(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 768 679**

(51) Int. CI.:

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **26.11.2015 E 15306879 (6)**

(97) Fecha y número de publicación de la concesión europea: **06.11.2019 EP 3174326**

(54) Título: **Procedimiento para proporcionar una estación de usuario inalámbrica para acceder a una red de telecomunicaciones a través de un punto de acceso inalámbrico a la red, un punto de acceso inalámbrico a la red asociado y una estación de usuario inalámbrica**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.06.2020

(73) Titular/es:

ALSTOM TRANSPORT TECHNOLOGIES (50.0%)
48, rue Albert Dhalenne
93400 Saint-Ouen, FR y
NERATEC SOLUTIONS AG (50.0%)

(72) Inventor/es:

FAYT, ETIENNE;
VETILLARD, JEAN-NOEL;
DUBOWIK, WOJCIECH y
HARJU, JUSSI

(74) Agente/Representante:

SALVÀ FERRER, Joan

DESCRIPCIÓN

Procedimiento para proporcionar una estación de usuario inalámbrica para acceder a una red de telecomunicaciones a través de un punto de acceso inalámbrico a la red, un punto de acceso inalámbrico a la red asociado y una estación de usuario inalámbrica

[0001] La presente invención se refiere generalmente a una red de telecomunicaciones que incluye puntos de acceso inalámbrico e implementa un esquema de autenticación entre puntos de acceso inalámbrico y estaciones de usuario inalámbricas antes de proporcionar servicios de telecomunicaciones a las estaciones de usuario inalámbricas a través de los puntos de acceso inalámbrico.

[0002] La invención se refiere más particularmente a un procedimiento para proporcionar una estación de usuario inalámbrica para acceder a una red de telecomunicaciones a través de un punto de acceso inalámbrico a la red, incluyendo las etapas de:

- derivar, por cada uno de la estación de usuario inalámbrica y el punto de acceso inalámbrico a la red, una segunda clave a partir de al menos una primera clave compartida por la estación de usuario inalámbrica y el punto de acceso a la red;
- realizar, a través de una comunicación inalámbrica, una etapa de autenticación entre la estación de usuario inalámbrica y el punto de acceso inalámbrico a la red en función de las segundas claves respectivas derivadas por la estación de usuario inalámbrica y el punto de acceso inalámbrico a la red;

- proporcionar acceso de la estación de usuario inalámbrica a la red de telecomunicaciones a través del punto de acceso inalámbrico a la red en función del resultado de la etapa de autenticación.

[0003] El documento US 2007/280481 A1 describe una alteración del conocido mecanismo de enlace de cuatro vías que comprende la adición de una etapa en la que un punto de acceso intenta utilizar una clave PSK de una lista de PSK para validar un código de integridad de mensaje proporcionado por una estación que intenta conectarse a la red hasta que una de las PSK valida el mensaje.

[0004] El documento WO 213/040042 A1 describe un mecanismo de autenticación de tres partes seguido de un mecanismo de enlace de cuatro vías alterado.

[0005] Por ejemplo, el estándar IEEE 802.11 define dos tipos de procedimientos de acceso a una red:

- procedimiento de acceso basado en el protocolo de autenticación extensible,
- procedimiento de acceso basado en claves precompartidas (PSK).

[0006] Cada procedimiento de acceso incluye una autenticación y un establecimiento de claves de grupo por pares. Estos procedimientos de acceso difieren según el protocolo de autenticación.

[0007] El procedimiento de acceso basado en el protocolo de autenticación extensible requiere el intercambio de información entre tres entidades: la estación de usuario de radio IEEE802.11 (el solicitante), el punto de acceso (el autenticador) y un servidor de autenticación. El servidor de autenticación se utiliza para certificar al punto de acceso que la estación de usuario puede asociarse y para certificar a la estación de usuario que el punto de acceso seleccionado es parte de la red. Este enfoque proporciona una autenticación mutua. El servidor de autenticación también se usa para la administración de claves.

[0008] El procedimiento de acceso basado en claves precompartidas requiere el intercambio de información solamente entre dos entidades: la estación de usuario de radio IEEE802.11 (el solicitante) y el punto de acceso (el autenticador). El punto de acceso simplifica y realiza la fase de autenticación. La autenticación y el establecimiento de la clave de grupo por pares se fusionan y se basan en el conocimiento por ambas entidades de una clave precompartida. La seguridad de la autenticación y la comunicación se basa en la confidencialidad de la clave precompartida.

[0009] Si el procedimiento de acceso basado en el protocolo de autenticación extensible proporciona el nivel de seguridad más alto debido a la autenticación mutua de la estación de usuario y el punto de acceso y también la administración de claves realizada por el servidor de autenticación, un procedimiento de acceso basado en una clave precompartida es mucho más rápido porque requiere un intercambio limitado de información entre solo dos entidades, y también es fácil de implementar porque no requiere un servidor de autenticación. La duración total de una operación de acceso entre la emisión de una solicitud de asociación y el éxito de la operación es superior a 1 segundo para el procedimiento de acceso basado en el protocolo de autenticación extensible y unos pocos milisegundos (ms) para el procedimiento de acceso basado en la clave precompartida.

[0010] Se debe considerar un equilibrio entre el nivel de seguridad y la complejidad y el rendimiento de un

sistema de radio, especialmente en los casos en los que se producen traspasos frecuentes, tal como considerar una estación de usuario dentro de un tren en funcionamiento y comunicarse con una red que incluye puntos de acceso fijos.

