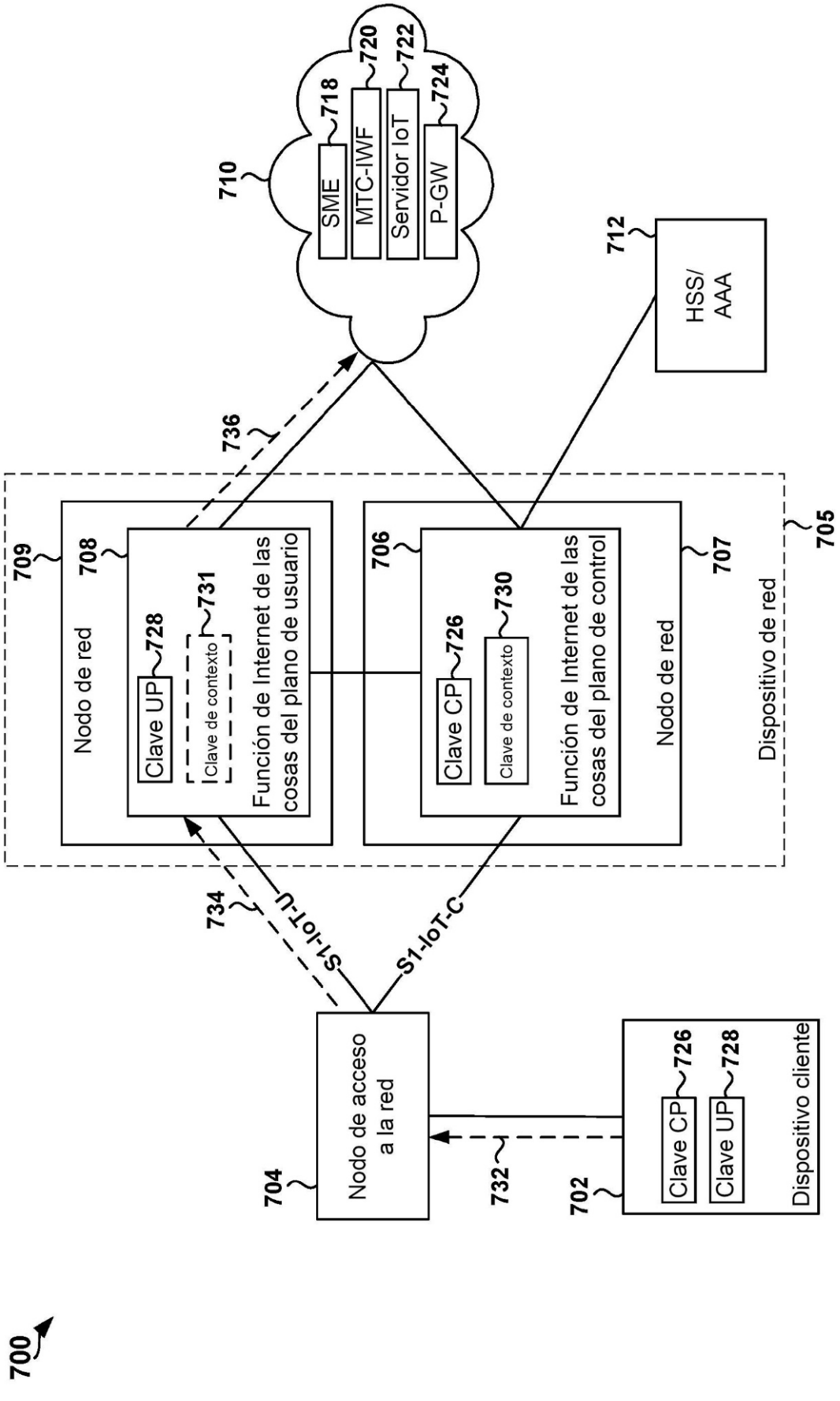
700
704
Nodo de acceso a la red
732
702
Clave CP
726
Clave UP
728
Dispositivo cliente
S1-IoT-U
734
S1-IoT-C
709
708
Nodo de red
Clave UP
728
Clave de contexto
731
Función de Internet de las cosas del plano de usuario
706
Clave CP
726
Clave de contexto
730
Función de Internet de las cosas del plano de control
707
Nodo de red
705
Dispositivo de red
736
710
SME
718
MTC-IWF
720
Servidor IoT
722
P-GW
724
712
HSS/ AAA

FIG. 7

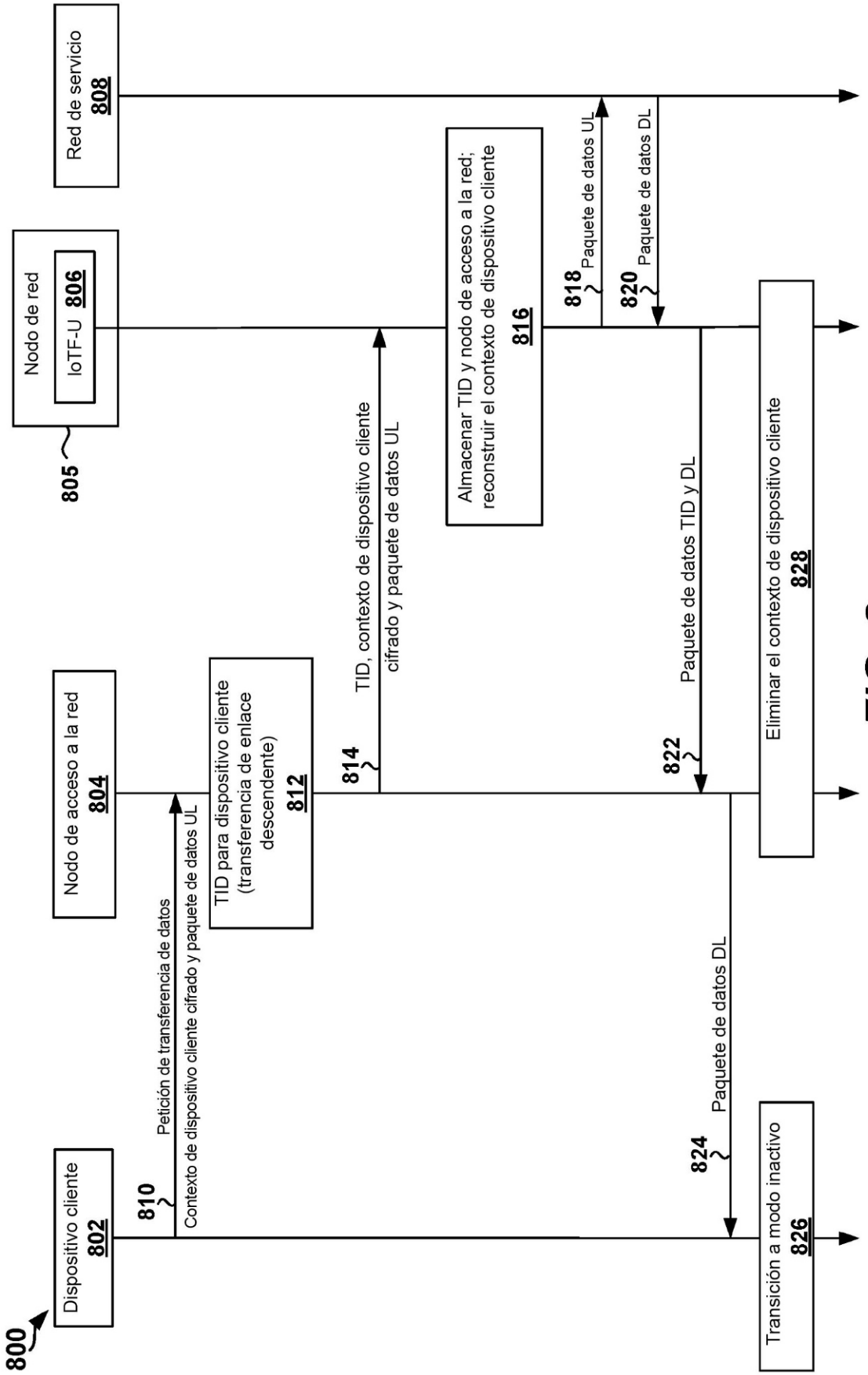
800
Dispositivo cliente
802
Nodo de acceso a la red
804
Nodo de red
IoTF-U 806
805
Red de servicio
808
810
Petición de transferencia de datos
Contexto de dispositivo cliente cifrado y paquete de datos UL
TID para dispositivo cliente (transferencia de enlace descendente)
812
814
TID, contexto de dispositivo cliente cifrado y paquete de datos UL
Almacenar TID y nodo de acceso a la red; reconstruir el contexto de dispositivo cliente
816
818
Paquete de datos UL
820
Paquete de datos DL
822
Paquete de datos TID y DL
Eliminar el contexto de dispositivo cliente
828
824
Paquete de datos DL
Transición a modo inactivo
826

FIG. 8

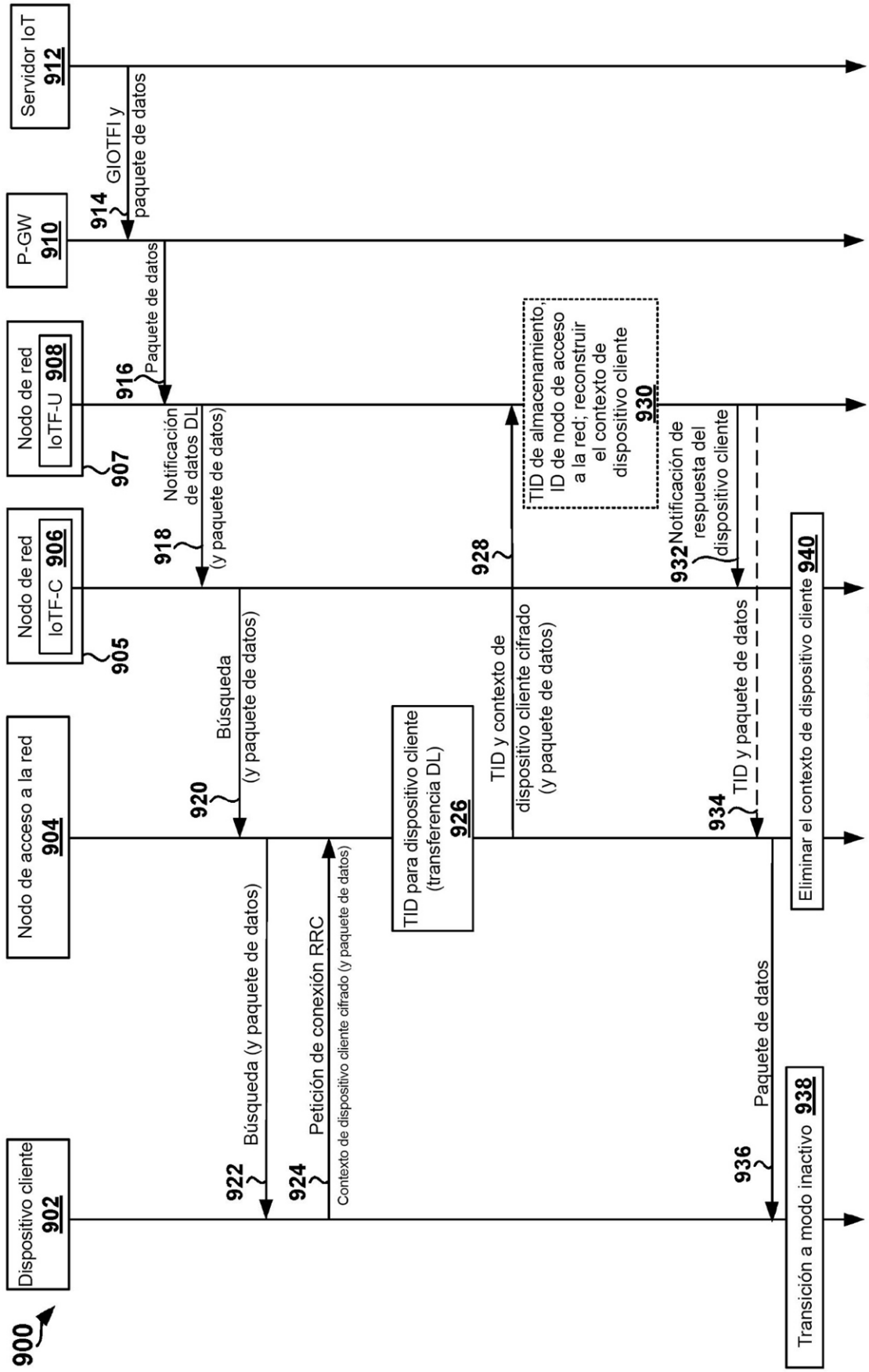
900
Dispositivo cliente 902
Nodo de acceso a la red 904
Nodo de red IoTF-C 906
Nodo de red IoTF-U 908
P-GW 910
Servidor IoT 912
905
907
914 GIOTFI y paquete de datos
916 Paquete de datos
918 Notificación de datos DL (y paquete de datos)
920 Búsqueda (y paquete de datos)
922 Búsqueda (y paquete de datos)
924 Petición de conexión RRC
Contexto de dispositivo cliente cifrado (y paquete de datos)
TID para dispositivo cliente (transferencia DL) 926
928 TID y contexto de dispositivo cliente cifrado (y paquete de datos)
TID de almacenamiento, ID de nodo de acceso a la red; reconstruir el contexto de dispositivo cliente 930
932 Notificación de respuesta del dispositivo cliente
934 TID y paquete de datos
936 Paquete de datos
Eliminar el contexto de dispositivo cliente 940
Transición a modo inactivo 938

FIG. 9

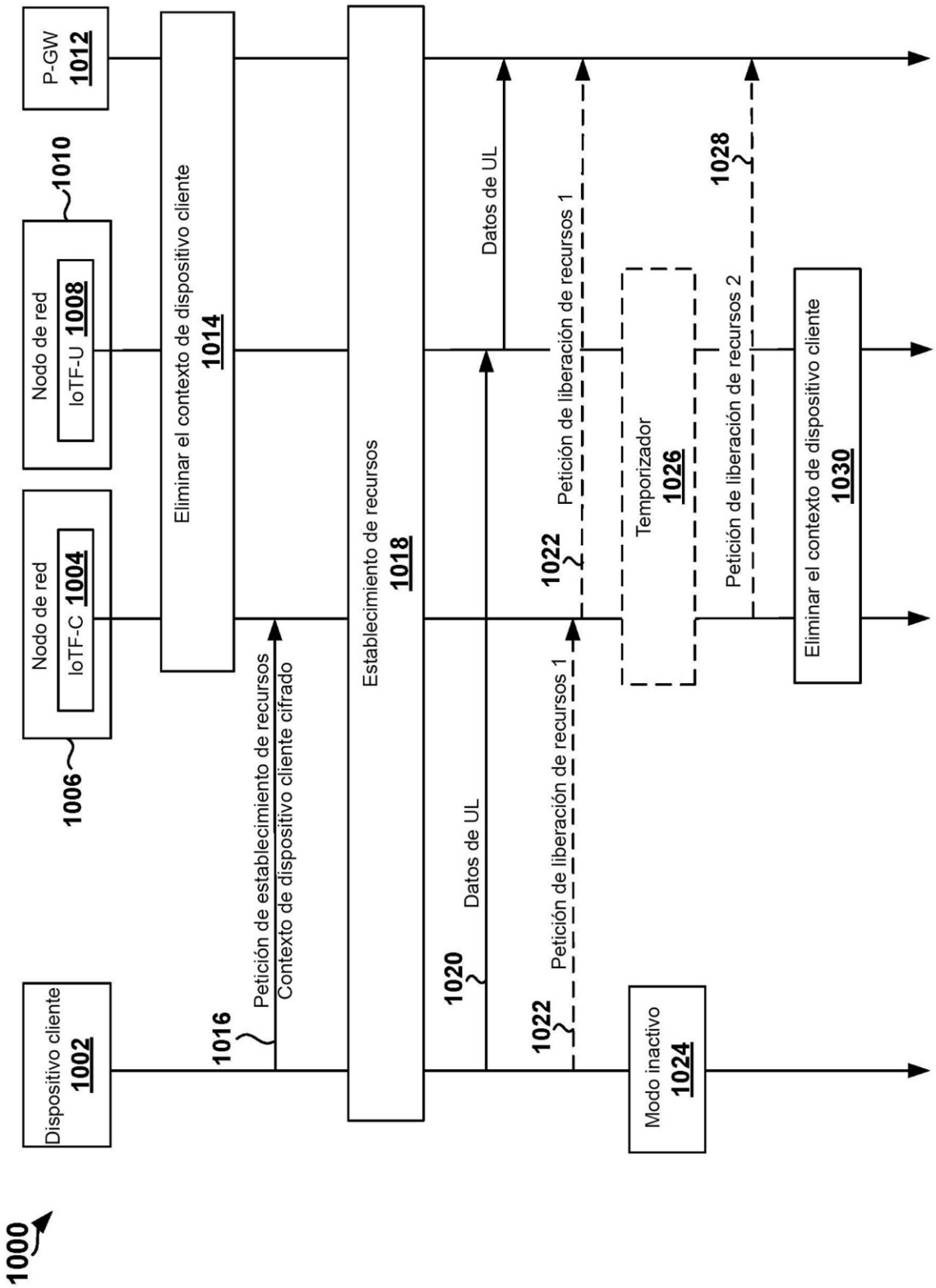
1000
Dispositivo cliente
1002
Nodo de red
IoTF-C 1004
1006
Nodo de red
IoTF-U 1008
1010
P-GW
1012
Eliminar el contexto de dispositivo cliente
1014
Establecimiento de recursos
1018
1016
Petición de establecimiento de recursos
Contexto de dispositivo cliente cifrado
1020
Datos de UL
1022
Petición de liberación de recursos 1
Modo inactivo
1024
Datos de UL
1022
Petición de liberación de recursos 1
Temporizador
1026
1028
Petición de liberación de recursos 2
Eliminar el contexto de dispositivo cliente
1030

