(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 831 314**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/00 (2009.01)
H04W 12/04 (2009.01)
H04L 9/08 (2006.01)
H04B 7/185 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.03.2014 PCT/EP2014/056354**

(87) Fecha y número de publicación internacional: **02.10.2014 WO14154890**

(96) Fecha de presentación y número de la solicitud europea: **28.03.2014 E 14713482 (9)**

(97) Fecha y número de publicación de la concesión europea: **07.10.2020 EP 2979421**

(54) Título: **Distribución de claves en un sistema de satélite**

(30) Prioridad:

28.03.2013 EP 13275084

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.06.2021

(73) Titular/es:

AIRBUS DEFENCE AND SPACE LIMITED (100.0%)
Gunnels Wood Road, Stevenage
Hertfordshire SG1 2AS, GB

(72) Inventor/es:

CLARKE, STEVE y
MCCOY, THOMAS

(74) Agente/Representante:

PONS ARIÑO, Ángel

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

DESCRIPCIÓN

Distribución de claves en un sistema de satélite

Campo de la invención

La presente invención se refiere a la distribución de claves en un sistema de satélite. En particular, la presente invención se refiere a la distribución de una clave en un sistema de satélite mediante el uso de cifrado de clave pública.

Antecedentes de la invención

Los satélites se utilizan en una amplia variedad de aplicaciones. Como algunos ejemplos, los satélites de telecomunicaciones pueden proporcionar transmisión de televisión u otros servicios como comunicaciones telefónicas, de video o radio, los satélites de observación de la Tierra pueden proporcionar imágenes detalladas en tiempo real de la superficie de la Tierra y los satélites de posicionamiento en un sistema global de navegación por satélite (GNSS) puede permitir que la posición de un receptor sea calculada con precisión mediante triangulación.

Para cualquier tipo de satélite, la capacidad de comunicarse de forma segura con el satélite es particularmente importante. El cifrado simétrico se utiliza a menudo para impedir que un tercero no autorizado reciba y descifre transmisiones del satélite, y para impedir que un agresor tome el control del satélite transmitiendo sus propias señales de control al satélite. Un esquema de cifrado simétrico requiere que se proporcione la misma clave de sesión a cualquier dispositivo autorizado en el sistema de satélite, como el propio satélite, una estación de control y cualquier usuario final que necesite recibir transmisiones desde el satélite. Los dispositivos autorizados en el sistema pueden comunicarse de forma segura cifrando un mensaje con la clave de sesión y transmitiendo el mensaje cifrado, y descifrando y/o autenticando un mensaje cifrado recibido utilizando la misma clave de sesión.

La seguridad de este sistema se vería comprometida si una parte no autorizada pudiera obtener la clave de sesión. Para protegerse contra esto, la clave de sesión caduca periódicamente y se reemplaza por una nueva clave de sesión. En un sistema convencional, se requiere una compleja infraestructura de administración de claves para distribuir la nueva clave de sesión a los dispositivos dentro del sistema de satélite. Cada dispositivo debe estar precargado con una clave de cifrado de clave raíz (KEK), y un sistema de administración de claves, que es un tercero de confianza, que almacena las KEK raíz de todos los dispositivos del sistema. El sistema de administración de claves puede a continuación distribuir periódicamente claves de sesión actualizadas a cada dispositivo utilizando la KEK raíz de ese dispositivo.

La invención se realiza en este contexto.

El documento US2005/204139 describe sistemas y procedimientos para facilitar el intercambio seguro de información entre agentes de serviciosEl documento US7055027 describe la inspección de un flujo de datos cifrados en una red privada virtual por un intermediario.El documento EP0957606 A2 describe un sistema de transmisión de datos que permite una transmisión segura y más fiable de datos desde un transmisor de datos a un receptor o receptores de datos.

Resumen de la invención

Según la presente invención, se proporciona un procedimiento para transmitir una clave de sesión en un sistema de satélite que comprende un satélite y un dispositivo dispuesto para recibir señales del satélite, según la reivindicación 1.

La transmisión de la clave de sesión protegida puede comprender la transmisión de la clave de sesión protegida y la información de detección de reproducción para determinar si la clave de sesión protegida se ha transmitido previamente.

La clave de sesión protegida y la información de detección de reproducción se pueden incluir en un mensaje de distribución de claves.

El flujo de datos puede ser un flujo de datos de telemetría (TM) según se define en el protocolo de TM del Comité Consultivo para Sistemas de Datos Espaciales (CCSDS).

La clave de sesión obtenida puede ser una clave de la sesión siguiente para usar en la siguiente sesión después de

una sesión actual, y el procedimiento puede comprender además obtener una clave de la sesión actual para usar en la sesión actual, protegiendo la clave de sesión actual en el satélite, según una clave privada del satélite y una clave pública del dispositivo, que transmite la clave de la sesión actual a través del flujo de datos y transmite información de validez a través del flujo de datos, definiendo la información de validez un período de tiempo en el que la clave de la sesión actual es válida y un período de tiempo en el que la clave de la siguiente sesión es válida.

El procedimiento puede comprender además determinar, en el satélite, cuándo va a caducar la clave de la sesión transmitida según una o más reglas de caducidad de clave predefinidas.

Según la presente invención, también se proporciona un procedimiento para obtener una clave de sesión en un sistema de satélite que comprende un satélite y un dispositivo dispuesto para recibir señales del satélite, según la reivindicación 5.

El procedimiento puede comprender además obtener información sobre una ubicación esperada del satélite cuando se transmitió la clave de sesión protegida y determinar que la clave de sesión protegida recibida es auténtica si una ubicación desde la cual se recibió la clave de sesión protegida coincide con la ubicación esperada del satélite, dentro de un margen de error predeterminado.

El procedimiento puede comprender además recibir información de detección de reproducción para determinar si la clave de sesión protegida se ha transmitido previamente.

La clave de sesión obtenida puede ser una clave de sesión siguiente para usar en la siguiente sesión después de una sesión actual, y el procedimiento puede comprender además recibir una clave de sesión actual protegida para usar en la sesión actual, e información de validez que define un período de tiempo en el que el la clave de sesión actual es válida y un período de tiempo en el que la clave de la siguiente sesión es válida, a través del flujo de datos, obteniendo la clave de sesión actual de la clave de sesión actual protegida en el dispositivo, basada en una clave pública del satélite y una clave privada del dispositivo, obtener información sobre un momento en el que se transmitieron los datos protegidos a través del flujo de datos y acceder a los datos protegidos en función de la clave de sesión actual si la información obtenida indica que los datos protegidos se transmitieron durante el período de tiempo en el que la clave de sesión es válida, o acceder a los datos protegidos en función de la siguiente clave de sesión si la información obtenida indica que los datos protegidos fueron transmitidos durante el período de tiempo en el que la siguiente clave de sesión es válida.

Se puede disponer un medio de almacenamiento legible por ordenador para almacenar un programa de ordenador que, cuando es ejecutado por un dispositivo, hace que el dispositivo realice el procedimiento, según la reivindicación 8.

Según la presente invención, se proporciona un satélite según la reivindicación 9.

El satélite puede comprender además un generador de información de reproducción dispuesto para generar información de detección de reproducción para determinar si la clave de sesión protegida se ha transmitido previamente, y el transmisor puede disponerse para transmitir la clave de sesión protegida y la información de detección de reproducción al dispositivo.

Según la presente invención, también se proporciona un dispositivo para recibir señales de un satélite, según la reivindicación 11.

Breve descripción de los dibujos

A continuación, se describen realizaciones de la presente invención solo a modo de ejemplo, con referencia a los dibujos adjuntos, de los que:

La figura 1 ilustra un sistema que incluye un satélite y un dispositivo para comunicarse con el satélite, según una realización de la presente invención;
La figura 2 ilustra un procedimiento para proporcionar una clave simétrica en el sistema de la figura 1, según una realización de la presente invención;
La figura 3 ilustra un procedimiento para administrar la distribución de claves simétricas en un sistema de satélite, según una realización de la presente invención;
La figura 4 ilustra un procedimiento para hacer caducar una clave simétrica en un sistema de satélite, según una realización de la presente invención;

La figura 5 ilustra un mensaje de distribución de claves para distribuir una clave simétrica en un sistema de satélite, según una realización de la presente invención;
La figura 6 ilustra un mensaje de distribución de claves en un sistema que funciona según un estándar de telecomando de paquetes del Comité Consultivo para Sistemas de Datos Espaciales (CCSDS), según una realización de la presente invención;
La figura 7 ilustra la transmisión de un mensaje de distribución de claves a través de un flujo de telemetría CCSDS, según una realización de la presente invención;
La figura 8 ilustra un procedimiento para recibir una clave simétrica en un sistema de satélite, según una realización de la presente invención;
La figura 9 ilustra un procedimiento para usar información de detección de reproducción, según una realización de la presente invención;
La figura 10 ilustra un dispositivo para transmitir una clave simétrica en un sistema de satélite, según una realización de la presente invención;
La figura 11 ilustra un dispositivo para recibir una clave simétrica en un sistema de satélite según una realización de la presente invención;
La figura 12 ilustra un procedimiento de autenticación de una clave de sesión recibida, según una realización de la presente invención.

Descripción Detallada

Con referencia ahora a la figura 1, se ilustra un sistema que incluye un satélite y un dispositivo para comunicarse con el satélite, según una realización de la presente invención. El sistema 100 puede denominarse sistema de satélite. En la presente realización, el dispositivo 101 es una estación de control basada en tierra dispuesta tanto para transmitir como para recibir señales, de modo que la estación de control 101 puede transmitir una señal 103 al satélite 102 y también recibir una señal 104 desde el satélite 102. Sin embargo, en otra realización, el dispositivo 101 solo puede estar dispuesto para transmitir señales al satélite o solo puede estar dispuesto para recibir señales del satélite. Por ejemplo, el dispositivo 101 podría ser una antena de sólo recepción para recibir señales de transmisión de televisión u otros tipos de señales del satélite 102, o podría ser otro satélite. Las realizaciones de la presente invención se pueden aplicar a las comunicaciones con cualquier tipo de satélite, incluidos, entre otros, un satélite de comunicaciones, un satélite de posicionamiento para su uso en un sistema global de navegación por satélite (GNSS), un satélite de investigación científica o un satélite de observación de la tierra. Aunque la figura 1 ilustra un satélite que se comunica con otro dispositivo, las realizaciones de la presente invención pueden incluir cualquier número de dispositivos, por ejemplo, cualquier número de satélites, estaciones terrestres, antenas receptoras, etc.

En el sistema 100 de la presente realización, la estación de control 101 está dispuesta para enviar señales de control 103 al satélite 102 y recibir señales de telemetría 104 desde el satélite 102. Ejemplos de señales de control 103 que pueden ser enviadas por la estación de control 101 incluyen telecomandos para hacer ajustes a la posición. y/o orientación del satélite 102 o para mover el satélite 102 a una nueva órbita. Las señales de telemetría 104 pueden proporcionar información sobre el estado actual del satélite 102, por ejemplo, la configuración del satélite, la energía o los datos de supervisión térmica.

Similar a un sistema convencional, las transmisiones en los canales del enlace ascendente 103 y del enlace descendente 104 se cifran utilizando claves de sesión para impedir que un usuario no autorizado controle el satélite u obtenga datos de telemetría del satélite. Durante una sesión, las transmisiones se cifran utilizando la clave de sesión actual, que es conocida por el transmisor y el(los) receptor(es). Al final de una sesión, la clave de sesión actual caduca y las transmisiones posteriores se cifran con la clave de la siguiente sesión. Sin embargo, a diferencia del sistema convencional, que requiere que un tercero de confianza distribuya periódicamente nuevas claves de sesión, en la presente realización la distribución de claves de sesión actualizadas puede ser manejada por el dispositivo 101 y/o el satélite 102 utiliza criptografía de clave pública, sin la necesidad de una infraestructura de gestión de claves separada.

Los principios básicos de la criptografía de clave pública están bien comprendidos y no se describirán en detalle aquí. En resumen, son generadas una clave privada y una clave pública para cada dispositivo en un sistema de satélite, tal como el dispositivo 101 y el satélite 102 en el sistema de satélite 100 de la figura 1. El dispositivo 101 y el satélite 102 están dispuestos para almacenar su propia clave privada, así como la clave pública del otro dispositivo 101, 102. En general, la clave pública de cada dispositivo en un sistema de satélite está disponible para cualquier otro dispositivo en el sistema de satélite.

En las realizaciones de la presente invención, un dispositivo en el sistema de satélite puede distribuir una clave de sesión protegiendo la clave de sesión en función de la clave privada del dispositivo y la clave pública del destinatario previsto, y transmitiendo la clave de la sesión protegida. Algunos ejemplos de tipos de protección que se pueden

aplicar a la clave de sesión incluyen el cifrado y/o autenticación de clave pública. El cifrado de clave pública se puede utilizar para derivar de forma auténtica un secreto compartido, y un algoritmo como Ajuste de Clave (Keywrap) Estándar de Cifrado Avanzado (AES) con relleno (padding) puede utilizar el secreto compartido para proporcionar confidencialidad e integridad al secreto compartido.

