(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 964 007**

(51) Int. Cl.:

H04W 12/04 (2011.01)
H04W 12/37 (2011.01)
H04W 4/70 (2008.01)
H04L 67/125 (2012.01)
H04B 3/54 (2006.01)
H04W 76/14 (2008.01)
H04W 84/18 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **08.08.2018 PCT/FR2018/052037**

(87) Fecha y número de publicación internacional: **14.02.2019 WO19030457**

(96) Fecha de presentación y número de la solicitud europea: **08.08.2018 E 18762586 (8)**

(97) Fecha y número de publicación de la concesión europea: **27.09.2023 EP 3665922**

(54) Título: **Gestión de la comunicación entre un terminal y un servidor de red**

(30) Prioridad:

11.08.2017 FR 1757658

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.04.2024

(73) Titular/es:

ORANGE (100.0%)
111, quai du Président Roosevelt
92130 Issy-les-Moulineaux, FR

(72) Inventor/es:

LAMPIN, QUENTIN

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Gestión de la comunicación entre un terminal y un servidor de red

La invención se sitúa en el campo de las telecomunicaciones.

La invención hace referencia más particularmente a un sistema de comunicación en el que un terminal se comunica con un servidor de aplicaciones capaz de proporcionar servicios de aplicación a este terminal a través de una red de telecomunicaciones, y más particularmente a un servidor de esta red. No existe ninguna limitación en cuanto a la naturaleza del terminal o la naturaleza de los servicios de aplicación proporcionados. El terminal puede ser un terminal fijo o móvil, como por ejemplo un contador de electricidad, un sensor, etc. El servidor de aplicaciones puede ser explotado por cualquier proveedor de servicios, como un proveedor de electricidad o de agua, por ejemplo.

La técnica anterior se conoce a partir del documento WO 2016/001316 A1 que hace referencia a la seguridad de los intercambios entre un terminal y un servidor de aplicaciones a través de un dispositivo de transmisión capaz de comunicarse con un servidor de gestión a través de un servidor de red.

La invención también tiene una aplicación privilegiada pero no restrictiva en el contexto de la Internet de los objetos, y en particular de las arquitecturas o redes extendidas de tipo LoRaWAN™ (por "Long Range Wide Area Network"). Como es sabido, el protocolo LoRaWAN™, actualmente en proceso de normalización, permite una radiocomunicación de baja velocidad (inferior a 50 kbit/s) y bajo consumo energético entre objetos que se comunican mediante la tecnología LoRa™ (de "Long Range") y están conectados a Internet a través de una red de comunicación.

En una arquitectura LoRaWAN™, cada terminal se comunica con un servidor de aplicaciones a través de una red de telecomunicaciones. Más concretamente, los datos transmitidos por cada terminal a través de un enlace de radio son recibidos por una serie de pasarelas o estaciones base, que los retransmiten a un servidor de red a través de una conexión por cable o celular. Este servidor de red filtra los mensajes recibidos de los terminales (y, en particular, comprueba su origen e integridad) y los retransmite a los servidores de aplicaciones correspondientes.

A pesar de tratarse de una tecnología de radio optimizada para el largo alcance, muchos terminales diseñados para utilizar la tecnología LoRa™ no consiguen comunicarse con las pasarelas de la red Lora™ deseadas porque las señales emitidas por estos terminales no llegan a las pasarelas. Esto ocurre sobre todo cuando estos terminales están colocados por ejemplo en zonas como sótanos, bodegas, edificios de chapa, etc.

Como es sabido, se pueden añadir pasarelas adicionales a la red LoRa™ para permitir que estos terminales se comuniquen con esta red.

Sin embargo, estas pasarelas son caras. Además, necesitan una conexión a la red eléctrica y una conexión móvil o por cable.

Además, se ha observado que algunos terminales conectados a la red porque inicialmente estaban colocados en una zona cubierta por una estación base pueden acabar en una zona no cubierta por una estación base.

Esta situación se produce, por ejemplo, cuando un terminal se encamina desde el establecimiento de un cliente donde se configura hasta su lugar de instalación final.

En efecto, una vez configurado, el terminal envía solicitudes de conexión con el fin de comunicarse con un servidor de red en la red LoRa. Si, mientras se desplaza, se encuentra en una zona cubierta por una pasarela de red LoRa, aunque sea temporalmente, se puede llevar a cabo el procedimiento de conexión. Una vez conectado, en algunas formas de realización, el terminal almacena la información de conexión hasta que se reinicia eventualmente.

Esto plantea problemas si el lugar de instalación final no está dentro de la cobertura de radio de los equipos de pasarela de la red LoRa.

Uno de los objetivos de la invención es subsanar las deficiencias/desventajas del técnica anterior y/o introducir mejoras en la misma.

Para ello, la invención hace referencia a un método de gestión.

De acuerdo con la invención, el método de gestión comprende las siguientes etapas implementadas por un dispositivo de transmisión capaz de comunicarse a través de un enlace de radio con un equipo de pasarela que forma un nodo de una red de telecomunicaciones y configurado para comunicarse con un servidor de gestión asociado a través de dicho equipo de pasarela y a través de un servidor de red de dicha red:

- recepción, procedente de dicho servidor de gestión, de una solicitud de gestión de un terminal capaz de comunicarse a través de un enlace de radio con un equipo de pasarela de la red y configurado para

comunicarse con un servidor de aplicaciones asociado a través del equipo de pasarela de la red y a través de dicho servidor de red y que haya establecido una sesión de comunicación con el servidor de red y/o el servidor de aplicaciones, siendo compartida al menos una clave de sesión entre el terminal y el servidor de red y/o el servidor de aplicaciones, conteniendo dicha solicitud de gestión al menos un identificador de dicho terminal y dicha al menos una clave de sesión;

tras la recepción de la solicitud de gestión, interceptación de al menos un mensaje transmitido por dicho terminal y transmisión, en respuesta a dicho mensaje, de al menos un mensaje de respuesta cifrado con dicha clave de sesión recibida.

Al mismo tiempo, la invención también hace referencia a un dispositivo de transmisión capaz de comunicarse a través de un enlace de radio con un equipo de pasarela que forma un nodo de una red de telecomunicaciones y configurado para comunicarse con un servidor de gestión asociado a través de dicho equipo de pasarela y a través de un servidor de red de dicha red.

De acuerdo con la invención, este dispositivo comprende:

un módulo para recibir, procedente de dicho servidor de gestión, una solicitud de gestión de un terminal capaz de comunicarse a través de un enlace de radio con un equipo de pasarela en la red y configurado para comunicarse con un servidor de aplicaciones asociado a través del equipo de pasarela en la red y a través del servidor de red y habiendo establecido una sesión de comunicación con el servidor de red y/o el servidor de aplicaciones, siendo compartida al menos una clave de sesión entre el terminal y el servidor de red y/o el servidor de aplicaciones, conteniendo dicha solicitud de gestión al menos un identificador de dicho terminal y dicha al menos una clave de sesión;

un módulo de procesamiento configurado para recibir, tras la recepción de la solicitud de gestión, al menos un mensaje enviado por dicho terminal, y

un módulo de transmisión, en respuesta a dicho mensaje, al menos un mensaje de respuesta cifrado con dicha clave de sesión recibida.

Durante una primera fase, un terminal situado en la zona de cobertura de radio de un equipo de pasarela de red establece una sesión de comunicación con un servidor de red de la red y/o con un servidor de aplicaciones asociado al terminal. Esta sesión de comunicación permite al terminal comunicarse a través del servidor de red con un servidor de aplicaciones asociado al terminal.

Durante una segunda fase en la que el terminal se sitúa fuera del área de cobertura de radio de un equipo de pasarela de red, las señales de radio transmitidas por el terminal no son recibidas por ningún equipo de pasarela de la red. En consecuencia, no llegan al servidor de aplicaciones.

Una solicitud de gestión enviada por un servidor de gestión a un dispositivo de transmisión situado en la zona de cobertura del terminal permite a este dispositivo de transmisión retransmitir por una parte los mensajes enviados por un terminal a un equipo de pasarela y por otra parte los mensajes destinados a este terminal.

Al recibir esta solicitud de gestión, el dispositivo de transmisión intercepta al menos un mensaje enviado por el terminal.

Utilizando la clave de sesión recibida en la solicitud de gestión, puede enviar uno o más mensajes con destino al terminal en respuesta a un mensaje enviado por el terminal. Estos mensajes son cifrados con la clave de sesión. Son similares a los mensajes enviados por el servidor de red.

De este modo, el terminal puede seguir comunicándose con el servidor de aplicaciones a través del servidor de red. No es necesario intervenir sobre el terreno para restablecer el terminal.

El dispositivo de transmisión sólo procesa mensajes de terminales para los que ha obtenido derechos de gestión. Estos derechos de gestión se transmiten en este caso en forma de solicitud de gestión.

El dispositivo de transmisión, también denominado dispositivo repetidor, se sitúa en la zona de cobertura de radio del terminal para permitir que este terminal acceda a la red y se comunique con un servidor de aplicaciones asociado al terminal a través del servidor de red. Gracias a este dispositivo de transmisión, un terminal configurado para conectarse a la red pero incapaz de acceder directamente a un equipo de pasarela de red a través de un enlace de radio, puede comunicarse con el servidor de red y, en consecuencia, con un servidor de aplicaciones a través del servidor de red.

La red es, por ejemplo, una red LoRa™.

El dispositivo de transmisión se comporta como un terminal en relación con la red. De este modo, se comunica con un equipo de pasarela a través de señales de radio, por ejemplo, señales de radio de largo alcance. El equipo de pasarela

retransmite la información del dispositivo de transmisión al servidor de red. Acto seguido, el servidor de red puede retransmitir esta información a un servidor de gestión asociado al dispositivo de transmisión si la información está destinada a este servidor. A la inversa, la información procedente del servidor de gestión y destinada al dispositivo de transmisión se transmite a este dispositivo a través del servidor o servidores de red y a través del equipo de pasarela.

Ventajosamente, los enlaces de comunicaciones entre los distintos servidores y entre un servidor de red y un equipo de pasarela son enlaces convencionales por cable o celulares.

Sin embargo, no hay restricciones en cuanto al tipo de enlace.

Ventajosamente, el enlace entre el dispositivo de transmisión y el terminal es un enlace de radio de largo alcance que utiliza la tecnología LoRa. De este modo, los terminales configurados para cumplir el protocolo LoRaWAN™ pueden acceder a los servidores de aplicaciones a través de una red LoRa mediante el dispositivo de transmisión sin tener que adaptarse.

Sin embargo, el enlace entre el dispositivo de transmisión y el terminal puede ser un enlace de radio con características diferentes, por ejemplo, un enlace de radio de corto alcance.

En una forma de realización, se establece una sesión de comunicación entre el dispositivo de transmisión y el servidor de red.

Este establecimiento de sesión puede implicar la autentificación mutua entre el dispositivo de transmisión y el servidor de red y/o basarse en secretos compartidos, normalmente una clave.

Esta sesión se establece, por ejemplo, cuando el dispositivo de transmisión envía una solicitud de conexión.

