(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 671 170**

(51) Int. CI.:

H04W 12/04 (2009.01)
H04L 9/08 (2006.01)
H04W 36/08 (2009.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **24.08.2007 PCT/US2007/076800**

(87) Fecha y número de publicación internacional: **28.02.2008 WO08024999**

(96) Fecha de presentación y número de la solicitud europea: **24.08.2007 E 07841355 (6)**

(97) Fecha y número de publicación de la concesión europea: **28.03.2018 EP 2070291**

(54) Título: **Sistemas y procedimientos para la gestión de claves para sistemas de comunicación inalámbrica**

(30) Prioridad:

24.08.2006 US 840141 P
22.08.2007 US 843583

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.06.2018

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
INTERNATIONAL IP ADMINISTRATION 5775 MOREHOUSE DRIVE
SAN DIEGO, CALIFORNIA 92121, US

(72) Inventor/es:

NARAYANAN, VIDYA;
DONDETI, LAKSHMINATH, REDDY;
AGASHE, PARAG, ARUN y
BENDER, PAUL, E.

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Sistemas y procedimientos para la gestión de claves para sistemas de comunicación inalámbrica

[0001] La presente solicitud de patente reivindica la prioridad de la solicitud provisional n.º 60/840141 titulada "Systems and Methods for Key Management for Wireless Communication Systems" [Sistemas y procedimientos para la gestión de claves para sistemas de comunicación inalámbrica], presentada el 24 de agosto de 2006 y asignada al cesionario de la misma.

ANTECEDENTES

Campo

[0002] Diversas características pertenecen a sistemas de comunicación inalámbrica. Al menos un aspecto se refiere a un sistema y procedimiento para la gestión de claves para el acceso a la red con baja latencia.

Antecedentes

[0003] Las redes de comunicación inalámbrica permiten a los dispositivos de comunicación transmitir y/o recibir información mientras está en movimiento. Estas redes de comunicación inalámbrica pueden estar comunicativamente acopladas a otras redes públicas o privadas para permitir la transferencia de información hacia y desde el terminal de acceso móvil. Dichas redes de comunicación incluyen típicamente una pluralidad de puntos de acceso (por ejemplo, estaciones base) que proporcionan enlaces de comunicación inalámbrica a terminales de acceso (por ejemplo, dispositivos de comunicación móvil, teléfonos móviles, terminales de usuario inalámbricos). Los puntos de acceso pueden ser estacionarios (por ejemplo, fijados al suelo) o móviles (por ejemplo, montados en satélites, etc.) y estar posicionados para proporcionar una amplia área de cobertura a medida que el terminal de acceso se desplace a través de diferentes áreas de cobertura.

[0004] A medida que un terminal de acceso móvil se mueve, su enlace de comunicación con un nodo de acceso puede degradarse. En esta situación, el nodo móvil puede cambiar o conectarse con otro punto de acceso para un enlace de comunicación de mejor calidad mientras su primer enlace todavía está activo. Este proceso de establecer un enlace de comunicación con otro punto de acceso se denomina "traspaso". El proceso de traspaso típicamente enfrenta el problema de mantener un enlace de comunicación fiable y seguro con la red de comunicación inalámbrica mientras se cambian los puntos de acceso. Los traspasos suaves y los traspasos duros son dos tipos de traspasos comúnmente usados. Un traspaso continuo es aquel en el que se establece un nuevo enlace de comunicación con un nuevo punto de acceso antes de que finalice el enlace de comunicación existente. En un traspaso duro, un enlace de comunicación existente típicamente termina antes de que se establezca un nuevo enlace de comunicación.

[0005] En algunos sistemas de comunicación, cuando un terminal de acceso móvil se conecta a una red de comunicación a través de un punto de acceso, realiza autentificación de acceso a la red para establecer una clave maestra segura. Cada vez que se produce un traspaso, este proceso puede repetirse. Sin embargo, repetir este proceso de autentificación en cada traspaso introduce una latencia inaceptable. Una solución actual para reducir esta latencia es compartir la clave maestra entre los puntos de acceso. Sin embargo, este enfoque crea un serio riesgo de seguridad si un punto de acceso se ve comprometido ya que la clave maestra no se protege y puede utilizarse para comprometer todas las comunicaciones en las que se utiliza esa clave maestra.

[0006] La solicitud de patente europea EP1439667 es otra técnica anterior.

[0007] En consecuencia, se necesita un procedimiento que proporciona un traspaso de baja latencia entre un terminal de acceso y puntos de acceso sin comprometer la seguridad.

SUMARIO

[0008] Una característica proporciona un sistema y procedimiento como se establece en las reivindicaciones adjuntas para la gestión de claves entre un terminal de acceso (por ejemplo, terminal móvil, terminal de usuario inalámbrico, etc.) y uno o más puntos de acceso (por ejemplo, estaciones base, etc.). En particular, se proporciona un esquema para establecer comunicaciones seguras entre un terminal de acceso y un punto de acceso sin riesgo de exposición a una clave maestra para el terminal de acceso. Este enfoque obtiene claves maestras temporales para traspasos de baja latencia y autentificación segura entre un nuevo punto de acceso y el terminal de acceso.

[0009] En un aspecto, se proporciona un esquema de gestión distributiva de claves en el que un punto de acceso actual genera una nueva clave de seguridad que es utilizada por el siguiente punto de acceso con el que se comunica un terminal de acceso. A medida que el terminal de acceso se mueve desde el punto de acceso actual a un nuevo punto de acceso, el punto de acceso actual genera una nueva clave de seguridad basada en su propia clave de seguridad y un identificador único para el nuevo punto de acceso. A continuación, la nueva clave de

seguridad se envía al nuevo punto de acceso. El terminal de acceso genera de forma independiente la misma nueva clave de seguridad con la que puede comunicarse de forma segura con el nuevo punto de acceso.

[0010] En otro aspecto, se proporciona un esquema de gestión centralizada de claves en el que un autentificador mantiene, genera y distribuye nuevas claves de seguridad a los puntos de acceso. Cuando un terminal de acceso se mueve desde un punto de acceso actual a un nuevo punto de acceso, el autentificador genera una nueva clave de seguridad basada en una clave de seguridad maestra (asociada con el terminal de acceso) y un identificador único para el nuevo punto de acceso. A continuación, la nueva clave de seguridad se envía al nuevo punto de acceso. El autentificador repite este proceso cuando el terminal de acceso cambia a otros puntos de acceso. El terminal de acceso genera de forma independiente la misma nueva clave de seguridad con la que puede comunicarse de forma segura con los nuevos puntos de acceso.

[0011] Sin embargo, otra característica proporciona un terminal de acceso que está configurado para establecer y/o mantener un conjunto activo de puntos de acceso con la que puede comunicarse. En lugar de obtener o negociar nuevas claves (por ejemplo, clave maestra o clave de sesión transitoria) cuando un terminal de acceso se mueve a un nuevo punto de acceso, el terminal de acceso mantiene un conjunto activo de claves. Es decir, el terminal de acceso puede mantener o establecer de forma simultánea o concurrente asociaciones de seguridad (por ejemplo, claves) con una pluralidad de puntos de acceso dentro de un sector, área o región. Las claves de seguridad preestablecidas pueden ser empleadas posteriormente por el terminal de acceso para comunicarse con los puntos de acceso en su conjunto activo sin la necesidad de restablecer una relación segura. Dichas claves se pueden obtener mediante un procedimiento de gestión centralizada o distributiva de claves.

[0012] Se proporciona un punto de acceso que comprende una memoria y un procesador. El procesador puede configurarse para (a) generar una segunda clave temporal a partir de una clave maestra; (b) ordenar la transmisión de la segunda clave temporal desde el punto de acceso a un segundo punto de acceso para permitir que el segundo punto de acceso se comunique con un terminal de acceso; (c) establecer una comunicación segura entre el punto de acceso y el terminal de acceso asegurada por una primera clave temporal, en el que la primera clave temporal se basa al menos parcialmente en una clave maestra diferente; y/o (d) recibir una solicitud del terminal de acceso para traspasar la comunicación segura desde el punto de acceso al segundo punto de acceso; en el que la clave maestra utilizada para generar la segunda clave temporal se basa al menos parcialmente en la clave maestra diferente. La clave maestra puede ser una clave maestra por pares que se puede basar en una clave maestra de nivel superior asociada con el terminal de acceso. El procesador puede generar la segunda clave temporal a partir de la clave maestra cuando se inicia un traspaso de comunicación con el terminal de acceso desde el punto de acceso al segundo punto de acceso. El procesador puede configurarse además para (a) establecer una comunicación segura entre el punto de acceso y el terminal de acceso asegurada por una primera clave temporal, en el que la primera clave temporal se basa al menos parcialmente en la clave maestra; (b) recibir una solicitud del terminal de acceso para traspasar la comunicación segura desde el punto de acceso al segundo punto de acceso; y/o (c) traspasar la sesión de comunicación al segundo punto de acceso.

[0013] El procesador puede configurarse además para (a) generar una tercera clave temporal, diferente de la segunda clave temporal, a partir de la clave maestra, y (b) ordenar la transmisión de la segunda clave temporal desde el punto de acceso a un tercer punto de acceso para comunicarse con el terminal de acceso. La segunda clave temporal también puede basarse en al menos un segundo identificador de punto de acceso único asociado con el segundo punto de acceso y la tercera clave temporal también se basa en al menos un tercer identificador de punto de acceso único asociado con el tercer punto de acceso. La segunda clave temporal y la tercera clave temporal pueden ser claves de sesión transitorias. La tercera clave temporal también puede basarse en al menos un número pseudoaleatorio obtenido por el segundo punto de acceso.