El cifrado proporciona confidencialidad al impedir la exposición de la clave de sesión u otros datos cifrados a terceros no autorizados. La autenticación proporciona la garantía de que la transmisión proviene de una fuente confiable. Un ejemplo de un algoritmo de cifrado criptográfico es un algoritmo de Encadenamiento de Bloques de Cifrado Estándar de Cifrado Avanzado (AES-CBC - Advanced Encryption Standard Cipher Block Chaining), y un ejemplo de un algoritmo de autenticación criptográfica es un algoritmo de Código de Autenticación de Mensajes basado en Cifrado Estándar de Cifrado Avanzado (AES-CMAC - Advanced Encryption Standard Cipher-based Message Authentication Code). Un Contador Estándar de Cifrado Avanzado con algoritmo CBC-MAC (AES-CCM) proporciona cifrado y autenticación. También se conocen en la técnica otros algoritmos que proporcionan cifrado o autenticación, o tanto cifrado como autenticación.

Para descifrar o cifrar una clave de sesión, un dispositivo deriva un secreto compartido basado en su propia clave privada y la clave pública del remitente o destinatario, según corresponda. El secreto compartido se puede a continuación utilizar para cifrar una clave de sesión o para descifrar una clave de sesión cifrada recibida. El secreto compartido puede denominarse clave de cifrado de clave, es decir, una clave que se utiliza para cifrar la clave de sesión. Mecanismos de ejemplo para derivar el secreto compartido incluyen un procedimiento Diffe-Helman de curva elíptica (ECDH) y un protocolo Diffe Helman seguro de alto rendimiento (HMQV). Debido a que las claves privadas no se comparten entre dispositivos, la clave de sesión cifrada solo puede ser descifrada por el dispositivo 101, 102 cuya clave pública se utilizó para cifrar el mensaje.

En el ejemplo de una estación de control que transmite una clave de sesión, la autenticación se puede utilizar con o sin cifrado. La autenticación permite al satélite verificar que la clave de sesión recibida proviene de una fuente confiable. En otro ejemplo, un satélite puede transmitir una clave de sesión usando cifrado con o sin autenticación. En este ejemplo, es posible que no se requiera autenticación debido a la dificultad de falsificar una señal de un satélite. Específicamente, para falsificar una señal de un satélite, un atacante tendría que transmitir una señal desde la misma posición que el satélite, lo que actualmente no es práctico. Al mismo tiempo, el cifrado impide que la clave de sesión sea obtenida por cualquier tercero no autorizado que reciba señales del satélite.

Se apreciará que para descifrar y/o autenticar una clave de sesión recibida, que ha sido protegida mediante criptografía de clave pública, el receptor necesita saber qué clave pública debe utilizarse en el descifrado/autenticación. En los sistemas satelitales que solo incluyen dos dispositivos, cada dispositivo solo tiene que almacenar una clave pública, que es la clave pública del otro dispositivo. En tales sistemas, cada dispositivo puede asumir que los mensajes recibidos provienen del único otro dispositivo en el sistema y descifrar cualquier mensaje recibido usando la clave pública almacenada del otro dispositivo. Sin embargo, en los sistemas de satélite que incluyen más de dos dispositivos, cada dispositivo puede almacenar una pluralidad de claves públicas, específicamente, una clave pública para cada otro dispositivo en el sistema. En tales realizaciones, cuando un dispositivo transmite un mensaje usando criptografía de clave pública, por ejemplo, un mensaje de distribución de clave, el dispositivo también puede transmitir un identificador para identificar el dispositivo fuente desde el cual se originó la transmisión. Luego, cualquier dispositivo en el sistema que reciba el mensaje puede identificar el dispositivo fuente en base al identificador incluido y seleccionar la clave pública correspondiente al dispositivo identificado para descifrar y/o autenticar la clave de sesión incluida en el mensaje. El identificador debe transmitirse sin protección de clave pública, de modo que el dispositivo receptor pueda obtener el identificador sin tener que utilizar una clave pública del dispositivo fuente.

Como alternativa, se puede transmitir una clave de sesión sin un identificador. En este caso, el receptor podría identificar la clave pública apropiada por ensayo y error, intentando descifrar y/o autenticar el mensaje de distribución de claves con cada conjunto de atributos de seguridad asociados con cada uno de los posibles transmisores en el sistema, y procesar el que descifra y/o autentica con éxito. Alternativamente, el dispositivo puede seleccionar el conjunto apropiado de atributos de seguridad basándose en algún otro parámetro conocido, como la ubicación física del transmisor o la antena particular a través de la cual se recibió el mensaje.

En la presente realización, el dispositivo 101 y el satélite 102 pueden ser responsables de la distribución de claves de sesión en el sistema de satélites 100. Específicamente, uno de los dispositivos 101, 102 puede cifrar una nueva clave de sesión utilizando el cifrado de clave pública como se describió anteriormente, y transmitir la clave de sesión cifrada al otro dispositivo 101, 102. De esta manera, ambos dispositivos 101, 102 pueden obtener la misma clave de sesión y pueden comunicarse posteriormente utilizando el cifrado de clave simétrica, que es más eficiente que el cifrado de clave pública. Al mismo tiempo, el uso de cifrado de clave pública para transmitir la clave de sesión impide que un

tercero no autorizado obtenga la clave de sesión.

Aquí, el término "sesión" se refiere a un período definido en el que se intercambian una o más comunicaciones entre dispositivos que utilizan la misma clave de sesión para el cifrado simétrico. La clave de sesión en uso durante la sesión actual puede denominarse "clave de sesión actual", y una clave de sesión para usar en una sesión posterior puede denominarse "clave de sesión siguiente".

La duración de cualquier sesión dada puede ser predefinida por la arquitectura del sistema, y puede ser un período definido con respecto al tiempo o cualquier otra variable adecuada. Por ejemplo, en una realización, la clave de sesión actual puede caducar después de que se haya transmitido un número predeterminado de telecomandos y se haya reemplazado por la siguiente clave de sesión. En este caso, cada sesión se puede definir como un período en el que se transmite el número predeterminado de telecomandos. En otra realización, cada sesión puede ser un período de tiempo predeterminado, por ejemplo, un día, una semana o un mes. Al final de cada período de tiempo predeterminado, la sesión finaliza y la clave de la sesión actual caduca, y en la siguiente sesión los dispositivos se comunican utilizando la clave de la siguiente sesión. Otros ejemplos de formas en las que se pueden definir sesiones incluyen un límite predeterminado de datos transmitidos que se alcanzan, por ejemplo 250 megabytes (MB), o un número predeterminado de pasadas aéreas de un satélite. Como un ejemplo más, en el caso de un satélite de observación de la tierra que transmite imágenes a uno o más usuarios o grupos de usuarios, cada sesión puede durar un número predeterminado de imágenes. Después de que se haya transmitido el número predeterminado de imágenes en una sesión, la clave de sesión actual caduca y comienza la siguiente sesión, y los dispositivos se comunican utilizando la clave de la siguiente sesión.

Los dispositivos en el sistema de satélite se pueden proporcionar cada uno con una o más reglas predefinidas que definen la duración de las sesiones en ese sistema en particular, como las reglas descritas anteriormente, para permitir que cada dispositivo determine de forma independiente cuándo termina cada sesión y cuándo comienza la próxima sesión. Alternativamente, un dispositivo podría determinar cuándo termina una sesión y cuándo comienza la siguiente, y este dispositivo podría señalar el final de cada sesión a otros dispositivos en el sistema para que los otros dispositivos sepan cuándo va a caducar la clave de sesión actual y se va a comenzar a usar la siguiente clave de sesión en las comunicaciones.

Un procedimiento para distribuir una clave de sesión en el sistema de la figura 1 se describirá ahora con más detalle, con referencia a la figura 2. El dispositivo responsable de transmitir la clave de sesión se denominará en lo sucesivo un primer dispositivo, y el dispositivo que recibe la clave de sesión se denominará segundo dispositivo. Por ejemplo, en el sistema de la figura 1, el satélite 102 y la estación de control 101 pueden ser el primer dispositivo, siendo el otro el satélite 102 y la estación de control 101 el segundo dispositivo. En general, el procedimiento puede ser utilizado por cualquier dispositivo en un sistema de satélite para proporcionar una clave de sesión a cualquier otro dispositivo en el sistema de satélite. Por ejemplo, un satélite puede usar el procedimiento para proporcionar una clave de sesión a un dispositivo si ese dispositivo puede recibir señales del satélite, o un dispositivo puede usar el procedimiento para proporcionar una clave de sesión a un satélite si el dispositivo puede transmitir señales al satélite.

En la primera etapa S201, se obtiene la clave de sesión a transmitir. Aquí, la clave de sesión puede ser generada por el primer dispositivo, o puede ser obtenida por el primer dispositivo de una fuente separada, que puede denominarse generador de claves. En la presente realización, la clave de sesión es generada por el mismo dispositivo que se va a utilizar para distribuir la clave de sesión, es decir, por el primer dispositivo.

Una vez obtenida la clave de sesión, en la etapa S202 el primer dispositivo protege la clave de sesión basándose en su propia clave privada y la clave pública del segundo dispositivo, es decir, la clave pública del dispositivo al que se enviará la clave de sesión. Para proteger la clave de sesión, el primer dispositivo puede utilizar el cifrado y/o autenticación de clave pública. Luego, en la etapa S203, el primer dispositivo transmite la clave de sesión protegida al segundo dispositivo, que es el dispositivo cuya clave pública se utilizó al proteger la clave de sesión. Cuando se utiliza el cifrado, la clave de sesión cifrada se puede difundir a una pluralidad de dispositivos en el sistema, pero sólo se puede descifrar utilizando la clave privada del segundo dispositivo. Por lo tanto, incluso si otros dispositivos del sistema reciben la clave de sesión cifrada, solo el segundo dispositivo puede descifrar la señal recibida para obtener la clave de sesión. Cuando se usa la autenticación, el segundo dispositivo solo aceptará la clave de sesión recibida si la autenticación con la clave pública del primer dispositivo es exitosa.

Con referencia ahora a la figura 3, se ilustra un procedimiento para administrar la distribución de claves en un sistema de satélite, según una realización de la presente invención. Como en la figura 2, el dispositivo responsable de obtener y distribuir claves de sesión puede denominarse un primer dispositivo, y cualquier dispositivo del sistema de satélite que recibe las claves de sesión puede denominarse segundo dispositivo. En la presente realización, el primer

dispositivo es la estación de control 101 de la figura 1, y el segundo dispositivo es el satélite 102 de la figura 1. Sin embargo, en general, en las realizaciones de la presente invención, la tarea de administrar la distribución de claves de sesión en el sistema de satélite puede asignarse a cualquier dispositivo del sistema que sea capaz de transmitir datos a otros dispositivos del sistema, por ejemplo, un satélite o equipo terrestre, como una estación de control.

Primero, en la etapa S301, la estación de control y el satélite se comunican usando la clave de sesión actual, que es la clave de sesión que es válida para la sesión actual. La clave de sesión actual puede ser una clave que se distribuyó previamente usando un procedimiento como el que se muestra en la figura 2, o usando un procedimiento diferente. Por ejemplo, el satélite y la estación de control podrían precargarse con una o más claves de sesión inicial durante la configuración del sistema de satélite, antes de que se lance el satélite. Sin embargo, en las realizaciones de la presente invención, la precarga no es esencial, porque las claves de sesión se pueden distribuir de forma segura una vez que el satélite esté en órbita. Como se describió anteriormente, la estación de control puede comunicarse con el satélite cifrando datos usando la clave de sesión actual y transmitiendo los datos cifrados al satélite, que luego puede descifrar los datos cifrados usando la misma clave de sesión actual. De manera similar, el satélite puede comunicarse con la estación de control transmitiendo datos que han sido cifrados usando la clave de sesión actual.

Aunque en la presente realización los dispositivos se comunican usando una clave de sesión actual en la etapa S301, en algunos escenarios es posible que el dispositivo no tenga conocimiento inicialmente de la clave de sesión actual. Por ejemplo, cuando un dispositivo se enciende después de estar inactivo durante un período de tiempo, es posible que el dispositivo no se haya actualizado con la clave de sesión actual. De manera similar, cuando se agrega un nuevo dispositivo al sistema, por ejemplo, cuando un nuevo usuario se ha suscrito para recibir servicios por satélite, el dispositivo no tendrá conocimiento de la clave de sesión actual. Para abordar este problema, en algunas realizaciones de la presente invención, el dispositivo responsable de la distribución de claves puede transmitir periódicamente mensajes de distribución de claves que incluyen tanto la clave de sesión actual como la clave de sesión siguiente. Esto asegura que un dispositivo sin conocimiento previo de la clave de sesión actual pueda recibir comunicaciones durante la sesión actual en lugar de tener que esperar a que comience la siguiente sesión.