Esta sesión de comunicación permite que el dispositivo de transmisión y un servidor de gestión identificado en la solicitud de conexión se comuniquen de forma segura a través del servidor de red. El servidor de gestión es un servidor de aplicaciones asociado al dispositivo de transmisión.

En una forma de realización particular del método de gestión, la solicitud de gestión se recibe a través de dicho equipo de pasarela y a través del servidor de red.

De este modo, el dispositivo de transmisión recibe la solicitud de gestión a través de un enlace de radio. Por lo tanto, no es necesario proporcionar otros medios de comunicación, como por ejemplo un enlace por cable, un enlace 4G, etc., entre el dispositivo de transmisión y el servidor de gestión.

Ventajosamente, la solicitud de gestión se transmite tras el establecimiento de una sesión de comunicación entre el dispositivo de transmisión y el servidor de red y/o el servidor de gestión. Esto permite que la solicitud de gestión se envíe de forma segura.

De acuerdo con una forma de realización particular del método de gestión, dicho al menos un mensaje de respuesta contiene al menos un parámetro de configuración del terminal, y más particularmente de un módulo de radiocomunicación del terminal.

El envío de parámetros de configuración permite al terminal adaptar la configuración de las señales de radio transmitidas o recibidas por el terminal a las limitaciones del dispositivo de transmisión. Esta adaptación optimiza el enlace de radio entre el terminal y el dispositivo de transmisión.

De acuerdo con una característica particular, dicho al menos un parámetro de configuración comprende una lista de al menos un canal de radio que el terminal debe habilitar o deshabilitar.

De acuerdo con una configuración particular, el terminal transmite cada mensaje a transmitir de forma sucesiva en varios canales con el objetivo de que un equipo reciba este mensaje en uno de los canales en los que está a la escucha.

Cuando se establece una sesión de comunicación entre un terminal y un equipo, por ejemplo, un servidor, este equipo puede proporcionar al terminal una lista de canales en los que está a la escucha o, a la inversa, una lista de canales en los que nunca está a la escucha. Estas listas están vinculadas a las capacidades del equipo.

La transmisión por parte del dispositivo de transmisión que ha recibido la solicitud de gestión de una lista de canales que deben habilitarse o deshabilitarse permite al terminal adaptar el enlace de radio a las capacidades del dispositivo de transmisión.

De acuerdo con otra característica particular, utilizada sola o en combinación con la anterior, dicho al menos un parámetro de configuración comprende al menos un valor de retardo a respetar entre un mensaje enviado y un mensaje recibido por el terminal.

Cuando se establece una sesión de comunicación entre un terminal y un equipo, este equipo puede indicar al terminal un retardo dentro del cual pretende responder. Durante una sesión de comunicación establecida entre un terminal y un equipo de pasarela, este retardo es, por ejemplo, del orden de un segundo.

Cuando el terminal se comunica con el servidor de red a través de un dispositivo de transmisión, este retardo inicialmente configurado puede no ser suficiente, por ejemplo, para retransmitir mensajes. El envío de un nuevo valor de retardo permite al terminal adaptar el tiempo de espera de una respuesta tras la transmisión de un mensaje. Esto puede hacerse, por ejemplo, ampliando el retardo o desplazándolo en el tiempo.

De acuerdo con una forma de realización particular del método de gestión, dicho al menos un mensaje de respuesta contiene una solicitud para que dicho terminal envíe una solicitud de conexión.

El envío de una solicitud de conexión al terminal tiene por objeto hacer que el terminal envíe una nueva solicitud de conexión y, en consecuencia, establecer una nueva sesión de comunicación. Cuando se establece esta sesión de comunicación, se generan una o más claves de sesión. Esto impide que la(s) clave(s) de sesión previamente generada(s) y transmitida(s) al dispositivo de transmisión en la solicitud de gestión pueda(n) ser pirateada(s). La seguridad se ve así reforzada.

Esta forma de realización es especialmente adecuada para los terminales que no están configurados para enviar una nueva solicitud de conexión por iniciativa propia cuando dejan de recibir respuestas a los mensajes que envían.

Enviar una solicitud de conexión al terminal permite establecer rápidamente una nueva sesión.

De acuerdo con una forma de realización particular del método de gestión, la solicitud de gestión contiene datos de autentificación que permiten a dicho dispositivo de transmisión establecer una sesión de comunicación con el terminal.

La transmisión de datos de autentificación permite al dispositivo de transmisión sustituir al servidor de red para establecer una sesión de comunicación con el terminal.

De acuerdo con una forma de realización particular, el método de gestión comprende, tras la transmisión de dicho al menos un mensaje de respuesta, una etapa de recepción de una solicitud de conexión enviada por dicho terminal y una etapa de establecimiento de una sesión de comunicación entre dicho terminal y dicho dispositivo de transmisión.

De acuerdo con una forma de realización particular, el método de gestión comprende, tras el establecimiento de la sesión de comunicación entre dicho terminal y dicho dispositivo de transmisión, una etapa de envío al servidor de red de los datos de establecimiento de dicha sesión de comunicación.

Estos datos de establecimiento de sesión son datos utilizados para establecer la sesión de comunicación entre el terminal y el dispositivo de transmisión. Estos datos son datos generados por el terminal y comunicados por éste al dispositivo de transmisión o datos generados por el dispositivo de transmisión.

Estos datos de configuración de sesión contienen, por ejemplo, la clave de sesión o los datos, por ejemplo, uno o más valores aleatorios, necesarios para calcular la clave de sesión.

Los datos de establecimiento de sesión permiten al servidor de red actuar como si hubiera establecido él mismo la sesión de comunicación.

La comunicación entre el terminal y un servidor de aplicaciones asociado, a través del servidor de red, es por tanto transparente tanto para el terminal como para el servidor de aplicaciones.

En una forma de realización particular, el servidor de red transfiere los datos recibidos al servidor de gestión. Este servidor de gestión interpreta la recepción de estos datos como una prueba de que el terminal está conectado a la red. A continuación, informa al servidor de red de esta conexión comunicándole información relativa a esta conexión. Esta información se almacena en una memoria accesible por el servidor de red. De este modo, el servidor de red no rechazará los mensajes destinados al servidor de aplicaciones enviados por este terminal.

Los datos de establecimiento de sesión también pueden ser transmitidos al servidor de aplicaciones por el servidor de gestión.

Una vez que el servidor de gestión ha puesto a disposición los datos de la sesión de configuración, el servidor de red y posiblemente el servidor de aplicaciones disponen de la misma información que habrían obtenido el servidor de red y el servidor de aplicaciones en el caso de una conexión directa entre un terminal y un equipo de pasarela, es decir, en el caso de un terminal que se encuentra en la zona de cobertura de un equipo de pasarela.

Ventajosamente, la información de conexión registrada contiene la clave o claves de sesión generadas para esta conexión. Utilizando esta clave de sesión, el servidor de red puede autenticar, cifrar y descifrar los mensajes de datos procedentes del terminal o destinados a él y retransmitidos en cada dirección mediante el dispositivo de transmisión.

Tras esta fase de conexión, el dispositivo de transmisión retransmite, a través de la red con destino al servidor de aplicaciones, los mensajes destinados a este servidor de aplicaciones y enviados por el terminal. Simétricamente, el dispositivo de transmisión retransmite al terminal los mensajes destinados a este terminal y transmitidos a través de la red por el servidor de aplicaciones. Igualmente, el dispositivo de transmisión retransmite al servidor de red los mensajes destinados a este servidor de red y enviados por el terminal, así como los mensajes procedentes del servidor de red con destino al terminal.

Este dispositivo de transmisión permite al terminal comunicarse con la red y el servidor de aplicaciones al que está conectado. Por lo tanto, actúa como un relé.

No es necesaria ninguna modificación a nivel del terminal.

El dispositivo de transmisión es barato. No necesita incluir un módulo de conexión por cable o celular. Se comunica, por una parte, con uno o más terminales y, por otra parte, con una pasarela de red a través de un enlace de radio. Este medio de comunicación consume muy poca energía para el dispositivo de transmisión. De este modo, no es necesario conectar el dispositivo de transmisión a una toma de corriente eléctrica. Basta con una batería o pilas para alimentarlo. Esto facilita su instalación.

De acuerdo con una característica particular del método de gestión, la solicitud de gestión se recibe en respuesta a un mensaje enviado por el dispositivo de transmisión.

Esta forma de realización se adapta especialmente a los casos en los que el servidor de red no puede interrogar directamente a los terminales conectados a la red, y más concretamente en este caso al dispositivo de transmisión. En esta forma de realización, el dispositivo de transmisión envía periódicamente mensajes al servidor de red. El servidor de red puede entonces comunicar información al dispositivo de transmisión respondiendo a un mensaje de este tipo.

La invención también hace referencia a un producto de programa informático que comprende instrucciones para la implementación de un método de gestión como el descrito anteriormente, cuando este programa es ejecutado por un procesador.

Así pues, la invención hace referencia a un software o a un programa, susceptible de ser ejecutado por un ordenador o por un procesador de datos, comprendiendo dicho software/programa instrucciones para controlar la ejecución de las etapas de un método de gestión. Estas instrucciones están destinadas a ser almacenadas en una memoria de un dispositivo informático, cargadas y, a continuación, ejecutadas por un procesador de este dispositivo informático.

Este software/programa puede utilizar cualquier lenguaje de programación, y estar en forma de código fuente, código objeto, o código intermedio entre el código fuente y el código objeto, tal como en una forma parcialmente compilada, o en cualquier otra forma deseable.

El dispositivo informático puede ser implementado por una o más máquinas distintas físicamente y tiene la arquitectura general de un ordenador, incluidos los componentes de una arquitectura de este tipo: memoria(s) de datos, procesador(es), bus de comunicación, interfaz(es) de hardware para conectar el dispositivo informático a una red u otro equipo, interfaz(es) de usuario, etc.

La invención también hace referencia a un soporte de información legible por un procesador de datos, y que comprende instrucciones de un programa tal como el mencionado anteriormente. El soporte de información puede ser cualquier entidad o dispositivo capaz de almacenar el programa.

Otras particularidades y ventajas de la presente invención serán evidentes a partir de la siguiente descripción de las formas de realización dadas a modo de ejemplo no restrictivo, con referencia a los dibujos adjuntos, en los que:

- la figura 1 es un diagrama que ilustra un sistema en un primer estado de configuración y de acuerdo con una forma de realización particular de la invención;
- la figura 2 es un diagrama que ilustra el sistema de la figura 1 en un segundo estado de configuración;
- la figura 3 es un diagrama que muestra un dispositivo de transmisión adecuado para implementar un método de transmisión de acuerdo con una forma de realización de la invención;
- la figura 4 es un organigrama que ilustra las diferentes etapas de un método de gestión de acuerdo con una primera forma de realización particular de la invención;

- la figura 5 es un organigrama que ilustra las diferentes etapas de un método de gestión de acuerdo con una segunda forma de realización particular de la invención.

La invención se implementa mediante componentes de software y/o hardware. Desde esta óptica, el término "módulo" puede corresponder en este documento tanto a un componente de software, un componente de hardware como un conjunto de componentes de hardware y/o software, capaces de implementar una función o un conjunto de funciones, de acuerdo con lo que se describe a continuación para el módulo en cuestión.