[0011] Por lo tanto, la invención propone un procedimiento para proporcionar acceso a una red de telecomunicaciones, un punto de acceso inalámbrico a la red configurado para proporcionar a la estación o estaciones de usuario inalámbricas acceso a la red de telecomunicaciones, una estación de usuario inalámbrica configurada para obtener acceso a la red de telecomunicaciones según las reivindicaciones adjuntas.

[0012] Por lo tanto, la invención permite mejorar el nivel de seguridad de los procedimientos de acceso basados en claves precompartidas.

[0013] En algunas realizaciones, el procedimiento según la invención incluye además una o varias de las siguientes características:

- en cada tiempo de actualización de un patrón de actualización que incluye varios tiempos de actualización, el punto de acceso inalámbrico a la red obtiene un valor actualizado del parámetro y transmite de forma inalámbrica el valor actualizado del parámetro obtenido de este modo; y en el que cualquier etapa de autenticación futura relativa a la estación de usuario inalámbrica que ha recibido el valor actualizado del parámetro se realiza en función de la segunda clave derivada por la estación de usuario inalámbrica de al menos la primera clave y más allá del valor actualizado transmitido del parámetro;
- un servidor proporciona varios puntos de acceso, a través de la red de telecomunicaciones (3), con dicho valor actualizado del parámetro y cualquiera de estos varios puntos de acceso transmite de forma inalámbrica el valor actualizado del parámetro;
- la etapa de autenticación entre la estación de usuario inalámbrica y el punto de acceso inalámbrico a la red se realiza según el estándar IEEE 802.11;
- el valor actualizado del parámetro se transmite de forma inalámbrica por el punto de acceso inalámbrico según se incluye en los mensajes de baliza del punto de acceso inalámbrico incluyendo además información de identificación del punto de acceso inalámbrico y transmitidos cíclicamente.

[0014] La presente invención se ilustra a modo de ejemplo, y no a modo de limitación, en las figuras de los dibujos adjuntos y en los que los números de referencia similares se refieren a elementos similares, y en las que:

- La Figura 1 muestra esquemáticamente una red de telecomunicaciones que implementa una realización de la invención;

- la Figura 2 es un diagrama de flujo que ilustra las etapas de un procedimiento según una realización de la invención;

- la figura 3 es un diagrama de flujo que representa las etapas de un procedimiento según una realización de la invención.

[0015] La Figura 1 muestra esquemáticamente un sistema de telecomunicaciones 1 que implementa una realización de la invención.

[0016] El sistema de telecomunicaciones 1 incluye:

- una red troncal 3 desde la cual se pueden proporcionar servicios de telecomunicaciones, tales como servicios de Internet;

- una o varias estaciones de usuario inalámbricas 6;

- varios puntos de acceso inalámbrico 2, incluidos los puntos de acceso inalámbrico 2 llamados AP_1, AP_2, AP_3, cada uno conectado a la red troncal 3.

[0017] Un servidor administrador de red (NMS (*Network Manager Server*)) 4 también está conectado a la red troncal 3.

[0018] En la realización considerada, una estación de usuario 6 es una estación de usuario de radio 6, que incluye una interfaz de radio, una antena de radiofrecuencia, un microordenador y una memoria (no mostrada en las figuras).

[0019] La memoria de una estación de usuario 6 incluye instrucciones de software que, una vez ejecutadas en el microordenador de la estación de usuario 6, implementan las etapas descritas en lo sucesivo, incluyendo las etapas que se refieren a las Figuras 2 y 3 y realizadas por la estación de usuario 6.

[0020] En la realización considerada, cada uno de los puntos de acceso AP_1, AP_2, AP_3 incluye una interfaz de radio, una antena de radiofrecuencia, un microordenador y una memoria (no mostrada en las Figuras). Cada uno de los puntos de acceso AP_1, AP_2, AP_3 corresponde a un área de cobertura de radio respectiva y está adaptado para entregar los servicios de telecomunicaciones proporcionados por la red troncal 3 a las estaciones de usuario de radio ubicadas dentro del área de cobertura de radio de dicho punto de acceso.

[0021] La memoria de cada uno de los puntos de acceso AP_1, AP_2, AP_3 incluye instrucciones de software que una vez ejecutadas en el microordenador del punto de acceso, implementan las etapas descritas en lo sucesivo, incluyendo las etapas que se refieren a las Figuras 2 y 3 y realizadas por el punto de acceso.

[0022] La interfaz de radio de una estación de usuario 6 está adaptada para comunicarse con la interfaz de radio del punto de acceso 2. En la realización considerada de la invención, las interfaces de radio respectivas están adaptadas para comunicarse según el estándar IEEE 802.11 (modificación 802.11i) completado como se describe en lo sucesivo con respecto a la generación de la clave transitoria por pares (PTK) que se genera a partir de la clave precompartida (PSK) como se conoce, y también se genera según la invención, además según un parámetro modificado regularmente.

[0023] En la realización específica considerada en referencia a la Figura 1, una estación de usuario de radio 6, considerada en lo sucesivo, es, por ejemplo, una estación de usuario de un sistema de radio de control de tren de base de comunicación, y está dentro de un tren 5. Mientras que el tren 5 avanza por su línea ferroviaria, la estación de usuario 6 pasa sucesivamente por el área de cobertura de radio del punto de acceso AP_3, después a través del área de cobertura de radio del punto de acceso AP_2 y finalmente a través del área de cobertura de radio del punto de acceso AP_1. Por lo tanto, se producen varias transferencias de la estación de usuario 6 con estos puntos de acceso sucesivos 2.

[0024] El uso de IEEE 802.11i proporciona protección contra la intercepción intencional o no intencional por un mecanismo de autenticación y cifrado de todos los paquetes con datos de carga útil. El mecanismo de autenticación evita que un usuario no autorizado establezca una conexión de radio y el cifrado de paquetes con datos de carga útil evita que estos sean interceptados por cualquier usuario no autorizado.