Luego, en la etapa S302, la estación de control obtiene una segunda clave de sesión, que es la clave de la sesión siguiente que será válida en la siguiente sesión. Como en la etapa S201 de la figura 2, la clave de sesión siguiente puede ser generada por la estación de control o puede obtenerse de otra fuente, por ejemplo, un proveedor de claves tercero. En la presente realización, en la etapa S302 la clave de sesión siguiente es generada por la estación de control. La estación de control puede obtener la clave de sesión siguiente en cualquier momento.

Después de que se ha obtenido la clave de sesión siguiente, en la etapa S303, la estación de control protege la siguiente clave de sesión usando la clave privada de la estación de control y la clave pública del dispositivo al que se transmitirá la clave de sesión siguiente, en este caso el satélite. En la presente realización, la estación de control utiliza un mecanismo de establecimiento de claves públicas/privadas junto con un algoritmo de cifrado de claves para brindar protección de confidencialidad, integridad y autenticidad a la clave de sesión. En otras realizaciones, el mecanismo de establecimiento de clave puede proporcionar protección directa de la clave de sesión, sin el uso de un algoritmo de cifrado de clave separado. A continuación, en la etapa S304, la clave de sesión siguiente protegida se transmite al satélite. Las etapas S303 y S304 se pueden realizar de manera similar a las etapas S202 y S203 del procedimiento de la figura 2.

En cualquier momento después de que la siguiente clave de sesión protegida haya sido transmitida al satélite en la etapa S304, la clave de sesión actual puede expirar en la etapa S305. Aquí, "caducado" significa que la clave de sesión actual ya no se puede utilizar en las comunicaciones entre el primer y segundo dispositivo. Por ejemplo, la clave de sesión caducada se puede eliminar de la memoria o se puede retener, pero marcar como "caducada" para impedir que esa clave se utilice en el futuro. Como se describió anteriormente, un dispositivo puede determinar cuándo va a caducar una clave de sesión según una regla predefinida, que define cuándo termina una sesión y comienza la otra. La clave de sesión actual caduca al final de la sesión actual, y la clave de la siguiente sesión se usa cuando comienza la siguiente. La siguiente sesión puede comenzar inmediatamente después de que finalice la sesión actual, o algún tiempo después de que finalice la sesión actual.

Aunque la clave de sesión actual haya caducado, ambos dispositivos tienen ahora la clave de la siguiente sesión que se transmitió previamente en la etapa S304. Por lo tanto, en la etapa S306, el primer y segundo dispositivo pueden continuar comunicándose en la siguiente sesión usando la siguiente clave de sesión para cifrar las comunicaciones. Por lo tanto, los dispositivos de un sistema de satélite pueden utilizar el procedimiento de la figura 3 para distribuir periódicamente nuevas claves de sesión de forma segura, sin la necesidad de una infraestructura de gestión de claves por tercero. Cambiar regularmente las claves de sesión que se utilizan para el cifrado proporciona seguridad adicional, ya que controla la cantidad de datos cifrados con la misma clave, lo que reduce la cantidad de datos disponibles en

un tiempo determinado para que un agresor los utilice en un ataque de fuerza bruta.

Aunque el procedimiento de la figura 3 se ha descrito anteriormente en relación con la comunicación entre una estación de control y un satélite, en otras realizaciones el procedimiento puede ser utilizado por cualquier dispositivo dentro de un sistema de satélite.

La expiración de la clave puede ser manejada por cualquier dispositivo en el sistema de satélite, que no necesariamente tiene que ser el mismo dispositivo que es responsable de distribuir nuevas claves de sesión. En la presente realización, la caducidad de la clave la gestiona el satélite y la distribución de la clave la gestiona la estación de control. Hacer que el satélite sea responsable de la expiración de la clave permite que el satélite aplique el acceso de seguridad al satélite. Ahora se describirá un procedimiento para hacer que caduque una clave de sesión en un sistema de satélite con referencia a la figura 4.

Primero, en la etapa S401, un dispositivo comienza a usar una clave de sesión actual para cifrar las comunicaciones en un sistema de satélite. Por ejemplo, el dispositivo puede comenzar a usar la clave de sesión actual después de que la clave de sesión anterior haya expirado, como se describió anteriormente con referencia a la figura 3.

Mientras la clave de sesión actual está en uso, el dispositivo puede verificar repetidamente si se debe iniciar una nueva sesión según reglas predeterminadas. En la presente realización, las reglas predeterminadas definen límites predeterminados para una pluralidad de indicadores de uso, y el dispositivo determina que la clave de sesión actual debe expirar y comenzar una nueva sesión si se ha alcanzado o excedido alguno de los límites predeterminados. Por ejemplo, el dispositivo puede realizar la verificación periódicamente y/o puede realizar la verificación cada vez que se transmiten o reciben datos cifrados utilizando la clave de sesión actual. En la presente realización, los indicadores de uso incluyen una cantidad de datos que se han cifrado con la clave de sesión actual hasta el momento actual, y un período de tiempo total durante el cual la clave de sesión actual ha estado en uso, aunque diferentes indicadores de uso podrían ser usados. En otras realizaciones, puede usarse una regla o una pluralidad de reglas predeterminadas diferentes.

Específicamente, en la etapa S402 el dispositivo verifica si la cantidad total de datos enviados y recibidos usando la clave de sesión actual ha alcanzado o excedido el límite de datos predefinido, y si no, en la etapa S403 el dispositivo verifica si la clave de sesión actual ha estado en uso durante un período de tiempo predeterminado. Si el resultado de ambas comprobaciones es negativo, el dispositivo vuelve a la etapa S401 y continúa usando la clave de sesión actual. Sin embargo, si el resultado de cualquiera de las comprobaciones es positivo, entonces el dispositivo hace que expire la clave de sesión actual en la etapa S404.

La cantidad total de datos que se han cifrado con la clave de sesión actual puede incluir datos que ha recibido el dispositivo, así como datos que han sido transmitidos por el dispositivo. Como ejemplo, cuando el dispositivo es una estación de control dispuesta para transmitir mensajes de comando, que también pueden denominarse telecomandos, al satélite, el número total de mensajes de comando que se han cifrado utilizando la clave de sesión actual se puede registrar como la cantidad total de datos. Como otro ejemplo, cuando el dispositivo es un satélite de observación de la Tierra dispuesto para transmitir datos de observación de la Tierra a los usuarios terrestres a través de un flujo de datos, la cantidad total de datos puede ser la cantidad total de datos transmitidos a través del flujo de datos utilizando la clave de sesión actual.

El riesgo de que una clave de sesión se vea comprometida, por ejemplo, por un tercero que rompa el cifrado mediante una estrategia de fuerza bruta, puede aumentar a medida que se cifran y transmiten más datos utilizando la clave de sesión actual, y en la medida en que la clave de sesión actual sea usada durante períodos de tiempo más largos. Por lo tanto, un procedimiento como el que se muestra en la figura 4 puede garantizar que la clave de sesión actual caduque y se reemplace por una nueva clave de sesión antes de que el riesgo de una violación de seguridad sea demasiado alto.

Con referencia ahora a la figura 5, se ilustra un mensaje de distribución de claves para distribuir una clave de sesión en un sistema de satélite, según una realización de la presente invención. El mensaje 500 de distribución de claves incluye una parte de datos de clave 501 y una parte de integridad 502. En otras realizaciones, la parte de integridad 502 puede ser eliminada. La parte de datos clave 501 incluye un identificador de usuario (ID) 503, datos efímeros 504 y datos de clave protegidos 505. Los datos efímeros 504 dependen del algoritmo criptográfico usado y pueden incluir una clave efímera para usar en la derivación de un secreto compartido.

En la presente realización, los datos de clave protegida 505 contienen atributos de seguridad 506 sobre la clave de sesión que se está transmitiendo, así como la clave de sesión en sí 507. En otras realizaciones, la información de

seguridad 506 puede omitirse y los datos de clave cifrada 505 solo pueden incluir la clave cifrada 507. Se puede utilizar un atributo de seguridad para habilitar una función o servicio de seguridad, como el cifrado o el descifrado. Ejemplos de atributos de seguridad que se pueden transmitir en el mensaje de distribución de claves 500 incluyen la clave de sesión siguiente, información de verificación de integridad, información de validez de clave para definir el período durante el cual la clave es válida y reproducir información de detección para garantizar que la clave no ha sido utilizada antes. Los atributos de seguridad también pueden incluir otra información, como los derechos asociados con el rol del usuario y los derechos de acceso para diferentes usuarios que se pueden almacenar junto con las claves públicas de los diferentes usuarios. Estos se pueden usar para identificar a los usuarios que están autorizados, por ejemplo, a controlar el satélite, controlar un módulo criptográfico en el satélite, cargar o eliminar las claves públicas de otros usuarios, etc.

En la presente realización, un dispositivo receptor almacena claves públicas para una pluralidad de otros dispositivos en el sistema de satélite. El dispositivo receptor, por ejemplo, el satélite o la estación de control de la figura 1, obtiene el mensaje de distribución de claves 500 a partir de los datos recibidos, identifica la fuente del mensaje de distribución de claves 500 basándose en el identificador de usuario 503 y deriva el secreto compartido asociado con ese usuario con el fin de descifrar los datos de clave cifrados 505. De esta forma, el dispositivo puede utilizar el secreto compartido para obtener los atributos de seguridad 506 y la clave de sesión 507. Debido a que se usa cifrado asimétrico, solo el dispositivo para el cual está destinado el mensaje de distribución de claves 500 puede obtener los atributos de seguridad 506 y la clave de sesión 507. Mecanismos de ejemplo para derivar el secreto compartido incluyen ECDH y HMQV. Los atributos de seguridad se pueden obtener, por ejemplo, mediante el uso de Ajuste de Clave (Keywrap) Estándar de Cifrado Avanzado (AES) con relleno (padding).

El dispositivo responsable de la distribución de claves de sesión en el sistema de satélite puede almacenar atributos de seguridad separados para diferentes dispositivos en el sistema de satélite. Ejemplos de atributos de seguridad que se pueden almacenar para cada otro dispositivo incluyen una identificación de usuario del otro dispositivo, una clave pública del otro dispositivo, información de detección de reproducción, una clave de sesión actualmente en uso por el otro dispositivo e información de validez de clave que define un período en el que la clave de sesión actual es válida.

La información de detección de reproducción puede ser utilizada por un dispositivo que recibe el mensaje de distribución de claves 500 para determinar si el mismo mensaje de distribución de claves 500 se ha transmitido previamente, lo que puede ser un indicador de que el mensaje recibido es uno que se ha reproducido por un agresor, por ejemplo, para engañar al dispositivo receptor para que use la clave de sesión incorrecta. Si el mensaje se ha reproducido, esto significa que la clave de sesión cifrada 507 incluida en el mensaje de distribución de claves 500 se ha transmitido previamente. Para detectar cuándo se ha reproducido un mensaje de distribución de claves, el dispositivo responsable de distribuir nuevas claves de sesión puede incluir información de detección de reproducción única en el mensaje cada vez que se transmite un mensaje de distribución de claves.

La información de detección de reproducción cambia de un mensaje al siguiente de una manera predecible. Un ejemplo de información de detección de reproducción es un contador, es decir, un valor numérico incluido en una posición predeterminada en el mensaje de distribución de claves. El valor del contador se incrementa de un mensaje de distribución de claves al siguiente. Por ejemplo, el primer mensaje transmitido después de que se inicializa el sistema puede incluir el valor del contador 1, el segundo mensaje puede incluir el valor del contador 2, el tercer mensaje puede incluir el valor del contador 3, y así sucesivamente. Se entenderá que un contador es solo un ejemplo de información de detección de reproducción, y otro ejemplo podría ser un número seudoaleatorio (NSA) obtenido mediante un algoritmo conocido tanto por el remitente como por el receptor. El uso de la información de detección de reproducción se describirá con más detalle más adelante con referencia a la figura 9.

Se entenderá que, aunque en la figura 5 se muestra una estructura ejemplar de un mensaje de distribución de claves, la presente invención no se limita a esta estructura particular y en otras realizaciones de la invención se pueden usar diferentes estructuras de mensajes para el mensaje de distribución de claves. Por ejemplo, si se requiere compatibilidad con un estándar de comunicaciones particular, una realización de la presente invención podría adaptar una estructura de mensaje definida en ese estándar como un mensaje de distribución de claves.