Un componente de software corresponde a uno o más programas informáticos, uno o más subprogramas de un programa o, de forma más general, a cualquier elemento de un programa o software. Un componente de software de este tipo se almacena en la memoria y, a continuación, se carga y ejecuta mediante un procesador de datos de una entidad física (terminal, servidor, pasarela, decodificador, enrutador, etc.) y es capaz de acceder a los recursos de hardware de dicha entidad física (memorias, soportes de registro, buses de comunicación, tarjetas electrónicas de entrada/salida, interfaces de usuario, etc.).

Del mismo modo, un componente de hardware es cualquier elemento de un conjunto de hardware. Puede ser un componente de hardware programable o con un procesador integrado para la ejecución de software, por ejemplo, un circuito integrado, una tarjeta inteligente, una tarjeta electrónica para ejecutar firmware, etc.

La **figura 1** muestra un sistema de comunicación SYS de acuerdo con la invención, en una forma de realización particular.

En el ejemplo de la figura 1, el sistema de comunicación SYS se basa en una red de telecomunicaciones ampliada que utiliza el protocolo LoRaWAN™. Como es sabido, el protocolo LoRaWAN™ es especialmente adecuado en el contexto del Internet de los objetos, ya que permite que varios objetos comunicantes intercambien datos con servidores en Internet.

No hay ninguna limitación en cuanto a la naturaleza de los objetos comunicantes. Pueden ser diversos terminales, como por ejemplo sensores, actuadores o cualquier otro tipo de objeto. Como es sabido, debido a sus limitaciones de hardware y/o software, dichos objetos no se pueden conectar a través de redes de acceso convencionales como por ejemplo WiFi, celular o por cable a Internet para acceder a los servidores de aplicaciones a los que están conectados: se comunican con estos servidores a través de una red de telecomunicaciones adaptada a sus limitaciones, como por ejemplo LoRaWAN™, de acuerdo con una topología en estrella.

El sistema de comunicación SYS comprende al menos un dispositivo de transmisión P, al menos un terminal C, al menos un equipo de pasarela, un servidor de red SR, un servidor de gestión SG y al menos un servidor de aplicaciones SA.

El sistema de comunicación SYS comprende, por ejemplo, 2 equipos de pasarela EP1 y EP2.

No hay limitación en el número de servidores de aplicaciones, el número de dispositivos de transmisión, el número de equipos de pasarela o el número de terminales.

El servidor de red SR se puede comunicar, por una parte, con el servidor de gestión SG y, por otra parte, con el servidor de aplicaciones SA a través de un enlace LS.

El enlace LS es un enlace por cable, por ejemplo.

El enlace LS es preferiblemente seguro.

El equipo de pasarela EP1, respectivamente el equipo de pasarela EP2, es capaz, por una parte, de comunicarse con uno o más terminales a través de un enlace de radio y, por otra parte, de comunicarse con el servidor de red SR u otro equipo de red a través de un enlace de comunicación L.

El enlace de comunicación L es, por ejemplo, un enlace por cable o celular.

No hay restricciones ni en el tipo de enlace LS ni en el tipo de enlace L.

Como es sabido, el servidor de red SR se encarga de filtrar y controlar la integridad y autenticidad de los mensajes recibidos a través del enlace L antes de transmitirlos a los servidores de aplicaciones correspondientes.

El servidor de red SR también tiene acceso a una memoria ML que contiene una lista LT de terminales conectados. Para cada terminal conectado, la lista LT incluye en particular un identificador de dicho terminal asociado a informaciones relativas a la sesión de comunicación establecida para este terminal. Esta información incluye, por

ejemplo, un identificador del servidor de aplicaciones con el que está conectado, una o más claves de sesión, una dirección asignada al terminal conectado, etc.

La información contenida en la lista LT permite al servidor de red SR realizar comprobaciones de integridad antes de transmitir o no un mensaje recibido.

Por ejemplo, la información almacenada para un terminal conectado se elimina de la lista LT al final de la sesión de comunicación.

Los datos intercambiados entre los distintos servidores SR, SA y SG de la red R se pueden cifrar utilizando claves compartidas o pares de claves privadas-públicas o cualquier otro método de cifrado, o se pueden transmitir en claro. No existe ninguna restricción sobre la forma en que se intercambian estos datos.

El terminal C se configura para comunicarse con el servidor de aplicaciones SA a través del servidor de red SR, y posiblemente a través de pasarelas o estaciones base.

Más concretamente, el terminal C se configura para transmitir y recibir datos a través de un enlace de radio.

El terminal C es un contador de agua, por ejemplo.

El servidor de aplicaciones SA es, por ejemplo, un servidor de un proveedor de agua capaz de procesar los datos enviados por el contador de agua C y de proporcionar un servicio de aplicación. Este servicio de aplicación es, por ejemplo, la preparación de una factura a partir de los datos enviados, y el suministro de esta factura a un usuario asociado con el contador C. También se puede proporcionar al usuario un historial detallado de su consumo en un portal web del proveedor de agua...

El terminal C se configura para comunicarse con el servidor de aplicaciones SA a través del servidor de red SR, y posiblemente a través de pasarelas o estaciones base.

Esto significa que cuando está instalado en una zona de cobertura de radio de un equipo de pasarela, por ejemplo, el equipo de pasarela EP2, se puede comunicar con el servidor de aplicaciones SA a través de un enlace de radio L2 entre el terminal y este equipo de pasarela EP2, a través del equipo de pasarela EP2, el enlace L, el servidor de red SR y el enlace LS.

Para ello, el terminal C incluye una memoria en la que se han almacenado un identificador IdC del terminal C, un identificador IdS del servidor de aplicaciones SA asociado al terminal C y una clave criptográfica principal (o maestra) KPC durante una fase de inicialización previa. La clave primaria KPC se almacena, por ejemplo, en una memoria segura del terminal C.

La clave primaria KPC también se almacena en una memoria segura del servidor de red SR, por ejemplo, en asociación con el identificador IdC del terminal C y el identificador IdS del servidor de aplicaciones SA.

El dispositivo de transmisión P se configura para comunicarse con el servidor de gestión SG a través del servidor de red SR y a través de un equipo de pasarela.

En el ejemplo mostrado en este caso, el dispositivo de transmisión P se comunica con el equipo de pasarela EP1 a través de un enlace de radio L1.

El dispositivo de transmisión P también es capaz de recibir señales de radio transmitidas por uno o más terminales, para los que ha obtenido derechos de gestión, por ejemplo, en forma de una solicitud de gestión tal como se describe más adelante, y de transmitir señales de radio.

La figura 1 muestra un ejemplo de un primer estado de configuración del sistema SYS.

En este diagrama, el terminal C está situado cerca del equipo de pasarela EP2 y se puede comunicar con este equipo de pasarela EP2 a través de un enlace de radio L2.

La **figura 2** muestra un ejemplo de un segundo estado de configuración del sistema SYS.

En esta figura, el terminal C se encuentra ahora cerca del dispositivo de transmisión P.

Por ejemplo, el terminal C ha sido trasladado. En este caso, se supone que el terminal C está ahora instalado en una zona, denominada zona blanca, en la que no tiene acceso directo ni a un servidor de red ni a ningún equipo de pasarela. Más concretamente, las señales de radio transmitidas por el terminal C no llegan a ningún equipo de pasarela de red EP1, EP2.

El terminal C se sitúa bajo tierra, por ejemplo, en el sótano de un edificio, en un edificio de chapa, etc.

A continuación, el terminal C y el dispositivo de transmisión P se comunican a través de un enlace de radio L3.

En la forma de realización descrita, los enlaces de radio L1, L2 y L3 se basan en la tecnología LoRa de bajo caudal y bajo consumo LoRa. Las señales de radio transmitidas y recibidas son señales de bajo caudal (menos de 50 Kbits/s) con un gran alcance (es decir, de tipo Long range).

Alternativamente, uno o más de los enlaces L1, L2 y L3 son enlaces de radio de un tipo diferente.

Según se ilustra en la **figura 3**, el dispositivo de transmisión P comprende, de manera conocida, en particular una unidad de procesamiento UT equipada con un microprocesador, una memoria de sólo lectura de tipo ROM y una memoria de acceso aleatorio de tipo RAM.

La memoria de sólo lectura de tipo ROM comprende registros que almacenan un programa informático PG que comprende instrucciones de programa adaptadas para implementar un método de gestión de acuerdo con una forma de realización de la invención descrito más adelante con referencia a las figuras 4 y 5.

El dispositivo de transmisión P también comprende una memoria MP, por ejemplo, una memoria segura, en la que se han almacenado un identificador IdP del dispositivo de transmisión P, un identificador IdG del servidor de gestión SG asociado al dispositivo de transmisión P y una clave criptográfica principal (o maestra) KPP durante una fase de inicialización previa, por ejemplo durante su instalación. La clave primaria KPP es una clave asociada al servidor de gestión SG. Se comparte por el dispositivo de transmisión P y por el servidor de red SR.

El dispositivo de transmisión P también comprende un primer módulo de recepción RCP, un segundo módulo de recepción RCC y un módulo de transmisión EMC.

El primer módulo de recepción RCP se configura para recibir señales de radio transmitidas a través del enlace L1, normalmente por el equipo de pasarela EP1.

El segundo módulo de recepción RCC se configura para recibir señales de radio transmitidas por el terminal C.

El módulo de transmisión CEM se configura para transmitir señales de radio.

El dispositivo de transmisión P también puede incluir un módulo de autentificación AUT y un tercer módulo de recepción RCP3. El tercer módulo de comunicación RCP3 está configurado para comunicarse directamente con el servidor de gestión SG, por ejemplo, a través de un enlace por cable o celular.

A continuación, se describirá, con referencia a **la figura 4,** una primera forma de realización de un método de gestión implementado en el sistema SYS.

Durante una etapa E2, el dispositivo de transmisión P y el servidor de red SR establecen una sesión de comunicación SC 1 entre ellos.

El establecimiento de la sesión de comunicación SC1 implica la generación de una clave de sesión KSP por una parte por el dispositivo de transmisión P y por otra parte por el servidor de red SR.

La clave de sesión KSP se genera a partir de la clave primaria KPP.

La información relativa a la sesión establecida SC1 es almacenada en asociación con un identificador del dispositivo de transmisión P por el servidor de red SR en una memoria accesible por el servidor de red, por ejemplo, en la lista LT de la memoria ML.

Como es sabido, el establecimiento de la sesión SC1 permite al dispositivo de transmisión P transmitir mensajes de datos con destino al servidor de gestión SG. Los mensajes de datos contienen un identificador IdP para el dispositivo de transmisión P, un identificador IdG para el servidor de gestión SG y datos cifrados con la clave de sesión KSP. Los mensajes de datos son recibidos por el servidor de red SR, que descifra los datos utilizando su clave de sesión KC1. Acto seguido, el servidor de red SR transmite los datos descifrados a través del enlace LS al servidor de gestión SG asociado al dispositivo de transmisión P.

Recíprocamente, el servidor de gestión SG puede transmitir un mensaje en respuesta a un mensaje recibido del dispositivo de procesamiento P. Este mensaje es transmitido por el servidor de gestión SG al servidor de red SR, que cifra su contenido con la clave de sesión KSP antes de transmitirlo con destino al dispositivo de transmisión P.