[0014] También se proporciona un procedimiento para (a) generar una segunda clave temporal a partir de una clave maestra en un primer punto de acceso, utilizándose la clave maestra para la comunicación entre el primer punto de acceso y un terminal de acceso; (b) transmitir la segunda clave temporal desde el primer punto de acceso a un segundo punto de acceso para permitir que el segundo punto de acceso se comunique con el terminal de acceso; (c) establecer una comunicación segura entre el primer punto de acceso y el terminal de acceso asegurada por una primera clave temporal, en el que la primera clave temporal se basa al menos parcialmente en una clave maestra diferente; (d) recibir una solicitud desde el terminal de acceso para traspasar la sesión de comunicación segura desde el primer punto de acceso al segundo punto de acceso, en el que la clave maestra utilizada para generar la segunda clave temporal se basa al menos parcialmente en la clave maestra diferente; (e) establecer una comunicación segura entre el primer punto de acceso y el terminal de acceso asegurada por una primera clave temporal, en el que la primera clave temporal se basa al menos parcialmente en la clave maestra; (f) recibir una solicitud del terminal de acceso para traspasar la comunicación segura desde el primer punto de acceso al segundo punto de acceso; y/o (g) traspasar la comunicación segura al segundo punto de acceso. La clave maestra puede ser una clave maestra por pares basada en una clave maestra de nivel superior asociada con el terminal de acceso. La clave maestra diferente puede ser recibida por el primer punto de acceso desde un tercer punto de acceso con el que el terminal de acceso se comunicó previamente. Adicionalmente, generar la segunda clave temporal puede comprender generar la segunda clave temporal cuando se inicia un traspaso de comunicación con el terminal de acceso desde el primer punto de acceso al segundo punto de acceso.

[0015] El procedimiento puede comprender además (a) generar una tercera clave temporal, diferente de la segunda clave temporal, a partir de la clave maestra y transmitir la tercera clave temporal desde el primer punto de acceso a un tercer punto de acceso para comunicarse con el terminal de acceso. La segunda clave temporal también puede basarse en al menos un segundo identificador de punto de acceso único asociado con el segundo punto de acceso y la tercera clave temporal también se basa en al menos un tercer identificador de punto de acceso único asociado con el tercer punto de acceso. La segunda clave temporal y la tercera clave temporal pueden ser claves de sesión transitorias.

[0016] En consecuencia, se proporciona un aparato, que comprende: (a) medios para generar una segunda clave temporal a partir de una clave maestra en un primer punto de acceso, utilizándose la clave maestra para la comunicación entre el primer punto de acceso y un terminal de acceso; (b) medios para transmitir la segunda clave temporal desde el primer punto de acceso a un segundo punto de acceso para permitir que el segundo punto de acceso se comunique con el terminal de acceso; (c) medios para generar una tercera clave temporal, diferente de la segunda clave temporal, a partir de la clave maestra; (d) medios para transmitir la tercera clave temporal desde el primer punto de acceso a un tercer punto de acceso para comunicarse con el terminal de acceso; (e) medios para iniciar un traspaso de comunicación desde el primer punto de acceso al segundo punto de acceso; (f) medios para establecer una comunicación segura entre el primer punto de acceso y el terminal de acceso asegurada por una primera clave temporal, en el que la primera clave temporal se basa al menos parcialmente en la clave maestra; (g) medios para recibir una solicitud desde el terminal de acceso para traspasar la comunicación segura desde el primer punto de acceso al segundo punto de acceso; y/o (h) medios para traspasar la comunicación segura al segundo punto de acceso.

[0017] El aparato puede comprender además (a) medios para establecer una comunicación segura entre el primer punto de acceso y el terminal de acceso asegurada por una primera clave temporal, en el que la primera clave temporal se basa al menos parcialmente en una clave maestra diferente; y/o (b) medios para recibir una solicitud desde el terminal de acceso para traspasar la comunicación segura desde el primer punto de acceso al segundo punto de acceso; en el que la clave maestra utilizada para generar la segunda clave temporal se basa al menos parcialmente en la clave maestra diferente.

[0018] El aparato también puede comprender (a) medios para generar una tercera clave temporal, diferente de la segunda clave temporal, a partir de la clave maestra y transmitir la tercera clave temporal desde el primer punto de acceso a un tercer punto de acceso para comunicarse con el terminal de acceso. La segunda clave temporal también puede basarse en al menos un segundo identificador de punto de acceso único asociado con el segundo punto de acceso y la tercera clave temporal también se basa en al menos un tercer identificador de punto de acceso único asociado con el tercer punto de acceso. La segunda clave temporal y la tercera clave temporal pueden ser claves de sesión transitorias.

[0019] Un medio legible por procesador que comprende instrucciones que pueden ser utilizadas por uno o más procesadores, comprendiendo las instrucciones: (a) instrucciones para generar una segunda clave temporal a partir de una clave maestra en un primer punto de acceso, usándose la clave maestra para la comunicación entre el primer punto de acceso y un terminal de acceso; (b) instrucciones para transmitir la clave temporal desde el primer punto de acceso a un segundo punto de acceso para permitir que el segundo punto de acceso se comunique con el terminal de acceso; (c) instrucciones para establecer una comunicación segura entre el primer punto de acceso y el terminal de acceso asegurada por una primera clave temporal, en el que la primera clave temporal se basa al menos parcialmente en una clave maestra diferente; (d) instrucciones para recibir una solicitud del terminal de acceso para traspasar la comunicación segura desde el primer punto de acceso al segundo punto de acceso; en el que la clave maestra utilizada para generar la segunda clave temporal se basa al menos parcialmente en la clave maestra diferente; (e) instrucciones para establecer una comunicación segura entre el primer punto de acceso y el terminal de acceso asegurada por una primera clave temporal, en el que la primera clave temporal se basa al menos parcialmente en la clave maestra; (f) instrucciones para recibir una solicitud desde el terminal de acceso para traspasar la comunicación segura desde el primer punto de acceso al segundo punto de acceso; y/o (g) instrucciones para traspasar la comunicación segura al segundo punto de acceso.

[0020] La segunda clave temporal puede generarse para iniciar un traspaso de comunicación desde el primer punto de acceso al segundo punto de acceso. El medio legible por procesador también puede incluir instrucciones para generar una tercera clave temporal, diferente de la segunda clave temporal, a partir de la clave maestra y transmitir la tercera clave temporal desde el primer punto de acceso a un tercer punto de acceso para comunicarse con el terminal de acceso.

[0021] También se proporciona un procesador que comprende: un circuito de procesamiento configurado para (a) establecer una comunicación segura entre el primer punto de acceso y el terminal de acceso asegurada por una primera clave temporal, en el que la primera clave temporal se basa al menos parcialmente en una clave maestra diferente; y/o (b) recibir una solicitud desde el terminal de acceso para traspasar la sesión de comunicación segura desde el primer punto de acceso al segundo punto de acceso; en el que la clave maestra utilizada para generar la segunda clave temporal se basa al menos parcialmente en la clave maestra diferente. El circuito de procesamiento

también puede configurarse para generar una tercera clave temporal, diferente de la segunda clave temporal, a partir de la clave maestra y transmitir la tercera clave temporal desde el primer punto de acceso a un tercer punto de acceso para comunicarse con el terminal de acceso; en el que la segunda clave temporal también se basa en al menos un segundo identificador de punto de acceso único asociado con el segundo punto de acceso y la tercera clave temporal también se basa en al menos un tercer identificador de punto de acceso único asociado con el tercer punto de acceso. En algunas implementaciones, el circuito de procesamiento también puede configurarse para (a) establecer una comunicación segura entre el primer punto de acceso y el terminal de acceso asegurada por una primera clave temporal, en el que la primera clave temporal se basa al menos parcialmente en la clave maestra; (b) recibir una solicitud del terminal de acceso para traspasar la comunicación segura desde el primer punto de acceso al segundo punto de acceso; y/o (c) traspasar la comunicación segura al segundo punto de acceso.

[0022] También se proporciona un punto de acceso que comprende: una memoria y un procesador acoplado con la memoria. El procesador puede configurarse para (a) recibir una primera clave temporal desde otro punto de acceso; (b) ordenar la comunicación con un terminal de acceso utilizando la primera clave temporal para asegurar la comunicación; (c) recibir una indicación de que la comunicación con el terminal de acceso debe ser traspasada a un segundo punto de acceso; (d) generar una segunda clave temporal basada en la primera clave temporal; y/o (e) enviar la segunda clave temporal al segundo punto de acceso. El procesador puede configurarse además para recibir la primera clave temporal desde el otro punto de acceso cuando se inicia el traspaso al punto de acceso desde el otro punto de acceso para la comunicación con el terminal de acceso. La primera clave temporal puede funcionar durante un período de tiempo limitado, y el procesador está configurado además para recibir una clave maestra para asegurar la comunicación entre el terminal de acceso y el punto de acceso y para descartar la utilización de la primera clave temporal.

[0023] También se proporciona un procedimiento que comprende: (a) recibir una primera clave temporal en un primer punto de acceso desde otro punto de acceso; (b) comunicarse con un terminal de acceso utilizando la primera clave temporal para asegurar la comunicación; (c) recibir una indicación de que una comunicación con el primer terminal de acceso debe ser traspasada a un segundo punto de acceso; (d) generar una segunda clave temporal basada en la primera clave temporal; y/o (e) enviar la segunda clave temporal al segundo punto de acceso.

[0024] La primera clave temporal puede funcionar durante un período de tiempo limitado. El procedimiento puede comprender además (a) recibir una clave maestra para la comunicación entre el terminal de acceso y el primer punto de acceso y descartar la utilización de la primera clave temporal; y/o (b) recibir la primera clave temporal desde el otro punto de acceso cuando se inicia el traspaso al primer punto de acceso desde el otro punto de acceso para la comunicación con el terminal de acceso.

[0025] En consecuencia, se proporciona un aparato, que comprende: (a) medios para recibir una primera clave temporal en un primer punto de acceso, desde otro punto de acceso; (b) medios para comunicarse con un terminal de acceso utilizando la primera clave temporal para asegurar la comunicación; (c) medios para recibir una clave maestra para la comunicación entre el terminal de acceso y el primer punto de acceso; (d) medios para recibir la primera clave temporal desde el otro punto de acceso cuando se inicia el traspaso al primer punto de acceso desde el otro punto de acceso para la comunicación con el terminal de acceso; (e) medios para recibir una indicación de que la comunicación con el primer terminal de acceso debe ser traspasada a un segundo punto de acceso; (f) medios para generar una segunda clave temporal basada en la primera clave temporal; (g) medios para enviar la segunda clave temporal al segundo punto de acceso; y/o (h) medios para descartar la utilización de la primera clave temporal.

[0026] También se proporciona un medio legible por procesador que comprende instrucciones que pueden ser utilizadas por uno o más procesadores, comprendiendo las instrucciones: (a) instrucciones para recibir una primera clave temporal en un primer punto de acceso, desde otro punto de acceso; (b) instrucciones para comunicarse con un terminal de acceso utilizando la primera clave temporal para asegurar la comunicación; (c) instrucciones para recibir una indicación de que la comunicación con el primer terminal de acceso debe ser traspasada a un segundo punto de acceso; (d) instrucciones para generar una segunda clave temporal basada en la primera clave temporal; y/o (e) instrucciones para enviar la segunda clave temporal al segundo punto de acceso. La primera clave temporal desde el otro punto de acceso puede recibirse cuando se inicia un traspaso al primer punto de acceso desde el otro punto de acceso para la comunicación con el terminal de acceso.