Haciendo referencia ahora a la figura 6, se ilustra un mensaje de distribución de claves en un sistema que funciona según un estándar del Comité Consultivo para Sistemas de Datos Espaciales (CCSDS) según una realización de la presente invención. En la presente realización, el mensaje de distribución de claves 500 de la figura 5 se adjunta a un telecomando de la capa de transferencia cifrada 600 y se transmite como datos de la capa de codificación CCSDS 601. Esta estrategia de transmisión puede ser utilizada, por ejemplo, por una estación de control que está dispuesta para enviar telecomandos a un satélite con el fin de controlar el satélite. Se entenderá que también se puede usar una estrategia similar para transmitir un mensaje de distribución de claves en sistemas que operan según protocolos

distintos de CCSDS, y se puede aplicar para otras capas de seguridad en diferentes posiciones dentro de la pila.

Cuando un satélite recibe la transmisión que se muestra en la figura 6, que incluye un mensaje de distribución de clave 500 vinculado a un mensaje de telecomando 600, el satélite descifra el mensaje de telecomando 600 utilizando la clave de sesión actual que es actualmente válida para transmisiones entre el satélite y el dispositivo fuente desde el que se recibió la transmisión. La clave de sesión actual puede ser una que se haya recibido previamente y que sea válida durante un período de tiempo en el que se recibió el telecomando 600, o puede ser una nueva clave de sesión definida en el mensaje de distribución de claves 500 precedido por el telecomando recibido 600. En una realización de la presente invención, una estación de control está dispuesta para transmitir únicamente un mensaje de distribución de claves a un satélite cuando se inicia una nueva sesión. En esta realización, el satélite está dispuesto para responder a un mensaje de distribución de clave haciendo que caduque la clave de sesión anterior y usando la clave de sesión recibida como clave de sesión actual. Por lo tanto, el inicio de una nueva sesión se indica mediante la presencia de un mensaje de distribución de claves, lo que significa que no es necesario transmitir también información de validez que defina el período en el que cada clave de sesión es válida.

En la presente realización, la información de detección de reproducción se incluye en el mensaje de distribución de claves 500 como se describió anteriormente con referencia a la figura 5. El satélite puede comprobar la información de detección de reproducción recibida para determinar si el mensaje de distribución de claves 500 es auténtico.

El mensaje de distribución de claves 500 también se puede vincular al telecomando 600, como se muestra en la figura 6. Esto permite al satélite determinar que el telecomando 600 es auténtico si se determina que el mensaje de distribución de claves 500 también es auténtico. Una vez que se ha verificado la autenticidad del mensaje 500 de distribución de claves y el telecomando 600, el telecomando 600 puede pasarse a su función de destino dentro de la nave espacial, por ejemplo, el ordenador de la nave espacial, la carga útil o el controlador criptográfico.

En otra realización, la información de detección de reproducción se incluye en el telecomando 600 en lugar del mensaje de distribución de claves 500. El satélite puede utilizar la información de detección de reproducción para determinar si el telecomando es auténtico, y si se determina que el telecomando es auténtico, se supone que el mensaje de distribución de claves y la clave contenida en él también son válidos.

Cuando un mensaje de distribución de claves 500 está vinculado a un telecomando 600, la información de detección de reproducción se puede compartir entre el mensaje de distribución de claves 500 y el telecomando 600. Por lo tanto, no es necesario incluir información de detección de reproducción tanto en el mensaje de distribución de claves 500 como en el telecomando 600.

Aunque la presente realización se describe en relación con una estación de control que envía un mensaje de telecomando a un satélite, en otras realizaciones se puede aplicar una estrategia similar a la utilizada en la figura 6 a las comunicaciones entre dos dispositivos cualesquiera en un sistema de satélite, transmitiendo un mensaje de distribución de claves vinculado a otro mensaje, que podría ser un telecomando o podría ser cualquier otro tipo de mensaje.

Con referencia ahora a la figura 7, se ilustra la transmisión de un mensaje de distribución de claves a través de un flujo de telemetría CCSDS, según una realización de la presente invención. Se puede recibir un flujo de telemetría CCSDS de un satélite, por ejemplo, mediante un equipo terrestre, como una estación de control, para monitorear el estado del satélite. Aunque la presente realización se describe en relación con un flujo de telemetría CCSDS, se entenderá que la presente invención no se limita al estándar CCSDS y se pueden usar realizaciones para distribuir claves de sesión a través de cualquier tipo de flujo de datos.

Como se muestra en la figura 7, el flujo de datos de telemetría CCSDS 710 se divide en una pluralidad de cuadros de transferencia, cada uno de los cuales incluye un encabezado primario de cuadro de transferencia y datos de cuadro de transferencia. Los datos del cuadro de transferencia contienen bytes de los datos que se están transmitiendo a través del flujo de datos, que en la presente realización son datos de telemetría, pero, en general, podrían ser cualquier tipo de datos. El encabezado primario del cuadro de transferencia es el encabezado del cuadro de transferencia estándar definido en el estándar CCSDS.

Además, en la presente realización cada cuadro de transferencia incluye un aencabezado secundario 711 del cuadro de transferencia que se utiliza para proporcionar un flujo de distribución de claves a uno o más receptores. En particular, cada encabezado secundario 711 del cuadro de transferencia incluye un ID de encabezado 712, una marca de tiempo (TS) 713 y una parte de entrega de clave 714 que contiene un número predeterminado de bytes de un flujo de distribución de claves 715. De esta manera, el flujo de distribución de claves 715 se subconmuta en el flujo de

datos de telemetría 710. Un dispositivo que recibe el flujo de datos de telemetría 710 puede reconstruir el flujo de distribución de claves 715 extrayendo los bytes de entrega de claves 714 del encabezado secundario del cuadro de transferencia 711 de cada cuadro y combinando los bytes extraídos.

Los bytes de entrega de claves 714 y los datos del cuadro de transferencia están protegidos usando las claves públicas/privadas de las partes asociadas, y el receptor puede usar el TS 713 para identificar qué clave de sesión usar para descifrar y/o autenticar los datos del cuadro de transferencia. Específicamente, el TS 713 indica el momento en el que el satélite transmitió ese cuadro de transferencia y, por lo tanto, determina qué clave de sesión usó el satélite para proteger los datos en el cuadro de transferencia.

Por ejemplo, un satélite puede transmitir un flujo de telemetría que incluye un mensaje de distribución de claves para el usuario A y un mensaje de distribución de claves para el usuario B. Cada mensaje de distribución de claves incluye una clave de sesión actual y una clave de sesión siguiente, e información de validez que define el período en que cada clave es válida, como se muestra a continuación:

Mensaje de distribución de clave del Usuario A:

Clave 1, cifrada para el usuario A, válida de 12:00 a 14:59
Clave 2, cifrada para el usuario A, válida de 15:00 a 17:59

Mensaje de distribución de clave del Usuario B:

Clave 1, cifrada para el usuario B, válida de 12:00 a 14:59
Clave 2, cifrada para el usuario B, válida de 15:00 a 17:59

Los períodos de validez se definen con referencia al reloj interno del satélite. Si, por ejemplo, se recibe un cuadro de transferencia con una marca de tiempo de 15:00 cuando el reloj interno del receptor indica un tiempo de 14:59, el receptor determinará que la clave 2 es la clave de sesión actual basándose en la marca de tiempo recibida, aunque el reloj interno del receptor parecería indicar que la clave de sesión actual es en realidad la clave 1.

En el ejemplo anterior, si el usuario A recibe un cuadro de transferencia que incluye la marca de tiempo "12:20", el receptor puede determinar que la clave de sesión actual es la clave 1, válida de 12:00 a 14:59. Por lo tanto, el receptor utiliza la clave 1 para descifrar y/o autenticar los bytes de entrega de claves y transferir los datos del cuadro en el cuadro de transferencia actual. Sin embargo, cuando el usuario A recibe posteriormente un cuadro de transferencia que incluye la marca de tiempo "15:00", el receptor determina que la clave 2 es ahora la clave de sesión actual, por lo tanto, utiliza la clave 2 para descifrar y/o autenticar los bytes de entrega de claves y transferir los datos del cuadro.

Además, cuando o después de que la marca de tiempo pase de 14:59 a 15:00, el contenido de los mensajes de distribución de claves cambiará para reflejar las nuevas claves de sesión 'actual' y 'siguiente', de la siguiente manera:

Mensaje de distribución de clave del Usuario A:

Clave 2, cifrada para el usuario A, válida de 15:00 a 17:59
Clave 3, cifrada para el usuario A, válida de 18:00 a 20:59

Mensaje de distribución de clave del Usuario B:

Clave 2, cifrada para el usuario B, válida de 15:00 a 17:59
Clave 3, cifrada para el usuario B, válida de 18:00 a 20:59

Aunque en la presente realización la marca de tiempo y los períodos de validez se definen en horas y minutos, en otras realizaciones la marca de tiempo y los períodos de validez podrían definirse, por ejemplo, usando un contador arbitrario.

Además, aunque en la presente realización el receptor usa una marca de tiempo en el cuadro de transferencia para determinar qué clave de sesión usar para ese cuadro de transferencia, en otras realizaciones se puede omitir la marca de tiempo. Por ejemplo, el receptor podría obtener información sobre un desfase entre el reloj interno del receptor y el reloj interno del satélite, por ejemplo, a partir de un desfase de tiempo calculado al obtener una posición fija del sistema de posicionamiento global (GPS). El receptor podría utilizar la hora local en la que se recibió el cuadro de transferencia, el desfase entre los relojes del receptor y del satélite, y un tiempo de viaje estimado de la señal para estimar la hora

según el reloj del satélite en el que se transmitió el cuadro de transferencia.

Como se muestra en la figura 7, el flujo de distribución de claves 715 incluye mensajes de distribución de claves 700 para una pluralidad de grupos de usuarios. Cada grupo de usuarios podría representar un solo usuario o podría incluir una pluralidad de usuarios que compartirán las mismas claves de sesión y, por lo tanto, tendrán acceso a los mismos datos. Cada mensaje de distribución de claves 700 puede, por ejemplo, formatearse como se muestra en la figura 5. En un flujo de datos como el flujo 710 que se muestra en la figura 7, los datos destinados a diferentes grupos de usuarios pueden cifrarse utilizando diferentes claves simétricas y transmitirse a través del flujo de datos. Al proporcionar mensajes de distribución de claves separados para diferentes grupos de usuarios, cada grupo de usuarios puede recibir su propia clave simétrica para descifrar sus propios datos, mientras se impide que los usuarios de un grupo accedan a los datos destinados a otro grupo de usuarios. La clave de cada grupo de usuarios puede caducar periódicamente y reemplazarse por una clave actualizada.

La estrategia ilustrada en la figura 7 proporciona un mecanismo de entrega de claves de ancho de banda eficiente para múltiples terminales terrestres, y puede implementarse usando protocolos existentes, como el estándar de telemetría de paquetes CCSDS. Específicamente, el ancho de banda en el flujo de datos de telemetría se conserva porque solo se pasa un pequeño número de bytes del flujo de distribución de claves en cada cuadro de enlace descendente. Por lo tanto, la presente realización puede proporcionar claves de sesión a uno o más usuarios finales sin ningún impacto significativo en el ancho de banda disponible para los datos del flujo de transferencia primario, que en la presente realización son datos de telemetría. La estrategia se puede utilizar para distribuir claves a terminales en el sistema de satélite que tienen una capacidad de solo recepción y, como tales, no tienen un mecanismo mediante el cual puedan cargar una clave para su uso. Por ejemplo, un satélite de observación de la Tierra puede utilizar la estrategia mostrada en la figura 7 para distribuir claves de sesión a través de un flujo de datos a una pluralidad de receptores terrestres operados por usuarios autorizados.

Como ejemplo, en un sistema típico de observación de la Tierra en el que el enlace descendente funciona a 150 megabits por segundo (Mbps), con cuadros de 16 kilobits (Kbits), la marca de tiempo se ajusta cada 5 días. Si cada clave tuviera un tamaño de 1024 bits y hubiera 500 usuarios finales, cada usuario tardaría poco más de 3 segundos en recibir su clave actual y la siguiente. En otro ejemplo, en un sistema típico de comunicaciones de seguimiento y comando de telemetría (TT&C) en el que el enlace descendente funciona a 64 kilobits por segundo (Kbps), con un tamaño de cuadro de 4 Kbits, la marca de tiempo se ajusta cada 8,5 años, y con 3 usuarios finales, los usuarios tardarían aproximadamente 12 segundos en recibir sus claves actuales y siguientes.

Aunque en la presente realización las claves de sesión se distribuyen a través de un flujo de telemetría CCSDS que incluye una pluralidad de cuadros, en otras realizaciones las claves de sesión se pueden distribuir a través de cualquier flujo de datos que esté dividido en una pluralidad de partes predefinidas, que, por ejemplo, pueden denominarse cuadros o paquetes según el estándar particular elegido para esa realización. Los mensajes de distribución de claves se pueden incluir en el flujo de datos usando subconmutación, incluyendo un número predeterminado de bytes del mensaje de distribución de claves en cada parte del flujo de datos.