FIG. 10

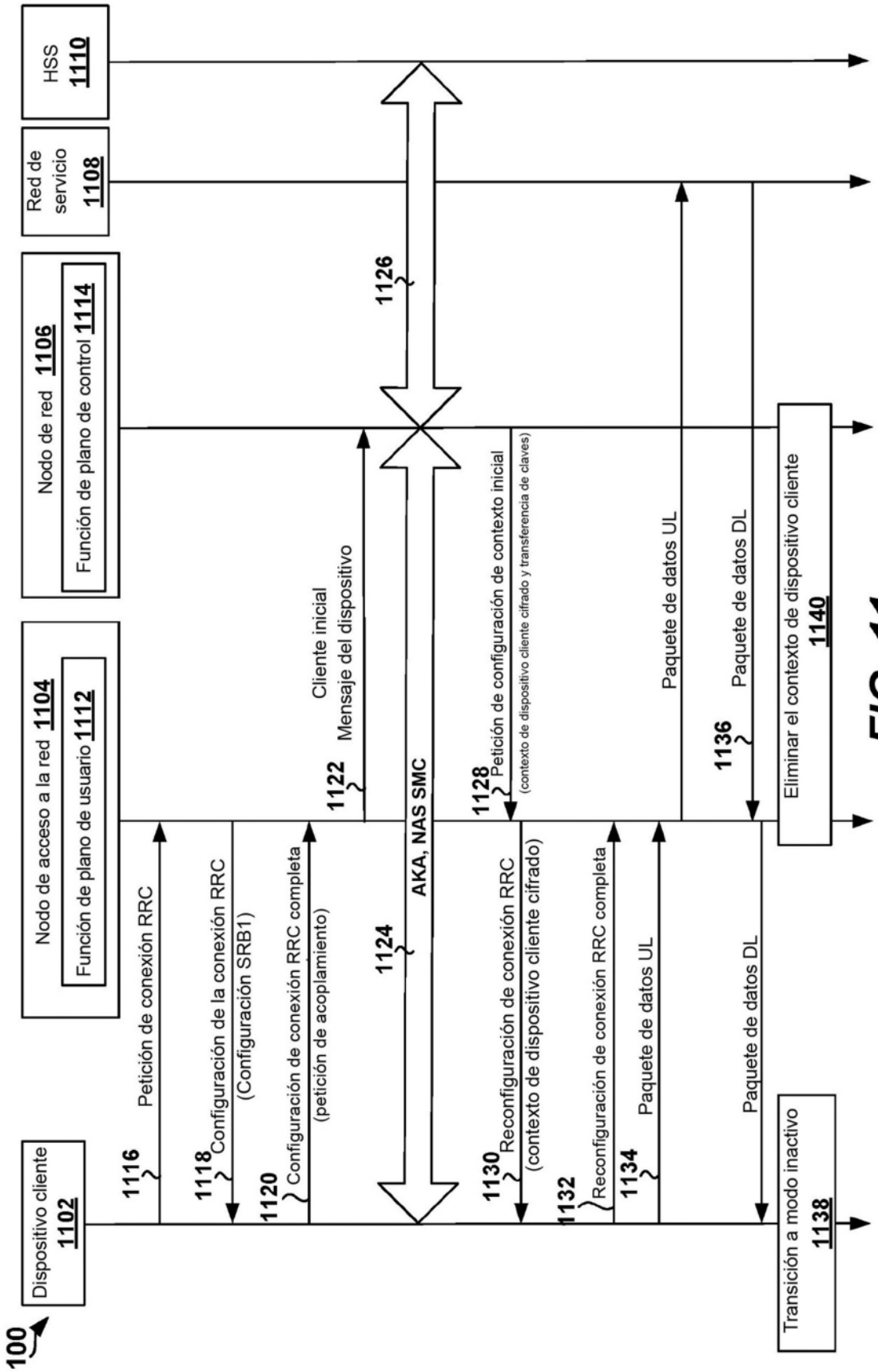
1100
Dispositivo cliente 1102
Nodo de acceso a la red 1104
Función de plano de usuario 1112
Nodo de red 1106
Función de plano de control 1114
Red de servicio 1108
HSS 1110
1116 Petición de conexión RRC
1118 Configuración de la conexión RRC (Configuración SRB1)
1120 Configuración de conexión RRC completa (petición de acoplamiento)
1122 Cliente inicial Mensaje del dispositivo
1124 AKA, NAS SMC
1126
1128 Petición de configuración de contexto inicial (contexto de dispositivo cliente cifrado y transferencia de claves)
1130 Reconfiguración de conexión RRC (contexto de dispositivo cliente cifrado)
1132 Reconfiguración de conexión RRC completa
1134 Paquete de datos UL
1136 Paquete de datos DL
Paquete de datos UL
Paquete de datos DL
Eliminar el contexto de dispositivo cliente 1140
Transición a modo inactivo 1138

FIG. 11

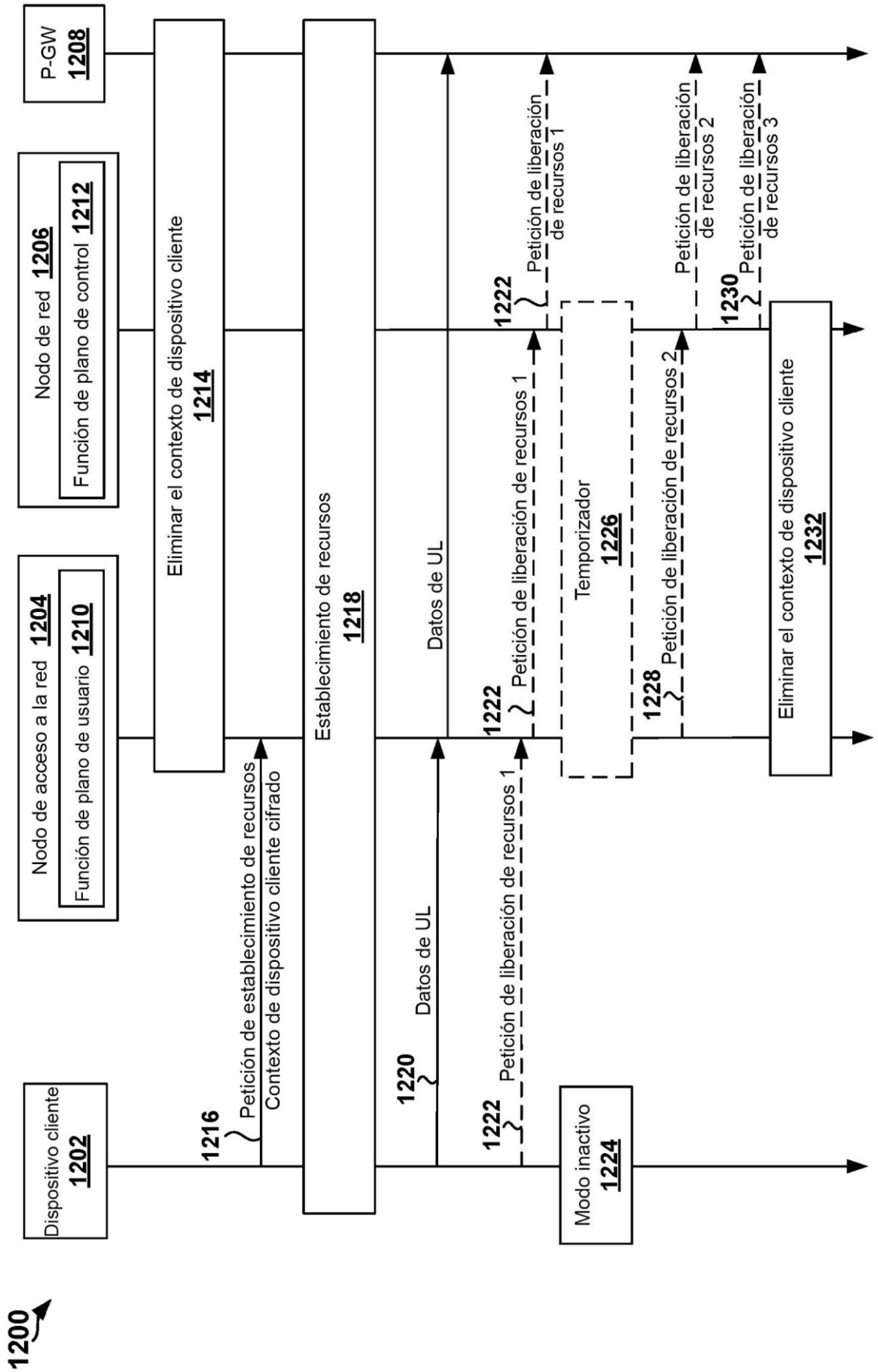
1200
Dispositivo cliente 1202
Nodo de acceso a la red 1204
Función de plano de usuario 1210
Nodo de red 1206
Función de plano de control 1212
P-GW 1208
Eliminar el contexto de dispositivo cliente 1214
Establecimiento de recursos 1218
Modo inactivo 1224
Eliminar el contexto de dispositivo cliente 1232
1216 Petición de establecimiento de recursos
Contexto de dispositivo cliente cifrado
1220 Datos de UL
1222 Petición de liberación de recursos 1
Datos de UL
1222 Petición de liberación de recursos 1
Temporizador 1226
1228 Petición de liberación de recursos 2
1222 Petición de liberación de recursos 1
Petición de liberación de recursos 2
1230 Petición de liberación de recursos 3

FIG. 12

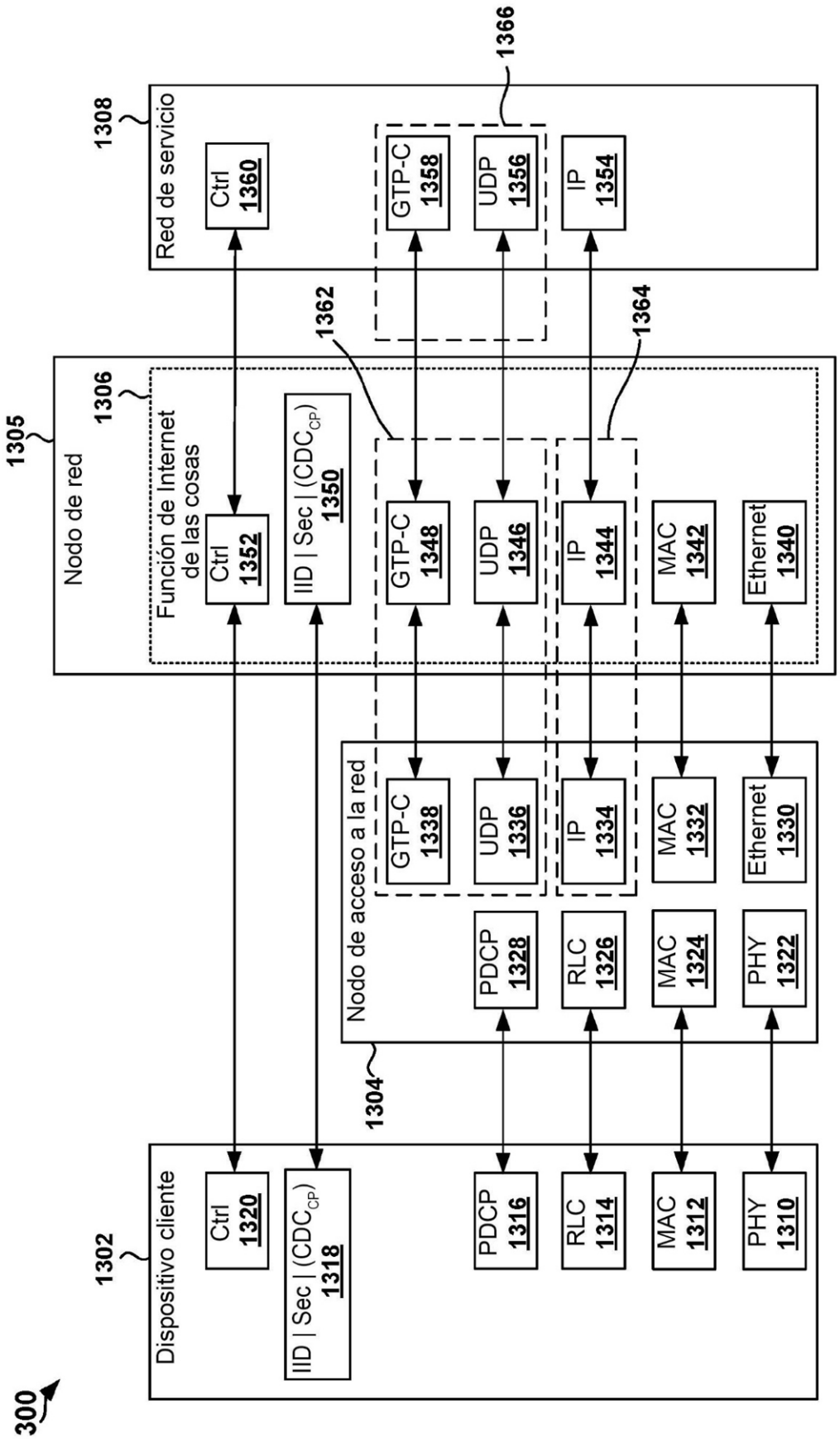
1300
1302
Dispositivo cliente
Ctrl 1320
IID | Sec | (CDC$_{CP}$) 1318
PDCP 1316
RLC 1314
MAC 1312
PHY 1310
1304
Nodo de acceso a la red
GTP-C 1338
UDP 1336
IP 1334
MAC 1332
Ethernet 1330
PDCP 1328
RLC 1326
MAC 1324
PHY 1322
1305
Nodo de red
1306
Función de Internet de las cosas
Ctrl 1352
IID | Sec | (CDC$_{CP}$) 1350
1362
GTP-C 1348
UDP 1346
1364
IP 1344
MAC 1342
Ethernet 1340
1308
Red de servicio
Ctrl 1360
1366
GTP-C 1358
UDP 1356
IP 1354