Durante una etapa E4, se establece una sesión de comunicación SC2 entre el terminal C y el servidor de red SR.

El establecimiento de la sesión de comunicación SC2 implica la generación de una clave de sesión KC1 por una parte por el terminal C y por otra parte por el servidor de red SR.

La clave de sesión KC1 se genera a partir de la clave primaria KPC.

La información relativa a la sesión establecida SC2 es registrada en asociación con un identificador IdC del terminal C por el servidor de red SR, por ejemplo, en la lista LT de terminales conectados.

Como es sabido, el establecimiento de la sesión SC2 permite al terminal C transmitir mensajes de datos con destino al servidor de aplicaciones SA. Los mensajes de datos contienen un identificador IdC para el terminal C, un identificador para el servidor de aplicaciones SA y datos cifrados con la clave de sesión KC1. Los mensajes de datos son recibidos por el servidor de red SR, que descifra los datos utilizando su clave de sesión KC1. Acto seguido, el servidor de red SR transmite los datos descifrados a través del enlace LS al servidor de aplicaciones SA asociado al terminal C.

Recíprocamente, el servidor de aplicaciones SA puede transmitir un mensaje en respuesta a un mensaje recibido del terminal C. Este mensaje es transmitido por el servidor de aplicaciones SA al servidor de red SR, que cifra su contenido con la clave de sesión KC1 antes de transmitirlo con destino al terminal C.

Durante una etapa E6, el servidor de gestión SG obtiene una solicitud de gestión DGC1 relativa al terminal C.

La solicitud de gestión DGC1 es, por ejemplo, obtenida por el servidor de gestión SG tras la acción de un usuario, normalmente un operador. La solicitud de gestión DGC del terminal C es, por ejemplo, introducida por el operador a través de una interfaz de usuario mostrada en una pantalla del servidor de gestión SG o de un terminal asociado al servidor de gestión SG.

Esta acción se lleva a cabo, por ejemplo, a raíz de una alerta emitida por el servidor de aplicaciones SA. Por ejemplo, esta alerta es activada por el servidor de aplicaciones SA tras la no recepción de mensajes de datos procedentes del terminal C durante un periodo de tiempo predefinido.

Esta falta de recepción de datos es interpretada por el servidor de aplicaciones SA como un problema con la cobertura de radio del terminal C.

El fallo en la recepción de mensajes de datos puede deberse al desplazamiento, es decir, a un cambio de posición, del terminal C, al desplazamiento del equipo de pasarela EP2 inicialmente situado cerca del terminal C, a la construcción de una o más paredes entre el terminal C y el equipo de pasarela EP2, etc.

La solicitud de gestión DGC1 contiene un identificador del terminal C, por ejemplo, el identificador IdC, y un identificador del dispositivo de gestión P, por ejemplo, el identificador IdP.

En el caso de que el sistema SYS contenga varios dispositivos de transmisión, el dispositivo de transmisión P es seleccionado por el operador de entre los varios dispositivos de transmisión.

Alternativamente, la solicitud de gestión DGC1 no contiene un identificador de dispositivo de transmisión P y el dispositivo de transmisión P es seleccionado por el servidor de gestión SG entre varios dispositivos de transmisión de acuerdo con uno o más criterios predefinidos. El dispositivo de transmisión seleccionado es, por ejemplo, el dispositivo de transmisión más cercano a la ubicación conocida del terminal C. Esto supone que una posición para cada dispositivo de transmisión y la posición del terminal C están disponibles para el servidor de gestión SG.

No hay restricciones en la elección del dispositivo de transmisión P.

A la etapas E6 le sigue una etapa E8 durante el cual el servidor de gestión SG envía al servidor de red SR una solicitud de gestión DGC2 del terminal C por parte del dispositivo de transmisión P. La solicitud de gestión DGC2 contiene un identificador del terminal C, por ejemplo, el identificador IdC, y un identificador del dispositivo de gestión P, por ejemplo el identificador IdP.

La etapa E8 va seguida de una etapa E10 durante el cual el servidor de red SR envía una solicitud de gestión DGC3 para el terminal C con destino al dispositivo de transmisión P.

La solicitud de gestión DGC3, por ejemplo, se transmite al dispositivo de transmisión P en respuesta a un mensaje transmitido por este último.

La solicitud de gestión DGC3 contiene el identificador IdC del terminal C y la clave de sesión KC1 generada durante la etapa de establecimiento de la sesión de comunicación SC2 entre el terminal C y el servidor de red SR.

Alternativamente, la solicitud de gestión DGC3 también contiene datos utilizados por el servidor de red SR para comunicarse con el terminal C. Estos datos incluyen, por ejemplo, valores de contador de tramas o, de forma más general, valores utilizados para evitar un ataque de repetición.

La clave de sesión KC2, por ejemplo, es extraída de la lista LT de terminales conectados por el servidor de red SR.

En una forma de realización particular, la solicitud de gestión DGC3 también contiene datos de autentificación como, por ejemplo, la clave primaria KPC asociada al terminal C.

Tras la recepción de la solicitud de gestión DGC3 por el primer módulo de recepción RCP del dispositivo de transmisión P, los valores contenidos en la solicitud de gestión DGC3 se registran en una memoria del dispositivo de transmisión P (etapa E12).

, durante una etapa E14, el segundo módulo de recepción RCC del dispositivo de transmisión P recibe un mensaje M1 enviado por el terminal C y destinado al servidor de aplicaciones SA.

El mensaje M1 es, por ejemplo, un mensaje que contiene datos, por ejemplo, datos de medición, cifrados con la clave de sesión KC1.

A la etapa E14 le sigue una etapa E16 durante la cual el módulo de transmisión EMC del dispositivo de transmisión P transmite uno o más mensajes M2 al terminal C. Estos mensajes M2 son cifrados por el dispositivo de transmisión P utilizando la clave de sesión KC1.

Los mensajes M2 contienen parámetros de configuración del terminal C. Estos parámetros de configuración permiten modificar uno o más parámetros de la sesión de comunicación SC2. Por ejemplo, se pueden utilizar para reconfigurar las señales de radio transmitidas o recibidas por dicho terminal.

Los parámetros de configuración contenidos en el/los mensaje(s) M2 incluyen, por ejemplo, una lista de canales soportados por el dispositivo de transmisión P y/o una lista de canales a deshabilitar por no ser soportados por el dispositivo de transmisión P.

Estos parámetros de configuración permiten al terminal C actualizar la lista de canales de radio en los que en los que el terminal C transmite los mensajes.

Los parámetros de configuración contenidos en el/los mensaje(s) M2 también pueden incluir uno o más valores de retardo de respuesta. Estos valores de retardo de respuesta permiten definir intervalos de tiempo tras la transmisión de un mensaje durante los cuales el terminal C está a la espera de una respuesta.

Una vez recibidos los parámetros de configuración, el terminal C tiene en cuenta estos nuevos parámetros de configuración.

La etapa E16 va seguida de una o más etapas E20 durante las cuales el terminal C se comunica con el servidor de aplicaciones SA a través del dispositivo de transmisión P y el servidor de red SR.

Más concretamente, los mensajes M3 enviados por el terminal C con destino al servidor de aplicaciones SA incluyen datos D previamente firmados por el terminal C con la clave de sesión KC1. Son interceptados por el dispositivo de transmisión P y retransmitidos por éste con destino al servidor de red SR.

El servidor de red SR descifra estos mensajes M3 utilizando la clave KC1 que posee y transmite su contenido descifrado D al servidor de aplicaciones SA.

Recíprocamente, los mensajes transmitidos por el servidor de aplicaciones SA son cifrados con la clave de sesión KC1 por el servidor de red SR y transmitidos por este último con destino al terminal C. Estos mensajes son recibidos por el dispositivo de transmisión P, que los transfiere al terminal C.

En una forma de realización alternativa, los mensajes M2 transmitidos por el dispositivo de transmisión P durante la etapa E16 también incluyen una solicitud DC para enviar una nueva solicitud de conexión.

Tras recibir la solicitud de CC, el terminal C retransmite una nueva solicitud de conexión.

La solicitud de conexión enviada por el terminal C es interceptada por el dispositivo de transmisión P y se establece una sesión de comunicación SC3 entre el dispositivo de transmisión P y el terminal C.

El establecimiento de la sesión de comunicación SC3 implica la generación de una clave de sesión KC2 por una parte por el dispositivo de transmisión P y por otra parte por el terminal C.

Una vez establecida esta sesión de comunicación SC3, los mensajes transmitidos por el terminal C se firman utilizando la clave de sesión KC2.

Estos mensajes son interceptados por el dispositivo de transmisión P.

Acto seguido, estos mensajes o su contenido son transmitidos por el dispositivo de transmisión P al servidor de red SR.

No existe ninguna restricción a la transmisión del contenido de estos mensajes.

Por ejemplo, los mensajes recibidos del terminal C son descifrados por el dispositivo de transmisión P utilizando la clave de sesión KC2 y, a continuación, cifrados utilizando la clave de sesión KSP compartida por el dispositivo de transmisión P y el servidor de red SR antes de ser transmitidos al servidor de red SR.

Recíprocamente, los mensajes transmitidos por el servidor de aplicaciones SA son cifrados con la clave de sesión KSP por el servidor de red SR y transmitidos por este último con destino al terminal C. Estos mensajes son recibidos por el dispositivo de transmisión P, que los descifra con la clave de sesión KSP, los cifra con la clave de sesión KC2 y los transmite con destino al terminal C.

En esta forma de realización alternativa, los mensajes M2 incluyen parámetros de configuración del terminal y una solicitud de conexión DC.

Alternativamente, los mensajes M2 incluyen la solicitud de conexión DC pero no incluyen ningún parámetro de configuración del terminal.

En la forma de realización descrita, la solicitud de gestión DGC3 se transmite al dispositivo de transmisión P a través del servidor de red SR y el equipo de pasarela EP1. En este caso, es recibida por el primer módulo de recepción RCP del dispositivo de transmisión P.

Alternativamente, el dispositivo de transmisión P también comprende un módulo de comunicación por cable o celular RCP3 y la solicitud de gestión DGC3 es transmitida directamente por el servidor de gestión SG al dispositivo de transmisión P a través de un enlace por cable o celular.

A continuación, el módulo de comunicación RCP3 del dispositivo de transmisión P recibe la solicitud de gestión DGC3.
En la forma de realización descrita, la sesión de comunicación SC1 se establece entre el dispositivo de transmisión P y el servidor de red SR y la sesión de comunicación SC2 se establece entre el terminal C y el servidor de red SR. Alternativamente, la sesión de comunicación SC1 se establece entre el dispositivo de transmisión P y el servidor de gestión SG y la sesión de comunicación SC2 se establece entre el terminal C y el servidor de aplicaciones SA. En esta alternativa, el servidor de red SR desempeña una función de enrutamiento.