Con referencia ahora a la figura 8, se ilustra un procedimiento para recibir una clave de sesión en un sistema de satélite, según una realización de la presente invención. El procedimiento puede ser utilizado por cualquier dispositivo en un sistema de satélites, incluidos, entre otros, un satélite u otra nave espacial, una estación de control y un receptor de usuario final (por ejemplo, receptor de transmisión de televisión).

Primero, en la etapa S801, se recibe una clave de sesión protegida. Por ejemplo, la clave de sesión se puede proteger mediante cifrado y/o autenticación. La clave de sesión puede recibirse en un mensaje de distribución de claves como el que se muestra en la figura 5, y podría recibirse vinculada a un telecomando como se muestra en la figura 6 o a través de un flujo de datos de telemetría como se muestra en la figura 7.

Luego, en la etapa S802, la clave de sesión protegida es autenticada y/o descifrada en base a la clave privada del receptor y la clave pública del remitente. Por ejemplo, se puede obtener un secreto compartido mediante ECDH o HMQV y utilizar para descifrar la clave de sesión. Una vez que la clave de sesión recibida se ha descifrado y/o autenticado, se puede utilizar en comunicaciones posteriores entre los dos dispositivos en el sistema de satélite.

Con referencia ahora a la figura 9, se ilustra un procedimiento de uso de la información de detección de reproducción, según una realización de la presente invención. Al igual que con el procedimiento de la figura 8, el procedimiento de la figura 9 puede ser utilizado por cualquier dispositivo en un sistema de satélite.

Primero, en la etapa S901, se recibe información de detección de reproducción junto con una clave de sesión cifrada.

En la presente realización, la información de detección de reproducción se incluye en un comando vinculado a la clave de sesión cifrada como se muestra en la figura 6. Sin embargo, en otra realización, la información de detección de reproducción se puede incluir con la clave cifrada en un mensaje de distribución de claves como se muestra en figura 5. Cuando se recibe la información de detección de reproducción, en la etapa S902 el dispositivo receptor compara el valor de la información de detección de reproducción recibida con el valor recibido previamente, es decir, el valor de la información de detección de reproducción en el último mensaje exitoso que precede al mensaje de distribución de claves actual.

En la etapa S903, se comprueba si se cumple una condición predeterminada. Un ejemplo de una condición predeterminada podría ser si el valor actual de la información de detección de reproducción es mayor que el valor anterior. Si el valor actual es mayor, se supone que el mensaje no se ha vuelto a reproducir. Sin embargo, si el valor actual es igual o menor que el valor anterior, se determina que el mensaje es un mensaje anterior que se ha reproducido. Una condición alternativa podría ser si el valor recibido de la información de detección de reproducción coincide con un valor esperado, que es el valor siguiente en una secuencia conocida. Otro ejemplo más de una condición predeterminada podría ser si el valor actual cae dentro de un intervalo predeterminado de valores aceptables que son mayores que el valor anterior, pero dentro de un cierto intervalo del valor anterior.

Si se satisface la condición predeterminada, entonces en la etapa S904 se determina que el mensaje de comando vinculado al mensaje de distribución de claves recibido no se ha reproducido y, por lo tanto, el mensaje de distribución de claves tampoco se ha reproducido. Por consiguiente, se determina que la clave de sesión cifrada recibida es auténtica y se puede usar, y el valor anterior almacenado de la información de detección de reproducción se reemplaza por el valor actual. Por otro lado, si no se satisface la condición predeterminada, entonces en la etapa S905 se determina que el mensaje de comando recibido y la clave de sesión cifrada vinculada se han reproducido y no deberían usarse.

Utilizando información de detección de reproducción como se muestra en la figura 9, la seguridad de un sistema de satélite puede mejorarse detectando cuando un agresor ha reproducido un mensaje en un intento de comprometer el sistema.

Con referencia ahora a la figura 10, se ilustra un dispositivo para transmitir una clave de sesión en un sistema de satélite, según una realización de la presente invención. En la presente realización, el dispositivo 1000 es un satélite, pero en otras realizaciones, el dispositivo 1000 podría ser un equipo terrestre, como la estación de control que se muestra en la figura 1.

El satélite 1000 comprende un módulo de obtención de claves 1001 dispuesto para obtener una clave de sesión, un módulo de protección de claves 1002 dispuesto para proteger la clave de sesión obtenida en base a una clave privada del satélite y una clave pública de un dispositivo al que la clave de sesión se va a transmitir, por ejemplo, aplicando cifrado y/o autenticación, y un módulo transmisor 1003 dispuesto para transmitir la clave de sesión protegida al dispositivo. Además, en la presente realización, el satélite 1000 incluye un generador de información de detección de reproducción 1004 para generar información de detección de reproducción. El módulo transmisor 1003 recibe la clave de sesión protegida del módulo de protección de clave 1002 y recibe la información de detección de reproducción del generador de información de detección de reproducción 1004, y transmite la clave de sesión protegida y la información de detección de reproducción a otro dispositivo en el sistema de satélite, por ejemplo como un mensaje de distribución de claves vinculado a un mensaje de comando, o mediante un flujo de datos. En otras realizaciones, el generador 1004 de información de detección de reproducción se puede omitir si no se requiere información de detección de reproducción.

Con referencia ahora a la figura 11, se ilustra un dispositivo para recibir una clave de sesión en un sistema de satélite, según una realización de la presente invención. En la presente realización, el dispositivo 1100 es un satélite, pero en otras realizaciones, el dispositivo 1100 podría ser un equipo terrestre, como la estación de control que se muestra en la figura 1.

El satélite 1100 comprende un módulo receptor 1101 dispuesto para recibir una clave de sesión protegida desde otro dispositivo en el sistema de satélite. Por ejemplo, la clave de sesión protegida puede recibirse como un mensaje de distribución de claves vinculado a un telecomando como se muestra en la figura 6, o recibirse a través de un flujo de datos de telemetría como se muestra en la figura 7. El satélite 1100 comprende además un módulo de extracción de claves 1103 dispuesto para extraer la clave de sesión de un mensaje recibido, por ejemplo, descifrando y/o autenticando la clave de sesión protegida, basada en una clave privada del satélite y una clave pública del dispositivo desde el que se recibió la clave de sesión. Además, en la presente realización el satélite 1100 comprende además un módulo de detección de reproducción 1102 dispuesto para recibir información de detección de reproducción desde el

módulo receptor 1101, que puede extraer la información de detección de reproducción de un mensaje de distribución de claves recibido o un telecomando. El módulo de detección de reproducción 1102 compara la información de detección de reproducción recibida con un valor esperado de la información de detección de reproducción, como se describió anteriormente con referencia a la figura 9. Si la información de detección de reproducción recibida satisface una condición predeterminada, como se describió anteriormente con referencia a la etapa S903 de la figura 9, el módulo de detección de reproducción 1102 señala al módulo de extracción de clave 1103 que la clave de sesión recibida es auténtica y puede pasarse de forma segura a otras funciones dentro del dispositivo 1100 según se requiera. En otras realizaciones, el módulo de detección de reproducción 1102 puede omitirse si no se requiere la detección de reproducción.

Con referencia ahora a la figura 12, se ilustra un procedimiento para autenticar una clave de sesión recibida, según una realización de la presente invención. El procedimiento de la figura 12 es particularmente adecuado para su uso en realizaciones en las que la clave de sesión recibida solo está protegida mediante cifrado. Primero, en la etapa S1201, se recibe la clave de sesión protegida. Luego, en la etapa S1202, se obtiene información sobre una ubicación esperada del transmisor en el momento en que se transmitió la clave de sesión protegida. En la etapa S1203, la ubicación esperada se compara con una ubicación detectada desde la que se recibió la clave de sesión, por ejemplo, detectada por una antena direccional. Cuando la clave de sesión protegida se recibe de un satélite en una órbita geoestacionaria, la ubicación esperada puede ser una posición conocida del satélite. Por otro lado, para un satélite en una órbita no geoestacionaria, la ubicación esperada se puede determinar en función de la información sobre la órbita del satélite, el momento en el que se recibió la clave de sesión protegida y un tiempo de viaje estimado de la señal del satélite al receptor. Cuando la clave de sesión protegida se recibe desde un transmisor fijo, por ejemplo, una estación de control en tierra, la ubicación esperada puede ser una ubicación conocida del transmisor.

A continuación, en la etapa S1204 se comprueba si la ubicación detectada coincide con la ubicación esperada, dentro de un margen de error predeterminado. Si la ubicación detectada coincide con la ubicación esperada, entonces en la etapa S1205 se supone que la clave de sesión recibida es auténtica y puede aceptarse. Por otro lado, si la ubicación detectada no coincide con la ubicación esperada, a continuación, en la etapa S1206, se descarta la clave de sesión recibida.

Se han descrito realizaciones de la presente invención en las que la distribución de claves de sesión en un sistema de satélite es manejada por un dispositivo en el sistema de satélite, por ejemplo el satélite o equipo terrestre tal como una estación de control. En cualquier etapa durante el funcionamiento del sistema de satélite, se puede agregar un nuevo dispositivo al sistema transmitiendo la clave pública del nuevo dispositivo al dispositivo responsable de la distribución de la clave. A continuación, las claves de sesión se pueden distribuir al nuevo dispositivo cifrando las claves de sesión utilizando la clave pública del nuevo dispositivo, utilizando cualquiera de los procedimientos descritos anteriormente. De manera similar, en cualquier etapa durante el funcionamiento del sistema de satélite, un dispositivo puede ser eliminado del sistema eliminando la clave pública de dicho dispositivo del dispositivo responsable de la distribución de la clave. Esto impedirá que al dispositivo eliminado se emitan nuevas claves simétricas.

Aunque se han descrito anteriormente ciertas realizaciones de la presente invención con referencia a los dibujos, la persona experta entenderá que muchas variaciones y modificaciones son posibles sin apartarse del alcance de la invención, tal como se define en las reivindicaciones.

REIVINDICACIONES

1. Un procedimiento para transmitir una clave de sesión (507) en un sistema de satélite que comprende un satélite (102) y un dispositivo (101) dispuesto para recibir señales del satélite, el procedimiento comprende:

obtener la clave de sesión (507) en el satélite (102);
proteger la clave de sesión (507) en el satélite (102), en base a una clave privada del satélite (102) y una clave pública del dispositivo (101); y
transmitir la clave de sesión protegida desde el satélite (102) al dispositivo (101),
donde transmitir la clave de sesión protegida comprende transmitir la clave de sesión protegida a través de un flujo de datos que incluye una pluralidad de partes predefinidas, insertando un número predeterminado de bytes de la clave de sesión protegida en cada una de la pluralidad de partes predefinidas.

2. El procedimiento de la reivindicación 1, donde la transmisión de la clave de sesión protegida comprende transmitir la clave de sesión protegida y la información de detección de reproducción para determinar si la clave de sesión protegida se ha transmitido previamente.

3. El procedimiento de la reivindicación 2, donde la clave de sesión protegida y la información de detección de reproducción se incluyen en un mensaje de distribución de claves (500).

4. El procedimiento de la reivindicación 1, 2 o 3, donde la clave de sesión obtenida es una clave de sesión siguiente para usar en la siguiente sesión después de una sesión actual, el procedimiento comprende además:

obtener una clave de sesión actual para usar en la sesión actual;
proteger la clave de sesión actual en el satélite, basada en una clave privada del satélite y una clave pública del dispositivo;
transmitir la clave de sesión actual a través del flujo de datos; y
transmitir información de validez a través del flujo de datos, definiendo la información de validez un período de tiempo donde la clave de sesión actual es válida y un período de tiempo donde es válida la clave de sesión siguiente.

5. Un procedimiento para obtener una clave de sesión (507) en un sistema de satélite que comprende un satélite (102) y un dispositivo (101) dispuesto para recibir señales del satélite (102), comprendiendo el procedimiento:

recibir un flujo de datos del satélite (102) en el dispositivo (101), incluyendo el flujo de datos una pluralidad de partes predefinidas;
extraer un número predeterminado de bytes de una clave de sesión protegida de cada una de la pluralidad de partes predefinidas;
combinar los bytes extraídos de la clave de sesión protegida para obtener la clave de sesión protegida; y
obtener la clave de sesión (507) de la clave de sesión protegida recibida en el dispositivo (101), en base a una clave pública del satélite (102) y una clave privada del dispositivo (101).

6. El procedimiento de la reivindicación 5, que comprende, además:

obtener información sobre una ubicación esperada del satélite cuando se transmitió la clave de sesión protegida; y
determinar que la clave de sesión protegida recibida es auténtica si una ubicación desde la que se recibió la clave de sesión protegida coincide con la ubicación esperada del satélite, dentro de un margen de error predeterminado.