FIG. 13

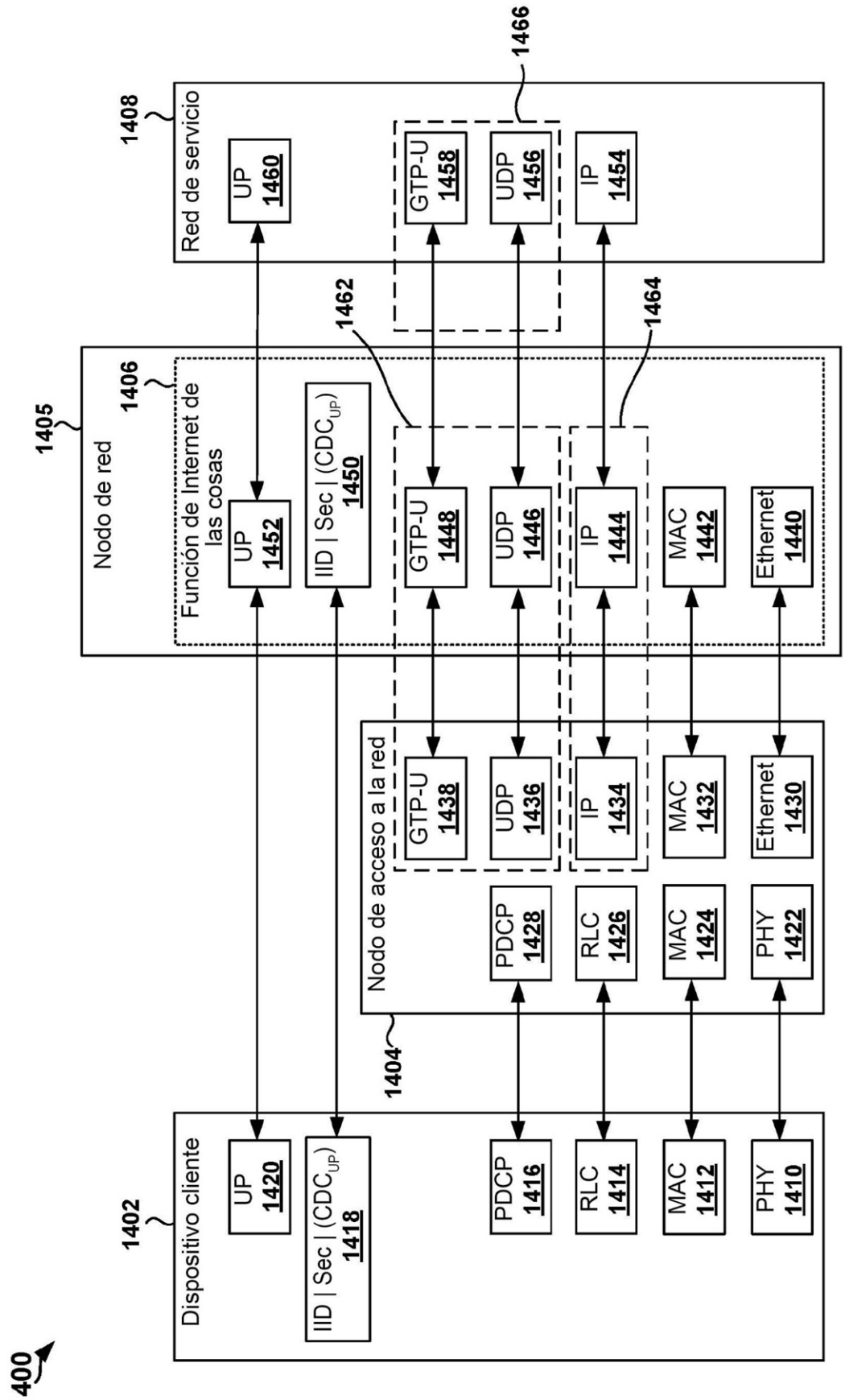
1400
1402
Dispositivo cliente
UP 1420
IID | Sec | (CDC$_{UP}$) 1418
1404
Nodo de acceso a la red
PDCP 1416
RLC 1414
MAC 1412
PHY 1410
PDCP 1428
RLC 1426
MAC 1424
PHY 1422
GTP-U 1438
UDP 1436
IP 1434
MAC 1432
Ethernet 1430
1405
Nodo de red
1406
Función de Internet de las cosas
UP 1452
IID | Sec | (CDC$_{UP}$) 1450
1462
GTP-U 1448
UDP 1446
1464
IP 1444
MAC 1442
Ethernet 1440
1408
Red de servicio
UP 1460
1466
GTP-U 1458
UDP 1456
IP 1454

FIG. 14

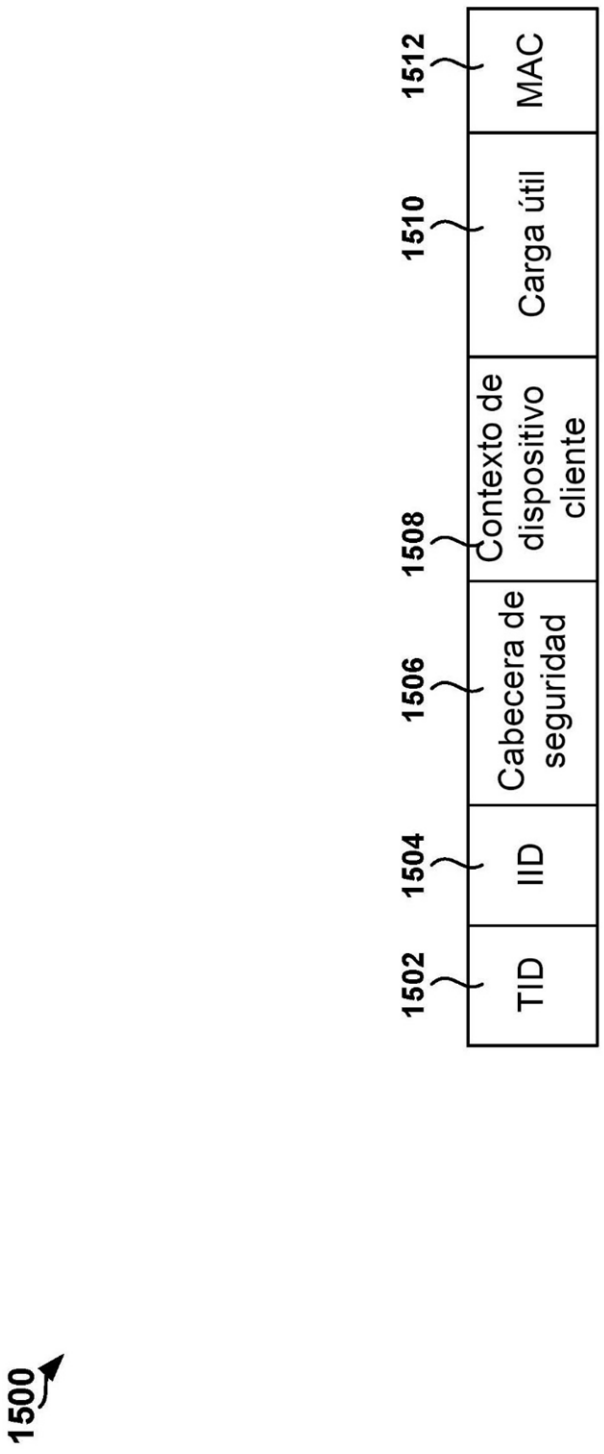
1500
1502
TID
1504
IID
1506
Cabecera de seguridad
1508
Contexto de dispositivo cliente
1510
Carga útil
1512
MAC

FIG. 15

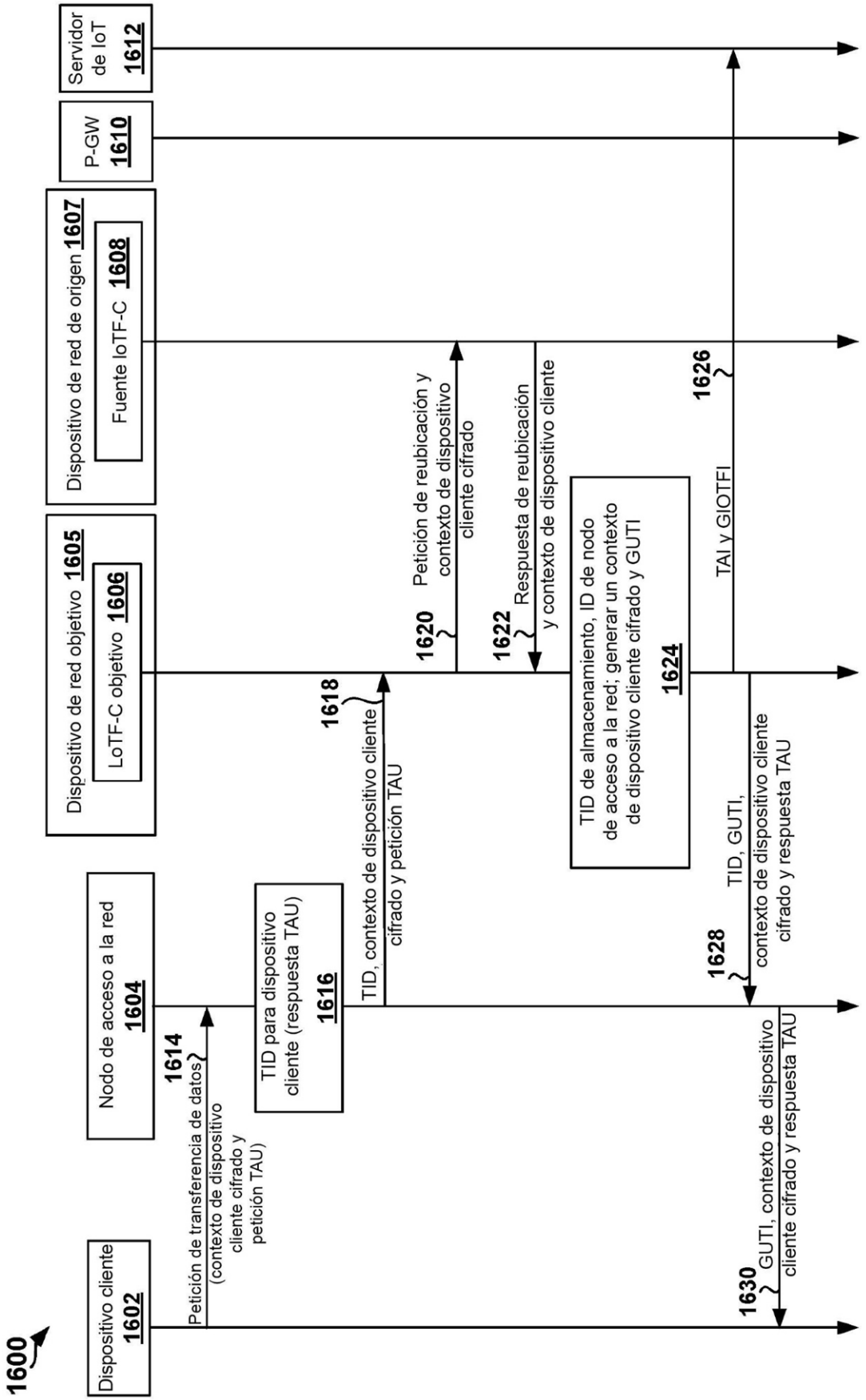
1600
Dispositivo cliente 1602
Nodo de acceso a la red 1604
Dispositivo de red objetivo 1605
LoTF-C objetivo 1606
Dispositivo de red de origen 1607
Fuente IoTF-C 1608
P-GW 1610
Servidor de IoT 1612
1614
Petición de transferencia de datos (contexto de dispositivo cliente cifrado y petición TAU)
TID para dispositivo cliente (respuesta TAU) 1616
1618
TID, contexto de dispositivo cliente cifrado y petición TAU
1620
Petición de reubicación y contexto de dispositivo cliente cifrado
1622
Respuesta de reubicación y contexto de dispositivo cliente
TID de almacenamiento, ID de nodo de acceso a la red; generar un contexto de dispositivo cliente cifrado y GUTI 1624
1626
TAI y GIOTFI
1628
TID, GUTI, contexto de dispositivo cliente cifrado y respuesta TAU
1630
GUTI, contexto de dispositivo cliente cifrado y respuesta TAU

FIG. 16

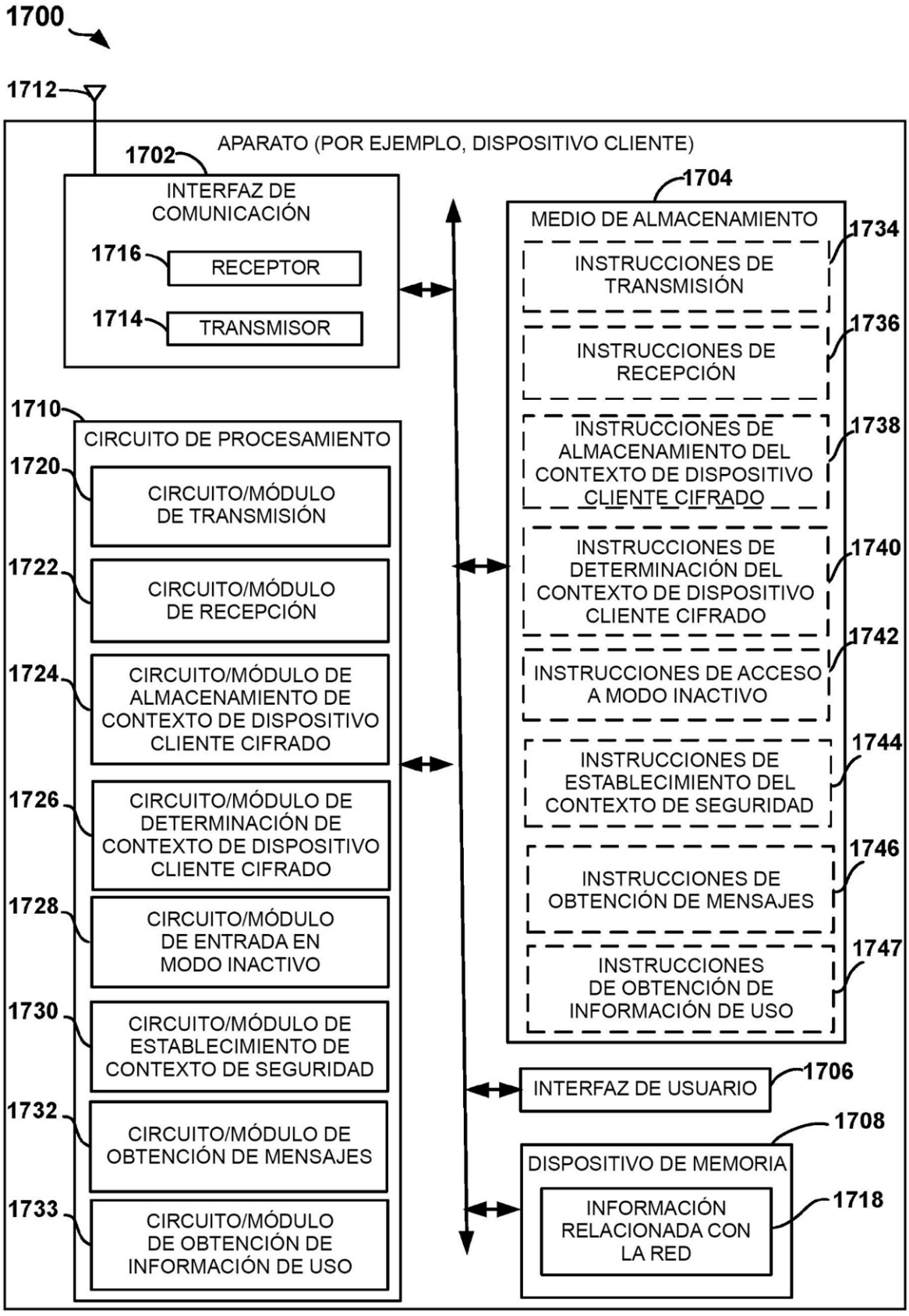
1700
1712
APARATO (POR EJEMPLO, DISPOSITIVO CLIENTE)
1702
INTERFAZ DE COMUNICACIÓN
1716
RECEPTOR
1714
TRANSMISOR
1704
MEDIO DE ALMACENAMIENTO
1734
INSTRUCCIONES DE TRANSMISIÓN
1736
INSTRUCCIONES DE RECEPCIÓN
1738
INSTRUCCIONES DE ALMACENAMIENTO DEL CONTEXTO DE DISPOSITIVO CLIENTE CIFRADO
1740
INSTRUCCIONES DE DETERMINACIÓN DEL CONTEXTO DE DISPOSITIVO CLIENTE CIFRADO
1742
INSTRUCCIONES DE ACCESO A MODO INACTIVO
1744
INSTRUCCIONES DE ESTABLECIMIENTO DEL CONTEXTO DE SEGURIDAD
1746
INSTRUCCIONES DE OBTENCIÓN DE MENSAJES
1747
INSTRUCCIONES DE OBTENCIÓN DE INFORMACIÓN DE USO
1710
CIRCUITO DE PROCESAMIENTO
1720
CIRCUITO/MÓDULO DE TRANSMISIÓN
1722
CIRCUITO/MÓDULO DE RECEPCIÓN
1724
CIRCUITO/MÓDULO DE ALMACENAMIENTO DE CONTEXTO DE DISPOSITIVO CLIENTE CIFRADO
1726
CIRCUITO/MÓDULO DE DETERMINACIÓN DE CONTEXTO DE DISPOSITIVO CLIENTE CIFRADO
1728
CIRCUITO/MÓDULO DE ENTRADA EN MODO INACTIVO
1730
CIRCUITO/MÓDULO DE ESTABLECIMIENTO DE CONTEXTO DE SEGURIDAD
1732
CIRCUITO/MÓDULO DE OBTENCIÓN DE MENSAJES
1733
CIRCUITO/MÓDULO DE OBTENCIÓN DE INFORMACIÓN DE USO
1706
INTERFAZ DE USUARIO
1708
DISPOSITIVO DE MEMORIA
1718
INFORMACIÓN RELACIONADA CON LA RED