[0025] Según el estándar IEEE 802.11i, las estaciones de usuario 6 del sistema de telecomunicaciones 1 y los puntos de acceso 2 del sistema de telecomunicaciones 1 tienen en la memoria una misma clave precompartida almacenada PSK.

[0026] La clave precompartida PSK se usa, como se muestra en lo sucesivo en referencia a las Figuras 2 y 3, para generar una clave transitoria por pares común PTK en una estación de usuario 6 y en paralelo en el punto de acceso que implementa la etapa de autenticación, utilizándose dicha PTK en la autenticación y utilizándose también en el cifrado/descifrado de todos los paquetes, incluyendo los datos de carga útil.

[0027] Se genera una nueva PTK en una estación de usuario 6 durante una etapa de autenticación con un punto de acceso, después de cada transferencia y después de cada etapa de encendido e inicialización de la estación de usuario 6.

[0028] Según la invención, haciendo referencia al conjunto 100 de etapas representadas por el diagrama de flujo en la Figura 2, en una etapa 101, se genera un valor modificado de un parámetro, denominado en lo sucesivo número de semilla, por ejemplo, un valor aleatorio, por el NMS 4, y se transmite a los puntos de acceso 2 por el NMS 4 a través de la red troncal 3, por ejemplo, según el protocolo simple de administración de red (SNMP).

[0029] La etapa 101 se repite según un patrón de actualización de número de semilla determinado, por ejemplo, se da aleatoriamente un nuevo valor al número de semilla en una base cíclica (por ejemplo, un número de semilla renovado por semana, por día o por hora).

[0030] En una etapa 102, el último nuevo valor del número de semilla se transmite regularmente por la interfaz de radio de cualquier punto de acceso 2.

[0031] En una realización de esta etapa 102, cada vez que un punto de acceso 2 recibe un nuevo valor del número de semilla desde el NMS 4, el punto de acceso 2 reemplaza, en un campo dado de su mensaje de baliza, el valor del número de semilla recibido previamente por el valor del número de semilla recién recibido. Como se sabe, el mensaje de baliza incluye además datos de identificación del punto de acceso 2 que se utilizan por las estaciones de usuario 6, además de la medición del nivel de recepción de baliza cuando se intenta conectar al sistema de telecomunicaciones 1 a través del punto de acceso para usar los servicios de telecomunicaciones proporcionados por el sistema de telecomunicaciones. El mensaje de baliza de un punto de acceso 2 se transmite repetidamente por la interfaz de radio del punto de acceso, por ejemplo, cada 30 ms.

[0032] Los mensajes de baliza transmitidos en la realización considerada son de conformidad con los mensajes de baliza del estándar IEEE 802.11, insertándose el valor del número de semilla en el campo del mensaje de baliza dedicado a la información de propiedad.

[0033] Además, en una realización de esta etapa 102, cada vez que un punto de acceso 2 del NMS 4 recibe un nuevo valor del número de semilla, el punto de acceso 2 reemplaza, en un campo dado de sus tramas de respuesta de sonda, el valor del número de semilla recibido previamente por el valor del número de semilla recién recibido.

[0034] Como se sabe, las tramas de respuesta de sonda del estándar IEEE 802.11, incluyendo los datos de identificación de un punto de acceso, se transmiten por la interfaz de radio del punto de acceso 2 en respuesta a cualquier solicitud de sonda enviada por una estación de usuario 6 y recibida por el punto de acceso.

[0035] Las tramas de respuesta de sonda transmitidas según la realización considerada de la invención cumplen el estándar IEEE 802.11, insertándose el valor del número de semilla en el campo dedicado a la información de propiedad.

[0036] En una etapa 103, el nuevo valor del número de semilla transmitido por un punto de acceso 2 en la etapa 102 se recibe por la interfaz de radio de una estación de usuario 6 ubicada dentro del área de cobertura de radio del punto de acceso 2 y se almacena en su memoria. La estación de usuario 6 genera una clave PTK en función de la clave PSK almacenada en la memoria de la estación de usuario y de este último valor almacenado del número de semilla.

[0037] Dicha clave PTK se genera cada vez que la estación de usuario a bordo 6 realiza una transferencia o se enciende, durante una etapa de autenticación entre la estación de usuario y el punto de acceso, y también se utiliza para el cifrado/descifrado posterior.

[0038] La invención permite aumentar la seguridad del sistema de telecomunicaciones 1 con un impacto muy limitado en el rendimiento del sistema de telecomunicaciones (por ejemplo, en la duración de la transferencia) y la complejidad.

[0039] Dichas ventajas son valiosas, por ejemplo, en trenes que circulan a una velocidad de hasta 100 km/h, en los que las estaciones de usuario a bordo realizan traspasos frecuentes entre puntos de acceso y la duración del traspaso debe ser lo más corta posible con un valor inferior a 100 ms en el 90 por ciento de los traspasos.

[0040] En una realización de la etapa 103, cada vez que la estación de usuario a bordo 6 realiza una transferencia o se enciende, la estación de usuario 6 busca un nuevo punto de acceso adecuado 2 escuchando las balizas transmitidas por los puntos de acceso circundantes 2, según el estándar IEEE 802.11. Para acelerar la búsqueda de puntos de acceso adecuados, opcionalmente la estación de usuario 6 envía una solicitud de sonda, según el estándar IEEE 802.11.