7. El procedimiento de la reivindicación 5 o 6, donde la clave de sesión obtenida es una clave de sesión siguiente para usar en la siguiente sesión después de una sesión actual, el procedimiento comprende, además:

recibir una clave de sesión actual protegida para usar en la sesión actual, e información de validez que define un período de tiempo en el que la clave de sesión actual es válida y un período de tiempo en el que es válida la clave de sesión siguiente, a través del flujo de datos;
obtener la clave de sesión actual a partir de la clave de sesión actual protegida en el dispositivo, basándose en una clave pública del satélite y una clave privada del dispositivo;
obtener información sobre un momento en el que se transmitieron datos protegidos a través del flujo de datos; y
acceder a los datos protegidos en función de la clave de sesión actual si la información obtenida indica que los datos protegidos fueron transmitidos durante el período de tiempo en el que la clave de sesión actual es válida, o
acceder a los datos protegidos en función de la siguiente clave de sesión si la información obtenida indica que los

datos protegidos se transmitieron durante el período de tiempo en el que la siguiente clave de sesión es válida.

8. Un medio de almacenamiento legible por ordenador dispuesto para almacenar un programa de ordenador que, cuando es ejecutado por un dispositivo, hace que el dispositivo realice un procedimiento según cualquiera de las reivindicaciones anteriores.

9. Un satélite (1000) que comprende:

un módulo de obtención de claves (1001) dispuesto para obtener una clave de sesión;
un módulo de protección de claves (1002) dispuesto para proteger la clave de sesión obtenida, basado en una clave privada del satélite (1000) y una clave pública de un dispositivo (1100) al que se va a transmitir la clave de sesión protegida; y
un transmisor (1003) dispuesto para transmitir la clave de sesión protegida al dispositivo (1100),
donde el transmisor (1003) está dispuesto para transmitir la clave de sesión protegida a través de un flujo de datos que incluye una pluralidad de partes predefinidas, insertando un número predeterminado de bytes de la clave de sesión protegida en cada una de la pluralidad de partes predefinidas.

10. El satélite de la reivindicación 9, que comprende además:

un generador de información de reproducción (1004) dispuesto para generar información de detección de reproducción para determinar si la clave de sesión protegida se ha transmitido previamente,
donde el transmisor está dispuesto para transmitir la clave de sesión protegida y la información de detección de reproducción al dispositivo.

11. Un dispositivo (1100) para recibir señales de un satélite (1000), comprendiendo el dispositivo (1100):

un receptor (1101) dispuesto para recibir un flujo de datos del satélite (1000), incluyendo el flujo de datos una pluralidad de partes predefinidas; y
un módulo de extracción de claves (1103) dispuesto para extraer un número predeterminado de bytes de una clave de sesión protegida de cada una de la pluralidad de partes predefinidas, combinar los bytes extraídos de la clave de sesión protegida para obtener la clave de sesión protegida y obtener la clave de sesión de la clave de sesión protegida basada en una clave privada del dispositivo (1100) y una clave pública del satélite (1000) desde el que se recibió la clave de sesión protegida.

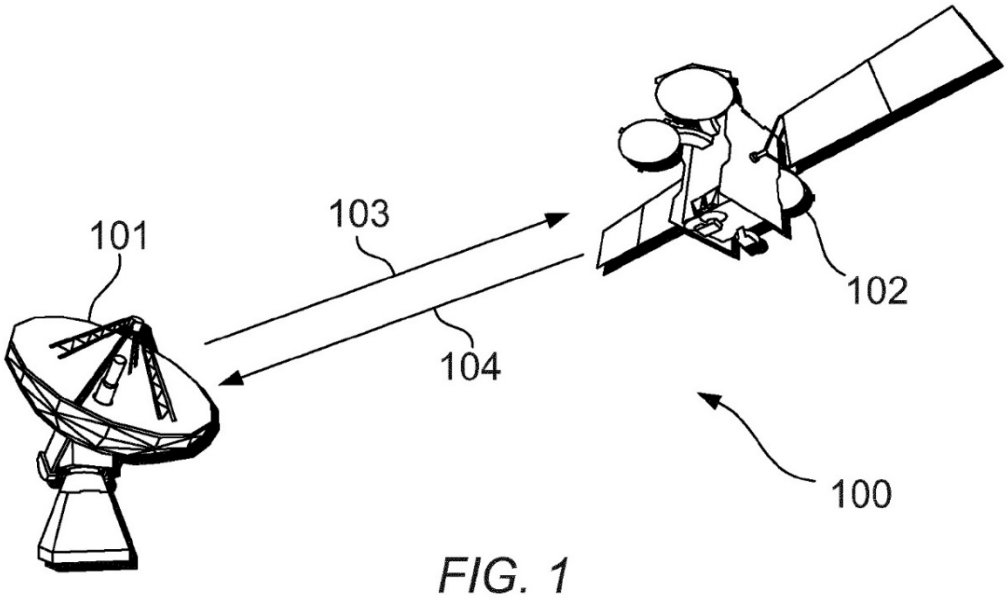

101
103
102
104
100

FIG. 1

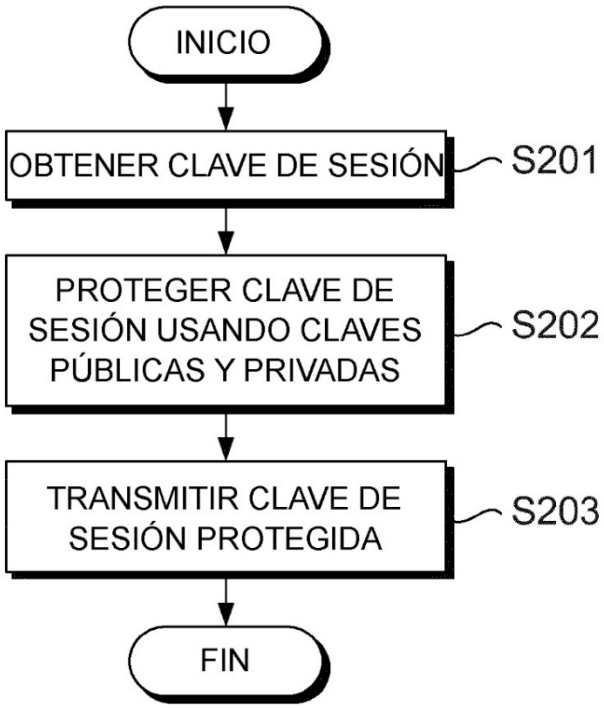

INICIO
OBTENER CLAVE DE SESIÓN
S201
PROTEGER CLAVE DE SESIÓN USANDO CLAVES PÚBLICAS Y PRIVADAS
S202
TRANSMITIR CLAVE DE SESIÓN PROTEGIDA
S203
FIN

FIG. 2

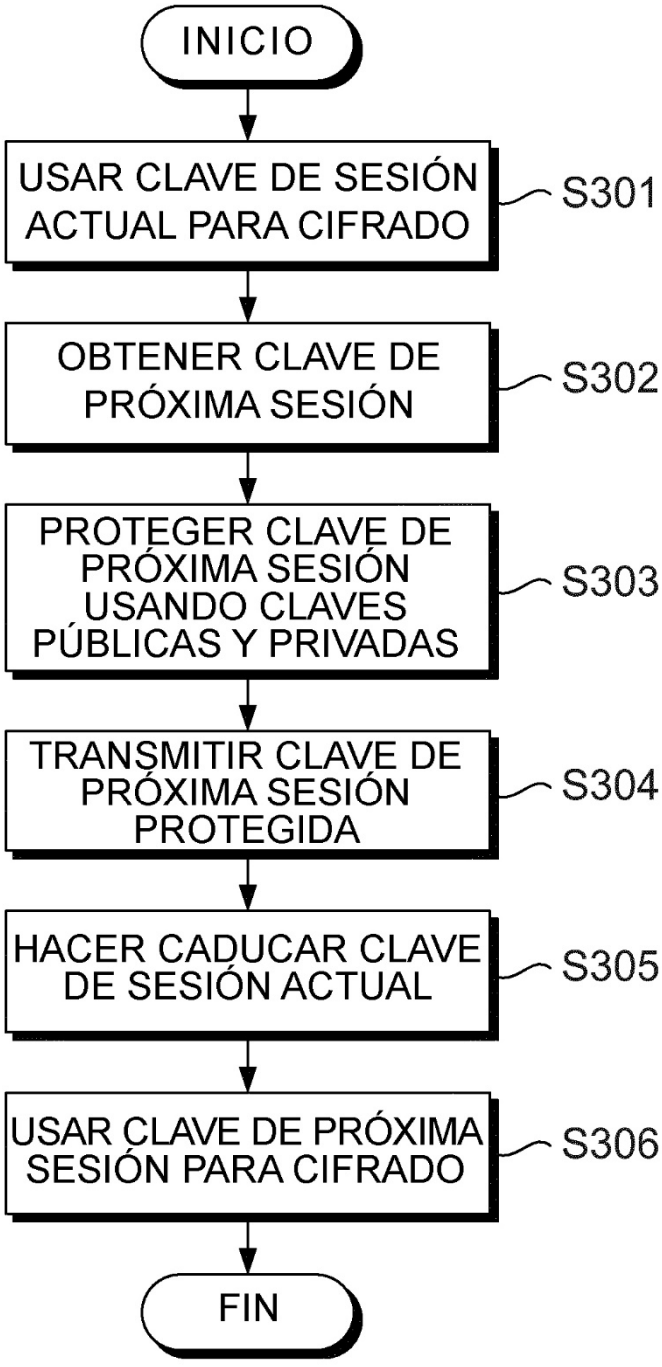

INICIO
USAR CLAVE DE SESIÓN ACTUAL PARA CIFRADO
S301
OBTENER CLAVE DE PRÓXIMA SESIÓN
S302
PROTEGER CLAVE DE PRÓXIMA SESIÓN USANDO CLAVES PÚBLICAS Y PRIVADAS
S303
TRANSMITIR CLAVE DE PRÓXIMA SESIÓN PROTEGIDA
S304
HACER CADUCAR CLAVE DE SESIÓN ACTUAL
S305
USAR CLAVE DE PRÓXIMA SESIÓN PARA CIFRADO
S306
FIN

FIG. 3

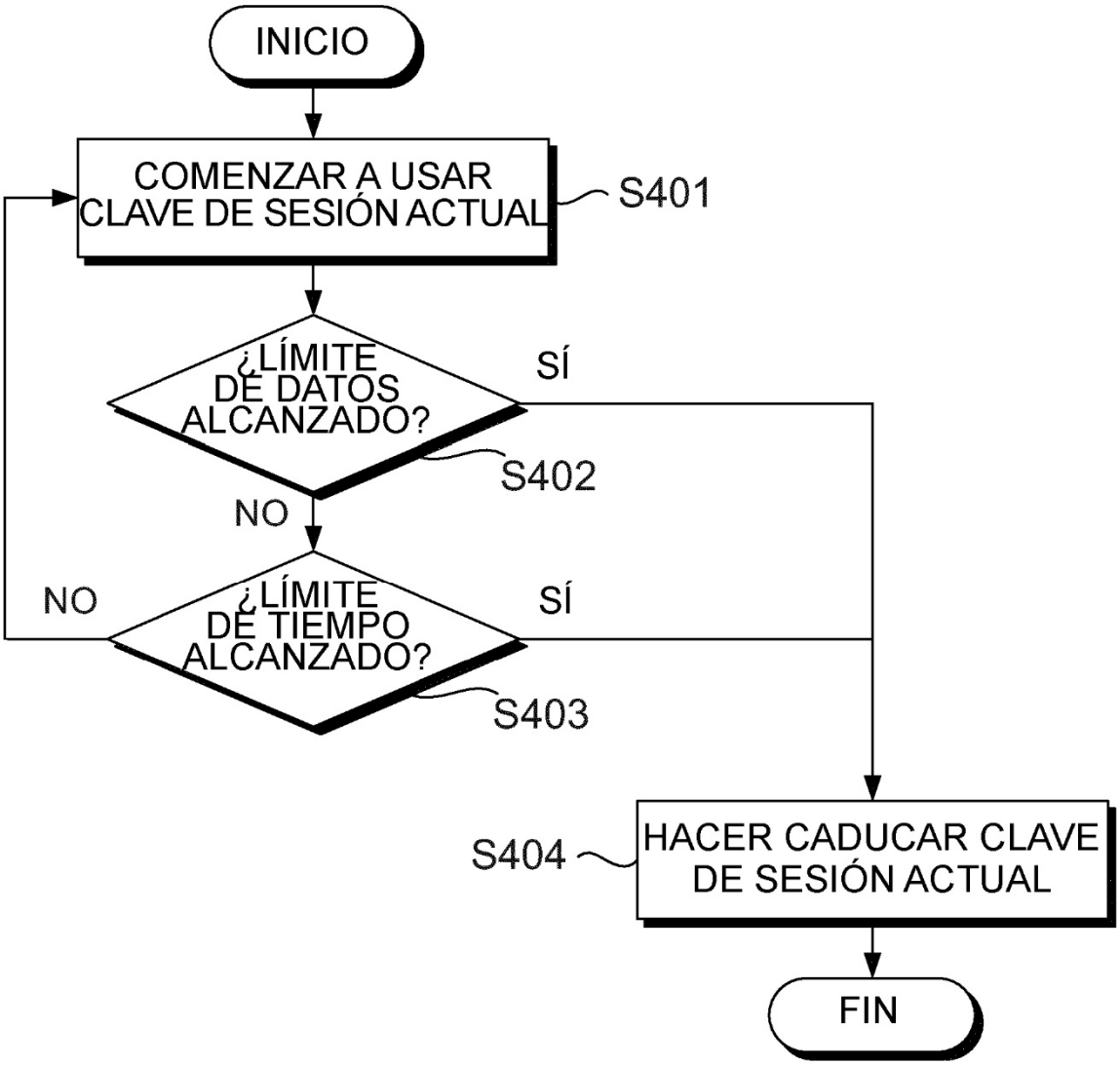

INICIO
COMENZAR A USAR CLAVE DE SESIÓN ACTUAL
S401
¿LÍMITE DE DATOS ALCANZADO?
SÍ
S402
NO
¿LÍMITE DE TIEMPO ALCANZADO?
NO
SÍ
S403
S404
HACER CADUCAR CLAVE DE SESIÓN ACTUAL
FIN