[0027] También se proporciona un procesador que comprende un circuito de procesamiento configurado para (a) recibir una primera clave temporal en un primer punto de acceso desde otro punto de acceso; y (b) comunicarse con un terminal de acceso utilizando la primera clave temporal para asegurar la comunicación. La primera clave temporal puede funcionar durante un período de tiempo limitado y el circuito de procesamiento puede configurarse además para recibir una clave maestra para la comunicación entre el terminal de acceso y el primer punto de acceso y descartar la utilización de la primera clave temporal. En algunas implementaciones, el circuito de procesamiento puede configurarse adicionalmente para recibir la primera clave temporal desde el otro punto de acceso cuando se inicia el traspaso al primer punto de acceso desde el otro punto de acceso para la comunicación con el terminal de acceso. En otras implementaciones, el circuito de procesamiento también puede configurarse para (a) recibir una indicación de que una comunicación con el primer terminal de acceso debe ser traspasada a un segundo punto de

acceso; (b) generar una segunda clave temporal basada en la primera clave temporal; y/o (c) enviar la segunda clave temporal al segundo punto de acceso.

[0028] Puede disponerse también de un terminal de acceso comprendiendo: una memoria y un procesador acoplado con la memoria. El procesador puede configurarse para (a) generar una primera clave temporal a partir de una clave maestra utilizada para la comunicación entre un primer punto de acceso y el terminal de acceso; (b) ordenar la comunicación utilizando la primera clave temporal entre un segundo punto de acceso y el terminal de acceso; (c) ordenar a un servidor de autentificación que proporcione otra clave maestra para la comunicación con el segundo punto de acceso y que interrumpa el uso de la primera clave temporal; y/o (d) proporcionar una indicación de que la comunicación con el segundo punto de acceso debe ser traspasada a un tercer punto de acceso. La clave maestra puede ser una segunda clave temporal utilizada para la comunicación entre un primer punto de acceso y el terminal de acceso.

[0029] El procesador puede también configurarse para (a) generar una segunda clave temporal a partir de la primera clave temporal utilizada para la comunicación entre el segundo punto de acceso y el terminal de acceso, y/u (b) ordenar la comunicación utilizando la segunda clave temporal entre un tercer punto de acceso y el terminal de acceso.

[0030] El procesador puede también configurarse para (a) generar una segunda clave temporal a partir de la clave maestra; y/u (b) ordenar la comunicación utilizando la segunda clave temporal entre un tercer punto de acceso y el terminal de acceso.

[0031] En algunas implementaciones del terminal de acceso, el procesador puede configurarse además para (a) escanear en busca de puntos de acceso; (b) agregar puntos de acceso a un conjunto activo de puntos de acceso a medida que se identifican; y/o (c) establecer una clave segura con cada punto de acceso a medida que se agrega al conjunto activo. En un sistema de gestión distributiva de claves, el procesador se configura adicionalmente para generar una clave de sesión transitoria para cada punto de acceso a medida que se agrega al conjunto activo, en el que la clave de sesión transitoria se basa en una clave maestra provisional asociada con otro punto de acceso en el conjunto activo. En un sistema centralizado de gestión de claves, el procesador puede configurarse adicionalmente para generar una clave de sesión transitoria para cada punto de acceso a medida que se agrega al conjunto activo, en el que la clave de sesión transitoria se basa en una clave transitoria maestra y un identificador de punto de acceso único para el punto de acceso.

[0032] También se proporciona un procedimiento operativo en un terminal de acceso, que comprende: (a) comunicarse con un primer punto de acceso utilizando una clave maestra; (b) generar una primera clave temporal a partir de la clave maestra; (c) comunicarse con un segundo punto de acceso utilizando la primera clave temporal; (d) ordenar a un servidor de autentificación que proporcione otra clave maestra para la comunicación con el segundo punto de acceso y que interrumpa el uso de la primera clave temporal; (e) proporcionar una indicación de que la comunicación con el segundo punto de acceso debe ser traspasada a un tercer punto de acceso. La clave maestra puede ser una segunda clave temporal utilizada para asegurar la comunicación entre un primer punto de acceso y el terminal de acceso. La clave maestra puede ser una clave maestra por pares compartida con un servidor de autentificación.

[0033] En algunas implementaciones, el procedimiento puede comprender también: (a) generar una segunda clave temporal desde la primera clave temporal utilizada para la comunicación entre el segundo punto de acceso y el terminal de acceso, y/u (b) ordenar la comunicación utilizando la segunda clave temporal entre un tercer punto de acceso y el terminal de acceso.

[0034] En otras implementaciones, el procedimiento puede comprender también: (a) generar una segunda clave temporal a partir de la clave maestra; y/u (b) ordenar la comunicación utilizando la segunda clave temporal entre un tercer punto de acceso y el terminal de acceso.

[0035] En aún otras implementaciones, el procedimiento puede comprender además: (a) escanear en busca de puntos de acceso; (b) agregar puntos de acceso a un conjunto activo de puntos de acceso a medida que se identifican; y/o (c) establecer una clave segura con cada punto de acceso a medida que se agrega al conjunto activo. En un sistema de gestión distributiva de claves, el procedimiento puede comprender además generar una clave de sesión transitoria para cada punto de acceso a medida que se agrega al conjunto activo, en el que la clave de sesión transitoria se basa en una clave maestra provisional asociada con otro punto de acceso en el conjunto activo. En un sistema centralizado de gestión de claves, el procedimiento puede comprender además generar una clave de sesión transitoria para cada punto de acceso a medida que se agrega al conjunto activo, en el que la clave de sesión transitoria se basa en una clave transitoria maestra y un identificador único de punto de acceso para el punto de acceso.

[0036] En consecuencia, también se proporciona un terminal de acceso que comprende: (a) medios para comunicarse con un primer punto de acceso utilizando una clave maestra; (b) medios para generar una primera clave temporal a partir de la clave maestra; (c) medios para comunicarse con un segundo punto de acceso utilizando

la primera clave temporal; (d) medios para ordenar a un servidor de autentificación que proporcione otra clave maestra para la comunicación con el segundo punto de acceso y que interrumpa el uso de la primera clave temporal; y/o (e) medios para proporcionar una indicación de que la comunicación con el segundo punto de acceso debe ser traspasada a un tercer punto de acceso. La clave maestra es una segunda clave temporal utilizada para asegurar la comunicación entre un primer punto de acceso y el terminal de acceso.

[0037] En algunas implementaciones, el terminal de acceso puede incluir además (a) medios para generar una segunda clave temporal a partir de la primera clave temporal utilizada para la comunicación entre el segundo punto de acceso y el terminal de acceso, y/o (b) medios para ordenar la comunicación utilizando la segunda clave temporal entre un tercer punto de acceso y el terminal de acceso.

[0038] En algunas implementaciones, el terminal de acceso puede incluir además (a) medios para generar una segunda clave temporal a partir de la clave maestra; y/o (b) medios para ordenar la comunicación utilizando la segunda clave temporal entre un tercer punto de acceso y el terminal de acceso.

[0039] También se proporciona un medio legible por procesador que comprende instrucciones que pueden ser utilizadas por uno o más procesadores, comprendiendo las instrucciones: (a) instrucciones para comunicarse con un primer punto de acceso desde un terminal de acceso utilizando una clave maestra; (b) instrucciones para generar una primera clave temporal a partir de la clave maestra; (c) instrucciones para comunicarse con un segundo punto de acceso utilizando la primera clave temporal; (d) instrucciones para proporcionar una indicación de que la comunicación con el segundo punto de acceso debe ser traspasada a un tercer punto de acceso.

[0040] En algunas implementaciones, el medio legible por procesador puede incluir además (a) instrucciones para generar una segunda clave temporal a partir de la primera clave temporal utilizada para la comunicación entre el segundo punto de acceso y el terminal de acceso, y/o (b) instrucciones para ordenar la comunicación utilizando la segunda clave temporal entre un tercer punto de acceso y el terminal de acceso.

[0041] En otras implementaciones, el medio legible por procesador puede incluir además (a) instrucciones para generar una segunda clave temporal a partir de la clave maestra y/o (b) instrucciones para ordenar la comunicación utilizando la segunda clave temporal entre un tercer punto de acceso y el terminal de acceso.

[0042] También se proporciona un procesador que comprende un circuito de procesamiento configurado para (a) comunicarse con un primer punto de acceso utilizando una clave maestra; (b) generar una primera clave temporal a partir de la clave maestra; y/o (c) comunicarse con un segundo punto de acceso utilizando la primera clave temporal. La clave maestra puede ser una segunda clave temporal utilizada para asegurar la comunicación entre un primer punto de acceso y el terminal de acceso. El circuito de procesamiento también puede configurarse adicionalmente para ordenar a un servidor de autentificación que proporcione otra clave maestra para la comunicación con el segundo punto de acceso y que interrumpa el uso de la primera clave temporal. En algunas implementaciones, el circuito de procesamiento también puede configurarse para (a) generar una segunda clave temporal a partir de la primera clave temporal utilizada para la comunicación entre el segundo punto de acceso y el terminal de acceso, y/u (b) ordenar la comunicación utilizando la segunda clave temporal entre un tercer punto de acceso y el terminal de acceso. En otra implementación, el circuito de procesamiento también puede configurarse para (a) generar una segunda clave temporal a partir de la clave maestra; (b) ordenar la comunicación utilizando la segunda clave temporal entre un tercer punto de acceso y el terminal de acceso. En algunas implementaciones, el circuito de procesamiento está configurado además para (a) escanear en busca de puntos de acceso; (b) agregar puntos de acceso a un conjunto activo de puntos de acceso a medida que se identifican; y (c) establecer una clave segura con cada punto de acceso a medida que se agrega al conjunto activo.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0043] Las características, la naturaleza y las ventajas de los presentes aspectos pueden resultar más evidentes a partir de la descripción detallada expuesta a continuación cuando se tome en consideración junto con los dibujos, en los que caracteres de referencia iguales identifican a los mismos puntos en todo el documento.