[0041] Después, la estación de usuario 6 analiza las balizas escuchadas y/o las tramas de respuesta de sonda, selecciona un punto de acceso adecuado 2 según el estándar IEEE 802.11, por ejemplo, el punto de acceso AP_3 (como se sabe, el punto de acceso AP_3 se selecciona basándose en al menos el nivel de recepción, por la estación de usuario 6, de la señal de radio transmitida por el punto de acceso AP_3). La estación de usuario 6 almacena, en su memoria, la información contenida dentro de la baliza y/o la respuesta de sonda transmitida por el punto de acceso seleccionado AP_3, incluyendo los parámetros de seguridad, tales como el tipo de autenticación según el estándar IEEE 802.11 y el nuevo número de semilla. Después, la estación de usuario 6 transmite, a través de su interfaz de radio, al punto de acceso seleccionado AP_3, una solicitud de asociación según el estándar IEEE 802.11 que requiere asociación con el punto de acceso seleccionado AP_3. Una vez que los intercambios de la etapa de asociación entre la estación de usuario 6 se completan con éxito y el punto de acceso seleccionado AP_3 se asocia con la estación de usuario 6, a continuación, comienza la etapa de autenticación. No es posible la telecomunicación de datos de carga útil hasta la finalización de la etapa de autenticación entre el punto de acceso AP_3 y la estación de usuario 6.

[0042] La Figura 3 representa un diagrama de flujo que representa las etapas de la fase de autenticación 200 entre una estación de usuario 6 y el punto de acceso asociado del punto de acceso seleccionado AP_3, tal como se realiza en una realización de la etapa 103.

[0043] En la etapa 201, la estación de usuario 6 genera una clave compartida operativa OPSK, como resultado de una función (función F1) de la clave precompartida PSK almacenada en su memoria y del nuevo número de semilla que se almacenó por último en su memoria: OPSK = F1(PSK, número de semilla).

[0044] En una realización, la función F1 se basa en la función PBKDF2 definida en el IETF RFC2898.
En la etapa 202, la estación de usuario 6 genera un valor SNONCE, que puede ser un número aleatorio generado basándose en PBKDF2 definido en el RFC2898, siendo las entradas principales OPSK y un número aleatorio o un Aleatorio generado directamente según el IETF RFC 4086.

[0045] En paralelo a las etapas 201 y 202, en la etapa 301, el punto de acceso AP3 genera también una clave operativa compartida OPSK, como resultado de una función (función F1) de la clave precompartida PSK almacenada en su memoria y del número de semilla que se almacenó por último en su memoria (OPSK = F1(PSK, número de semilla), y en la etapa 302, el punto de acceso AP3 genera un ANONCE, que puede ser un número aleatorio generado basándose en PBKDF2 definido en el RFC2898, siendo las entradas principales OPSK y un número aleatorio o un Aleatorio generado según el IETF RFC 4086

[0046] En una etapa 303, el punto de acceso AP_3 transmite a la estación de usuario 6, a través de las interfaces de radio respectivas, un primer mensaje de autenticación que incluye el valor ANONCE generado.

[0047] En una etapa 304, la estación de usuario 6 recibe el primer mensaje de autenticación transmitido por el punto de acceso AP3 y deriva una clave transitoria por pares PTK del valor ANONCE incluido en el primer mensaje de autenticación recibido y del SNONCE y la clave compartida operativa OPSK generada en la etapa 201: PTK = F3(ANONCE, SNONCE, OPSK), en la que F3 es una función del valor ANONCE y del valor OPSK y también del valor SNONCE.

[0048] En una realización, la función F3 es la función PRF-n definida por el estándar IEEE802.11.

[0049] En una etapa 305, la estación de usuario 6 transmite al punto de acceso AP_3, a través de las interfaces de radio respectivas, un segundo mensaje de autenticación que incluye el valor SNONCE generado y un código de integridad de mensaje (MIC, *Message Integrity Code*) basado en CBTC-MAC como se define en el mecanismo de enlace de cuatro vías especificado por el estándar IEEE802.11. En una etapa 306, el punto de acceso AP_3 recibe el segundo mensaje de autenticación transmitido por la estación de usuario 6. El punto de acceso AP_3 verifica que el MIC en el segundo mensaje de autenticación recibido sea válido (por ejemplo, se considera válido si y solo si el MIC calculado por sí mismo por el punto de acceso es igual al MIC que se encuentra en el segundo mensaje de autenticación recibido y que se calculó por la estación de usuario basándose en el SNONCE y el encabezado en el mensaje), y solo en caso de que el MIC se verifique como válido (de lo contrario, la autenticación falla), el punto de acceso AP_3 deriva una clave transitoria por pares PTK del valor SNONCE incluido en el segundo mensaje de autenticación recibido y de la clave compartida operativa OPSK generada en la etapa 201 y también el ANONCE: PTK = F4(ANONCE, SNONCE, OPSK), en la que F4 es una función del valor ANONCE, el valor SNONCE y del valor OPSK. La función F4 es la función F3 que es la función PRF-n definida por el estándar IEEE802.11.

[0050] En una etapa 307, el punto de acceso AP_3 transmite a la estación de usuario 6, a través de las interfaces de radio respectivas, un tercer mensaje de autenticación que incluye una notificación de instalación de la PTK certificada con un MIC calculado a partir del encabezado del tercer mensaje de autenticación y del ANONCE.

[0051] En una etapa 308, la estación de usuario 6 recibe el tercer mensaje de autenticación transmitido por el punto de acceso AP_3 como se define en el mecanismo de enlace de cuatro vías del IEEE802.11. La estación de usuario 6 verifica si el MIC en el tercer mensaje de autenticación recibido es válido (de manera similar a la etapa 306, la estación de usuario calcula el MIC en el contenido del tercer mensaje de autenticación y lo compara con el MIC dentro del mensaje; si y solo si son el mismo, el mensaje se considera válido), y solo en caso de que el MIC se verifique como válido (de lo contrario, la autenticación falla), la estación de usuario 6 transmite un cuarto mensaje de autenticación al punto de acceso AP3 que incluye un MIC calculado a partir del encabezado del cuarto mensaje de autenticación y del SNONCE.