FIG. 4

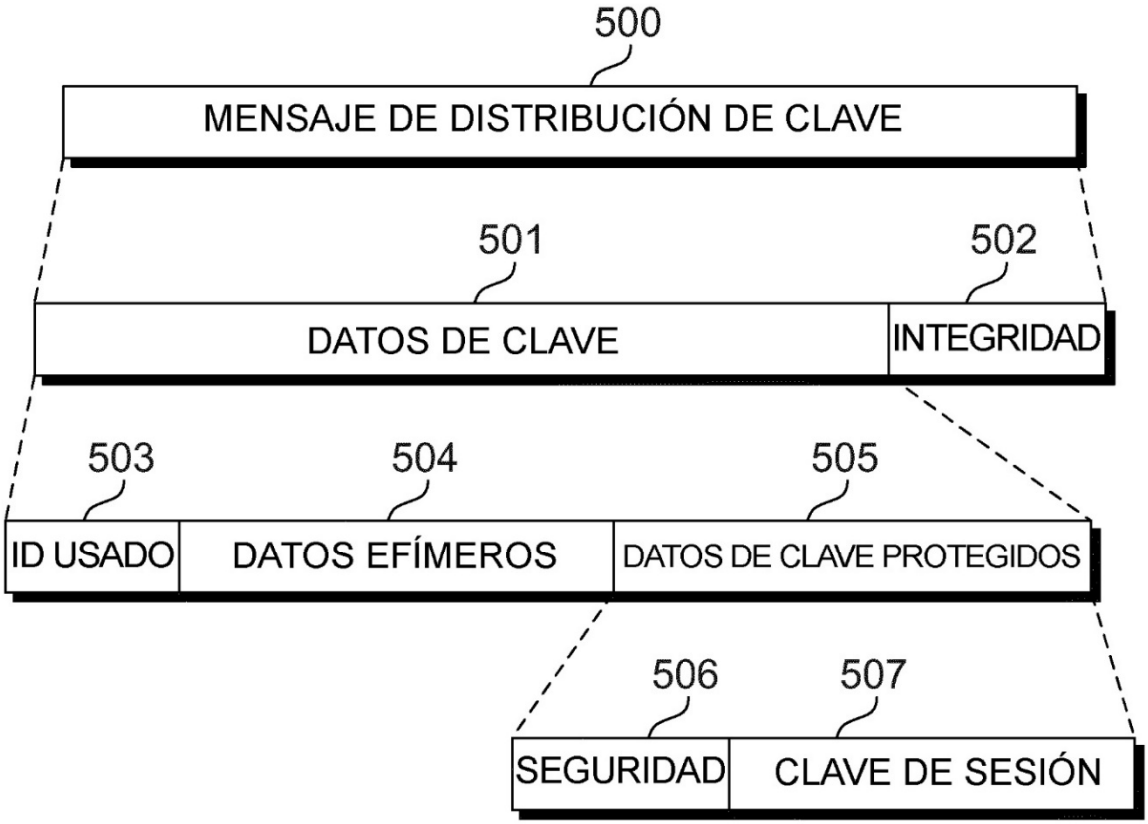

500
MENSAJE DE DISTRIBUCIÓN DE CLAVE
501
502
DATOS DE CLAVE
INTEGRIDAD
503
504
505
ID USADO
DATOS EFÍMEROS
DATOS DE CLAVE PROTEGIDOS
506
507
SEGURIDAD
CLAVE DE SESIÓN

FIG. 5

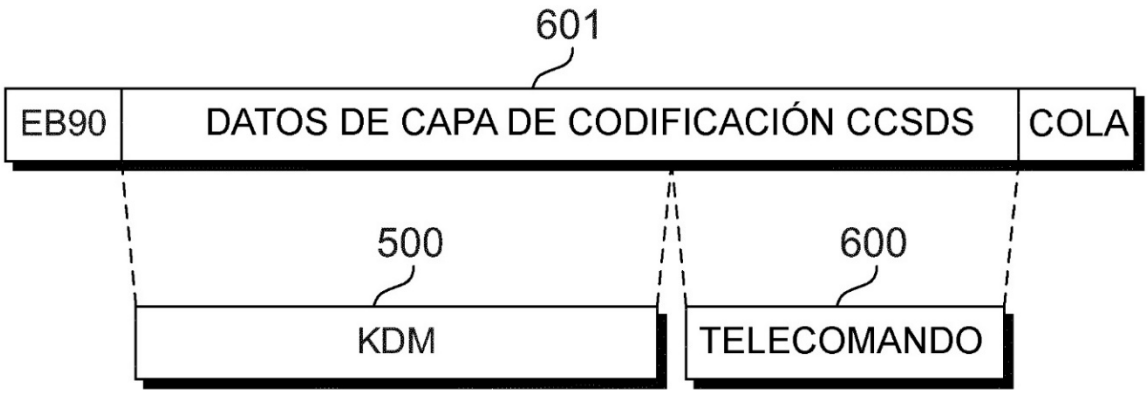

601
EB90
DATOS DE CAPA DE CODIFICACIÓN CCSDS
COLA
500
600
KDM
TELECOMANDO

FIG. 6

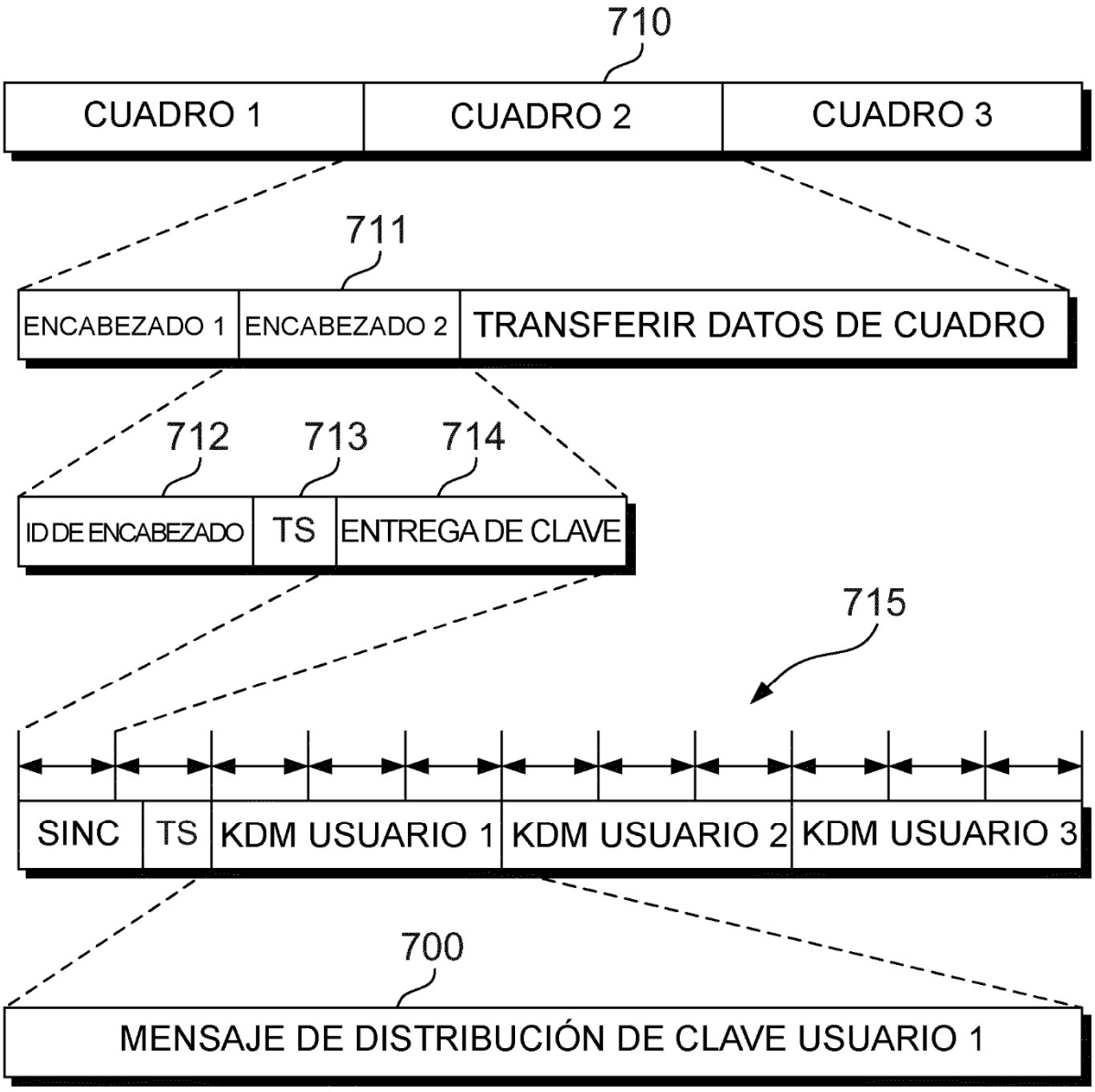

710
CUADRO 1
CUADRO 2
CUADRO 3
711
ENCABEZADO 1
ENCABEZADO 2
TRANSFERIR DATOS DE CUADRO
712
713
714
ID DE ENCABEZADO
TS
ENTREGA DE CLAVE
715
SINC
TS
KDM USUARIO 1
KDM USUARIO 2
KDM USUARIO 3
700
MENSAJE DE DISTRIBUCIÓN DE CLAVE USUARIO 1

FIG. 7

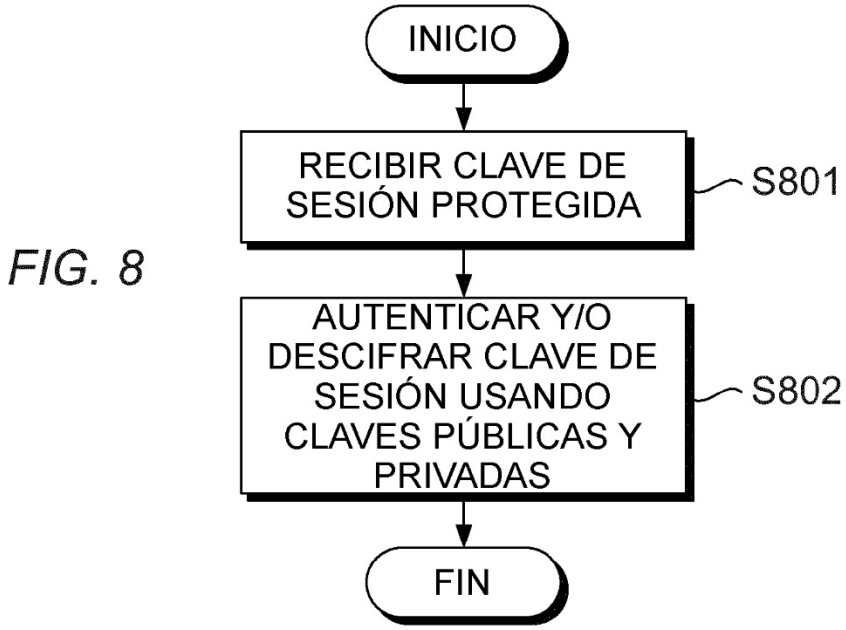

INICIO
RECIBIR CLAVE DE SESIÓN PROTEGIDA
S801
AUTENTICAR Y/O DESCIFRAR CLAVE DE SESIÓN USANDO CLAVES PÚBLICAS Y PRIVADAS
S802
FIN