FIG. 17

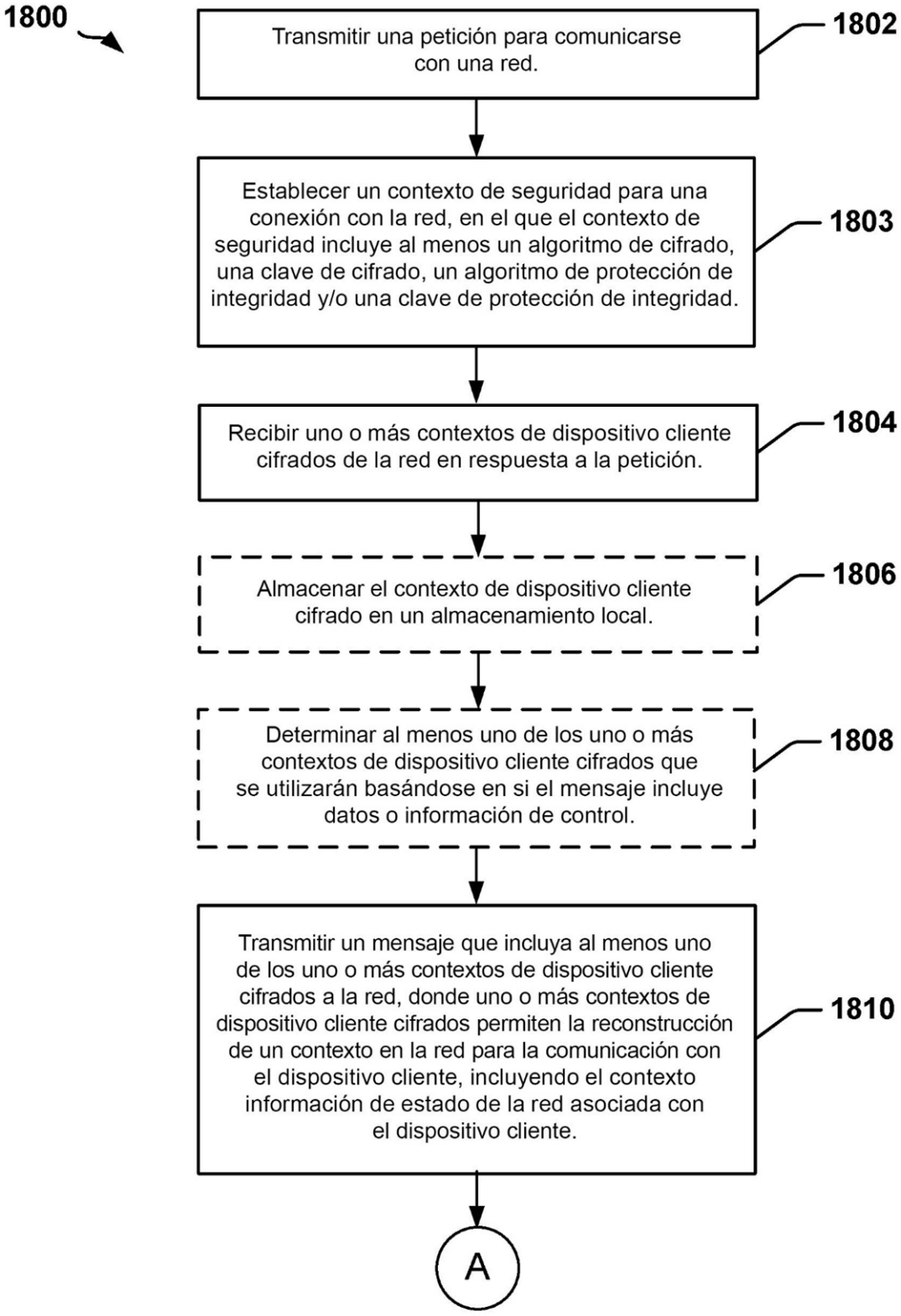
1800
Transmitir una petición para comunicarse con una red.
1802
Establecer un contexto de seguridad para una conexión con la red, en el que el contexto de seguridad incluye al menos un algoritmo de cifrado, una clave de cifrado, un algoritmo de protección de integridad y/o una clave de protección de integridad.
1803
Recibir uno o más contextos de dispositivo cliente cifrados de la red en respuesta a la petición.
1804
Almacenar el contexto de dispositivo cliente cifrado en un almacenamiento local.
1806
Determinar al menos uno de los uno o más contextos de dispositivo cliente cifrados que se utilizarán basándose en si el mensaje incluye datos o información de control.
1808
Transmitir un mensaje que incluya al menos uno de los uno o más contextos de dispositivo cliente cifrados a la red, donde uno o más contextos de dispositivo cliente cifrados permiten la reconstrucción de un contexto en la red para la comunicación con el dispositivo cliente, incluyendo el contexto información de estado de la red asociada con el dispositivo cliente.
1810
A

FIG. 18A

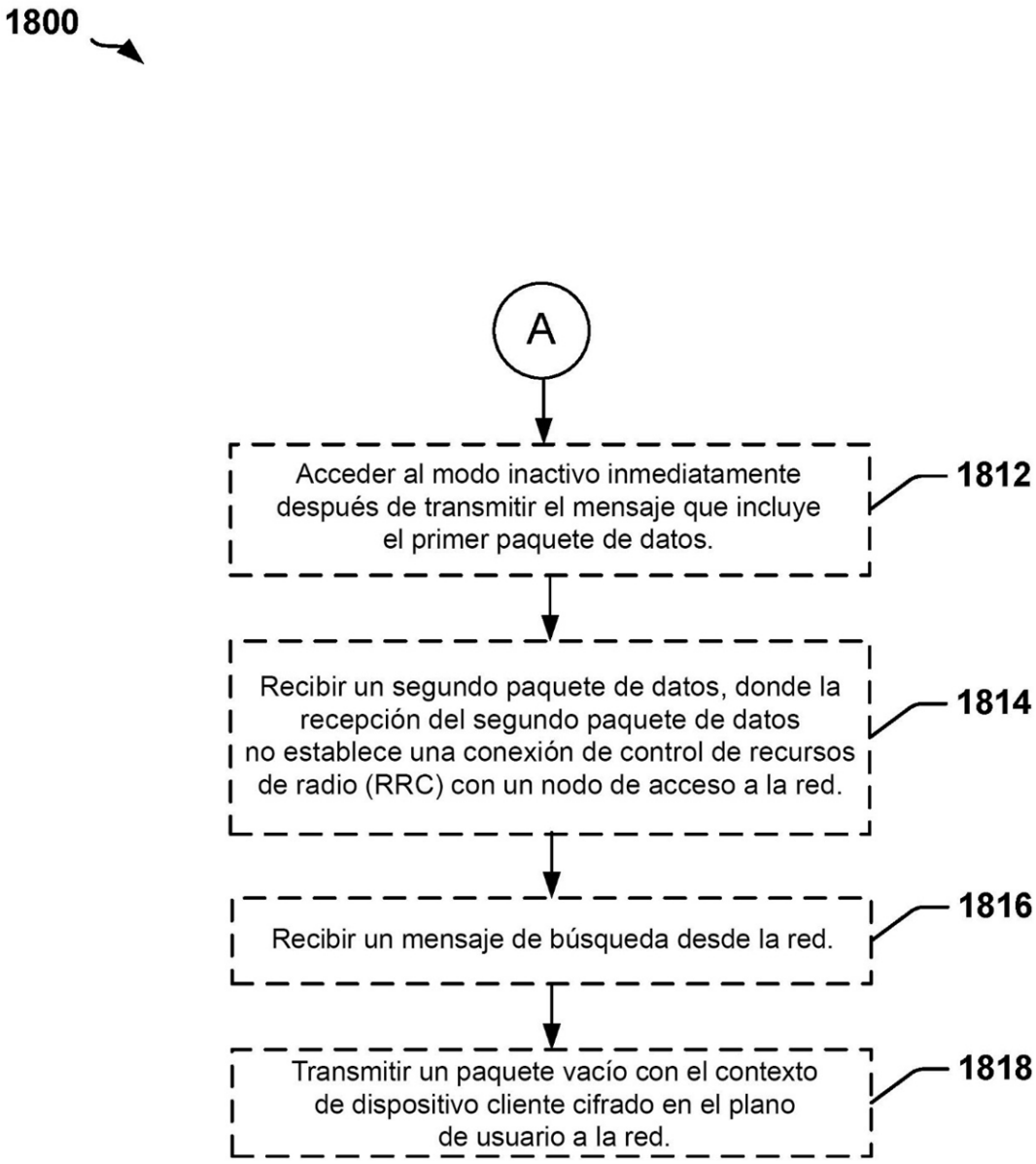
1800
A
Acceder al modo inactivo inmediatamente después de transmitir el mensaje que incluye el primer paquete de datos.
1812
Recibir un segundo paquete de datos, donde la recepción del segundo paquete de datos no establece una conexión de control de recursos de radio (RRC) con un nodo de acceso a la red.
1814
Recibir un mensaje de búsqueda desde la red.
1816
Transmitir un paquete vacío con el contexto de dispositivo cliente cifrado en el plano de usuario a la red.
1818

FIG. 18B

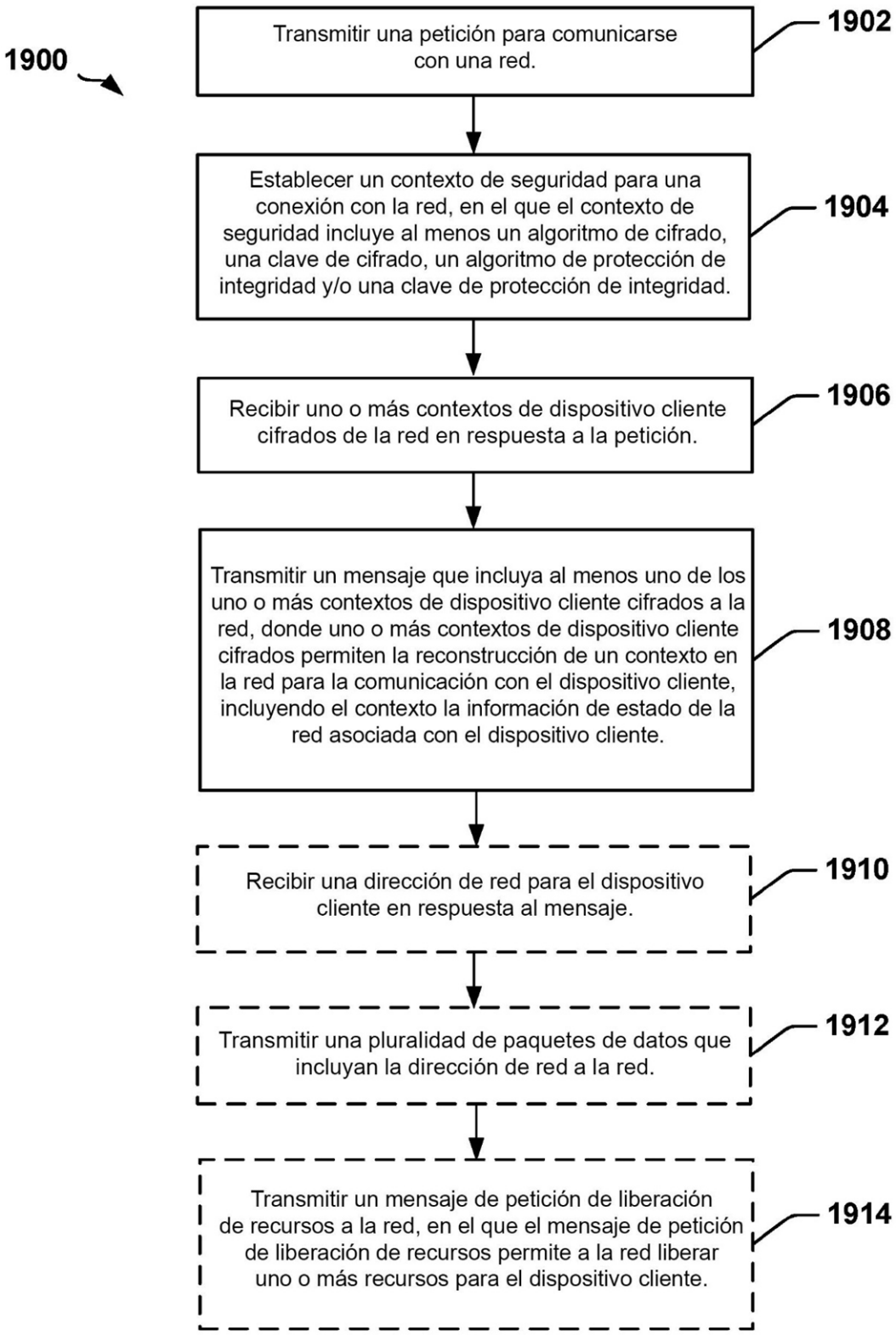
1900
Transmitir una petición para comunicarse con una red.
1902
Establecer un contexto de seguridad para una conexión con la red, en el que el contexto de seguridad incluye al menos un algoritmo de cifrado, una clave de cifrado, un algoritmo de protección de integridad y/o una clave de protección de integridad.
1904
Recibir uno o más contextos de dispositivo cliente cifrados de la red en respuesta a la petición.
1906
Transmitir un mensaje que incluya al menos uno de los uno o más contextos de dispositivo cliente cifrados a la red, donde uno o más contextos de dispositivo cliente cifrados permiten la reconstrucción de un contexto en la red para la comunicación con el dispositivo cliente, incluyendo el contexto la información de estado de la red asociada con el dispositivo cliente.
1908
Recibir una dirección de red para el dispositivo cliente en respuesta al mensaje.
1910
Transmitir una pluralidad de paquetes de datos que incluyan la dirección de red a la red.
1912
Transmitir un mensaje de petición de liberación de recursos a la red, en el que el mensaje de petición de liberación de recursos permite a la red liberar uno o más recursos para el dispositivo cliente.
1914

FIG. 19

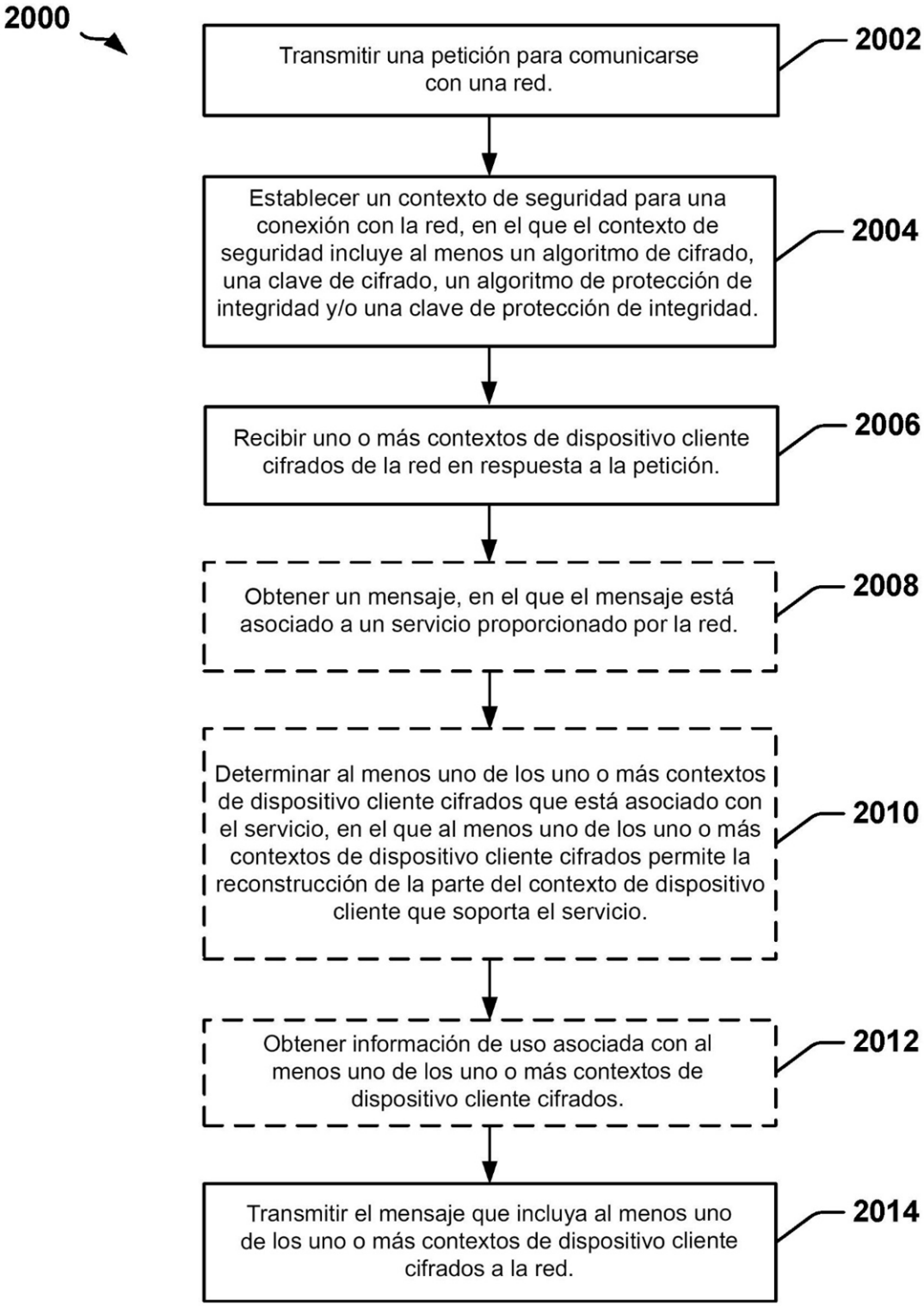
2000
Transmitir una petición para comunicarse con una red.
2002
Establecer un contexto de seguridad para una conexión con la red, en el que el contexto de seguridad incluye al menos un algoritmo de cifrado, una clave de cifrado, un algoritmo de protección de integridad y/o una clave de protección de integridad.
2004
Recibir uno o más contextos de dispositivo cliente cifrados de la red en respuesta a la petición.
2006
Obtener un mensaje, en el que el mensaje está asociado a un servicio proporcionado por la red.
2008
Determinar al menos uno de los uno o más contextos de dispositivo cliente cifrados que está asociado con el servicio, en el que al menos uno de los uno o más contextos de dispositivo cliente cifrados permite la reconstrucción de la parte del contexto de dispositivo cliente que soporta el servicio.
2010
Obtener información de uso asociada con al menos uno de los uno o más contextos de dispositivo cliente cifrados.
2012
Transmitir el mensaje que incluya al menos uno de los uno o más contextos de dispositivo cliente cifrados a la red.
2014