[0052] Después, en una etapa 309, la estación de usuario 6 instala en su memoria la clave PTK generada en la etapa 304.

[0053] En una etapa 310, el punto de acceso AP_3 recibe el cuarto mensaje de autenticación transmitido por la estación de usuario 6 y, a continuación, el punto de acceso AP_3 instala en su memoria la clave PTK generada en la etapa 306.

[0054] A continuación, la autenticación se completa y la comunicación de los datos de la carga útil puede entonces tener lugar (etapa 311), cifrándose/descifrándose estos datos de carga útil por la estación de usuario 6 usando una o más claves de cifrado/descifrado basándose en la clave PTK almacenada en su memoria (y de manera similar, cifrándose/descifrándose los datos de carga útil por el punto de acceso AP_3 utilizando la clave PTK almacenada en su memoria).

[0055] En el estándar IEEE 802.11 de la técnica anterior, considerando la Figura 3, las etapas 201 y 301 no existían y en las etapas 202, 302-311, se usó la clave precompartida PSK en lugar de la clave OPSK, para generar la clave transitoria por pares PTK. La invención permite transformar una clave estática (la clave PSK) en una dinámica (la clave OPSK).

[0056] En lo sucesivo, las etapas 202, 302, 303, 304, 305, 306, 307, 308, 309, 310 son las etapas definidos en

el estándar IEEE 802.11 para la fase de autenticación cuando se considera la OPSK dinámica en lugar de la PSK estática.

[0057] La invención permite aumentar el nivel de seguridad sin aumentar significativamente la complejidad de la arquitectura del sistema o la duración del traspaso.

[0058] Una realización de la invención se ha descrito aquí anteriormente haciendo referencia a las figuras en el caso de comunicaciones de radio IEEE 802.11 entre las estaciones de usuario y los puntos de acceso a la red. Por supuesto, el uso de una clave estática compartida por los puntos de acceso y las estaciones de usuario y de un número aleatorio regularmente modificado según la invención en la etapa de autenticación y/o la etapa de cifrado/descifrado se puede implementar usando protocolos de radio para comunicarse que son diferentes del estándar IEEE 802.11, y más generalmente en realizaciones de la invención, se pueden usar otras interfaces inalámbricas para comunicarse en lugar de interfaces de radio.

REIVINDICACIONES

1. Procedimiento para proporcionar acceso a una red de telecomunicaciones (3) de una estación de usuario inalámbrica (6) a través de puntos de acceso inalámbrico a la red (2), estando los puntos de acceso inalámbrico a la red conectados a un servidor administrador de red (4) a través de una red de telecomunicaciones (3), **caracterizado porque** el procedimiento incluye sucesivamente las etapas de:

- generar, por el servidor administrador de red, un valor actualizado de un parámetro, siendo dicho valor actualizado del parámetro transmitido a los puntos de acceso inalámbrico a la red;
- transmitir de forma inalámbrica por los puntos de acceso inalámbrico a la red el valor actualizado del parámetro;
- recibir de forma inalámbrica por la estación de usuario inalámbrica el valor actualizado del parámetro transmitido por los puntos de acceso inalámbrico a la red;
- derivar, por cada una de las estaciones de usuario inalámbricas y los puntos de acceso inalámbrico a la red, una segunda clave de al menos una primera clave y más allá del valor actualizado recibido del parámetro, siendo la primera clave una clave precompartida estática, que es compartida por la estación de usuario inalámbrica y los puntos de acceso a la red y que se almacena en la memoria de la estación de usuario inalámbrica y los puntos de acceso a la red, respectivamente;
- realizar, a través de la comunicación inalámbrica, una etapa de autenticación entre la estación de usuario inalámbrica y un punto de acceso determinado de los puntos de acceso inalámbrico a la red basándose en las segundas claves derivadas por la estación de usuario inalámbrica y el punto de acceso inalámbrico a la red;
- proporcionar acceso de la estación de usuario inalámbrica a la red de telecomunicaciones a través del punto de acceso inalámbrico a la red como resultado de la etapa de autenticación,

siendo la etapa de autenticación un mecanismo de enlace de cuatro vías entre la estación de usuario inalámbrica y el punto de acceso determinado según lo especificado por el estándar IEEE 802.11.

2. Procedimiento para proporcionar acceso a una red de telecomunicaciones (3) de una estación de usuario inalámbrica (6) a través de un punto de acceso inalámbrico a la red (2) según la reivindicación 1, en el que la etapa de autenticación comprende:

- la estación de usuario genera un primer número aleatorio, SNONCE;
- el punto de acceso determinado genera un segundo número aleatorio, ANONCE;
- el punto de acceso determinado transmite a la estación de usuario un primer mensaje de autenticación que incluye el segundo número aleatorio;
- la estación de usuario deriva una clave transitoria por pares, PTK, a partir del primer y segundo número aleatorio y la segunda clave, OPSK;
- la estación de usuario transmite al punto de acceso un segundo mensaje de autenticación que incluye el primer número aleatorio y un código de integridad de mensaje, MIC, basado en CBTC-MAC;
- el punto de acceso verifica si el código de integridad de mensaje recibido es válido y, solo en caso de que el código de integridad de mensaje sea válido, el punto de acceso deriva la clave transitoria por pares, PTK, del primer y segundo número aleatorio y la segunda clave, OPSK;
- el punto de acceso transmite a la estación de usuario un tercer mensaje de autenticación que incluye una notificación de instalación de la clave transitoria por pares, certificada con un código de integridad de mensaje calculado a partir del encabezado del tercer mensaje de autenticación y del segundo número aleatorio;
- la estación de usuario verifica si el código de integridad de mensaje es válido y, solo en caso de que el código de integridad de mensaje sea válido, la estación de usuario transmite un cuarto mensaje de autenticación al punto de acceso que incluye un código de integridad de mensaje calculado a partir del encabezado del mensaje de autenticación y del primer número aleatorio;
- la estación de usuario instala en su memoria la clave transitoria por pares generada y el punto de acceso, al recibir el cuarto mensaje de autenticación, instala en su memoria la clave transitoria por pares generada.