La figura 1 ilustra un sistema de comunicación inalámbrica con gestión distribuida de claves que facilita traspasos de sesiones de comunicación seguras y de baja latencia.

La figura 2 (que comprende las Figs. 2A y 2B) es un diagrama de flujo que ilustra el funcionamiento de un sistema de comunicación inalámbrica con gestión distribuida de claves que facilita traspasos seguros y de baja latencia.

La figura 3 ilustra un modelo distributivo de claves de seguridad que pueden usarse para asegurar sesiones de comunicación entre un terminal de acceso y un nuevo punto de acceso durante y/o después del traspaso.

La figura 4 ilustra un sistema de comunicación inalámbrica con administración centralizada de claves que facilita traspasos seguros de baja latencia.

La figura 5 (que comprende las Figs. 5A y 5B) es un diagrama de flujo que ilustra el funcionamiento de un sistema de comunicación inalámbrica con gestión centralizada de claves que facilita traspasos seguros y de baja latencia.

La figura 6 ilustra un modelo centralizado de claves de seguridad que puede usarse para asegurar sesiones de comunicación entre un terminal de acceso y un nuevo punto de acceso durante y/o después del traspaso.

La figura 7 es un diagrama de bloques que ilustra un terminal de acceso configurado para realizar traspasos de sesión de comunicación segura de baja latencia.

La figura 8 es un diagrama de flujo que ilustra un procedimiento operativo en un terminal de acceso para facilitar un traspaso de sesión de comunicación segura desde un primer punto de acceso a un nuevo punto de acceso usando un enfoque de gestión distributiva de claves.

La figura 9 es un diagrama de flujo que ilustra un procedimiento operativo en un terminal de acceso para facilitar un traspaso de sesión de comunicación segura desde un primer punto de acceso a un nuevo punto de acceso usando un enfoque de gestión centralizada de claves.

La figura 10 es un diagrama de bloques que ilustra un autentificador configurado para facilitar traspasos de sesión de comunicación segura de baja latencia.

La figura 11 es un diagrama de flujo que ilustra un procedimiento operativo en un autentificador para facilitar un traspaso de sesión de comunicación segura desde un primer punto de acceso a un nuevo punto de acceso usando un enfoque de gestión distributiva de claves.

La figura 12 es un diagrama de flujo que ilustra un procedimiento operativo en un autentificador para facilitar un traspaso de sesión de comunicación segura desde un primer punto de acceso a un nuevo punto de acceso usando un enfoque centralizado de gestión de claves.

La figura 13 es un diagrama de bloques que ilustra un punto de acceso configurado para facilitar traspasos de sesión de comunicación segura de baja latencia.

La figura 14 es un diagrama de bloques que ilustra un modo de realización alternativo de un punto de acceso que tiene un autentificador integrado

La figura 15 es un diagrama de flujo que ilustra un procedimiento operativo en un primer punto de acceso para facilitar un traspaso de sesión de comunicación segura desde el primer punto de acceso a un segundo punto de acceso usando un enfoque de gestión distributiva de claves.

La figura 16 es un diagrama de flujo que ilustra un procedimiento operativo en un primer punto de acceso para facilitar un traspaso de sesión de comunicación segura desde el primer punto de acceso a un segundo punto de acceso usando un enfoque de gestión centralizada de claves.

La figura 17 es un diagrama de flujo que ilustra un procedimiento operativo en un terminal de acceso para obtener y/o establecer un conjunto activo de puntos de acceso.

DESCRIPCIÓN DETALLADA

[0044] En la siguiente descripción, se dan detalles específicos para proporcionar una comprensión exhaustiva de los modos de realización. Sin embargo, se entenderá por un experto en la técnica que pueden llevarse a la práctica los modos de realización sin estos detalles específicos. Por ejemplo, pueden mostrarse circuitos en diagramas de bloques para no oscurecer los modos de realización con detalles innecesarios. En otros casos, pueden mostrarse en detalle circuitos ya conocidos, estructuras y técnicas para no complicar los modos de realización.

[0045] Además, debe observarse que los modos de realización pueden describirse como un proceso que se representa como un organigrama, un diagrama de flujo, un diagrama estructural o un diagrama de bloques. Aunque un diagrama de flujo puede describir las operaciones como un proceso secuencial, muchas de las operaciones pueden realizarse en paralelo o simultáneamente. Además, el orden de las operaciones puede reorganizarse. Un proceso se termina cuando sus operaciones se completan. Un proceso puede corresponder a un procedimiento, una función, un procedimiento, una subrutina, un subprograma, etc. Cuando un proceso se corresponde con una función, su finalización corresponde a un retorno de la función a la función de llamada o la función principal.

[0046] Además, un medio de almacenamiento puede representar uno o más dispositivos para almacenar datos, incluyendo memora de solo lectura (ROM), memoria de acceso aleatorio (RAM), medios de almacenamiento de disco magnético, medios de almacenamiento óptico, dispositivos de memoria flash y/u otros medios legibles por

máquina para almacenar información. La expresión "medio legible por máquina" incluye, pero sin limitación, dispositivos de almacenamiento portátiles o fijos, dispositivos de almacenamiento ópticos, canales inalámbricos y diversos otros medios capaces de almacenar, contener o llevar una instrucción o instrucciones y/o datos.

[0047] Además, los modos de realización pueden implementarse mediante hardware, software, firmware, middleware, microcódigo, o cualquier combinación de los mismos. Al implementarse en software, firmware, middleware o microcódigo, el código de programa o segmentos de código para realizar las tareas necesarias pueden almacenarse en un medio legible por máquina, tal como un medio de almacenamiento u otro almacenamiento o almacenamientos. Un procesador puede realizar las tareas necesarias. Un segmento de código puede representar un procedimiento, una función, un subprograma, un programa, una rutina, una subrutina, un módulo, un paquete de software, una clase o cualquier combinación de instrucciones, estructuras de datos o sentencias de programa. Un segmento de código puede acoplarse a otro segmento de código o a un circuito de hardware pasando y/o recibiendo información, datos, argumentos, parámetros o contenidos de memoria. La información, argumentos, parámetros, datos, etc. se puede pasar, enviar o transmitir a través de un medio adecuado que incluye compartir la memoria, el paso de mensajes, el paso de testigos, transmisión por red, etc.

[0048] Una característica proporciona un sistema y procedimiento para la gestión de claves entre un terminal de acceso (por ejemplo, terminal móvil, terminal de usuario inalámbrico, etc.) y uno o más puntos de acceso (por ejemplo, estaciones base, etc.). En particular, se proporciona un esquema para establecer comunicaciones seguras entre un terminal de acceso y un punto de acceso sin riesgo de exposición a una clave maestra para el terminal de acceso. Este enfoque obtiene claves maestras temporales para traspasos de baja latencia y autentificación segura entre un nuevo punto de acceso y el terminal de acceso.

[0049] En un aspecto, se proporciona un esquema de gestión distributiva de claves en el que un punto de acceso actual genera una nueva clave de seguridad que es utilizada por el siguiente punto de acceso con el que se comunica un terminal de acceso. A medida que el terminal de acceso se mueve desde el punto de acceso actual a un nuevo punto de acceso, el punto de acceso actual genera una nueva clave de seguridad basada en su propia clave de seguridad y un identificador único para el nuevo punto de acceso. A continuación, la nueva clave de seguridad se envía al nuevo punto de acceso. El terminal de acceso genera de forma independiente la misma nueva clave de seguridad con la que puede comunicarse de forma segura con el nuevo punto de acceso.

[0050] En otro aspecto, se proporciona un esquema de gestión centralizada de claves en el que un autentificador mantiene, genera y distribuye nuevas claves de seguridad a los puntos de acceso. Cuando un terminal de acceso se mueve desde un punto de acceso actual a un nuevo punto de acceso, el autentificador genera una nueva clave de seguridad basada en una clave de seguridad maestra (asociada con el terminal de acceso) y un identificador único para el nuevo punto de acceso. A continuación, la nueva clave de seguridad se envía al nuevo punto de acceso. El autentificador repite este proceso cuando el terminal de acceso cambia a otros puntos de acceso. El terminal de acceso genera de forma independiente la misma nueva clave de seguridad con la que puede comunicarse de forma segura con los nuevos puntos de acceso.

[0051] Sin embargo, otra característica proporciona un terminal de acceso que está configurado para establecer y/o mantener un conjunto activo de puntos de acceso con la que puede comunicarse. En lugar de obtener o negociar nuevas claves cuando un terminal de acceso se mueve a un nuevo punto de acceso, el terminal de acceso mantiene un conjunto activo de claves. Es decir, el terminal de acceso puede mantener o establecer de forma simultánea o concurrente asociaciones de seguridad (por ejemplo, claves) con una pluralidad de puntos de acceso dentro de un sector, área o región. Las claves de seguridad preestablecidas pueden ser empleadas posteriormente por el terminal de acceso para comunicarse con los puntos de acceso en su conjunto activo sin la necesidad de restablecer una relación segura. Dichas claves se pueden obtener mediante un procedimiento de gestión centralizada o distributiva de claves.

[0052] La figura 1 ilustra un sistema de comunicación inalámbrica con gestión distribuida de claves que facilita traspasos de sesiones de comunicación de baja latencia, seguros. El sistema de comunicación inalámbrica de acceso múltiple 100 puede incluir múltiples células, por ejemplo las células 102, 104 y 106. Cada célula 102, 104 y 106 puede incluir un punto de acceso 110, 112 y 114 que proporciona cobertura a múltiples sectores dentro de la célula. Cada punto de acceso 110, 112 y 114 puede incluir una o más antenas 116 que proporcionan cobertura de red a terminales móviles (por ejemplo, terminales de usuario) a través de múltiples sectores en una célula. Por ejemplo, en la célula 102, el punto de acceso 110 incluye un grupo de antenas 116 donde cada antena proporciona cobertura de red a un sector diferente dentro de la célula 102. De forma similar, en las células 104 y 106 los puntos de acceso 112 y 114 pueden incluir grupos de antenas, donde cada antena proporciona cobertura de red a un sector diferente dentro de una célula.

[0053] Los puntos de acceso 110, 112, y 114 dentro de cada célula 102, 104, y 106 puede proporcionar servicios de conexión de red a uno o más terminales de acceso. Por ejemplo, a medida que el terminal de acceso 118 se mueve a través de las diferentes células 102, 104, 106, puede estar en comunicación con los puntos de acceso 110, 112 y 114. Como se usa en el presente documento, las transmisiones desde un punto de acceso a un terminal de acceso

se denominan enlace directo o enlace descendente y las transmisiones desde el terminal de acceso al punto de acceso se denominan enlace inverso o enlace ascendente.