FIG. 20

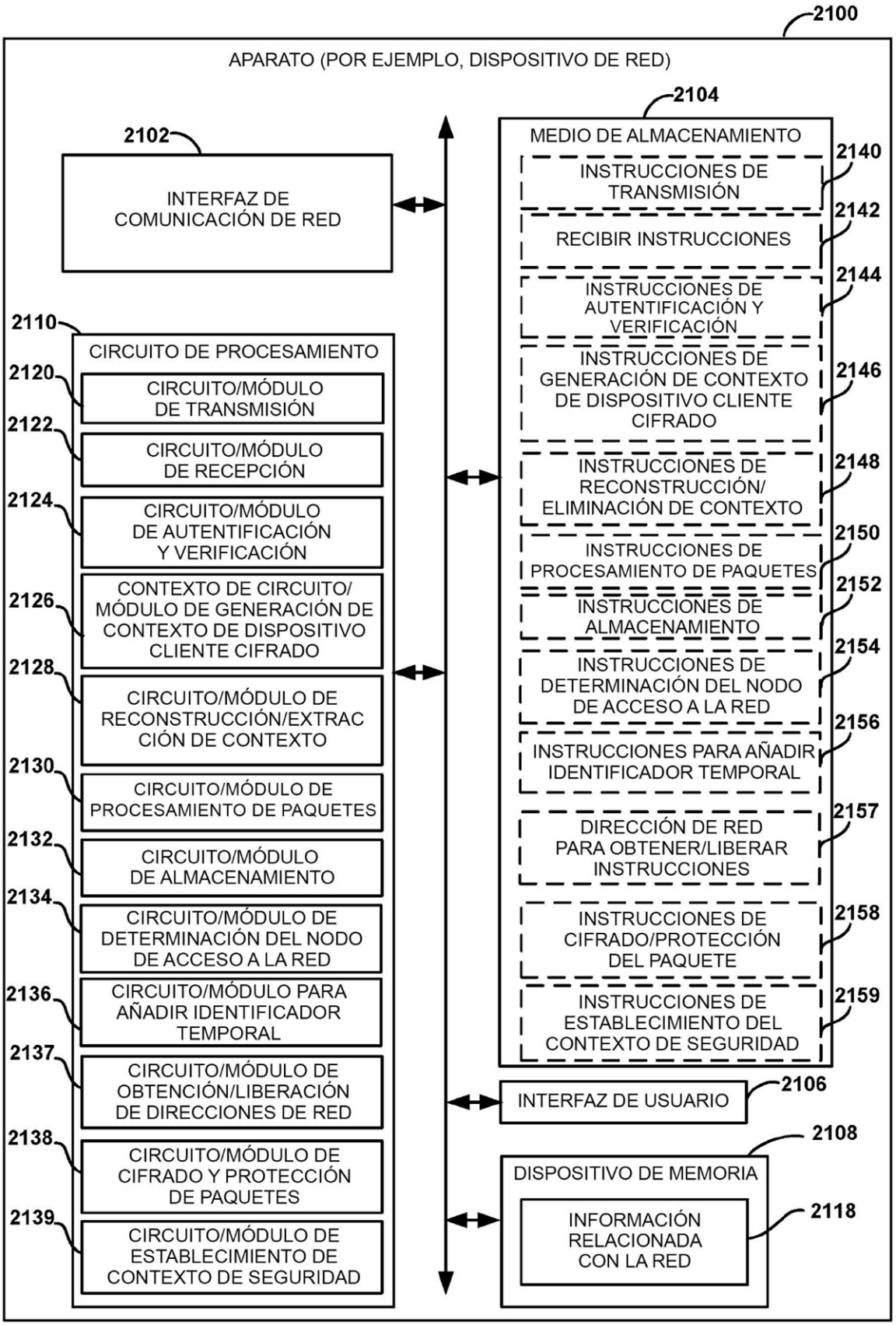
2100
APARATO (POR EJEMPLO, DISPOSITIVO DE RED)
2102
INTERFAZ DE COMUNICACIÓN DE RED
2104
MEDIO DE ALMACENAMIENTO
2140
INSTRUCCIONES DE TRANSMISIÓN
2142
RECIBIR INSTRUCCIONES
2144
INSTRUCCIONES DE AUTENTIFICACIÓN Y VERIFICACIÓN
2146
INSTRUCCIONES DE GENERACIÓN DE CONTEXTO DE DISPOSITIVO CLIENTE CIFRADO
2148
INSTRUCCIONES DE RECONSTRUCCIÓN/ ELIMINACIÓN DE CONTEXTO
2150
INSTRUCCIONES DE PROCESAMIENTO DE PAQUETES
2152
INSTRUCCIONES DE ALMACENAMIENTO
2154
INSTRUCCIONES DE DETERMINACIÓN DEL NODO DE ACCESO A LA RED
2156
INSTRUCCIONES PARA AÑADIR IDENTIFICADOR TEMPORAL
2157
DIRECCIÓN DE RED PARA OBTENER/LIBERAR INSTRUCCIONES
2158
INSTRUCCIONES DE CIFRADO/PROTECCIÓN DEL PAQUETE
2159
INSTRUCCIONES DE ESTABLECIMIENTO DEL CONTEXTO DE SEGURIDAD
2110
CIRCUITO DE PROCESAMIENTO
2120
CIRCUITO/MÓDULO DE TRANSMISIÓN
2122
CIRCUITO/MÓDULO DE RECEPCIÓN
2124
CIRCUITO/MÓDULO DE AUTENTIFICACIÓN Y VERIFICACIÓN
2126
CONTEXTO DE CIRCUITO/ MÓDULO DE GENERACIÓN DE CONTEXTO DE DISPOSITIVO CLIENTE CIFRADO
2128
CIRCUITO/MÓDULO DE RECONSTRUCCIÓN/EXTRAC CIÓN DE CONTEXTO
2130
CIRCUITO/MÓDULO DE PROCESAMIENTO DE PAQUETES
2132
CIRCUITO/MÓDULO DE ALMACENAMIENTO
2134
CIRCUITO/MÓDULO DE DETERMINACIÓN DEL NODO DE ACCESO A LA RED
2136
CIRCUITO/MÓDULO PARA AÑADIR IDENTIFICADOR TEMPORAL
2137
CIRCUITO/MÓDULO DE OBTENCIÓN/LIBERACIÓN DE DIRECCIONES DE RED
2138
CIRCUITO/MÓDULO DE CIFRADO Y PROTECCIÓN DE PAQUETES
2139
CIRCUITO/MÓDULO DE ESTABLECIMIENTO DE CONTEXTO DE SEGURIDAD
2106
INTERFAZ DE USUARIO
2108
DISPOSITIVO DE MEMORIA
2118
INFORMACIÓN RELACIONADA CON LA RED

FIG. 21

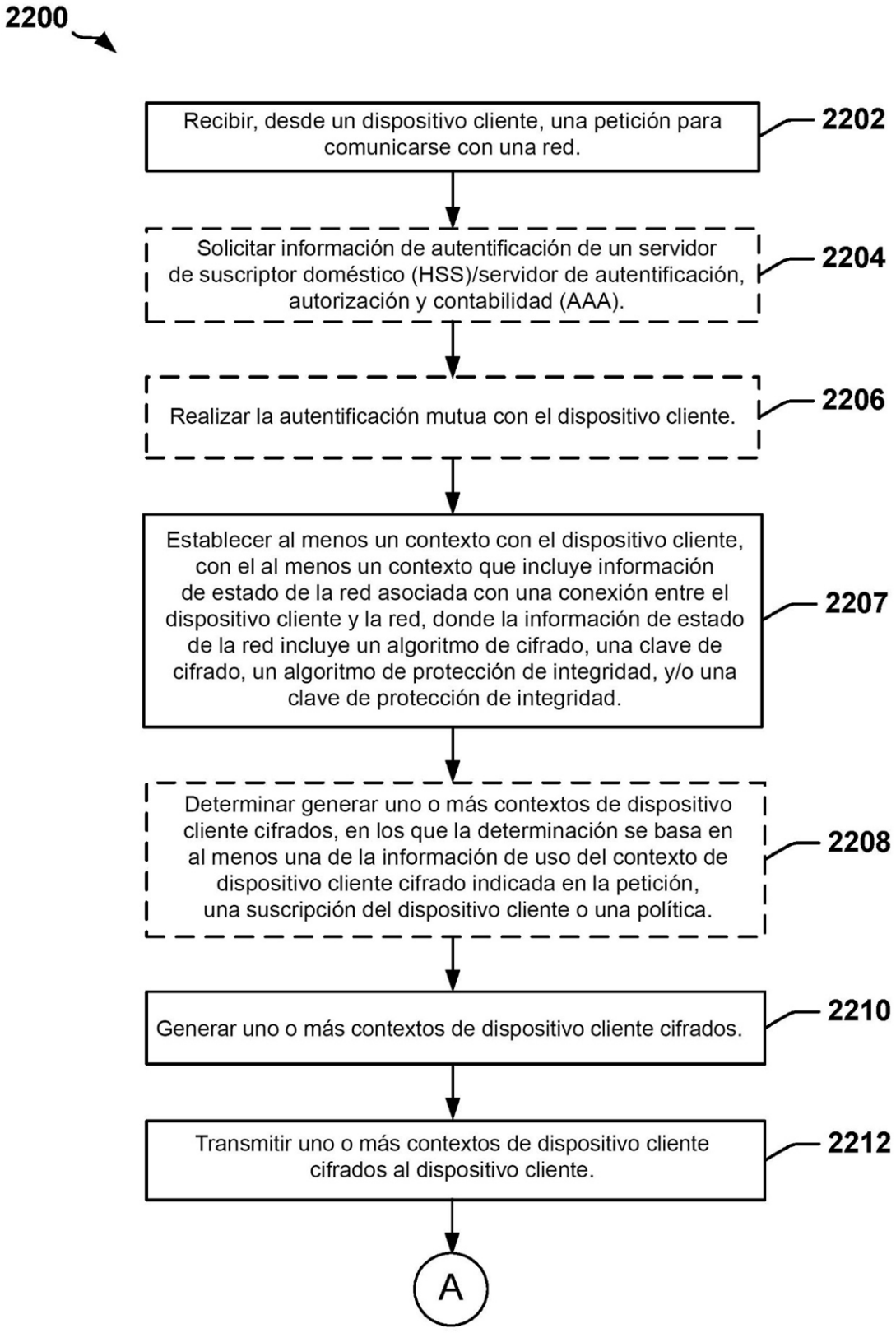
2200
Recibir, desde un dispositivo cliente, una petición para comunicarse con una red.
2202
Solicitar información de autentificación de un servidor de suscriptor doméstico (HSS)/servidor de autentificación, autorización y contabilidad (AAA).
2204
Realizar la autentificación mutua con el dispositivo cliente.
2206
Establecer al menos un contexto con el dispositivo cliente, con el al menos un contexto que incluye información de estado de la red asociada con una conexión entre el dispositivo cliente y la red, donde la información de estado de la red incluye un algoritmo de cifrado, una clave de cifrado, un algoritmo de protección de integridad, y/o una clave de protección de integridad.
2207
Determinar generar uno o más contextos de dispositivo cliente cifrados, en los que la determinación se basa en al menos una de la información de uso del contexto de dispositivo cliente cifrado indicada en la petición, una suscripción del dispositivo cliente o una política.
2208
Generar uno o más contextos de dispositivo cliente cifrados.
2210
Transmitir uno o más contextos de dispositivo cliente cifrados al dispositivo cliente.
2212
A

FIG. 22A

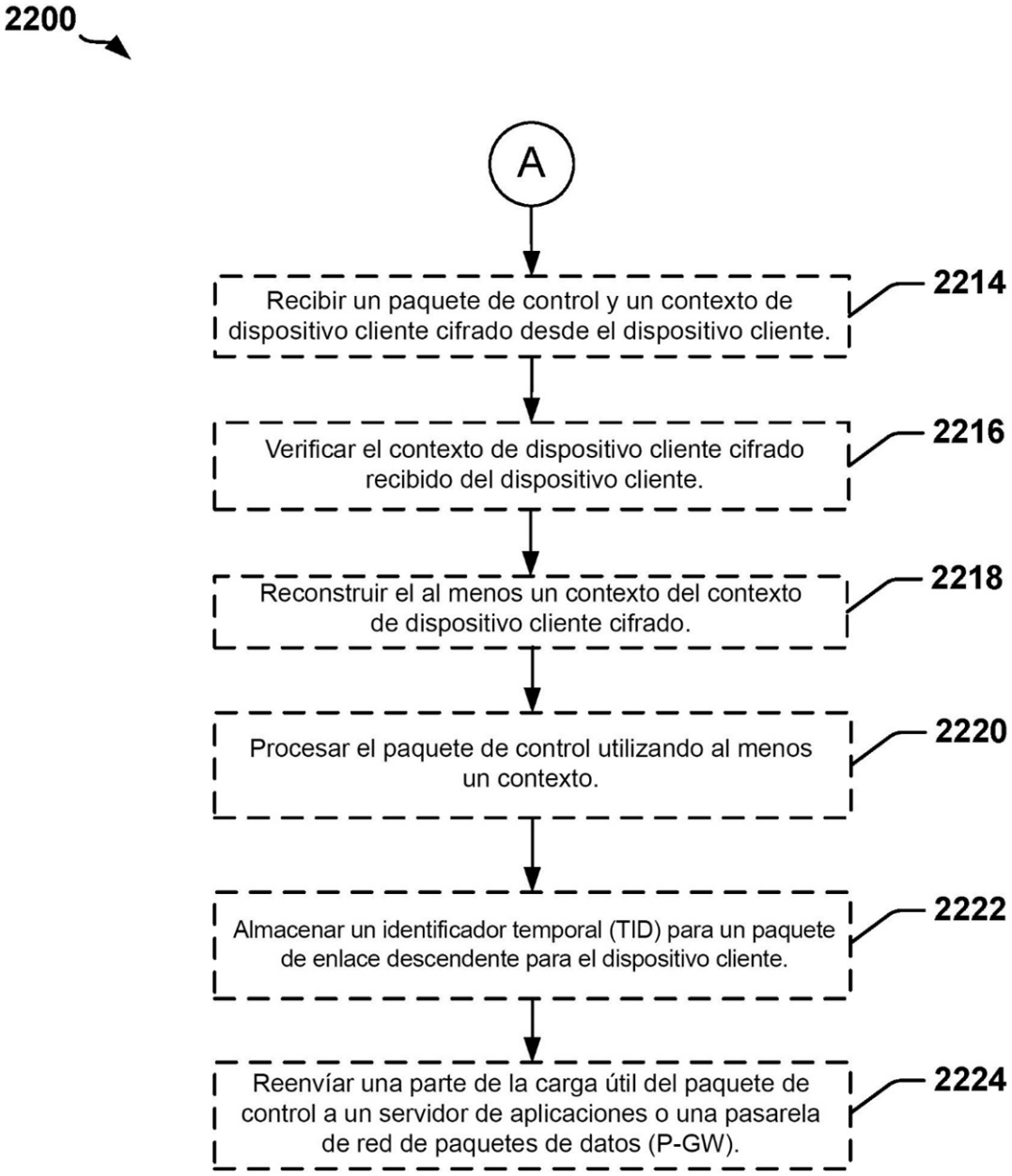
2200
A
Recibir un paquete de control y un contexto de dispositivo cliente cifrado desde el dispositivo cliente.
2214
Verificar el contexto de dispositivo cliente cifrado recibido del dispositivo cliente.
2216
Reconstruir el al menos un contexto del contexto de dispositivo cliente cifrado.
2218
Procesar el paquete de control utilizando al menos un contexto.
2220
Almacenar un identificador temporal (TID) para un paquete de enlace descendente para el dispositivo cliente.
2222
Reenvíar una parte de la carga útil del paquete de control a un servidor de aplicaciones o una pasarela de red de paquetes de datos (P-GW).
2224