3. Procedimiento para proporcionar acceso a una red de telecomunicaciones (3) de una estación de usuario inalámbrica (6) a través de un punto de acceso inalámbrico a la red (2) según la reivindicación 1 o la reivindicación 2, en el que la etapa de autenticación comienza con la estación de usuario que genera un primer número aleatorio, SNONCE, y el punto de acceso determinado que genera un segundo número aleatorio, ANONCE, siendo el primer y segundo número aleatorio números aleatorios generados basándose en la función PBKDF2 definida en rfc2898, siendo las entradas principales la segunda clave y un número aleatorio.

4. Procedimiento para proporcionar acceso a una red de telecomunicaciones (3) de una estación de usuario inalámbrica (6) a través de un punto de acceso inalámbrico a la red (2) según la reivindicación 1, en el que, en cada tiempo de actualización de un patrón de actualización que incluye varios tiempos de actualización, el punto de acceso inalámbrico a la red obtiene un valor actualizado del parámetro y transmite de forma inalámbrica el valor actualizado del parámetro obtenido de este modo; y en el que cualquier etapa de autenticación futura relativa a la estación de usuario inalámbrica que ha recibido el valor actualizado del parámetro se realiza en función de la segunda clave derivada por la estación de usuario inalámbrica de al menos la primera clave y más allá del valor actualizado

transmitido del parámetro.

5. Procedimiento para proporcionar acceso a una red de telecomunicaciones (3) de una estación de usuario inalámbrica (6) a través de un punto de acceso inalámbrico a la red (2) según cualquiera de las reivindicaciones anteriores, en el que el valor actualizado del parámetro se transmite de forma inalámbrica por el punto de acceso inalámbrico según se incluye en los mensajes de baliza del punto de acceso inalámbrico que incluyen además información de identificación del punto de acceso inalámbrico y transmitidos cíclicamente.

6. Punto de acceso inalámbrico a la red (2), configurado para proporcionar una estación de usuario inalámbrica (6) con acceso a una red de telecomunicaciones (3), estando el punto de acceso inalámbrico a la red conectado a un servidor administrador de red (4) a través de la red de telecomunicaciones (3), estando dicho punto de acceso inalámbrico a la red **caracterizado porque** comprende:

- medios para obtener un valor actualizado de un parámetro generado por el servidor administrador de red,
- medios para transmitir de forma inalámbrica por el punto de acceso inalámbrico a la red el valor actualizado del parámetro,
- medios para derivar una segunda clave de al menos una primera clave y más allá del valor actualizado transmitido del parámetro, siendo la primera clave una clave precompartida estática, compartida por la estación de usuario inalámbrica y el punto de acceso a la red y almacenada en la memoria de la estación de usuario inalámbrica y el punto de acceso a la red, respectivamente;
- medios para realizar, a través de la comunicación inalámbrica, una etapa de autenticación con la estación de usuario inalámbrica en función de la segunda clave derivada, y
- medios para proporcionar acceso de la estación de usuario inalámbrica a la red de telecomunicaciones en función del resultado de la etapa de autenticación,

siendo la etapa de autenticación un mecanismo de enlace de cuatro vías entre la estación de usuario inalámbrica y el punto de acceso determinado según lo especificado por el estándar IEEE 802.11.

7. Punto de acceso inalámbrico a la red (2) según la reivindicación 6, en el que la etapa de autenticación comienza con la estación de usuario que genera un primer número aleatorio, SNONCE, y el punto de acceso genera un segundo número aleatorio, ANONCE, siendo el primer y segundo número aleatorio números aleatorios generados basándose en la función PBKDF2 definida en rfc2898, siendo las entradas principales la segunda clave y un número aleatorio.

8. Punto de acceso inalámbrico a la red (2) según la reivindicación 6 o la reivindicación 7, adaptado para, en cada tiempo de actualización de un patrón de actualización que incluye varios tiempos de actualización, obtener un valor actualizado del parámetro y transmitir de forma inalámbrica el valor actualizado del parámetro obtenido de este modo.

9. Punto de acceso inalámbrico a la red (2) según cualquiera de las reivindicaciones anteriores 6 a 8, adaptado para transmitir de forma inalámbrica el valor actualizado del parámetro según se incluye en los mensajes de baliza del punto de acceso inalámbrico que incluyen además información de identificación del punto de acceso inalámbrico y transmitidos cíclicamente.