[0054] Un autentificador 120 puede servir para gestionar el funcionamiento de los puntos de acceso 110, 112, y 114 y/o para autentificar terminales de acceso. En algunas aplicaciones, el autentificador 120 puede mantener claves maestras de nivel superior asociadas de manera única con los terminales de acceso que son atendidos por la red 100. Las claves maestras (MK) pueden mantenerse entre el autentificador 120 y los terminales de acceso a los que sirve. Por ejemplo, el autentificador 120 y el terminal de acceso 118 conocen una primera clave maestra MK de nivel superior, y está asociada de manera única con el terminal de acceso. Cuando se implementa un protocolo de autentificación extensible (EAP), dicha clave maestra de nivel superior (MK) a menudo se denomina clave de sesión maestra (MSK). Debe entenderse que siempre que se use el término 'clave maestra', puede incluir dicha MSK para implementaciones de EAP.

[0055] En varias aplicaciones, el autentificador 120 puede ser parte de un controlador de red, controlador de estación base, o controlador de punto de acceso que sea remoto o esté alejado de los puntos de acceso 110, 112, y 114, o pueda ubicarse junto a uno de los puntos de acceso.

[0056] En algunos aspectos, cada terminal de acceso puede estar en comunicación con dos o más sectores de una o más células. Esto se puede hacer para permitir el traspaso entre diferentes sectores o células a medida que un terminal de acceso se mueve o viaja, para una gestión adecuada de la capacidad y/o por otros motivos.

[0057] Como se usa en el presente documento, un punto de acceso puede ser una estación fija utilizada para comunicarse con los terminales de acceso y también puede denominarse, e incluir parte de o la totalidad de la funcionalidad de, una estación base, un Nodo B, o alguna otra terminología. Un terminal de acceso también puede denominarse, e incluir parte de o la totalidad de la funcionalidad de, un equipo de usuario (UE), un dispositivo de comunicación inalámbrica, un terminal, un terminal móvil, una estación móvil o alguna otra terminología.

[0058] Las técnicas de transmisión descritas en el presente documento también pueden usarse para varios sistemas de comunicación inalámbrica tales como un sistema CDMA, un sistema TDMA, un sistema FDMA, un sistema de acceso múltiple por división de frecuencia ortogonal (OFDMA), un sistema FDMA de una sola portadora (SC-FDMA), etc. Un sistema OFDMA usa multiplexación por división de frecuencia ortogonal (OFDM), que es una técnica de modulación que divide el ancho de banda global del sistema en múltiples (K) sub-portadoras ortogonales. Estas sub-portadoras también se llaman tonos, bins, etc. Con el OFDM, cada sub-portadora puede modularse de forma independiente con datos. Un sistema de SC-FDMA puede usar FDMA intercalado (IFDMA) para transmitir en sub-portadoras que están distribuidas por el ancho de banda del sistema, FDMA localizado (LFDMA) para transmitir en un bloque de sub-portadoras adyacentes o FDMA mejorado (EFDMA) para transmitir en múltiples bloques de sub-portadoras adyacentes. En general, los símbolos de modulación se envían en el dominio de frecuencia con OFDM, y en el dominio del tiempo con SC-FDMA.

[0059] Algunos de los ejemplos descritos en el presente documento se refieren a un protocolo de autentificación extensible (EAP) que proporciona una clave maestra MK por pares en un punto de acceso y un terminal de acceso. La autentificación EAP puede realizarse entre el terminal de acceso y un servidor de autentificación (por ejemplo, en un controlador de red, servidor AAA, etc.) a través del punto de acceso que actúa como un autentificador; el autentificador puede actuar como servidor de autentificación en algunos casos. En algunos casos, el autentificador puede ubicarse junto a uno o más puntos de acceso.

[0060] Una clave de sesión transitoria (TSK) se establece y se mantiene entre un punto de acceso y un terminal de acceso. La TSK puede calcularse (por ejemplo, basándose en la clave maestra MK, o MSK para aplicaciones EAP) para asegurar las comunicaciones entre el terminal de acceso y el punto de acceso. Por ejemplo, la TSK se puede calcular de la forma siguiente: TSKn = PRF (MKn, Datos), donde PRF es una función pseudoaleatoria como HMAC-SHA-256 o AES-128-CMAC u otra función de obtención de clave, y los datos pueden ser parámetros como un identificador de punto de acceso (AP_ID), identificador de terminal de acceso (AT_ID), un número aleatorio generado por cualquiera de las partes o incluso una secuencia estática. Los parámetros de datos pueden conocerse de acuerdo con el diseño del sistema o pueden comunicarse durante la sesión. En este enfoque, no se usan variables dinámicas en la obtención de TSK y, por lo tanto, no se necesita intercambio de claves más allá de la re-autentificación EAP o EAP para la TSK.

[0061] A menudo, una sesión de comunicación entre un punto de acceso y un terminal de acceso utiliza algún tipo de cifrado para proteger los datos durante la transmisión, por ejemplo usando un esquema de cifrado de clave. Sin embargo, durante el traspaso de comunicaciones desde un punto de acceso actual a un nuevo punto de acceso, existe un problema sobre cómo continuar las comunicaciones seguras con el nuevo punto de acceso sin comprometer la sesión de comunicación transmitiendo la clave entre puntos de acceso u otros valores de generación de cifrado de forma inalámbrica. Dado que se debe establecer una nueva clave de sesión transitoria (TSK) con el nuevo punto de acceso, primero se debe establecer una nueva clave maestra (MK) entre el nuevo punto de acceso y el terminal de acceso. Además, sería preferible evitar el intercambio de claves de sesión entre los puntos de acceso, ya que esto introduce una vulnerabilidad en la que el compromiso de un punto de acceso da

como resultado el compromiso de puntos de acceso que participan en compartir claves con el punto de acceso comprometido. Sin embargo, negociar la nueva clave de sesión transitoria en la ruta crítica del traspaso aumenta la latencia de traspaso. Por lo tanto, sería deseable proporcionar una clave de sesión segura, de baja latencia para cada punto de acceso y par de terminales de acceso.

[0062] Según una característica, se proporciona un esquema de gestión distributiva de claves en el que un punto de acceso actual genera una clave de sesión maestra provisional (I-MK) que es utilizada por el siguiente punto de acceso para comunicarse con un terminal móvil después del traspaso. Por ejemplo, el terminal de acceso 118a puede asegurar las comunicaciones con su punto de acceso actual 110 usando una primera clave maestra provisional asegurada I-MK1. La primera clave maestra provisional I-MK1 puede haberse basado en la clave maestra de nivel superior MKo (conocida por el autentificador 120 y el terminal de acceso 118 que está asociado de forma única con el terminal de acceso 118). Cuando el terminal de acceso 118b se mueve a un sector o célula diferente, su sesión de comunicación puede ser traspasada a un nuevo punto de acceso 112. Para asegurar las comunicaciones entre el terminal de acceso 118b y el nuevo punto de acceso 112 inmediatamente después del traspaso, el punto de acceso actual 110 genera una segunda clave maestra provisional I-MK2 basada en su primera clave maestra provisional I-MK1 y proporciona esta nueva clave maestra I -MK2 al nuevo punto de acceso 112. El nuevo punto de acceso 112 usa entonces la segunda clave maestra de nivel superior I-MK2 para su sesión de comunicación con el terminal de acceso 118b. La segunda clave maestra provisional I-MK2 se puede usar durante un período de tiempo prolongado, o hasta que se obtenga otra clave maestra provisional, para asegurar las sesiones de comunicación. Si bien la segunda clave maestra provisional I-MK2 se puede generar basándose en la primera clave maestra provisional I-MK1, no es una clave maestra de nivel superior. De este modo, la clave maestra de nivel superior MKo asociada con el terminal de acceso 118 no se transmite ni por enlace cableado ni de forma inalámbrica. Una vez que se ha establecido una clave maestra provisional entre un punto de acceso y un terminal de acceso, se puede usar para obtener una clave de sesión transitoria provisional (I-TSK).

[0063] La figura 2 (que comprende las figuras 2A y 2B) es un diagrama de flujo que ilustra el funcionamiento de un sistema de comunicación inalámbrica con gestión distribuida de claves que facilita traspasos seguros y de baja latencia. En este ejemplo, el autentificador 120, el punto de acceso A 110, el terminal de acceso 118, y el punto de acceso B 112 de la figura 1 se usan con fines ilustrativos. El autentificador 120 y el terminal de acceso 118 pueden almacenar cada uno una clave maestra de nivel superior MKo 202 y 204 asociada de forma única con el terminal de acceso 118. El terminal de acceso 118 también puede mantener una lista de números de secuencia 206 utilizada para asociar un punto de acceso con un número de secuencia único.

[0064] El terminal de acceso 118 puede escuchar radiodifusiones de identificación de los puntos de acceso locales 208. En un ejemplo, el terminal de acceso puede seleccionar un punto de acceso A 110 basándose en su intensidad de señal en comparación con cualquier otro punto de acceso cercano. El terminal de acceso 118 asocia un identificador de punto de acceso AP_ID_A para el punto de acceso A 110 con un número de secuencia único SQN-A. El terminal de acceso 118 solicita entonces un enlace de comunicación con el punto de acceso A 110 usando el identificador AP_ID_A y SQN-A 212. Tanto el autentificador 120 como el terminal de acceso 118 pueden generar independientemente una clave maestra provisional I-MK1 basada, al menos parcialmente, en la clave maestra de nivel superior MKo y en el número de secuencia asignado SQN-A 214 y 216. Tenga en cuenta que dado que en el modelo de gestión distributiva de claves cada I-MKn se basa en una I-MK anterior diferente (n-1), no es necesario que el número secuencial SQN-A sea único en todas las obtenciones de todas las I-MK. El autentificador 120 envía entonces su clave maestra provisional I-MK1 al punto de acceso A 218. El punto de acceso A 110 y el terminal de acceso 118 generan a continuación una clave de sesión transitoria provisional (I-TSK1) como una función de la clave maestra provisional I-MK1 y (posiblemente) otros datos 220 y 222. Por ejemplo, en algunas implementaciones, tales otros datos pueden incluir un número aleatorio generado y/o suministrado por el terminal de acceso 118 y/o el punto de acceso actual A 110. Como tal, se puede implementar un protocolo entre el punto de acceso y/o el terminal de acceso para obtener, generar y/o intercambiar dicho número aleatorio antes de (o de forma concurrente con) la obtención de I-TSK1. Las comunicaciones se pueden establecer de forma segura entre el punto de acceso A 110 y el terminal de acceso 118 utilizando la clave de sesión I-TSK1 224.