A continuación, se describirá una segunda forma de realización de un método de gestión implementado en el sistema SYS con referencia a la **figura 5.**

Durante una etapa S0, el módulo de autentificación AUT del dispositivo de transmisión P transmite una solicitud de conexión DA1 al servidor de red SR. El dispositivo de transmisión P envía la solicitud de conexión DA1 a través del enlace de radio L1. Es retransmitida al servidor de red SR por el equipo de pasarela EP1 a través del enlace L.

La solicitud de conexión DA1 contiene el identificador IdP del dispositivo de transmisión P, el identificador IdG del servidor de gestión SG con el que el dispositivo de transmisión P solicita conectarse y un valor aleatorio AL1 generado por el dispositivo de transmisión P.

La solicitud de conexión DA1 es, por ejemplo, un mensaje JoinRequest definido en el estándar LoRaWAN™.

Durante una etapa S2, tras la recepción de la solicitud DA1, el dispositivo de transmisión P y el servidor de red SR establecen una sesión de comunicación SC1.

El establecimiento del enlace de comunicación SC1 incluye una etapa de autentificación llevada a cabo, por una parte, por el dispositivo de transmisión P y, por otra parte, por el servidor de red SR.

Más concretamente, el servidor de red SR genera un valor aleatorio AL2. A continuación, genera una clave de sesión KSP aplicando una función matemática predefinida F1 utilizando los siguientes parámetros: la clave primaria KPP, el valor aleatorio AL1 recibido, el valor aleatorio AL2.

La generación de una clave de sesión, también denominada clave derivada, a partir de una clave primaria (o maestra) es una técnica conocida por los expertos en la técnica y no se describirá en este caso.

La función F1, por ejemplo, es una función AES (por "Advanced Encryption Standard").

No hay restricciones para la función F1.

El servidor de red SR también genera una dirección ADP para el dispositivo de transmisión P.

A continuación, en respuesta a la solicitud de autentificación DA1, el servidor de red SR genera y transmite un mensaje de aceptación de conexión MA1. El mensaje MA1 contiene, en particular, el valor aleatorio AL2 y la dirección ADP generada. También puede contener parámetros de conexión como, por ejemplo, una lista de canales habilitados para comunicarse a través del enlace L1 y/o una lista de canales que se deben deshabilitar y/o un tiempo de respuesta máximo en el que debe recibirse una respuesta a un mensaje enviado por el terminal. Este tiempo de respuesta es, por ejemplo, de 1 segundo.

El mensaje MA1 es, por ejemplo, un mensaje JoinAccept definido en el estándar LoRaWAN™.

La información relativa a la conexión, es decir, a la sesión establecida, es registrada por el servidor de red SR en la lista LT de terminales conectados. Esta información incluye, por ejemplo, el identificador IdP del dispositivo de transmisión P, el identificador IdG del servidor de gestión SG y la clave de sesión KSP.

Tras la recepción del mensaje MA1, el módulo de autentificación AUT del dispositivo de transmisión P genera a su vez la clave de sesión KSP. La clave de sesión KSP se genera aplicando la función F1 a la clave primaria KPP almacenada en la memoria MP del dispositivo de transmisión P, al primer valor aleatorio AL1 generado por el dispositivo de transmisión P y al segundo valor aleatorio AL2 recibido en el mensaje MA1.

En la forma de realización descrita, el establecimiento de sesión implica la autentificación mutua del dispositivo de transmisión P y el servidor de red SR.

Alternativamente, la clave de sesión KSP, por ejemplo, es generada por un dispositivo de seguridad (no mostrado) y previamente es almacenada por una parte en el dispositivo de transmisión P y por otra parte en el servidor de red SR.

Tras la etapa S2, el dispositivo de transmisión P por una parte y el servidor de red SR tienen la misma clave de sesión KSP. En otras palabras, la clave de sesión KSP es compartida por el dispositivo de transmisión P y el servidor de red SR para la sesión de comunicación entre el dispositivo de transmisión P y el servidor de gestión SG.

Durante una etapa S3, el terminal C envía una solicitud de conexión DA2 al servidor de aplicaciones SA.

La solicitud de conexión DA2 contiene el identificador IdC del terminal C, el identificador IdS del servidor de aplicaciones SA con el que el terminal C solicita conectarse y un valor aleatorio AL3 generado por el terminal C.

La solicitud de conexión DA2 es, por ejemplo, un mensaje JoinRequest definido en el estándar LoRaWAN™.

A la etapa S3 le sigue una etapa S4 durante la cual se establece una sesión de comunicación SC2 entre el terminal C y el servidor de red SR.

Más concretamente, tras recibir la solicitud de conexión DA2, el servidor de red SR genera un valor aleatorio AL4, una clave de sesión KC1 y una dirección ADC1 para el terminal C. La clave de sesión KSC1 se genera de manera convencional utilizando la clave primaria KPC, el valor aleatorio recibido AL3 y el valor aleatorio AL4.

A continuación, el servidor de red SR genera y transmite un mensaje MA2 de aceptación de la conexión. El mensaje MA2 contiene en particular el valor aleatorio AL4 y la dirección ADC1 generada. También puede contener parámetros de configuración del terminal.

El mensaje MA2 es, por ejemplo, un mensaje JoinAccept definido en el estándar LoRaWAN™.

La información relativa a la conexión, es decir, a la sesión establecida, es registrada por el servidor de red SR en la lista LT de terminales conectados. Esta información incluye, por ejemplo, el identificador IdC del terminal C, el identificador IdS del servidor de aplicaciones SA y la clave de sesión generada KC1.

Tras recibir el mensaje MA2, el terminal C genera a su vez la clave de sesión KC 1.

Como es sabido, el establecimiento de la sesión SC2 permite al terminal C transmitir mensajes de datos con destino al servidor de aplicaciones SA. Los mensajes de datos contienen un identificador IdC para el terminal C, un identificador para el servidor de aplicaciones SA y datos cifrados con la clave de sesión KC1. Los mensajes de datos son recibidos por el servidor de red SR, que descifra los datos utilizando su clave de sesión KC1 almacenada en la lista LT en asociación con el identificador IdC del terminal C. Acto seguido, el servidor de red SR transmite los datos descifrados a través del enlace LS al servidor de aplicaciones SA asociado al terminal C.

Recíprocamente, el servidor de aplicaciones SA puede transmitir un mensaje en respuesta a un mensaje recibido del terminal C. Este mensaje es transmitido por el servidor de aplicaciones SA al servidor de red SR, que cifra su contenido con la clave de sesión antes de transmitirlo con destino al terminal C.

Durante una etapa S6, similar a la etapa E6 de la forma de realización anterior, el servidor de gestión SG recibe una solicitud de gestión DGC1 relativa al terminal C.

La solicitud de gestión DGC1 contiene un identificador del terminal C, por ejemplo, el identificador IdC, y un identificador del dispositivo de transmisión P, por ejemplo el identificador IdP.

La etapa S6 es seguida por una etapa S8 durante el cual el servidor de gestión SG envía al servidor de red SR una solicitud de gestión DGC2 del terminal C por el dispositivo de transmisión P.

En la forma de realización descrita, el servidor de gestión SG también envía al servidor de red SR una solicitud de extracción del terminal C DRC de la lista LT de terminales conectados.

La solicitud de gestión DGC2 contiene el identificador IdC del terminal C y el identificador IdP del dispositivo de transmisión P.

La etapa S8 va seguida de una etapa S10 durante el cual el servidor de red SR envía una solicitud de gestión DGC3 para el terminal C con destino al dispositivo de transmisión P.

La solicitud de gestión DGC3, por ejemplo, se transmite al dispositivo de transmisión P en respuesta a un mensaje transmitido por este último, por ejemplo un mensaje de interrogación.

La solicitud de gestión DGC3 contiene el identificador IdC del terminal C, la dirección ADC1 del terminal C generada durante la etapa de establecimiento de la sesión de comunicación SC2, la clave de sesión KC1 también generada durante la etapa de establecimiento de la sesión de comunicación SC2 y la clave de sesión primaria KP 1 asociada al terminal C.

La clave de sesión KC1 y la dirección ADC1 del terminal C, por ejemplo, se toman de la lista LT de terminales conectados por el servidor de red SR.

Alternativamente, la clave de sesión KC1 y la dirección ADC1 del terminal C son obtenidas por el servidor de gestión SG y transmitidas al servidor de red SR en la solicitud de gestión DGC2. Esta información está, por ejemplo, a disposición del servidor de aplicaciones SA y es transmitida por éste al servidor de gestión SG.

Alternativamente, la solicitud de gestión DGC3 también contiene datos utilizados por el servidor de red SR para comunicarse con el terminal C. Estos datos incluyen, por ejemplo, valores para contadores de tramas intercambiados, por ejemplo, valores "UPLINK" y "DOWNLINK" definidos en el estándar LoRaWAN™.

Los datos de solicitud de gestión DGC3 son cifrados por el servidor de red SR con la clave de sesión KSP compartida por el dispositivo de transmisión P y el servidor de red SR.

Tras la transmisión del mensaje DGC3, el servidor de red SR borra el identificador IdC del terminal C así como la información almacenada en asociación con este identificador de terminal de la lista LT de terminales conectados.

Después de recibir la solicitud de gestión DGC3, el dispositivo de transmisión P almacena los valores contenidos en la solicitud de gestión DGC3 en una memoria del dispositivo de transmisión P (etapa S12).

Posteriormente, durante una etapa S14, el dispositivo de transmisión P intercepta un mensaje MD 1 enviado por el terminal C y destinado al servidor de aplicaciones SA.

El mensaje MD1 es, por ejemplo, un mensaje que contiene datos, por ejemplo, datos de medición, cifrados con la clave de sesión KC1.

A la etapa S14 le sigue una etapa S16 durante la cual el dispositivo de transmisión P transmite uno o más mensajes M2 al terminal C. Estos mensajes M2 son cifrados con la clave de sesión KC1.

Estos mensajes contienen parámetros de configuración del terminal PAR y una solicitud DC para que el terminal C envíe una nueva solicitud de conexión.

Alternativamente, estos mensajes no incluyen parámetros de configuración de sesión.

Los parámetros de configuración PAR contenidos en el mensaje M2 incluyen, por ejemplo, una lista de canales soportados por el dispositivo de transmisión P y/o una lista de canales a deshabilitar por no ser soportados por el dispositivo de transmisión P.

La actualización de la lista de canales se solicita, por ejemplo, en forma de una solicitud de "Nuevo Canal" definida en el estándar LoRaWAN™.

Los parámetros de configuración PAR contenidos en el(los) mensaje(s) M2 también pueden incluir uno o más valores de retardo de respuesta. Dicho retardo de respuesta es, por ejemplo, un intervalo de tiempo entre el final de la transmisión de un mensaje por el terminal C y el inicio de una ventana de recepción durante la cual el terminal C está a la escucha de una respuesta.

Por ejemplo, este retardo se actualiza mediante una opción "MAC RXTimingSetupReq" definida en el estándar LoRaWAN™.

Tras recibir la solicitud de conexión DC, el terminal C retransmite una nueva solicitud de conexión DA3 (etapa S18).

La solicitud de conexión DA3 contiene el identificador IdC del terminal C, el identificador IdS del servidor de aplicaciones SA con el que el terminal C solicita conectarse y un valor aleatorio AL5 generado por el terminal C.