10. Estación de usuario inalámbrica (6) configurada para obtener acceso a una red de telecomunicaciones a través de un punto de acceso inalámbrico a la red (2), estando el punto de acceso inalámbrico a la red conectado a un servidor administrador de red (4) a través de la red de telecomunicaciones (3), **caracterizada porque** dicha estación de usuario inalámbrica comprende:

- medios para recibir de forma inalámbrica un valor actualizado de un parámetro transmitido por el punto de acceso inalámbrico a la red, siendo el valor actualizado del parámetro generado por el servidor administrador de red; y,
- medios para derivar una segunda clave de al menos una primera clave compartida y más allá del valor actualizado recibido del parámetro, siendo la primera clave una clave precompartida estática, compartida por la estación de usuario inalámbrica y el punto de acceso a la red y almacenada en la memoria de la estación de usuario inalámbrica y el punto de acceso a la red, respectivamente;
- medios para realizar, a través de una comunicación inalámbrica, una etapa de autenticación con el punto de acceso inalámbrico a la red en función de la segunda clave derivada; y,
- medios para acceder a la red de telecomunicaciones a través del punto de acceso inalámbrico a la red en función del resultado de la etapa de autenticación,

siendo la etapa de autenticación un mecanismo de enlace de cuatro vías entre la estación de usuario inalámbrica y el punto de acceso determinado según lo especificado por el estándar IEEE 802.11.

11. Estación de usuario inalámbrica (6) según la reivindicación 10, adaptada para realizar cualquier etapa de autenticación futura en función de la segunda clave derivada por la estación de usuario inalámbrica de al menos la

primera clave y más allá del valor actualizado del parámetro recibido en el último tiempo de actualización de un patrón de actualización que incluye varios tiempos de actualización,

12. Estación de usuario inalámbrica (6) según la reivindicación 10 u 11, en la que la etapa de autenticación comienza con la estación de usuario que genera un primer número aleatorio, SNONCE, y el punto de acceso genera un segundo número aleatorio, ANONCE, siendo el primer y segundo número aleatorio números aleatorios generados basándose en la función PBKDF2 definida en rfc2898, siendo las entradas principales la segunda clave y un número aleatorio.

13. Estación de usuario inalámbrica (6) según cualquiera de las reivindicaciones anteriores 10 a 12, adaptada para recibir el valor actualizado del parámetro según se incluye en los mensajes de baliza transmitidos cíclicamente por el punto de acceso inalámbrico e incluyendo además información de identificación del punto de acceso inalámbrico.