FIG. 22B

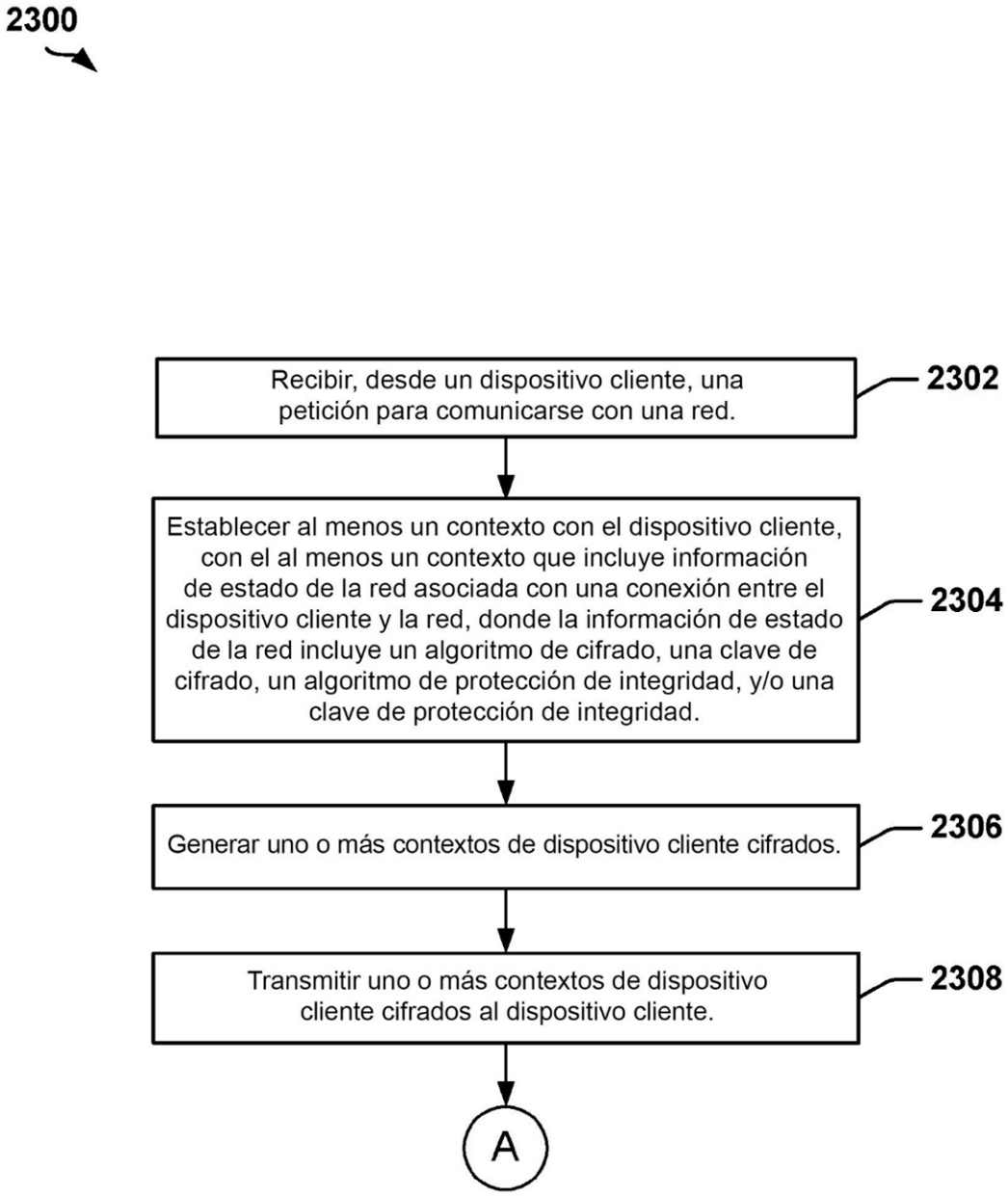
2300
Recibir, desde un dispositivo cliente, una petición para comunicarse con una red.
2302
Establecer al menos un contexto con el dispositivo cliente, con el al menos un contexto que incluye información de estado de la red asociada con una conexión entre el dispositivo cliente y la red, donde la información de estado de la red incluye un algoritmo de cifrado, una clave de cifrado, un algoritmo de protección de integridad, y/o una clave de protección de integridad.
2304
Generar uno o más contextos de dispositivo cliente cifrados.
2306
Transmitir uno o más contextos de dispositivo cliente cifrados al dispositivo cliente.
2308
A

FIG. 23A

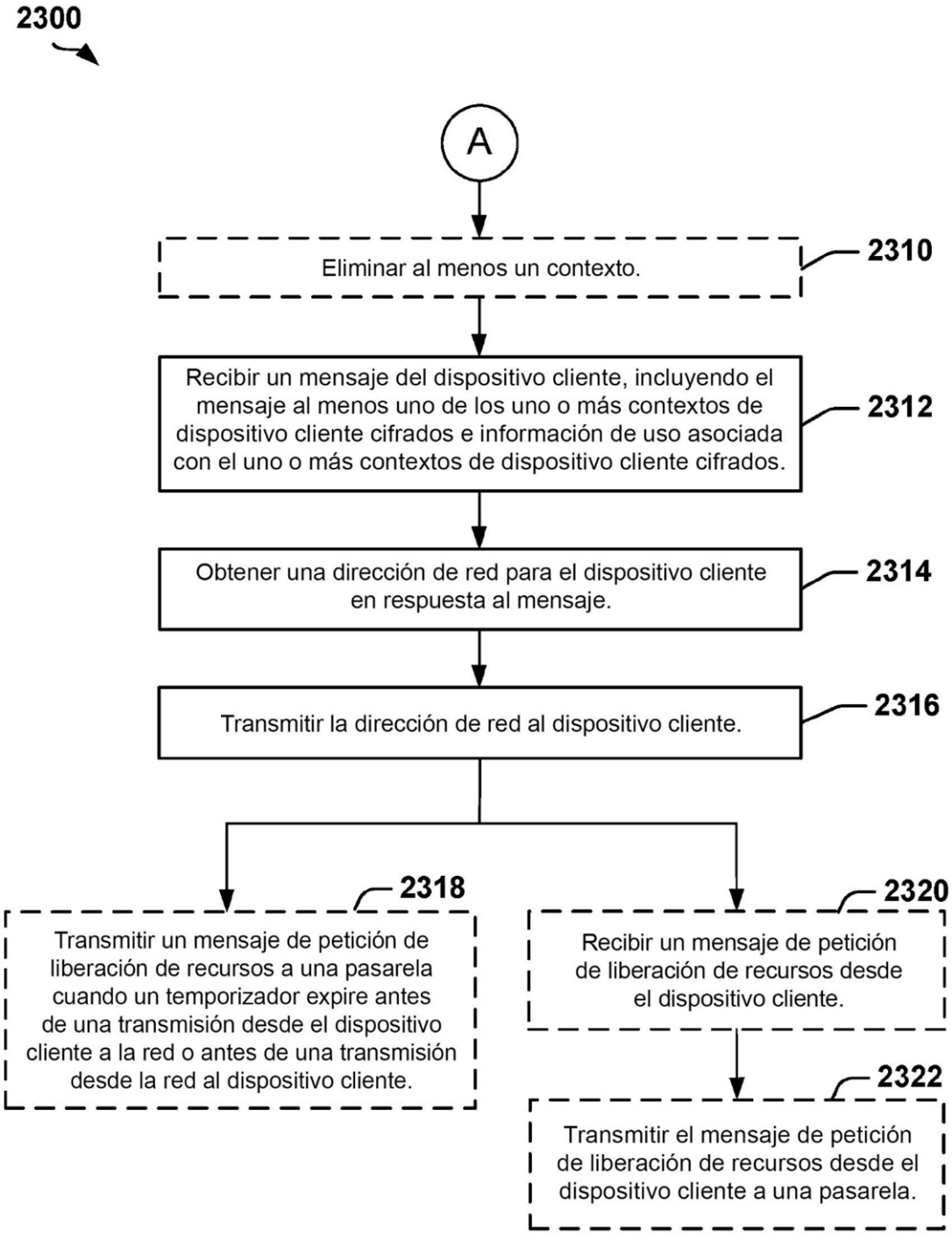
2300
A
Eliminar al menos un contexto.
2310
Recibir un mensaje del dispositivo cliente, incluyendo el mensaje al menos uno de los uno o más contextos de dispositivo cliente cifrados e información de uso asociada con el uno o más contextos de dispositivo cliente cifrados.
2312
Obtener una dirección de red para el dispositivo cliente en respuesta al mensaje.
2314
Transmitir la dirección de red al dispositivo cliente.
2316
2318
Transmitir un mensaje de petición de liberación de recursos a una pasarela cuando un temporizador expire antes de una transmisión desde el dispositivo cliente a la red o antes de una transmisión desde la red al dispositivo cliente.
2320
Recibir un mensaje de petición de liberación de recursos desde el dispositivo cliente.
2322
Transmitir el mensaje de petición de liberación de recursos desde el dispositivo cliente a una pasarela.

FIG. 23B

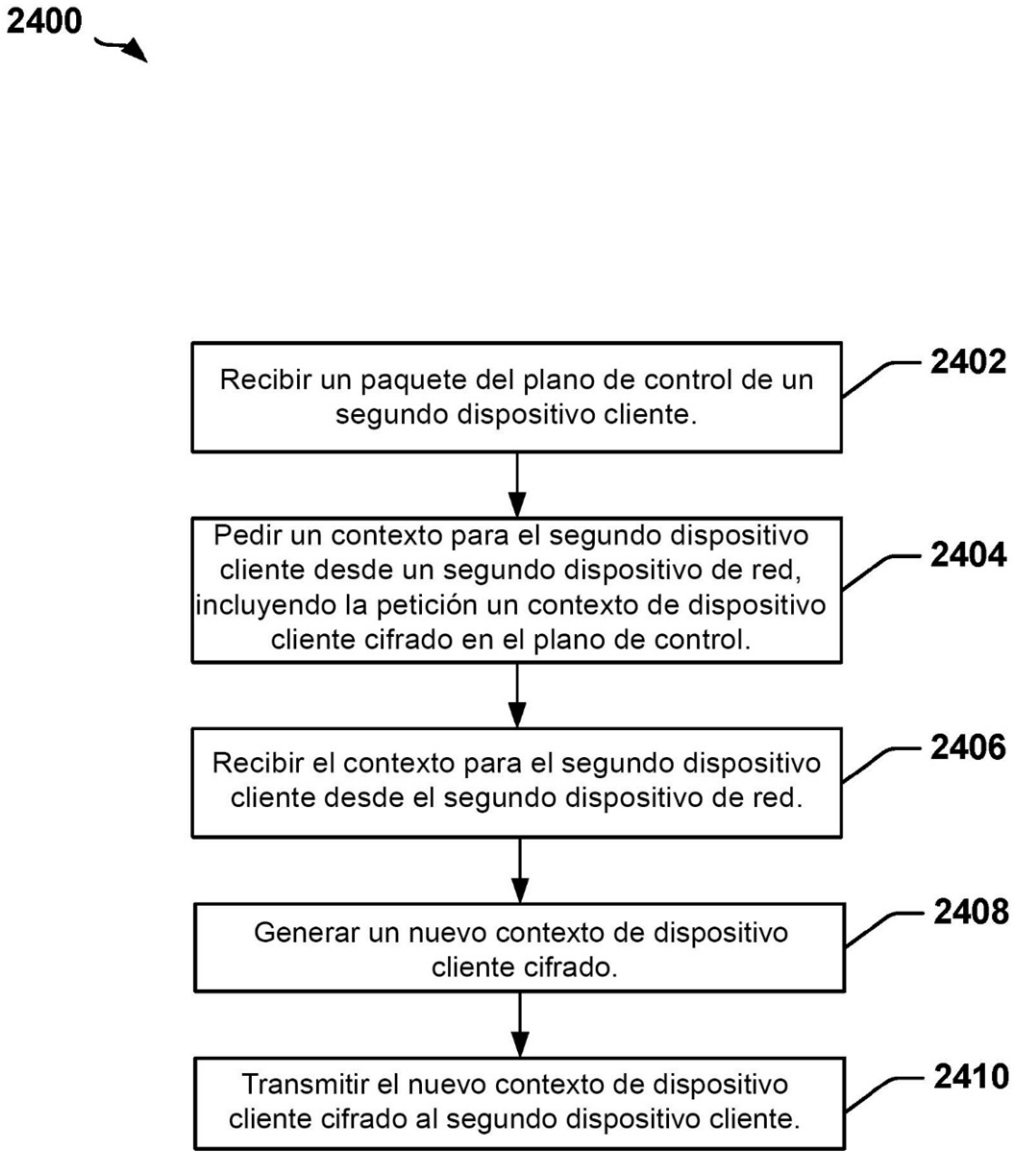
2400
Recibir un paquete del plano de control de un segundo dispositivo cliente.
2402
Pedir un contexto para el segundo dispositivo cliente desde un segundo dispositivo de red, incluyendo la petición un contexto de dispositivo cliente cifrado en el plano de control.
2404
Recibir el contexto para el segundo dispositivo cliente desde el segundo dispositivo de red.
2406
Generar un nuevo contexto de dispositivo cliente cifrado.
2408
Transmitir el nuevo contexto de dispositivo cliente cifrado al segundo dispositivo cliente.
2410

FIG. 24

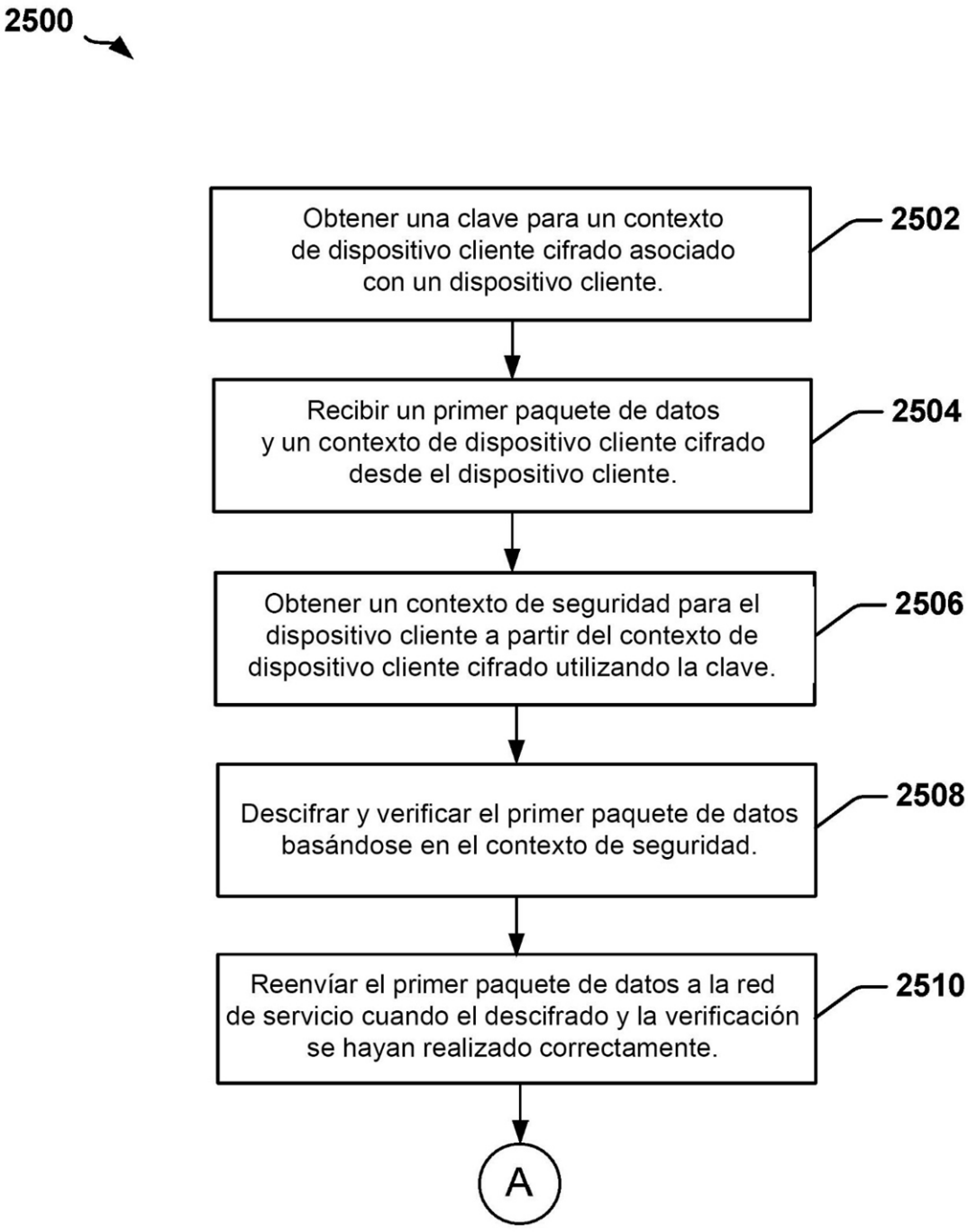
2500
Obtener una clave para un contexto de dispositivo cliente cifrado asociado con un dispositivo cliente.
2502
Recibir un primer paquete de datos y un contexto de dispositivo cliente cifrado desde el dispositivo cliente.
2504
Obtener un contexto de seguridad para el dispositivo cliente a partir del contexto de dispositivo cliente cifrado utilizando la clave.
2506
Descifrar y verificar el primer paquete de datos basándose en el contexto de seguridad.
2508
Reenvíar el primer paquete de datos a la red de servicio cuando el descifrado y la verificación se hayan realizado correctamente.
2510
A