FIG. 8

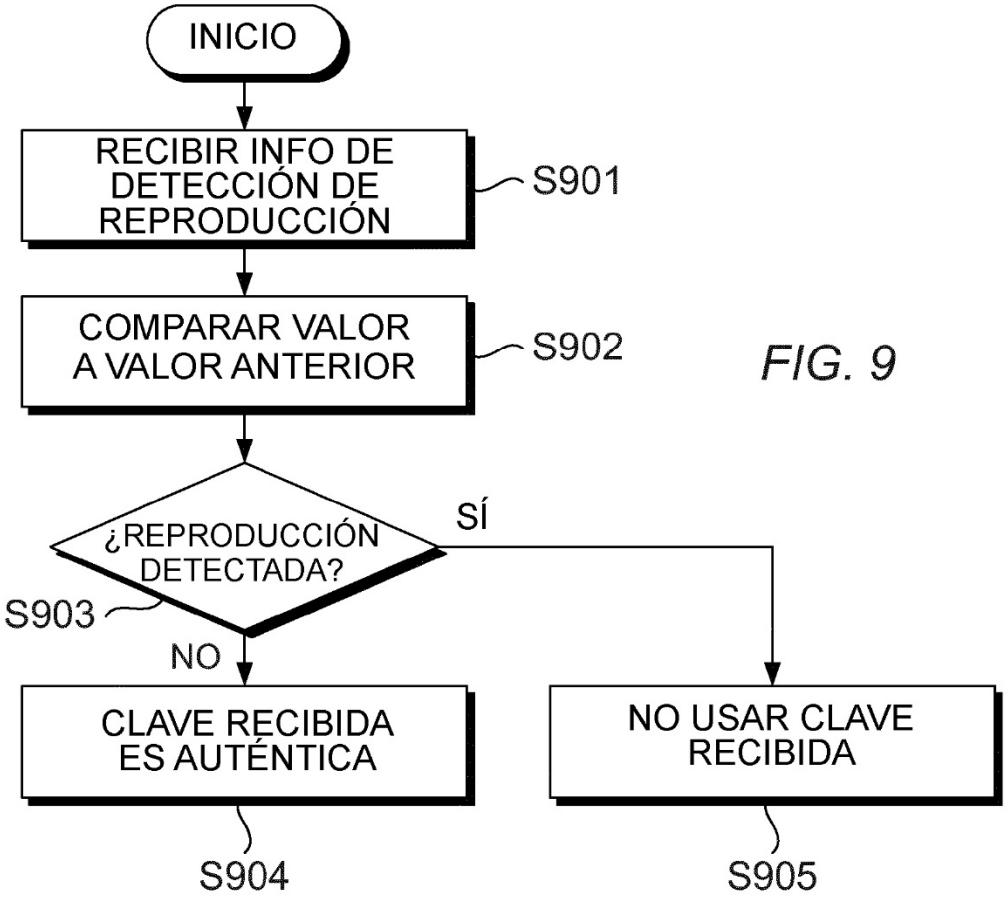

INICIO
RECIBIR INFO DE DETECCIÓN DE REPRODUCCIÓN
S901
COMPARAR VALOR A VALOR ANTERIOR
S902
¿REPRODUCCIÓN DETECTADA?
S903
SÍ
NO
CLAVE RECIBIDA ES AUTÉNTICA
S904
NO USAR CLAVE RECIBIDA
S905

FIG. 9

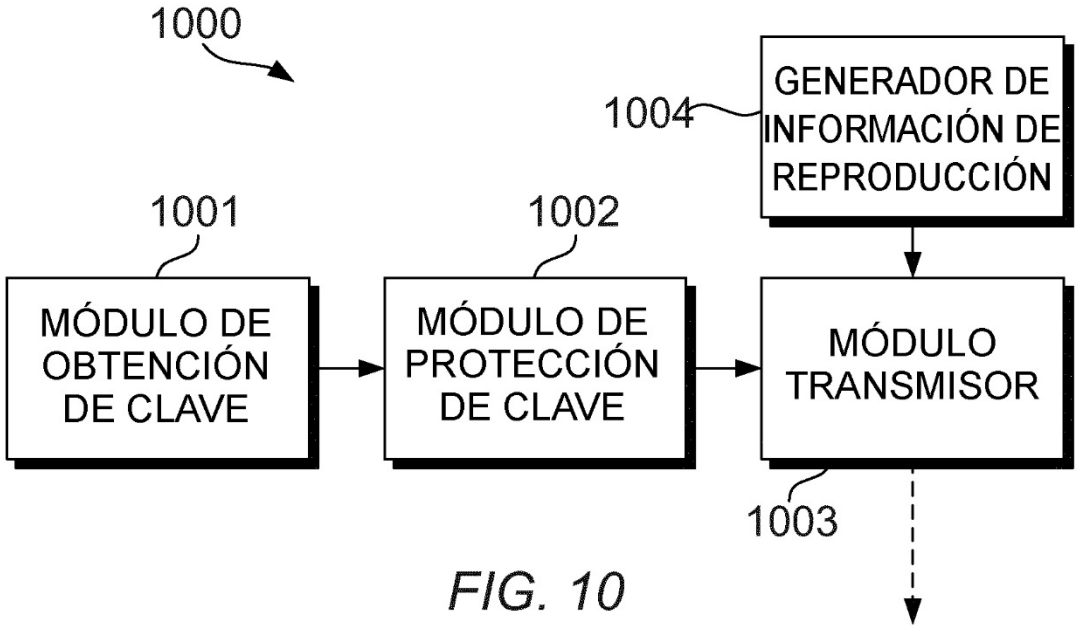

1000
1004
GENERADOR DE INFORMACIÓN DE REPRODUCCIÓN
1001
1002
MÓDULO DE OBTENCIÓN DE CLAVE
MÓDULO DE PROTECCIÓN DE CLAVE
MÓDULO TRANSMISOR
1003

FIG. 10

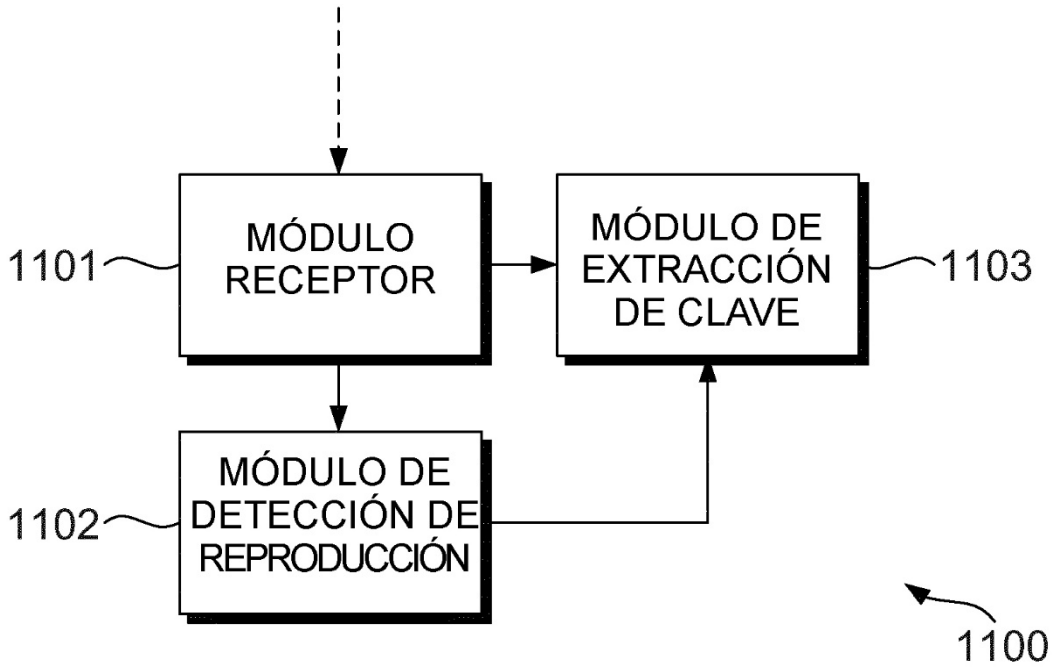

1101
MÓDULO RECEPTOR
MÓDULO DE EXTRACCIÓN DE CLAVE
1103
1102
MÓDULO DE DETECCIÓN DE REPRODUCCIÓN
1100

FIG. 11

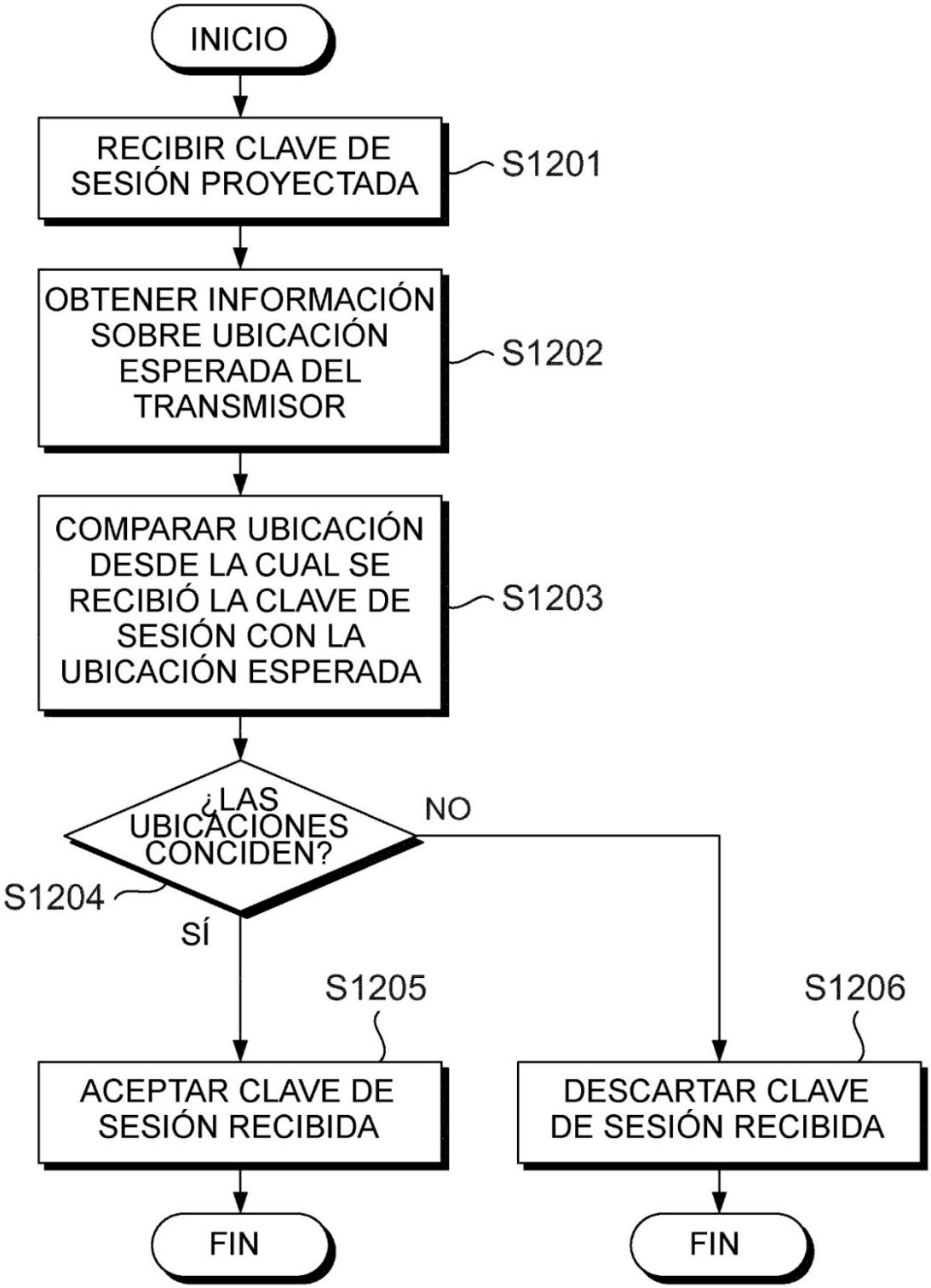

INICIO
RECIBIR CLAVE DE SESIÓN PROYECTADA
S1201
OBTENER INFORMACIÓN SOBRE UBICACIÓN ESPERADA DEL TRANSMISOR
S1202
COMPARAR UBICACIÓN DESDE LA CUAL SE RECIBIÓ LA CLAVE DE SESIÓN CON LA UBICACIÓN ESPERADA
S1203
¿LAS UBICACIONES CONCIDEN?
S1204
NO
SÍ
S1205
S1206
ACEPTAR CLAVE DE SESIÓN RECIBIDA
DESCARTAR CLAVE DE SESIÓN RECIBIDA
FIN
FIN

FIG. 12