La solicitud de conexión DA3 es, por ejemplo, un mensaje "JoinRequest" definido en el estándar LoRaWAN™.

El dispositivo de transmisión P gestiona la solicitud de conexión DA3 (etapa S20).

A continuación, el terminal C y el dispositivo de transmisión P establecen una sesión de comunicación SC3 durante la cual se autentican mutuamente.

Más concretamente, tras la recepción de la solicitud de conexión DA3, el dispositivo de transmisión P genera un valor aleatorio AL6, una clave de sesión KC2 y una dirección ADC2 para el terminal C. La clave de sesión KC2 se genera de manera convencional utilizando la clave primaria KPC, el valor aleatorio AL5 recibido y el valor aleatorio AL6 (etapa S20).

A continuación, el dispositivo de transmisión P genera y transmite un mensaje MA3 de aceptación de la conexión. El mensaje MA3 contiene en particular el valor aleatorio AL6 y la dirección ADC2 generada. También puede contener parámetros de configuración para el terminal C (etapa S22).

El mensaje MA3 es, por ejemplo, un mensaje JoinAccept definido en el estándar LoRaWAN™.

Tras recibir el mensaje MA3, el terminal C genera a su vez la clave de sesión KC2 (etapa S24).

Durante una etapa S26, el módulo de transmisión EMP del dispositivo de transmisión P transmite un mensaje MT1 destinado al servidor de gestión SG.

El mensaje MT1 contiene el identificador IdC del terminal C, la clave de sesión KC2 generada por el dispositivo de transmisión P y la dirección generada ADC2. Los datos contenidos en el mensaje

MT1 son cifrados con la clave de sesión KSP compartida entre el dispositivo de transmisión P y el servidor de red SR.

Alternativamente, el mensaje MT1 no contiene la clave de gestión KC2 pero sí datos que permiten generar esta clave, por ejemplo los valores aleatorios AL5 y AL6.

En una forma de realización particular, el dispositivo de transmisión P ordena que se borre de su memoria la clave KC2 generada previamente, por ejemplo, después de enviar el mensaje MT1.

A la etapa S26 le sigue una etapa S28 en la que el servidor de red SR recibe el mensaje MT1 y obtiene la clave de sesión KC2 y la dirección ADC2 descifrando los datos del mensaje MT1 utilizando la clave KSP almacenada en una de sus memorias.

Acto seguido, el servidor de red SR transmite un mensaje MT2 que contiene la clave de sesión KC2 y la dirección ADC2 al servidor de gestión SG a través del enlace LS.

Durante una etapa E30, el servidor de gestión SG controla el registro de la información IS relativa a la sesión SC3 establecida en la lista LT de terminales conectados. Para ello, envía al servidor de red SR un mensaje MR que contiene el identificador IdC del terminal C, la clave de sesión KC2 y la dirección ADC2.

A la etapa E30 le sigue una etapa E32 durante la cual el servidor de red SR recibe el mensaje MR y registra la información IS relativa a la sesión SC3 establecida en asociación con el identificador IdC del terminal C en la lista LT de terminales conectados. La información registrada es, por ejemplo, el identificador IdS del servidor de aplicaciones SA, la clave de sesión KC2 y la dirección ADC2.

En una forma de realización particular, la clave de sesión KC2 y la dirección ADC2 también se transmiten de forma segura al servidor de aplicaciones SA.

Durante una etapa S40, realizada después de las etapas descritas anteriormente, el terminal C, que tiene datos DATA para transmitir al servidor de aplicaciones SA, genera y envía un mensaje MD.

Los datos DATA son, por ejemplo, datos de medición obtenidos por el terminal C.

De forma más general, los datos DATA son datos que el terminal C desea transmitir al servidor de aplicaciones SA y/o al servidor de red SR.

No hay limitación en el tipo de datos DATA del mensaje de datos MD.

El mensaje MD contiene el identificador IdS del servidor de aplicaciones SA, la dirección ADC2 del terminal C y los datos DATA cifrados con la clave de sesión KC2 generada por el terminal C.

El mensaje MD es recibido por el dispositivo de transmisión P en una etapa S42.

El dispositivo de transmisión P comprueba que el mensaje MD procede del terminal C y con destino al servidor de aplicaciones SA (etapa S44).

Si la comprobación es positiva, el dispositivo de transmisión P ordena que el mensaje MD sea enviado por el dispositivo de transmisión P (etapa S46).

El mensaje de datos MD enviado por el terminal C, destinado al servidor de aplicaciones SA y recibido por el dispositivo de transmisión P, es de este modo retransmitido por este último.

Si la comprobación es negativa, por ejemplo, si el mensaje MD recibido por el dispositivo de transmisión P es un mensaje enviado por un terminal para el que el dispositivo de transmisión P no ha recibido derechos de gestión, por ejemplo el identificador del terminal y la clave primaria asociada a este terminal, o si el mensaje MD enviado por el terminal C no contiene el identificador IdS del servidor de aplicaciones SA, el mensaje no es retransmitido por el dispositivo de transmisión P.

El mensaje MD, retransmitido por el dispositivo de transmisión P, es recibido por el servidor de red SR en una etapa S48.

En la etapa S50, el servidor de red SR comprueba que el terminal C está registrado en la lista LT de terminales conectados.

Utilizando los datos IS almacenados en asociación con el identificador IdC del terminal C en la lista LT, el servidor de red SR también puede realizar comprobaciones de integridad en el mensaje MD.

Si el terminal no está incluido en la lista LT o si el servidor de red SR considera que las comprobaciones no son satisfactorias, se detiene el proceso de procesamiento de mensajes MD por parte del servidor de red SR.

De lo contrario, el servidor de red SR obtiene los datos DATA utilizando la clave de sesión KC2 almacenada en la lista LT en asociación con el identificador IdC del terminal C.

A continuación, los datos DATA obtenidos se transmiten al servidor de aplicaciones SA.

En la forma de realización descrita, en la etapa S46, el mensaje MD se retransmite sin someterse a ningún procesamiento por parte del dispositivo de transmisión P.

Alternativamente, el mensaje MD es cifrado con la clave de sesión KSP por el dispositivo de transmisión P antes de ser transmitido.

Los etapas S40 a S50 pueden repetirse una o más veces.

Una de las etapas S50 puede ir seguida de una etapa E52 durante la cual el servidor de aplicaciones SA, que tiene datos DAT2 para transmitir al terminal C, genera y transmite un mensaje MD2 con destino al terminal C.

La etapa S52 se realiza, por ejemplo, después de que el servidor de aplicaciones SA reciba un mensaje de consulta o un mensaje de datos

El servidor de red SR recibe el mensaje MD2.

Tras recibir el mensaje MD2, el servidor de red SR cifra los datos DAT2 con la clave de sesión KC2 y transmite un mensaje MD3 que contiene los datos DAT2 cifrados con destino al terminal C (etapa S54).

El mensaje MD3 es recibido por el dispositivo de transmisión P en la etapa E56.

En una etapa E58, el dispositivo de transmisión P retransmite el mensaje MD3 recibido y el mensaje MD3 es recibido por el terminal C en una etapa S60.

En la forma de realización descrita, la clave de sesión KC2 generada por el dispositivo de transmisión P es transmitida por este dispositivo al servidor de red SR.

Alternativamente, el valor aleatorio AL5 generado por el terminal C y el valor aleatorio AL6 generado por el dispositivo de transmisión P se transmiten al servidor de red SR en lugar de la clave de sesión KC2. La clave de sesión KC2 no se transmite. La clave de sesión KC2 es entonces generada por el servidor de aplicaciones SA o por el servidor de red SR aplicando la función matemática F2 a los valores aleatorios AL5 y AL6 y a la clave primaria KPC.

En otra forma de realización particular, el valor aleatorio AL6 y la dirección ADC2 del terminal son generados por el servidor de gestión SG, por el servidor de red SR o por el servidor de aplicaciones SA y, a continuación, transmitidos al dispositivo de transmisión P.

La clave de sesión KC2 puede no ser generada por el dispositivo de transmisión P. En este caso, sólo se transmite el valor aleatorio AL5 generado por el terminal C en asociación con el identificador IdC del terminal C durante la etapa S26. La clave de sesión KC2 es entonces generada por el servidor de aplicaciones SA o por el servidor de red SR aplicando la función matemática F2 a los valores aleatorios AL5 y AL6 y a la clave primaria KPC.

En la forma de realización descrita, cuando se establece una sesión con un servidor de aplicaciones, por ejemplo, el servidor de gestión SG o el servidor de aplicaciones SA, la autentificación de un terminal o de un dispositivo de transmisión es llevada a cabo por el servidor de red SR.

Alternativamente, dicha autentificación puede ser realizada por el servidor de gestión, el servidor de aplicaciones SA u otro equipo de red, por ejemplo, un servidor de autentificación de red. En esta variante, los datos asociados a un servidor de aplicaciones y necesarios para la implementación de la autentificación se ponen a disposición de este servidor.

Una clave secundaria generada a partir de una clave primaria puede ponerse a disposición del servidor de red, que entonces autentica y/o descifra los mensajes procedentes de un terminal o dispositivo de transmisión antes de transmitirlos, preferiblemente a través de un enlace seguro, al servidor de aplicaciones correspondiente.

A la inversa, los mensajes generados por un servidor de aplicaciones son firmados y/o cifrados con la clave secundaria por el servidor de red antes de su transmisión a un terminal o dispositivo de transmisión.

Una clave secundaria generada a partir de una clave primaria también puede ponerse a disposición del servidor de aplicaciones, que puede así cifrar los mensajes antes de su transmisión y descifrar los mensajes recibidos.

En la forma de realización descrita, se genera una clave de sesión para cada autentificación mutua. Se genera una clave de sesión KSP durante la autentificación mutua del dispositivo de transmisión P y el servidor de gestión SG, se genera una clave de sesión KC1 durante la autentificación mutua del terminal C y el servidor de aplicaciones SA y se genera una clave de sesión KC2 durante la autentificación mutua del terminal C y el dispositivo de transmisión P.

Tal y como se define en el estándar LoRaWAN™, estas claves de sesión son claves de sesión de aplicación.

En las arquitecturas de tipo LoRaWAN™, la seguridad de los intercambios entre los terminales y los servidores de aplicaciones se garantiza a dos niveles distintos, es decir, a nivel de la red mediante diversas comprobaciones de integridad efectuados por el servidor de red que actúa como intermediario entre los terminales y los servidores de aplicaciones y por los propios terminales, y a nivel de la aplicación mediante el cifrado/descifrado de los datos de aplicación intercambiados entre los terminales y los servidores de aplicaciones. Cada uno de estos mecanismos se basa, en cada sesión establecida por un terminal con un servidor de aplicaciones a través del servidor de red, en el conocido algoritmo de cifrado AES utilizado en el protocolo LoRaWAN™, a veces parametrizado mediante claves criptográficas de sesión de red, a veces mediante claves criptográficas de sesión de aplicación. Estas claves criptográficas tienen un tamaño de 128 bits. Cabe señalar, no obstante, que la invención permite prever fácilmente algoritmos de cifrado simétrico distintos del algoritmo de cifrado AES, así como otros tamaños de clave.

La invención también se aplica a esta arquitectura.