FIG. 25A

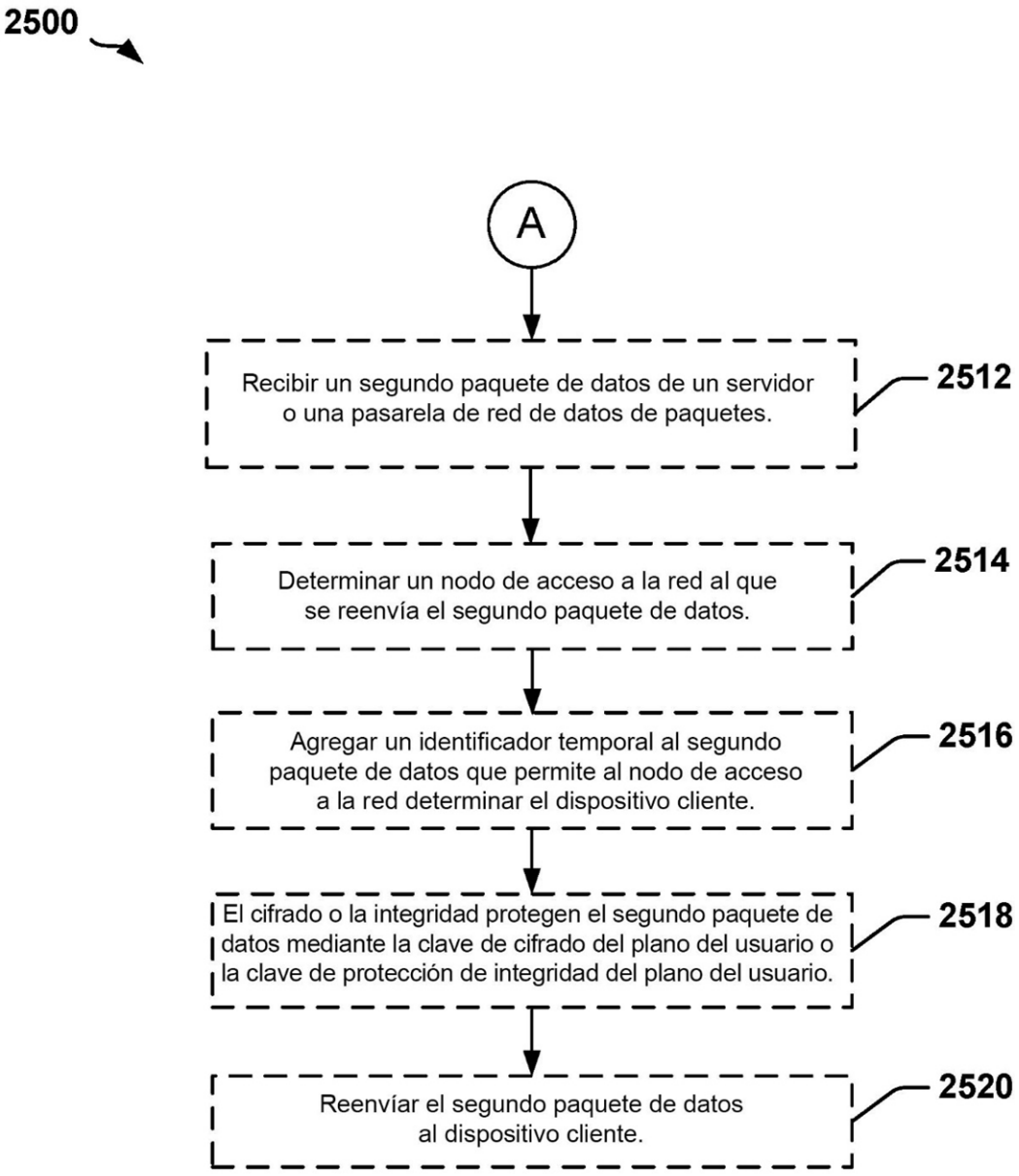
2500
A
Recibir un segundo paquete de datos de un servidor o una pasarela de red de datos de paquetes.
2512
Determinar un nodo de acceso a la red al que se reenvía el segundo paquete de datos.
2514
Agregar un identificador temporal al segundo paquete de datos que permite al nodo de acceso a la red determinar el dispositivo cliente.
2516
El cifrado o la integridad protegen el segundo paquete de datos mediante la clave de cifrado del plano del usuario o la clave de protección de integridad del plano del usuario.
2518
Reenvíar el segundo paquete de datos al dispositivo cliente.
2520

FIG. 25B

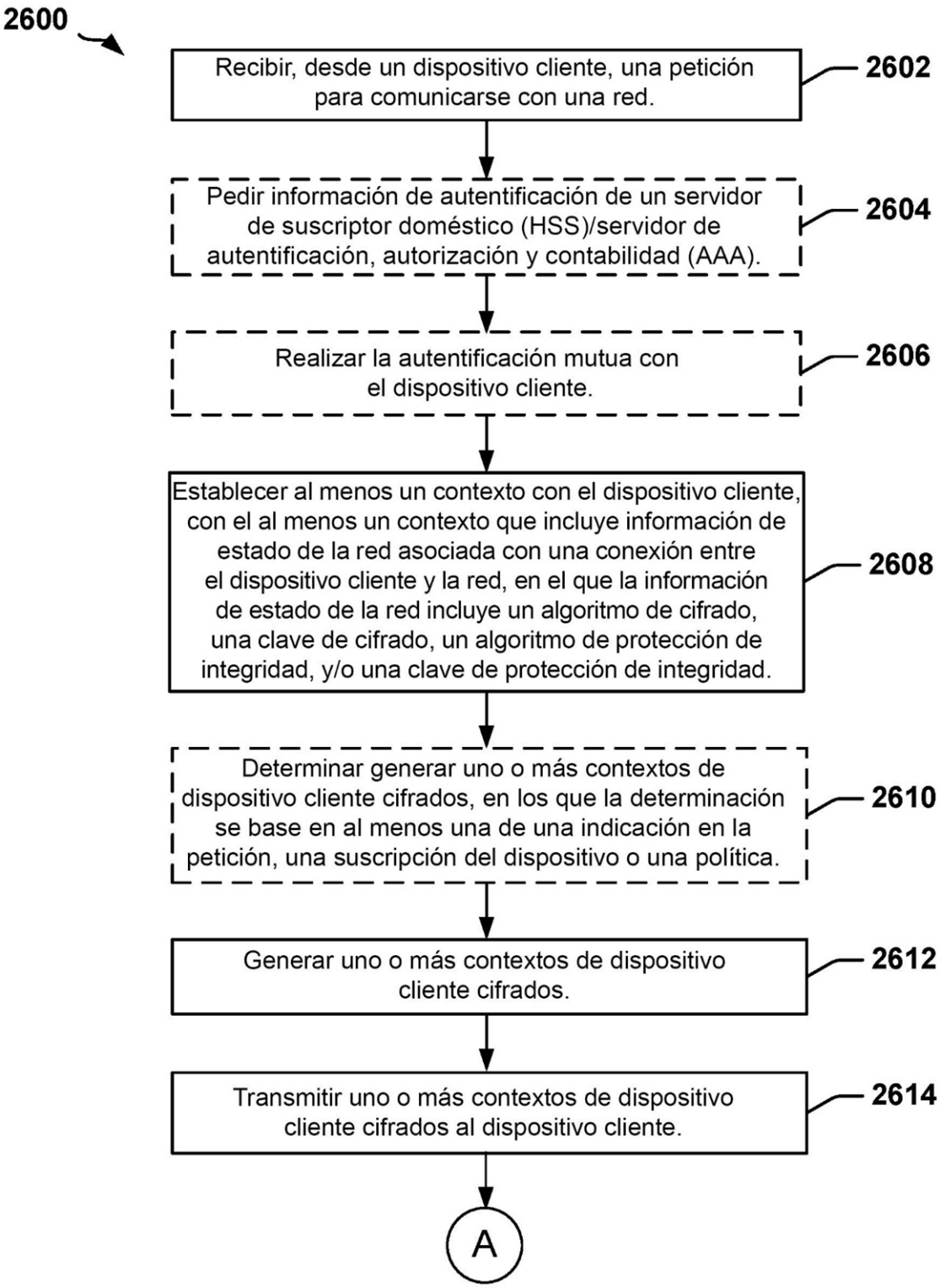
2600
Recibir, desde un dispositivo cliente, una petición para comunicarse con una red.
2602
Pedir información de autentificación de un servidor de suscriptor doméstico (HSS)/servidor de autentificación, autorización y contabilidad (AAA).
2604
Realizar la autentificación mutua con el dispositivo cliente.
2606
Establecer al menos un contexto con el dispositivo cliente, con el al menos un contexto que incluye información de estado de la red asociada con una conexión entre el dispositivo cliente y la red, en el que la información de estado de la red incluye un algoritmo de cifrado, una clave de cifrado, un algoritmo de protección de integridad, y/o una clave de protección de integridad.
2608
Determinar generar uno o más contextos de dispositivo cliente cifrados, en los que la determinación se base en al menos una de una indicación en la petición, una suscripción del dispositivo o una política.
2610
Generar uno o más contextos de dispositivo cliente cifrados.
2612
Transmitir uno o más contextos de dispositivo cliente cifrados al dispositivo cliente.
2614
A

FIG. 26A

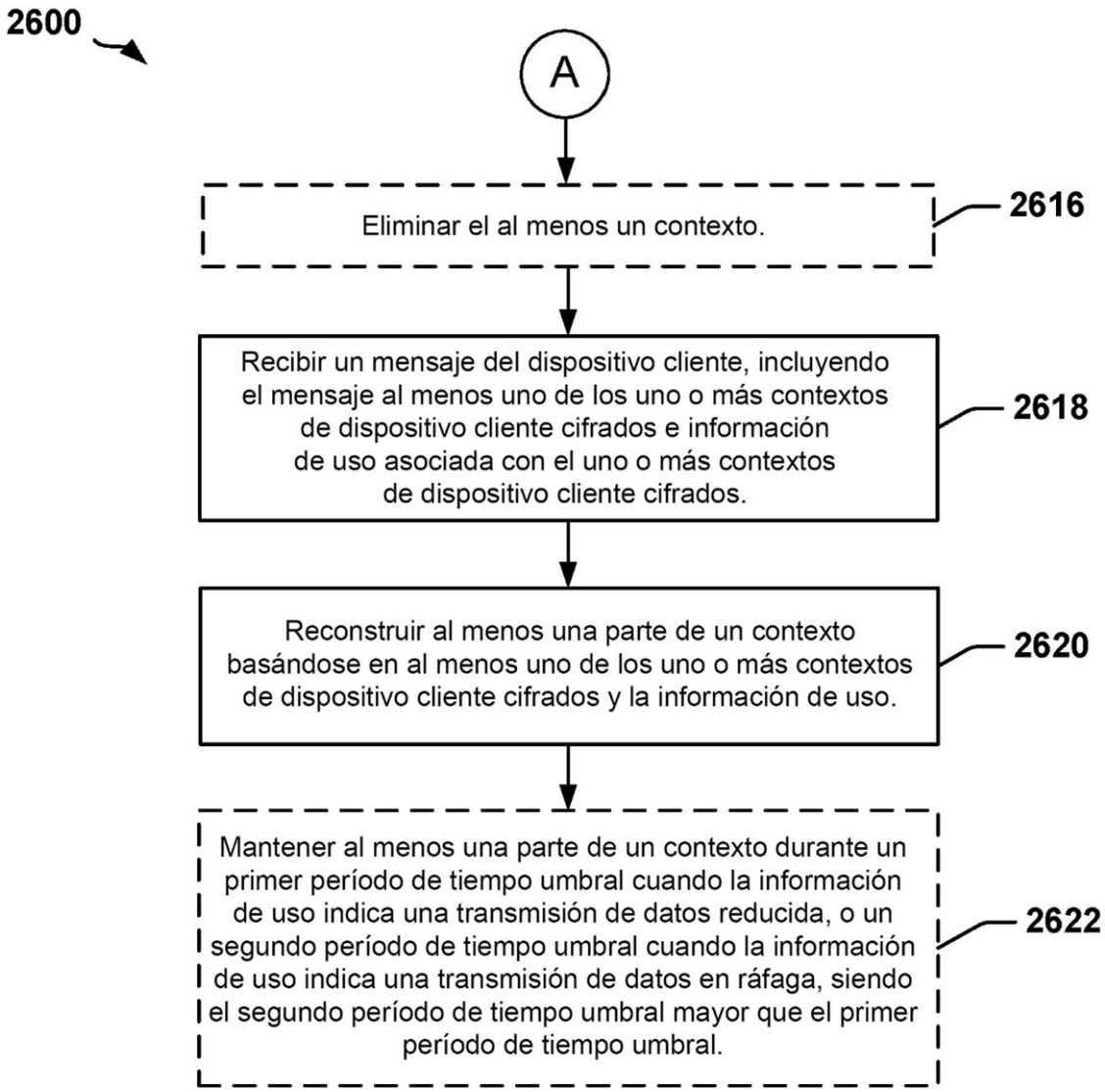
2600
A
Eliminar el al menos un contexto.
2616
Recibir un mensaje del dispositivo cliente, incluyendo el mensaje al menos uno de los uno o más contextos de dispositivo cliente cifrados e información de uso asociada con el uno o más contextos de dispositivo cliente cifrados.
2618
Reconstruir al menos una parte de un contexto basándose en al menos uno de los uno o más contextos de dispositivo cliente cifrados y la información de uso.
2620
Mantener al menos una parte de un contexto durante un primer período de tiempo umbral cuando la información de uso indica una transmisión de datos reducida, o un segundo período de tiempo umbral cuando la información de uso indica una transmisión de datos en ráfaga, siendo el segundo período de tiempo umbral mayor que el primer período de tiempo umbral.
2622