[0065] El acceso al terminal 118 puede seguir escuchando para las radiodifusiones desde los terminales de acceso local 226, para determinar si debe producirse un traspaso con un nuevo punto de acceso 228 B. Es decir, a medida que el terminal de acceso 118 pasa o se mueve hacia un sector o célula diferente, o se detecta una señal más intensa desde otro punto de acceso, puede ser deseable un traspaso a un nuevo punto de acceso. Si el terminal de acceso 118 decide un traspaso desde un punto de acceso A 110 actual al nuevo punto de acceso 112, asocia un número secuencial SQN-B con el nuevo identificador de punto de acceso AP_ID_B 230. Es decir, el número secuencial SQN-B asociado con el nuevo punto de acceso B 112 es secuencial con el número secuencial SQN-A asociado con el punto de acceso actual A 110. El uso de tales números secuenciales permite que el punto de acceso actual A 110 y el terminal de acceso 118 generen independientemente o por separado la nueva clave maestra provisional I-MK2.

[0066] El terminal de acceso 118 solicita entonces el traspaso de una sesión de comunicación para el nuevo punto de acceso B 112 utilizando el identificador AP_ID_B y SQN-B 232. En algunas implementaciones, el autentificador 120 puede responder a la solicitud de traspaso enviando un mensaje 234 al punto de acceso actual A 110 indicando

que una sesión de comunicación actual se traspasará al nuevo punto de acceso B 112. Tanto el punto de acceso actual A 110 como el terminal de acceso 118 puede generar independientemente una nueva clave maestra provisional I-MK2 basada, al menos parcialmente, en la clave maestra provisional actual I-MK1 y el número de secuencia SQN-B asociado con los nuevos puntos de acceso B 236 y 238. El punto de acceso actual 110 envía entonces la nueva clave maestra provisional I-MK2 al nuevo punto de acceso B 240.

[0067] El nuevo punto de acceso B 112 y el terminal de acceso 118 a continuación generan una nueva clave de sesión transitoria provisional (I-TSK2) como una función de la nueva clave maestra provisional I-MK2 y (posiblemente) otros datos 242 y 244. Por ejemplo, en algunas implementaciones, tales otros datos pueden incluir un número aleatorio generado y/o suministrado por el terminal de acceso 118, el punto de acceso actual A 110 o el nuevo punto de acceso B 112. Como tal, se puede implementar un protocolo entre los puntos de acceso y/o el terminal de acceso para obtener, generar y/o intercambiar dicho número aleatorio antes de (o de forma concurrente con) la obtención de I-TSK2. La sesión de comunicación segura puede entonces continuar entre el punto de acceso B 112 y el terminal de acceso 118 usando la nueva clave de sesión provisional I-TSK2 246. En consecuencia, las comunicaciones entre el terminal de acceso 118 y el punto de acceso A 110 terminan en 248.

[0068] El proceso de traspasar de forma segura una sesión de comunicación de un punto de acceso a otro se puede repetir varias veces. Por ejemplo, en la figura 1, el terminal de acceso 118 puede pasar o moverse desde una célula actual 104 a una nueva célula 106 y buscar traspasar una sesión desde un punto de acceso actual B 112 a un nuevo punto de acceso C 114. El terminal de acceso 118 asocia un número secuencial SQN-C con el nuevo punto de acceso C 114 y proporciona el SQN-C al punto de acceso actual B 112. El punto de acceso actual B 112 genera entonces una nueva clave maestra provisional I-MK3 basada en la clave maestra provisional actual I-MK2 y SQN-C y envía la nueva clave maestra provisional I-MK3 al nuevo punto de acceso C 114. El terminal de acceso 118 puede generar independientemente su propia versión de la nueva clave maestra provisional I-MK3. El terminal de acceso 118 y el nuevo punto de acceso C 114 pueden generar entonces una nueva clave de sesión transitoria provisional I-TSK3 que puede usarse para continuar la sesión de comunicación segura entre ellos.

[0069] La figura 3 ilustra un modelo distributivo de claves de seguridad que se puede usar para asegurar sesiones de comunicación entre un terminal de acceso y un nuevo punto de acceso durante y/o después del traspaso. Cuando un terminal de acceso desea conectarse a un nuevo punto de acceso, el punto de acceso actual APn genera una nueva clave maestra provisional I-MK(n+1) para el nuevo punto de acceso AP(n+1). Según un aspecto, la nueva clave maestra provisional I-MK(n+1) se puede generar como una función de la clave maestra provisional actual I-MKn y posiblemente de otros parámetros, como el nuevo identificador de punto de acceso (AP_ID), identificador de terminal de acceso (AT-ID), un número aleatorio generado por cualquiera de las partes, un número de secuencia SQN-n proporcionado por el terminal de acceso, y/o incluso una secuencia estática. El nuevo punto de acceso AP(n+1) y el terminal de acceso pueden entonces usar la nueva clave maestra provisional I-MK(n+1) para generar y/o negociar una clave de sesión transitoria que se use para asegurar las comunicaciones entre ellos. Después de cambiar las claves, el terminal de acceso deja de usar sus claves anteriores I-MKn e I-TSKn.

[0070] La nueva clave maestra provisional I-MK(n+1) puede ser utilizada exactamente como una clave maestra de nivel superior (MKo) entre el nuevo punto de acceso AP(n+1) y el terminal de acceso, pero se limita a un terminal de acceso y un par de puntos de acceso particulares. La nueva clave maestra provisional I-MK(n+1) se puede usar inmediatamente después del traspaso de una sesión de comunicación. Esto proporciona un traspaso de baja latencia para una sesión de comunicación existente, mientras se asegura dicha sesión de comunicación. En varias implementaciones, la nueva clave maestra provisional I-MK(n+1) puede usarse durante un período de tiempo reducido después del traspaso, o puede usarse indefinidamente, para asegurar las comunicaciones entre el terminal de acceso y el nuevo punto de acceso AP(n+1). En algunas aplicaciones, la autentificación o la re-autentificación EAP de un terminal de acceso a través de un punto de acceso puede realizarse posteriormente para reducir el potencial de comprometer la sesión de comunicación. De forma alternativa, la nueva clave maestra provisional I-MK(n+1) puede funcionar como una clave maestra de nivel superior (dentro del nuevo punto de acceso AP(n+1)) y servir para generar claves maestras provisionales adicionales para otros puntos de acceso si se desea un traspaso adicional de una sesión de comunicación. Por lo tanto, no puede haber diferencia entre cómo se utiliza una clave maestra provisional I-MK y una clave maestra MK de nivel superior para asegurar las comunicaciones.

[0071] En el enfoque de la técnica anterior, la misma clave maestra de nivel superior (MKo) para un terminal de acceso puede ser compartida entre todos los puntos de acceso para asegurar las sesiones de comunicación con el terminal de acceso. Si la clave maestra de nivel superior MKo se ve comprometida en cualquiera de los puntos de acceso, comprometería todas las sesiones de comunicación entre el terminal de acceso y todos los otros puntos de acceso. Una ventaja del uso de claves maestras provisionales I-MK es que si una clave maestra provisional I-MKn se ve comprometida en un punto de acceso, las claves maestras provisionales para otros puntos de acceso, I-MK1 ... I-MKn-1 o MKo no se ven comprometidas. Esto se debe a que cada clave maestra provisional es única para un terminal de acceso particular y un par de puntos de acceso.

[0072] Tal como se utiliza en las figuras 1-3 y la descripción en el presente documento, las claves maestras provisionales (I-MKs) y las claves de sesión transitorias provisionales (I-TSK) también puede denominarse claves temporales en el sentido de que son específicas para un determinado punto de acceso/par de terminales de acceso

y/o solo se utilizan durante un tiempo limitado después de que una sesión de comunicación se traspase. En algunas implementaciones, dichas claves temporales también se pueden usar durante un período de tiempo prolongado hasta que la sesión de comunicación se traspase a otro punto de acceso o la sesión de comunicación finalice.

[0073] La figura 4 ilustra un sistema de comunicación inalámbrica con gestión centralizada de claves que facilita traspasos seguros de baja latencia. En contraste con el enfoque de gestión distributiva de claves descrito en las figuras 1, 2 y 3, una entidad centralizada realiza una gestión de claves. El sistema de comunicación inalámbrica de acceso múltiple 400 puede incluir múltiples células, por ejemplo las células 402, 404 y 406. Cada célula 402, 404 y 406 puede incluir un punto de acceso 410, 412 y 414 que proporciona cobertura a múltiples sectores dentro de la célula. Los puntos de acceso 410, 412 y 414 dentro de cada célula 402, 404 y 406 pueden proporcionar servicios de conexión de red a uno o más terminales de acceso. Por ejemplo, cuando un terminal de acceso 418 se mueve a través de las diferentes células 402, 404, 406, puede estar en comunicación con los puntos de acceso 410, 412 y 414. Un autentificador 420 puede servir para gestionar el funcionamiento de los puntos de acceso 410, 412 y 414 y/o gestionar la autentificación de claves para los terminales de acceso. En algunas aplicaciones, el autentificador 420 puede mantener claves maestras de nivel superior asociadas de manera única con los terminales de acceso que son atendidos por la red 400. Por ejemplo, el autentificador 420 y el terminal de acceso 418 conocen una primera clave maestra de nivel superior MKo, y está asociada de manera única con el terminal de acceso 418. En diversas aplicaciones, el autentificador 420 puede ser parte de un controlador de red que es remoto o está alejado de los puntos de acceso 410, 412 y 414 o puede ubicarse junto a uno de los puntos de acceso. Cada terminal de acceso puede estar en comunicación con dos o más sectores de una o más células. Esto puede permitir sesiones de comunicación de traspasos entre diferentes sectores o células cuando un terminal de acceso 418 se mueve o se desplaza, para una gestión de capacidad adecuada, y/o por otros motivos.