De este modo, en una forma de realización alternativa, durante la autentificación mutua requerida por el dispositivo de transmisión P, la solicitud de autentificación DA1 enviada por el dispositivo de transmisión P es interceptada por un servidor de red SR de la red LoRa™.

Tras recibir la solicitud de autentificación DA1, el servidor de red SR genera por una parte una clave de red KRP y por otra parte la clave de sesión KSP.

Además de la clave de sesión KSP, el dispositivo de transmisión P también genera la clave de red KRP.

Los mensajes transmitidos por el dispositivo de transmisión P con destino al servidor de gestión SG contienen datos cifrados por la clave de sesión KSP y, a continuación, firmados por la clave de red KRP. Cada mensaje es recibido por el servidor de red SR, que comprueba su integridad y autenticidad utilizando su clave de red KRP, y lo transmite al servidor de gestión SG, que lo descifra utilizando la clave de sesión KSP. Alternativamente, si ha sido autorizado para ello, el servidor de red SR puede descifrar el mensaje con la clave de sesión KSP y transmitir el mensaje descifrado al servidor de gestión SG a través del enlace LS, que es preferiblemente seguro.

Del mismo modo, durante la etapa de autentificación mutua entre el terminal C y el servidor de red SR, puede generarse una clave de red KRC2 a partir de la clave primaria KPC, por una parte, por el terminal C y, por otra parte, por el servidor de red SR de la red LoRa™.

Del mismo modo, durante la etapa de autentificación mutua entre el terminal C y el dispositivo de transmisión DP, puede generarse una clave de red KRC2 a partir de la clave primaria KPC por una parte por el terminal C y por otra parte por el dispositivo de transmisión P.

Acto seguido, los mensajes transmitidos por el terminal C también están firmados por la clave de red KRC2.

Alternativamente a esta forma de realización, cuando se recibe procedente del terminal C un mensaje de datos cifrado con la clave de sesión KC2 y firmado con la clave de red KRC2, el dispositivo de transmisión P utiliza la clave de red KRC2 para obtener los datos DATA cifrados con la clave de sesión KC2, es decir, KC2(DATA). A continuación, cifra estos datos cifrados (KC2(DATA)) con la clave de sesión KSP y, a continuación, los firma con la clave de red KRP antes de transmitir el mensaje así obtenido.

El mensaje es obtenido por el servidor de red SR, que obtiene y transmite los datos cifrados con la clave de sesión KSP al servidor de gestión SG. Este mensaje es recibido por el servidor de gestión SG que, utilizando su clave KSP, obtiene los datos cifrados con la clave KC2 y transmite el mensaje resultante. Por último, este mensaje es recibido por el servidor de aplicaciones SA, que utiliza la clave KC2 para obtener los datos DATA.

REIVINDICACIONES

1. Método de gestión **caracterizado por que** comprende las siguientes etapas implementadas por un dispositivo de transmisión (P) capaz de comunicarse a través de un enlace de radio (L1) con un equipo de pasarela (EP1) que forma un nodo de una red de telecomunicaciones y configurado para comunicarse con un servidor de gestión asociado (SG) a través de dicho equipo de pasarela y a través de un servidor de red (SR) de dicha red:
recepción (E12, S12) desde dicho servidor de gestión (SG) de una solicitud de gestión (DGC3) procedente de un terminal (C) capaz de comunicarse a través de un enlace de radio (L2) con un equipo de pasarela (EP2) de la red y configurado para comunicarse con un servidor de aplicaciones asociado (SA) a través del equipo de pasarela de la red y dicho servidor de red y habiendo establecido una sesión de comunicación (SC2) con el servidor de red y/o el servidor de aplicaciones, al menos una clave de sesión (KC1) compartida entre el terminal y el servidor de red y/o el servidor de aplicaciones, conteniendo dicha solicitud de gestión al menos un identificador (IdC) de dicho terminal y dicha al menos una clave de sesión;
tras la recepción de la solicitud de gestión, recepción (E14, S14) de al menos un mensaje (M1, MD1) enviado por dicho terminal; y
transmisión (E16, M16), en respuesta a dicho mensaje, de al menos un mensaje de respuesta (M2), con destino al terminal, cifrado con dicha clave de sesión recibida.

2. Método de gestión de acuerdo con la reivindicación 1, en el que dicha solicitud de gestión se recibe (E12, S12) a través de dicho equipo de pasarela (EP1) y a través de dicho servidor de red.

3. Método de gestión de acuerdo con la reivindicación 1 o 2 en el que dicho al menos un mensaje de respuesta contiene al menos un parámetro de configuración del terminal.

4. Método de gestión de acuerdo con la reivindicación 3, en el que dicho al menos un parámetro de configuración comprende una lista de al menos un canal de radio que el terminal debe habilitar o deshabilitar.

5. Método de gestión de acuerdo con la reivindicación 3 o 4 en el que dicho al menos un parámetro de configuración comprende al menos un valor de retardo que se debe respetar entre un mensaje transmitido y un mensaje recibido por el terminal.

6. Método de gestión de acuerdo con una de las reivindicaciones 1 a 5, en el que dicho al menos un mensaje de respuesta contiene una solicitud de transmisión para que dicho terminal envíe una solicitud de conexión.

7. Método de gestión de acuerdo con una de las reivindicaciones precedentes en el que dicha solicitud de gestión contiene datos de autentificación que permiten a dicho dispositivo de transmisión establecer una sesión de comunicación con el terminal.

8. Método de gestión de acuerdo con una de las reivindicaciones precedentes, en el que el método comprende, tras la transmisión de dicho al menos un mensaje de respuesta, una etapa de recepción de una solicitud de conexión a dicho servidor de aplicaciones transmitida por dicho terminal y una etapa de establecimiento de una sesión de comunicación entre dicho terminal y dicho dispositivo de transmisión.

9. Método de gestión de acuerdo con la reivindicación 8, en el que el método comprende, tras el establecimiento de la sesión de comunicación entre dicho terminal y dicho dispositivo de transmisión, una etapa de envío de datos para establecer dicha sesión de comunicación a dicho servidor de red.

10. Método de gestión de acuerdo con una de las reivindicaciones precedentes en el que dicha solicitud de gestión se recibe en respuesta a un mensaje enviado por el dispositivo de transmisión.

11. Dispositivo de transmisión (P) apto para comunicarse a través de un enlace de radio con un equipo de pasarela (EP1) que forma un nodo de una red de telecomunicaciones y configurado para comunicarse con un servidor de gestión (SG) a través de dicho equipo de pasarela (EP1) y a través de un servidor de red (SR) de dicha red, **caracterizado por que** comprende:
un primer módulo (RCP, RCP3) para recibir, procedente de dicho servidor de gestión (SG), una solicitud de gestión de un terminal capaz de comunicarse a través de un enlace de radio con un equipo de pasarela (EP2) de la red y configurado para comunicarse con un servidor de aplicaciones asociado a través del equipo de pasarela (EP2) de la red y dicho servidor de red y habiendo establecido una sesión de comunicación con el servidor de red y/o el servidor de aplicaciones, al menos una clave de sesión compartida entre el terminal y el servidor de red y/o el servidor de aplicaciones, conteniendo dicha solicitud de gestión al menos un identificador de dicho terminal y dicha al menos una clave de sesión;
un segundo módulo de recepción (RCC) configurado para interceptar, tras la recepción de la solicitud de gestión, al menos un mensaje enviado por dicho terminal; y
un módulo de transmisión (EMC), en respuesta a dicho mensaje, de al menos un mensaje de respuesta con destino al terminal, cifrado con dicha clave de sesión recibida.