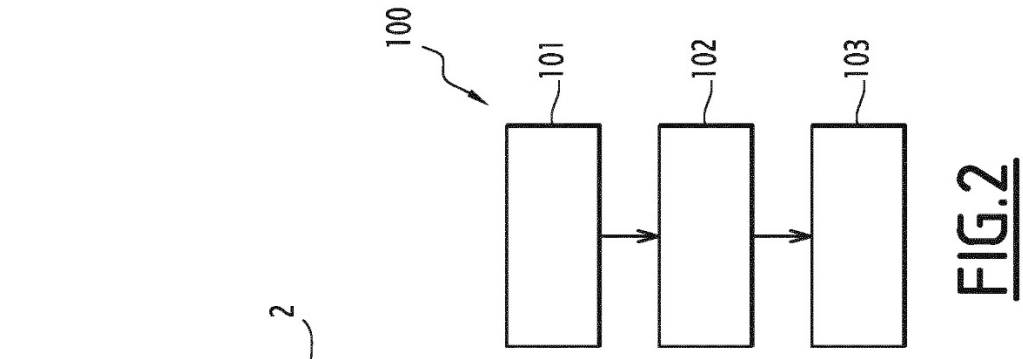

FIG.2

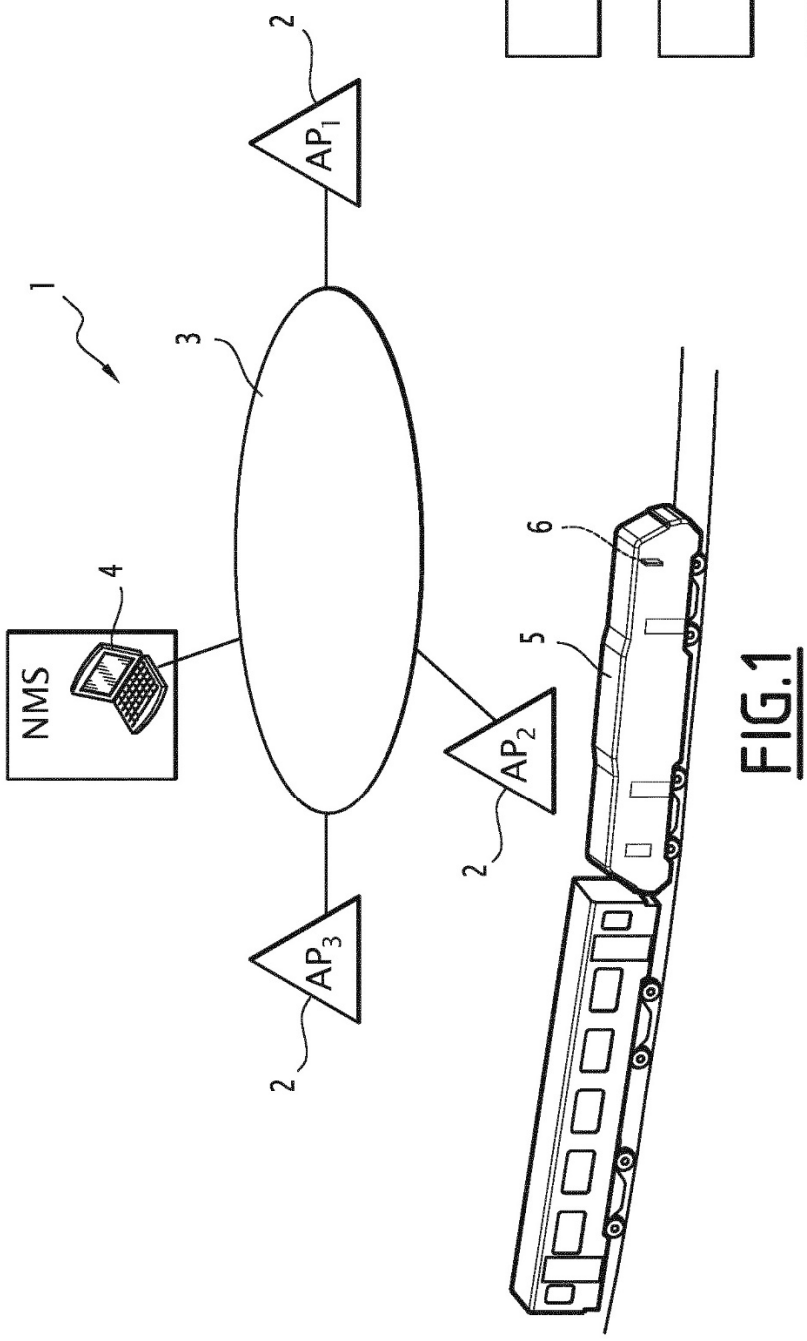

FIG.1

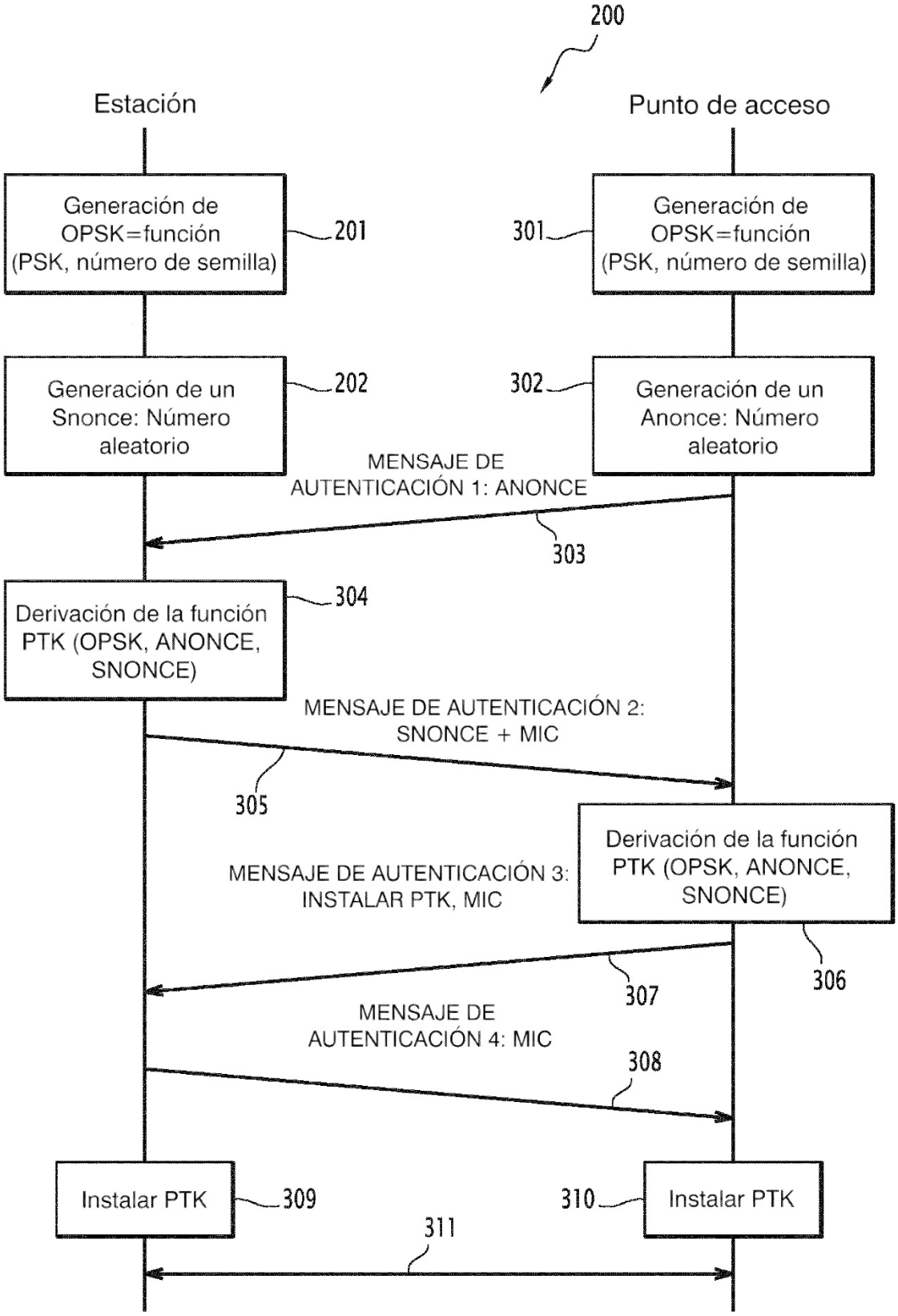
200
Estación
Punto de acceso
Generación de OPSK=función (PSK, número de semilla)
201
301
Generación de OPSK=función (PSK, número de semilla)
Generación de un Snonce: Número aleatorio
202
302
Generación de un Anonce: Número aleatorio
MENSAJE DE AUTENTICACIÓN 1: ANONCE
303
Derivación de la función PTK (OPSK, ANONCE, SNONCE)
304
MENSAJE DE AUTENTICACIÓN 2: SNONCE + MIC
305
Derivación de la función PTK (OPSK, ANONCE, SNONCE)
MENSAJE DE AUTENTICACIÓN 3: INSTALAR PTK, MIC
306
307
MENSAJE DE AUTENTICACIÓN 4: MIC
308
Instalar PTK
309
310
Instalar PTK
311

FIG.3