[0074] Para el traspaso de forma segura una sesión de comunicación desde un primer punto de acceso a un segundo punto de acceso, el autentificador 420 está configurado para negociar una clave transitoria maestra (MTK) con el terminal de acceso 418. Por ejemplo, cuando se establece por primera vez una sesión de comunicación, el autentificador 420 y el terminal de acceso 418 pueden usar la clave maestra de nivel superior MKo para establecer la clave transitoria maestra (MTK). El autentificador 420 puede generar entonces claves de sesión transitorias (TSK) para los puntos de acceso 410, 412 y 414 basadas (al menos parcialmente) en la clave transitoria maestra (MTK), un identificador de terminal de acceso (AT_ID) y/o un identificador de punto de acceso (AP_ID). La clave de sesión transitoria (TSK) puede ser generada y/o distribuida por el autentificador 420 de una sola vez o según se necesite para traspasar una sesión a un nuevo punto de acceso. El terminal de acceso 418 puede generar de manera similar una nueva clave de sesión transitoria cada vez que traspasa una sesión a un nuevo punto de acceso.

[0075] La figura 5 (que comprende las figuras 5A y 5B) es un diagrama de flujo que ilustra el funcionamiento de un sistema de comunicación inalámbrica con gestión centralizada de claves que facilita traspasos seguros y de baja latencia. En este ejemplo, el autentificador 420, el punto de acceso A 410, el terminal de acceso 418, y el punto de acceso B 412 de la figura 4 se usan con fines ilustrativos. El autentificador 420 y el terminal de acceso 418 pueden almacenar cada uno una clave maestra de nivel superior MKo 502 y 504 asociada de forma única con el terminal de acceso 418. El autentificador 420 y el terminal de acceso 418 también negocian una clave transitoria maestra (MTK) (y posiblemente un identificador MTK MTK_ID) a través de un intercambio de claves de 3 vías. La MTK puede estar basada (al menos parcialmente) en la clave maestra de nivel superior MKo y/o un identificador de terminal de acceso (AT_ID) 506. La MTK puede mantenerse de forma segura mediante el autentificador 420 y el terminal de acceso 418.

[0076] En algunas implementaciones, la obtención de MTK puede incluir también un número aleatorio generado y/o suministrado por el terminal de acceso 418 y/o el autentificador 420. Como tal, se puede implementar un protocolo entre el autentificador 420 y/o el terminal de acceso 418 para obtener, generar y/o intercambiar dicho número aleatorio antes de (o concurrentemente con) la obtención de la MTK.

[0077] El terminal de acceso 418 puede escuchar radiodifusiones de identificación de los puntos de acceso locales 508. En un ejemplo, el terminal de acceso 418 puede seleccionar un punto de acceso A 410 basado en su intensidad de señal en comparación con cualquier otro punto de acceso cercano. El terminal de acceso 418 solicita el establecimiento de una sesión de comunicación con el punto de acceso A 410 usando el identificador AP_ID_A 510. Tanto el autentificador 420 como el terminal de acceso 418 pueden generar independientemente una clave de sesión transitoria TSK1 basada, al menos parcialmente, en la clave transitoria maestra MTK y posiblemente el identificador de punto de acceso AP_ID_A, un identificador de terminal de acceso (AT_ID) y otros datos 514 y 516. Se puede generar una clave de sesión transitoria TSKn usando una función pseudoaleatoria (PRF) u otra función de obtención de claves adecuada. Debido a que las TSK de claves de sesión transitorias se generan utilizando una MTK común, al menos AP_ID o los datos utilizados en la obtención de cada TSK deben ser exclusivos de un punto de acceso particular y un par de terminales de acceso. El autentificador 420 envía luego la clave de sesión transitoria TSK1 al punto de acceso A 518. A continuación, se puede establecer una sesión de comunicaciones de forma segura entre el punto de acceso A 410 y el terminal de acceso 418 usando la clave de sesión TSK1 520.

[0078] En algunas implementaciones, la obtención de TSK también puede incluir datos adicionales, tales como un número aleatorio generado y/o suministrado por el terminal de acceso 418 y/o el autentificador 420. Como tal, puede

implementarse un protocolo entre el autentificador 420, el punto de acceso 410 y/o el terminal de acceso 418 para obtener, generar y/o intercambiar dicho número aleatorio antes de (o concurrentemente con) la obtención de la TSK.

[0079] El acceso al terminal 418 puede continuar para escuchar radiodifusiones desde los terminales de acceso locales 526, para determinar si debe producirse un traspaso con un punto de acceso nuevo 528 B. Es decir, cuando el terminal de acceso 418 pasa o se mueve a un sector o célula diferente, o se detecta una señal más intensa desde otro punto de acceso, puede ser deseable un traspaso a un nuevo punto de acceso B 412. Si el terminal de acceso 418 decide un traspaso desde un punto de acceso actual A 410 al nuevo punto de acceso B 412, solicita un traspaso de la sesión de comunicación al nuevo punto de acceso B 412 usando un identificador de punto de acceso AP_ID_B 532. Tanto el autentificador 420 como el terminal de acceso 418 pueden generar independientemente una nueva clave de sesión transitoria TSK2 basada, al menos parcialmente, en la clave transitoria maestra actual MTK y/o el identificador de punto de acceso AP_ID_B 536 y 538. El autentificador 420 envía entonces la nueva clave de sesión transitoria TSK2 al nuevo punto de acceso B 540. La sesión de comunicación segura puede continuar entonces entre el punto de acceso B 412 y el terminal de acceso 418 usando la nueva clave de sesión TSK2 542. En consecuencia, las comunicaciones entre el terminal de acceso 418 y el punto de acceso A 410 terminan en 544.

[0080] El proceso de traspasar de forma segura una sesión de comunicación de un punto de acceso a otro se puede repetir varias veces. Por ejemplo, en la figura 4, el terminal de acceso 418 puede pasar o moverse desde una célula actual 404 a una nueva célula 406 y buscar traspasar una sesión de comunicación desde un punto de acceso actual B 412 a un nuevo punto de acceso C 414. El terminal de acceso 418 puede solicitar un traspaso al nuevo punto de acceso asociado con el identificador de punto de acceso AP_ID_C. El autentificador 420 genera entonces una nueva clave de sesión transitoria TSK3 basada (al menos parcialmente) en la clave transitoria maestra MTK y envía la clave de sesión transitoria TSK3 al nuevo punto de acceso C 414. El terminal de acceso 418 puede generar independientemente su propia versión de la nueva clave de sesión transitoria TSK3. El terminal de acceso 418 y el nuevo punto de acceso C 414 pueden entonces usar la nueva clave de sesión transitoria TSK3 para continuar la sesión de comunicación segura entre ellos.

[0081] La figura 6 ilustra un modelo centralizado de claves de seguridad que se puede usar para asegurar las sesiones de comunicación entre un terminal de acceso y un nuevo punto de acceso durante y/o después del traspaso. En este modelo centralizado, el autentificador (por ejemplo, controlador de red, servidor de autentificación, etc.) y el terminal de acceso negocian una clave transitoria maestra (MTK) basada en (al menos parcialmente) una clave maestra de nivel superior MKo asociada de forma única con el terminal de acceso. El autentificador genera, administra y/o distribuye claves de sesión transitorias a cada punto de acceso. Debido a que la clave transitoria maestra MTK se negocia una sola vez (por ejemplo, cuando el terminal de acceso y el autentificador inician primero las comunicaciones), esto acelera el proceso de generación de claves de sesión. Además, incluso si la clave transitoria maestra MTK está comprometida, no compromete la clave maestra de nivel superior MKo. Además, dado que ni la clave maestra de nivel superior MKo ni la clave transitoria maestra MTK se distribuyen a los puntos de acceso (por ejemplo, solo se distribuyen las claves de sesión transitorias), se reduce el riesgo de comprometer la seguridad si se compromete un punto de acceso.

[0082] Esta gestión centralizada de claves proporciona un traspaso de baja latencia para una sesión de comunicación existente ya que las claves de sesión transitorias son generadas y proporcionadas por el autentificador, asegurando al mismo tiempo las sesiones de comunicación ya que ni la clave maestra de nivel superior MKo ni la clave transitoria maestra MTK se distribuyen a los puntos de acceso.

[0083] En varias implementaciones, la nueva clave de sesión transitoria TSKt puede utilizarse durante un período de tiempo reducido después del traspaso, o puede usarse indefinidamente, para proteger las comunicaciones entre el terminal de acceso y el nuevo punto de acceso AP-t. En algunas aplicaciones, la autentificación o la re-autentificación EAP de un terminal de acceso a través de un punto de acceso puede realizarse posteriormente (por ejemplo, para renovar la MTK) a fin de reducir el potencial de comprometer la sesión de comunicación.

[0084] Tal como se utiliza en las figuras 4-6 y la descripción en el presente documento, la clave transitoria maestra (MTK) y las claves de sesión transitorias (TSKs) también pueden denominarse claves temporales en el sentido de que son específicas para un par punto de acceso/terminal de acceso particular. La MTK se usa entre el autentificador (que también puede ser un punto de acceso) y el terminal de acceso. La TSK se usa entre un punto de acceso y un terminal de acceso. En algunas implementaciones, tales claves temporales también se pueden usar durante un período de tiempo reducido (hasta que se negocie una clave segura entre un terminal de acceso y un punto de acceso) o durante un período de tiempo prolongado (por ejemplo, hasta que la sesión de comunicación se traspase a otro punto de acceso o la sesión de comunicación finalice).

[0085] Mientras que los ejemplos ilustrados en las figuras 1-6 a menudo se refieren a la implementación de los esquemas de gestión distributiva y centralizada de claves en el contexto de traspasar comunicaciones desde un punto de acceso actual a un nuevo punto de acceso, estos dos procedimientos de gestión de claves pueden implementarse en otros contextos. En un ejemplo, en lugar de obtener o negociar nuevas claves cuando un terminal de acceso se mueve a un nuevo punto de acceso, el terminal de acceso mantiene un conjunto activo de claves. Es decir, el terminal de acceso puede establecer de forma simultánea o concurrente asociaciones de seguridad (por

ejemplo, claves) con una pluralidad de puntos de acceso dentro de un sector, área o región. Los puntos de acceso con los que el terminal de acceso mantiene tales asociaciones de seguridad (por ejemplo, claves) simultáneas o concurrentes se denominan "conjunto activo" de puntos de acceso. Cada vez que se agrega un nuevo punto de acceso al conjunto activo de un terminal de acceso, el terminal de acceso y el nuevo punto de acceso pueden establecer una clave segura. Por ejemplo, el terminal de acceso y el nuevo punto de acceso pueden establecer una clave maestra provisional (I-MK) (en el caso de un procedimiento de gestión distributiva de claves) o una clave de sesión transitoria (TSK) (en el caso de un procedimiento de gestión centralizada de claves).