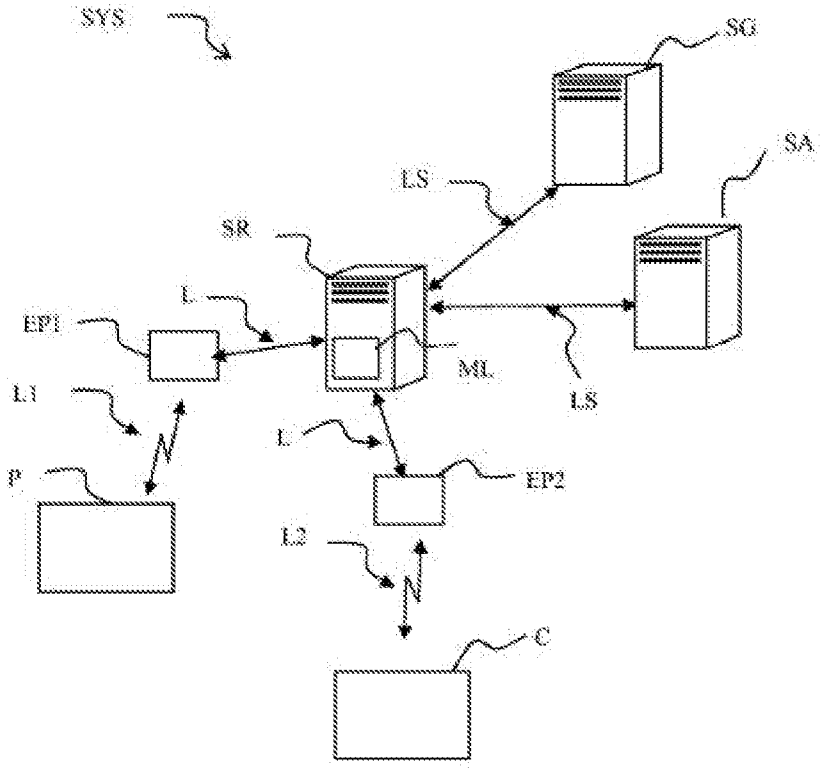

Figura 1

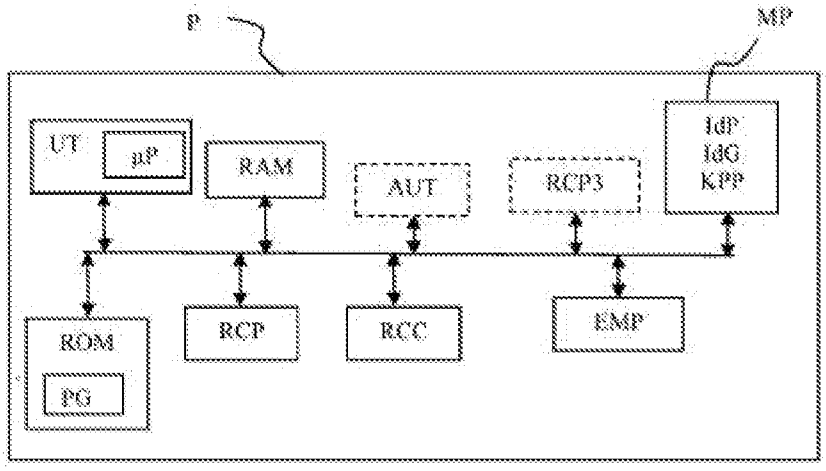

Figura 3

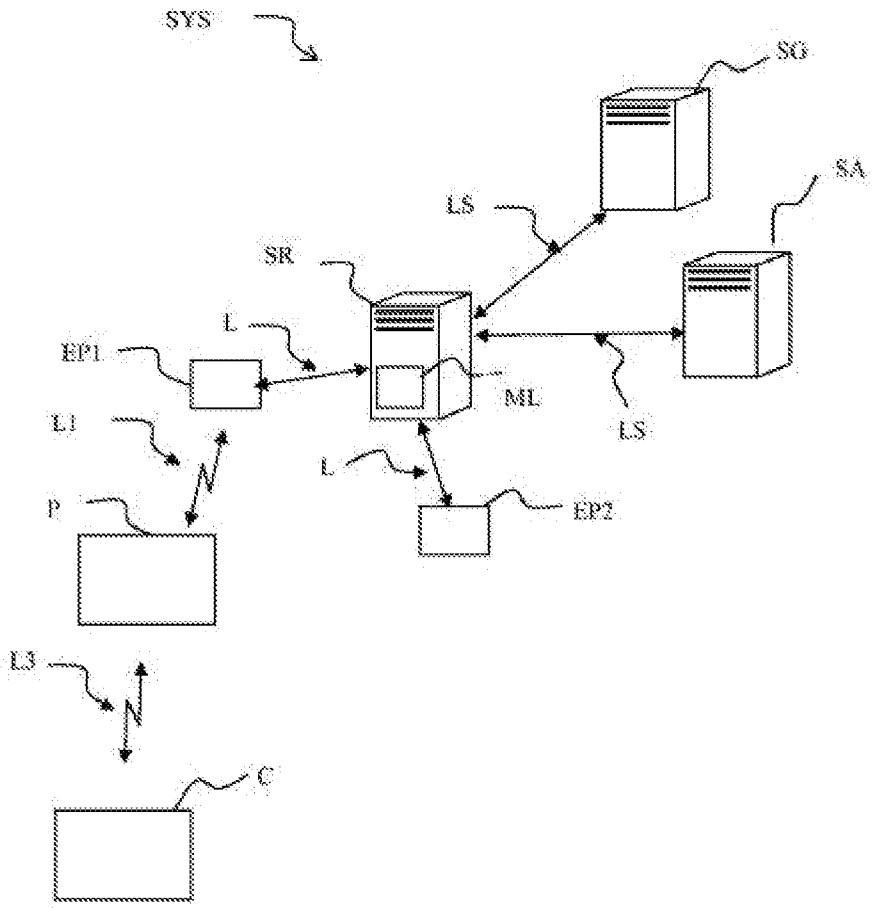

Figura 2

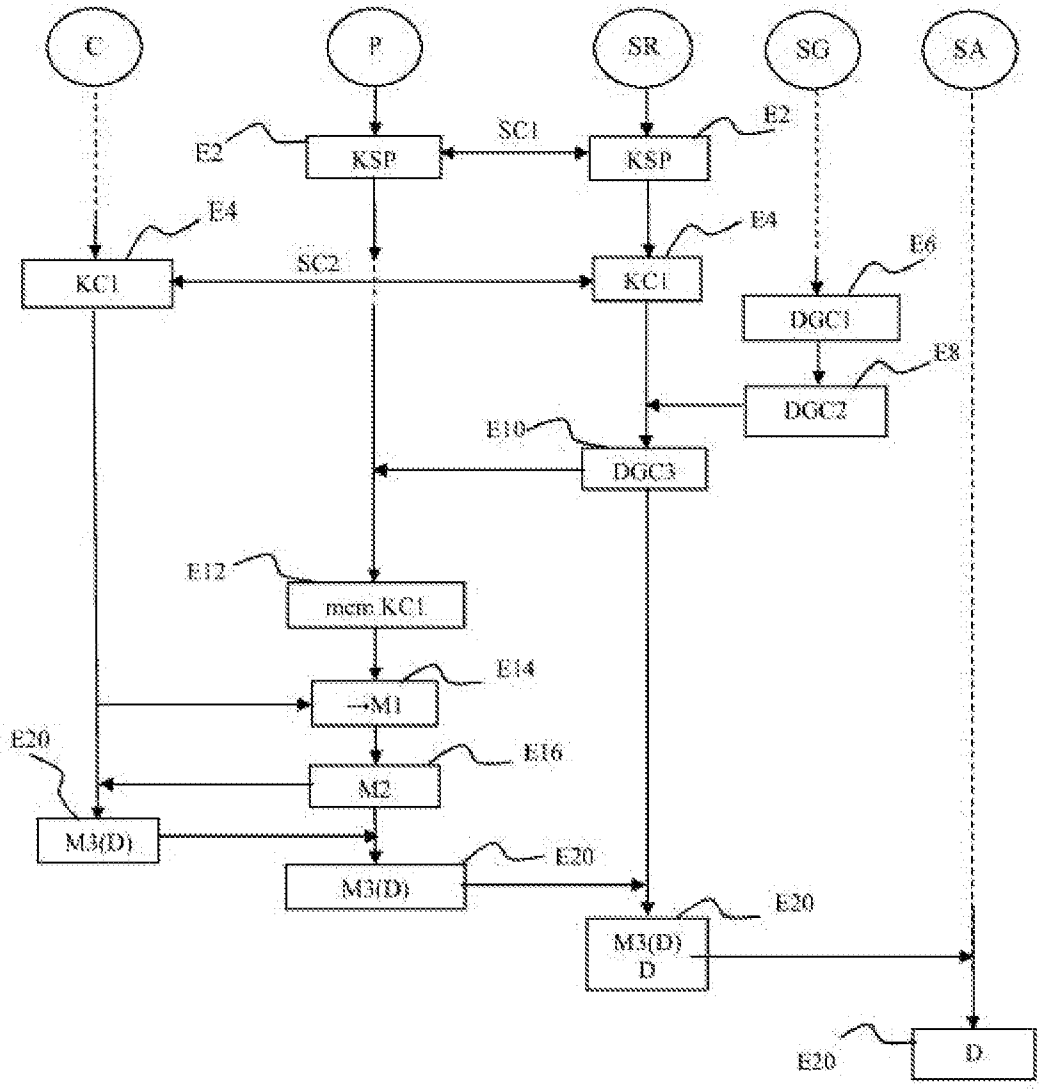
C
P
SR
SG
SA
E2
KSP
SC1
KSP
E2
E4
KC1
SC2
KC1
E4
E6
DGC1
E8
DGC2
E10
DGC3
E12
mem.KC1
E14
→M1
E16
M2
E20
M3(D)
E20
M3(D)
E20
M3(D)
D
E20
D

Figura 4

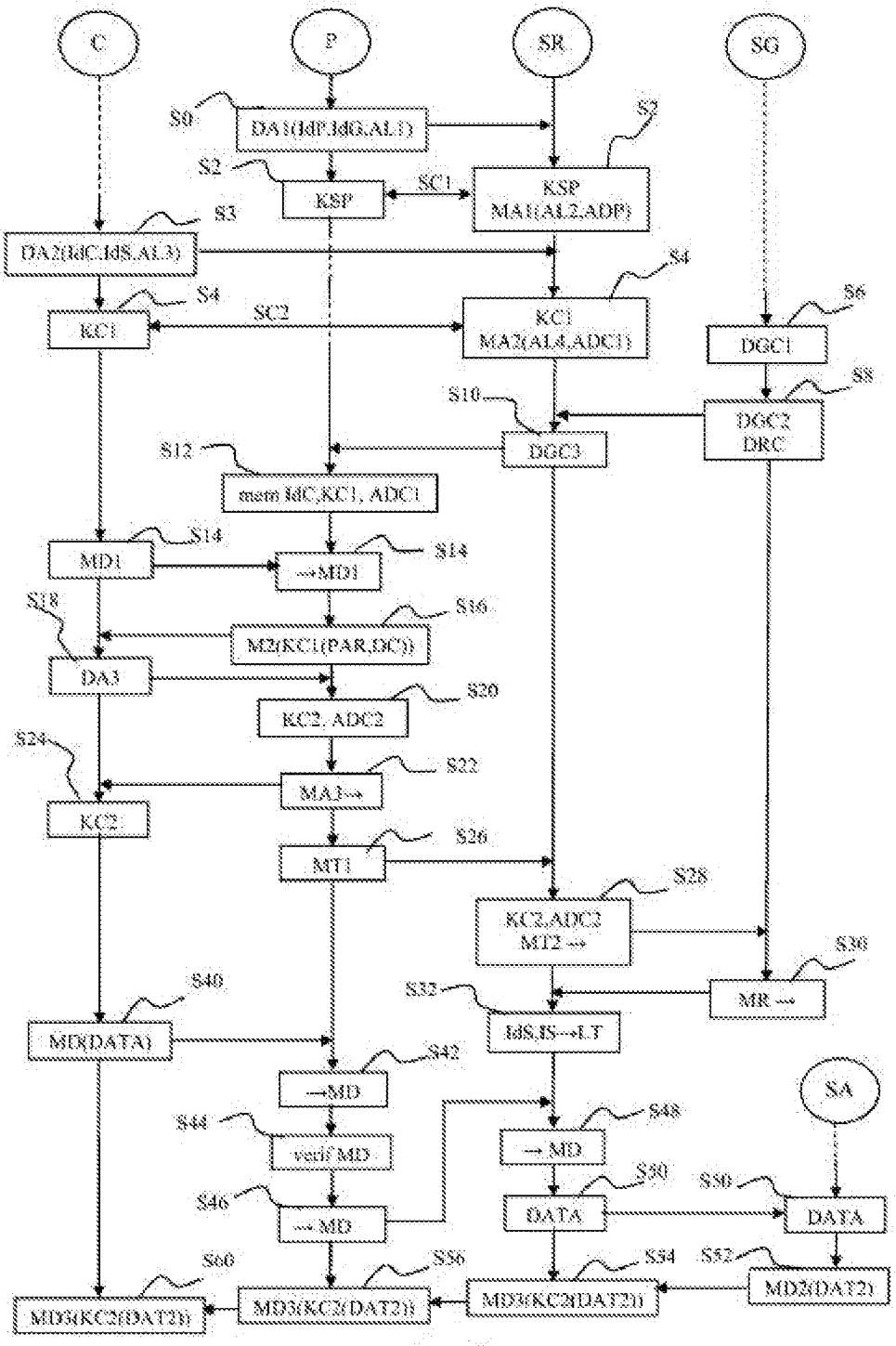
C
P
SR
SG
S0
DA1(IdP,IdG,AL1)
S2
KSP
SC1
KSP MA1(AL2,ADP)
S3
DA2(IdC,Id8,AL3)
S4
KC1
SC2
KC1 MA2(AL4,ADC1)
S6
DGC1
S8
DGC2 DRC
S10
DGC3
S12
mem IdC,KC1, ADC1
S14
MD1
→MD1
S16
M2(KC1(PAR,DC))
S18
DA3
S20
KC2, ADC2
S22
MA3→
S24
KC2;
S26
MT1
S28
KC2,ADC2 MT2 →
S30
MR →
S32
M8,IS→LT
S40
MD(DATA)
S42
→MD
S44
verif MD
S46
→MD
S48
→MD
S50
DATA
S52
MD2(DAT2)
SA
DATA
S54
MD3(KC2(DAT2))
S56
MD3(KC2(DAT2))
S60
MD3(KC2(DAT2))

Figura 5