FIG. 26B

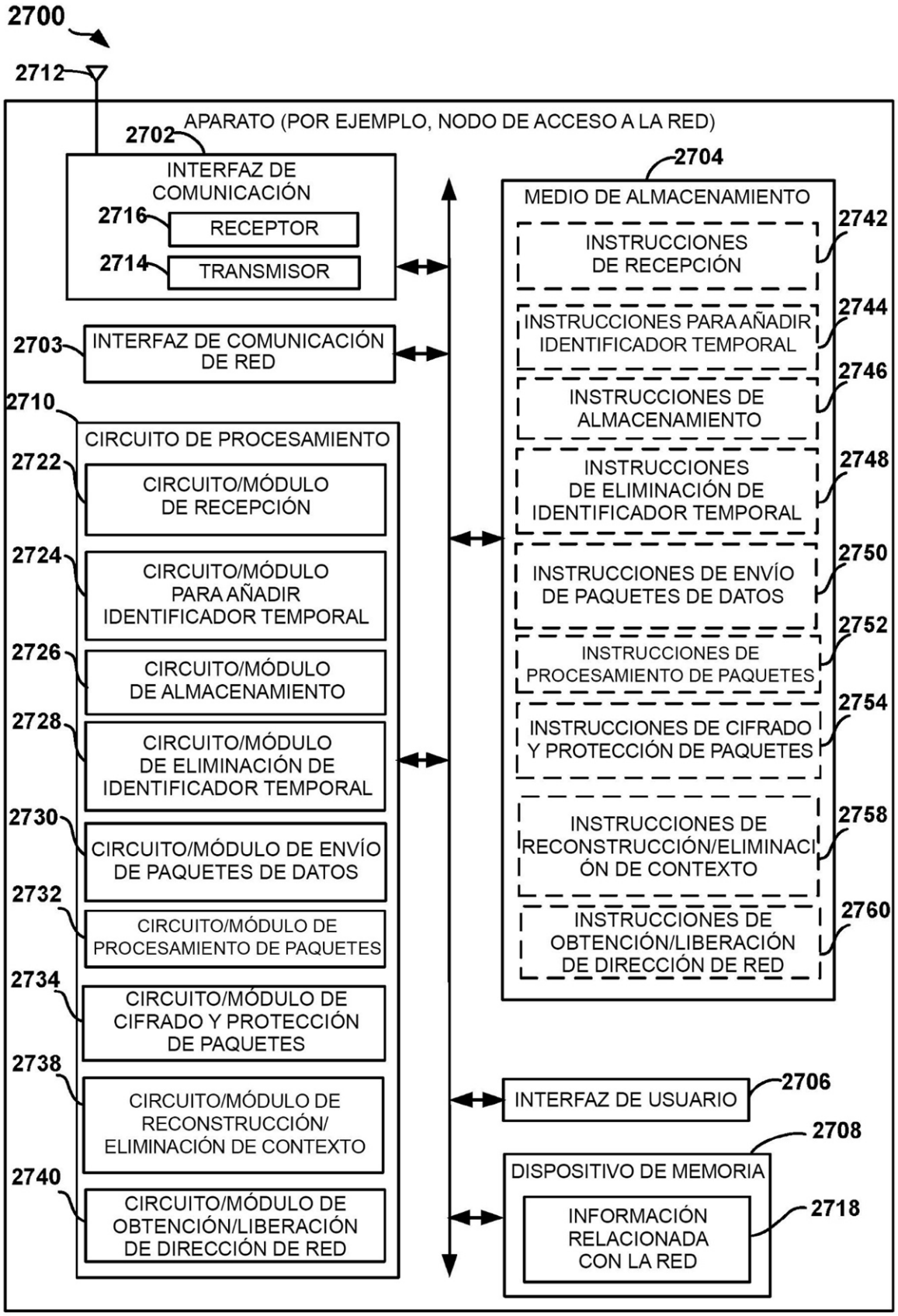
2700
2712
APARATO (POR EJEMPLO, NODO DE ACCESO A LA RED)
2702
INTERFAZ DE COMUNICACIÓN
2716
RECEPTOR
2714
TRANSMISOR
2703
INTERFAZ DE COMUNICACIÓN DE RED
2710
CIRCUITO DE PROCESAMIENTO
2722
CIRCUITO/MÓDULO DE RECEPCIÓN
2724
CIRCUITO/MÓDULO PARA AÑADIR IDENTIFICADOR TEMPORAL
2726
CIRCUITO/MÓDULO DE ALMACENAMIENTO
2728
CIRCUITO/MÓDULO DE ELIMINACIÓN DE IDENTIFICADOR TEMPORAL
2730
CIRCUITO/MÓDULO DE ENVÍO DE PAQUETES DE DATOS
2732
CIRCUITO/MÓDULO DE PROCESAMIENTO DE PAQUETES
2734
CIRCUITO/MÓDULO DE CIFRADO Y PROTECCIÓN DE PAQUETES
2738
CIRCUITO/MÓDULO DE RECONSTRUCCIÓN/ ELIMINACIÓN DE CONTEXTO
2740
CIRCUITO/MÓDULO DE OBTENCIÓN/LIBERACIÓN DE DIRECCIÓN DE RED
2704
MEDIO DE ALMACENAMIENTO
2742
INSTRUCCIONES DE RECEPCIÓN
2744
INSTRUCCIONES PARA AÑADIR IDENTIFICADOR TEMPORAL
2746
INSTRUCCIONES DE ALMACENAMIENTO
2748
INSTRUCCIONES DE ELIMINACIÓN DE IDENTIFICADOR TEMPORAL
2750
INSTRUCCIONES DE ENVÍO DE PAQUETES DE DATOS
2752
INSTRUCCIONES DE PROCESAMIENTO DE PAQUETES
2754
INSTRUCCIONES DE CIFRADO Y PROTECCIÓN DE PAQUETES
2758
INSTRUCCIONES DE RECONSTRUCCIÓN/ELIMINACIÓN DE CONTEXTO
2760
INSTRUCCIONES DE OBTENCIÓN/LIBERACIÓN DE DIRECCIÓN DE RED
2706
INTERFAZ DE USUARIO
2708
DISPOSITIVO DE MEMORIA
2718
INFORMACIÓN RELACIONADA CON LA RED

FIG. 27

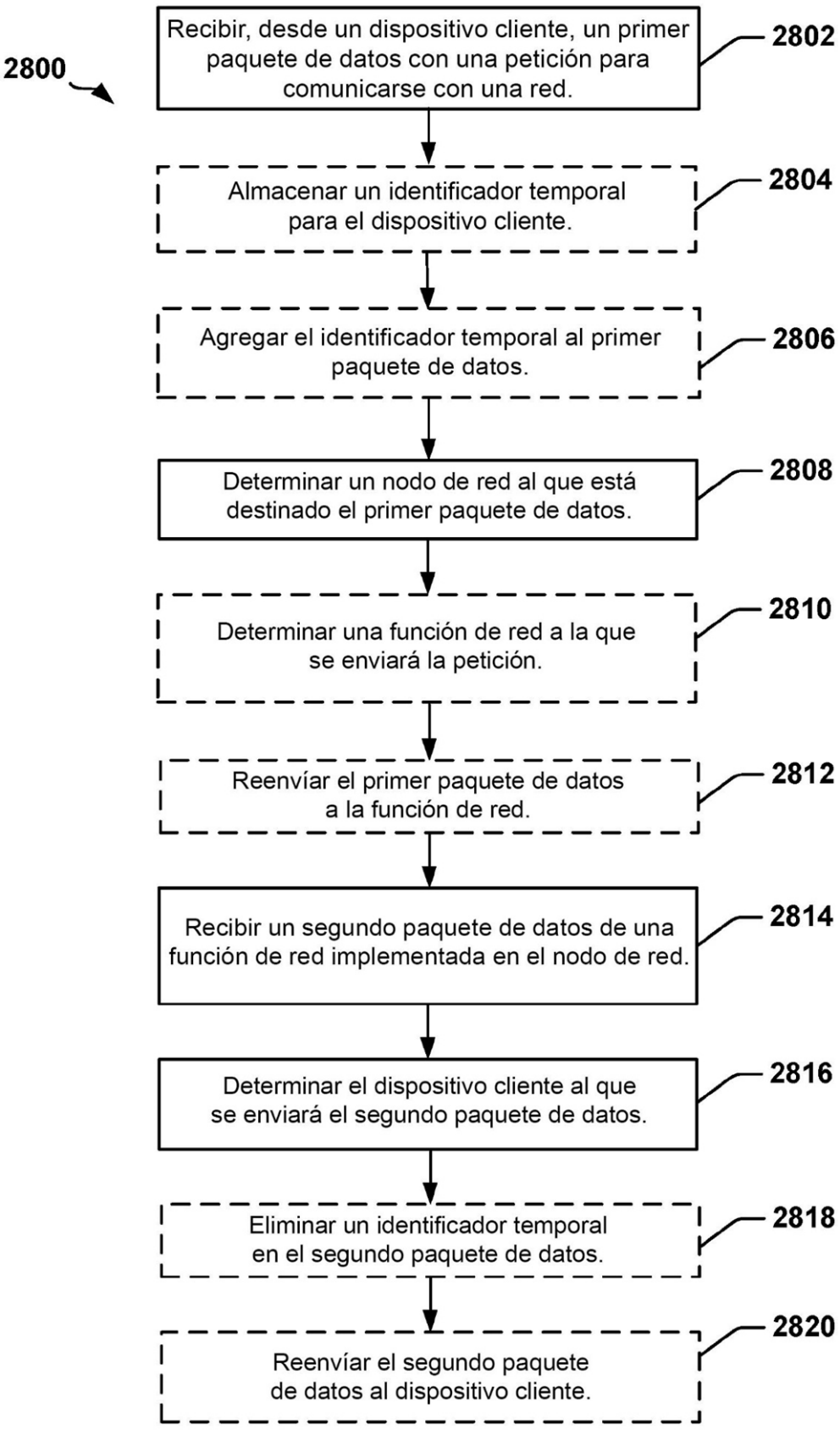
2800
Recibir, desde un dispositivo cliente, un primer paquete de datos con una petición para comunicarse con una red.
2802
Almacenar un identificador temporal para el dispositivo cliente.
2804
Agregar el identificador temporal al primer paquete de datos.
2806
Determinar un nodo de red al que está destinado el primer paquete de datos.
2808
Determinar una función de red a la que se enviará la petición.
2810
Reenviar el primer paquete de datos a la función de red.
2812
Recibir un segundo paquete de datos de una función de red implementada en el nodo de red.
2814
Determinar el dispositivo cliente al que se enviará el segundo paquete de datos.
2816
Eliminar un identificador temporal en el segundo paquete de datos.
2818
Reenviar el segundo paquete de datos al dispositivo cliente.
2820

FIG. 28

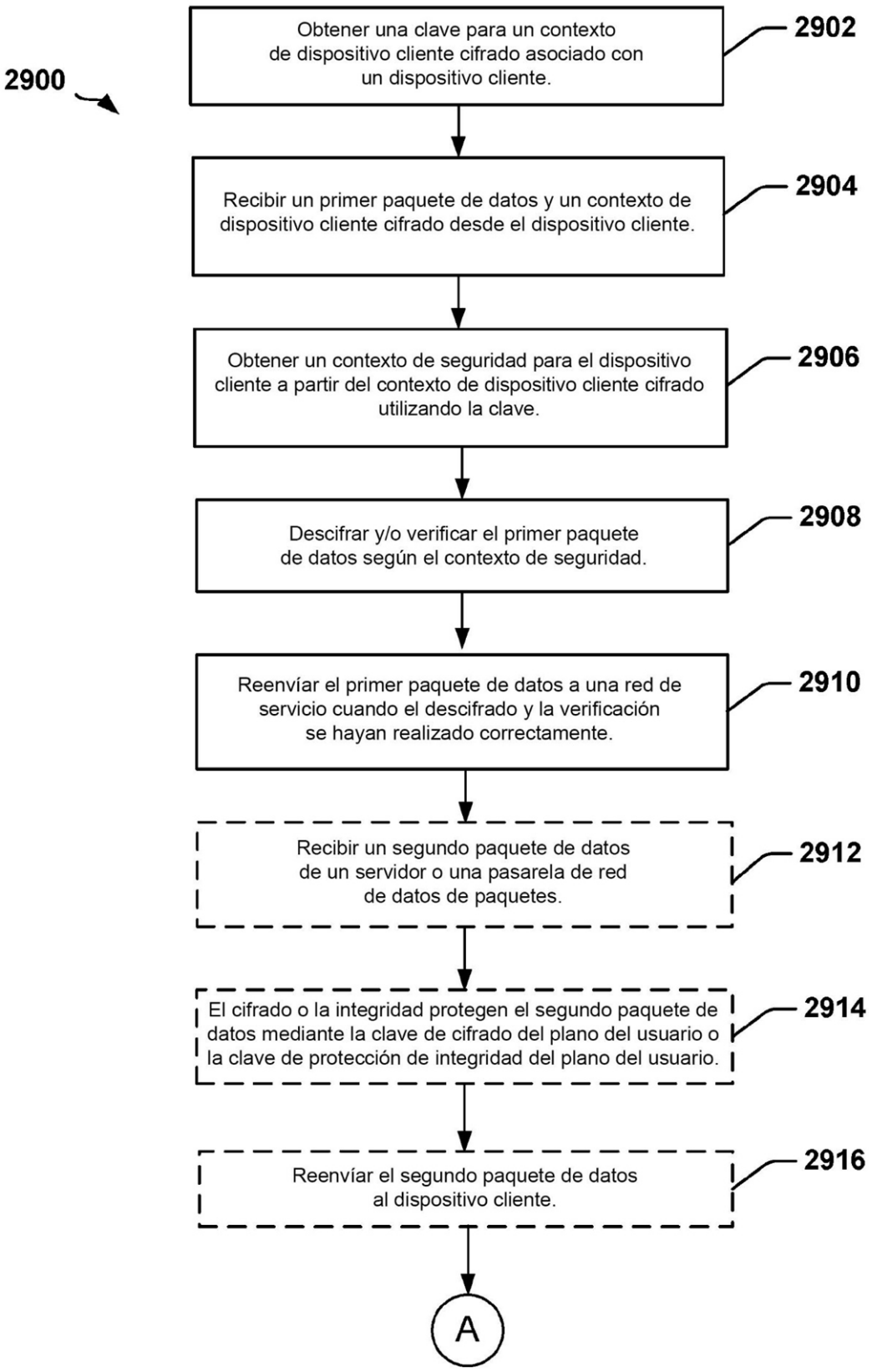
2900
Obtener una clave para un contexto de dispositivo cliente cifrado asociado con un dispositivo cliente.
2902
Recibir un primer paquete de datos y un contexto de dispositivo cliente cifrado desde el dispositivo cliente.
2904
Obtener un contexto de seguridad para el dispositivo cliente a partir del contexto de dispositivo cliente cifrado utilizando la clave.
2906
Descifrar y/o verificar el primer paquete de datos según el contexto de seguridad.
2908
Reenvíar el primer paquete de datos a una red de servicio cuando el descifrado y la verificación se hayan realizado correctamente.
2910
Recibir un segundo paquete de datos de un servidor o una pasarela de red de datos de paquetes.
2912
El cifrado o la integridad protegen el segundo paquete de datos mediante la clave de cifrado del plano del usuario o la clave de protección de integridad del plano del usuario.
2914
Reenvíar el segundo paquete de datos al dispositivo cliente.
2916
A

FIG. 29A

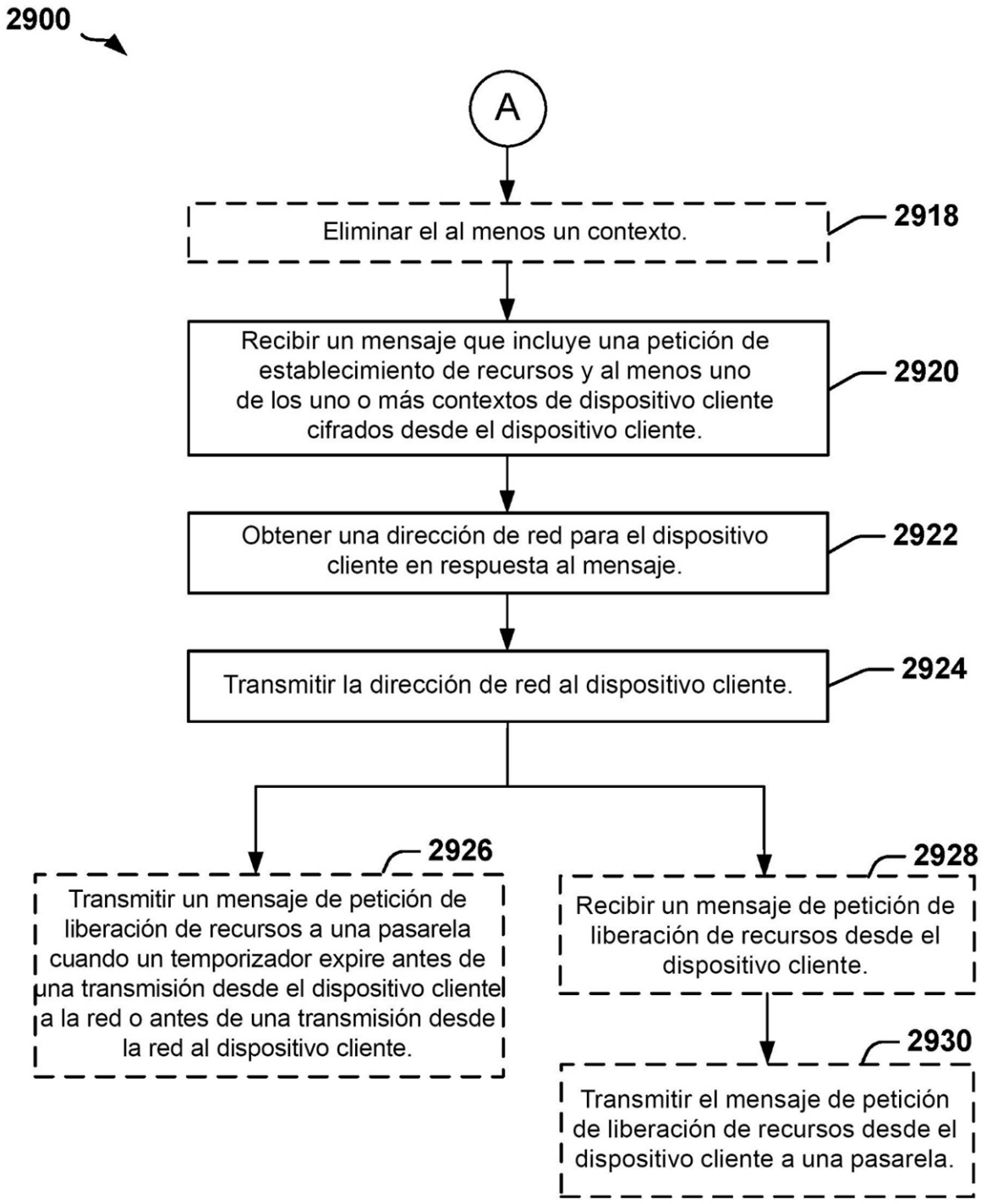
2900
A
Eliminar el al menos un contexto.
2918
Recibir un mensaje que incluye una petición de establecimiento de recursos y al menos uno de los uno o más contextos de dispositivo cliente cifrados desde el dispositivo cliente.
2920
Obtener una dirección de red para el dispositivo cliente en respuesta al mensaje.
2922
Transmitir la dirección de red al dispositivo cliente.
2924
2926
Transmitir un mensaje de petición de liberación de recursos a una pasarela cuando un temporizador expire antes de una transmisión desde el dispositivo cliente a la red o antes de una transmisión desde la red al dispositivo cliente.
2928
Recibir un mensaje de petición de liberación de recursos desde el dispositivo cliente.
2930
Transmitir el mensaje de petición de liberación de recursos desde el dispositivo cliente a una pasarela.

FIG. 29B