[0086] Cuando un procedimiento de gestión distributiva de claves se implementa en el contexto de un conjunto activo de puntos de acceso, la clave maestra provisional (I-MKn) para un nuevo punto de acceso se puede basar en la clave maestra anterior (I-MK(n-1)) para el punto de acceso anterior agregado al conjunto activo. En tal configuración, el terminal de acceso puede solicitar que el punto de acceso anterior envíe o proporcione su I-MK(n-1) al nuevo punto de acceso.

[0087] Cuando un procedimiento de gestión centralizada de claves se implementa en el contexto de un conjunto activo de puntos de acceso, el terminal de acceso puede simplemente obtener una nueva clave de sesión transitoria (TSK) con el autentificador para el nuevo punto de acceso y hace que el autentificador la proporcione al nuevo punto de acceso.

[0088] El uso de un conjunto activo de puntos de acceso con un procedimiento de gestión distributiva de claves (ilustrado en las figuras 1-3) o un procedimiento centralizado de gestión de claves (ilustrado en las figuras 4-6) permite que el terminal de acceso cambie rápidamente las comunicaciones con puntos de acceso en su conjunto activo.

[0089] La figura 7 es un diagrama de bloques que ilustra un terminal de acceso configurado para realizar traspasos de sesión de comunicación segura de baja latencia. El terminal de acceso 702 puede incluir un circuito de procesamiento 704 acoplado a una interfaz de comunicación inalámbrica 706 para comunicarse a través de una red inalámbrica y un dispositivo de almacenamiento 708 para almacenar una clave maestra única de nivel superior MKo (asociada con el terminal de acceso) y una lista de números secuenciales asociados con los puntos de acceso identificados. El circuito de procesamiento 704 puede configurarse de forma segura para traspasar una sesión de comunicación en curso sin interrupciones notables en la sesión de comunicación. El circuito de procesamiento 704 (por ejemplo, procesador, módulo de procesamiento, etc.) puede incluir un módulo generador de claves configurado para generar una o más claves que se pueden usar para asegurar una sesión de comunicación.

[0090] La figura 8 es un diagrama de flujo que ilustra un procedimiento operativo en un terminal de acceso para facilitar un traspaso de sesión de comunicación segura desde un primer punto de acceso a un nuevo punto de acceso usando un enfoque de gestión distributiva de claves. Inicialmente, se puede establecer una sesión de comunicación segura con un primer punto de acceso usando al menos una clave maestra de nivel superior (asociada con el terminal de acceso) y un primer número de secuencia asociado con el primer punto de acceso para generar una primera clave maestra provisional de la cual se obtiene una primera clave de sesión transitoria 802. La primera clave maestra provisional puede ser única para el terminal de acceso particular y la combinación del primer punto de acceso. El terminal de acceso puede entonces escuchar radiodifusiones desde los puntos de acceso locales 804. Si se identifica un segundo punto de acceso, el terminal de acceso determina si la sesión de comunicación existente debe ser traspasada desde el primer punto de acceso al segundo punto de acceso 806. Esto se puede determinar comparando la intensidad y/o la calidad de la señal con el primer punto de acceso y el segundo punto de acceso. El terminal de acceso puede determinar continuar la sesión de comunicación con el primer punto de acceso 808. De lo contrario, el terminal de acceso puede elegir iniciar el traspaso de la sesión de comunicación existente al segundo punto de acceso 810. Un segundo número de secuencia puede asociarse con el segundo punto de acceso y enviarse al primer punto de acceso 812. El terminal de acceso genera una segunda clave maestra provisional, basada en la primera clave maestra provisional y el segundo número de secuencia, y obtiene una segunda clave de sesión transitoria 814. A continuación, el terminal de acceso traspasa la sesión de comunicación segura desde el primer punto de acceso al segundo punto de acceso y la protege con la segunda clave de sesión transitoria 816. Este proceso de traspaso se puede repetir varias veces con cada punto de acceso actual generando la nueva clave maestra provisional para el siguiente punto de acceso.

[0091] La figura 9 es un diagrama de flujo que ilustra un procedimiento operativo en un terminal de acceso para facilitar un traspaso de sesión de comunicación segura desde un primer punto de acceso a un nuevo punto de acceso usando un enfoque centralizado de gestión de claves. Inicialmente, una clave transitoria maestra puede establecerse de forma segura con un autentificador basado en al menos una clave maestra de nivel superior asociada con el terminal de acceso 902. Se puede establecer una sesión de comunicación segura con un primer punto de acceso usando al menos una primera clave de sesión transitoria única generada basándose en la clave transitoria maestra y un primer identificador de punto de acceso asociado con el primer punto de acceso 904. El terminal de acceso puede entonces escuchar radiodifusiones desde los puntos de acceso locales 906. Si se identifica un segundo punto de acceso, el terminal de acceso determina si la sesión de comunicación existente debe ser traspasada desde el primer punto de acceso al segundo punto de acceso 908. Esto se puede determinar comparando la intensidad y/o la calidad de la señal con el primer punto de acceso y el segundo punto de acceso. El

terminal de acceso puede determinar continuar la sesión de comunicación con el primer punto de acceso 910. De lo contrario, el terminal de acceso puede elegir iniciar el traspaso de la sesión de comunicación existente al segundo punto de acceso 912. Se puede generar una segunda clave de sesión transitoria basada en un segundo identificador de punto de acceso asociado con el segundo punto de acceso y la clave transitoria maestra 914. A continuación, el terminal de acceso traspasa la sesión de comunicación segura desde el primer punto de acceso al segundo punto de acceso y la asegura con la segunda clave de sesión transitoria 916. Este proceso de traspaso puede repetirse varias veces utilizando la clave transitoria maestra y un nuevo identificador de punto de acceso para generar la siguiente clave de sesión transitoria.

[0092] La figura 10 es un diagrama de bloques que ilustra un autentificador configurado para facilitar traspasos de sesión de comunicación segura de baja latencia. El autentificador 1002 puede incluir un circuito de procesamiento 1004 acoplado a una interfaz de comunicación 1006 para comunicarse a través de una red y un dispositivo de almacenamiento 1008 para almacenar una clave maestra única de nivel superior MKo (asociada con un terminal de acceso). El circuito de procesamiento 1004 puede configurarse para facilitar un traspaso seguro de una sesión de comunicación en curso desde un punto de acceso a un terminal de acceso sin interrupciones perceptibles en la sesión de comunicación. El circuito de procesamiento 1004 (por ejemplo, procesador, módulo de procesamiento, etc.) puede incluir un módulo generador de claves configurado para generar una o más claves que se pueden usar para asegurar una sesión de comunicación. En diversas aplicaciones, el autentificador 1002 puede estar ubicado en un controlador de red o puede estar ubicado junto a uno o más puntos de acceso.

[0093] La figura 11 es un diagrama de flujo que ilustra un procedimiento operativo en un autentificador para facilitar un traspaso de sesión de comunicación segura desde un primer punto de acceso a un nuevo punto de acceso usando un enfoque de gestión distributiva de claves. El autentificador recibe una solicitud de un terminal de acceso para establecer una sesión de comunicación segura con un primer punto de acceso 1102. A continuación, genera una primera clave maestra provisional basada en una clave maestra de nivel superior asociada con el terminal de acceso y un primer número de secuencia (por ejemplo, recibido desde el terminal de acceso) asociado con el primer punto de acceso 1104. A continuación, el autentificador envía la primera clave maestra provisional al primer punto de acceso 1106. Posteriormente, se puede recibir otra solicitud desde el terminal de acceso para traspasar la sesión de comunicación desde el primer punto de acceso a un segundo punto de acceso 1108. El autentificador puede indicar al primer punto de acceso que debe generar una segunda clave maestra provisional basada en la primera clave maestra provisional y un segundo número de secuencia (por ejemplo, recibido desde el terminal de acceso) asociado con el segundo punto de acceso 1110.

[0094] La figura 12 es un diagrama de flujo que ilustra un procedimiento operativo en un autentificador para facilitar un traspaso de sesión de comunicación segura desde un primer punto de acceso a un nuevo punto de acceso usando un enfoque de gestión centralizada de claves. El autentificador recibe una solicitud de un terminal de acceso para establecer una sesión de comunicación segura con un primer punto de acceso 1202. El autentificador genera una clave transitoria maestra basada en una clave maestra de nivel superior asociada con el terminal de acceso 1204. El autentificador genera una primera clave de sesión transitoria basada al menos en la clave transitoria maestra y un primer identificador de punto de acceso 1206. La primera clave de sesión transitoria es enviada por el autentificador al primer punto de acceso 1208. Posteriormente, el autentificador puede recibir otra solicitud del terminal de acceso para traspasar la sesión de comunicación segura desde el primer punto de acceso a un segundo punto de acceso 1210. Se genera una segunda clave de sesión transitoria basada al menos en la clave transitoria maestra y un segundo identificador de punto de acceso 1212. A continuación, el autentificador envía la primera clave de sesión transitoria al primer punto de acceso 1214.

[0095] La figura 13 es un diagrama de bloques que ilustra un punto de acceso configurado para facilitar traspasos de sesión de comunicación segura de baja latencia. El punto de acceso 1302 puede incluir un circuito de procesamiento 1304 acoplado a una interfaz de comunicación inalámbrica 1306 para comunicarse con uno o más terminales de acceso, una interfaz de comunicación 1310 para comunicarse con un autentificador y/u otros puntos de acceso y un dispositivo de almacenamiento 1308 para almacenar una clave maestra única de nivel superior MKo (asociada a un terminal de acceso). El circuito de procesamiento 1304 puede configurarse para facilitar un traspaso seguro de una sesión de comunicación en curso desde el punto de acceso 1302 a un terminal de acceso sin interrupciones perceptibles en la sesión de comunicación. El circuito de procesamiento 1304 (por ejemplo, procesador, módulo de procesamiento, etc.) puede incluir un módulo generador de claves configurado para generar una o más claves que se pueden usar para asegurar una sesión de comunicación.

[0096] La figura 14 es un diagrama de bloques que ilustra un modo de realización alternativo de un punto de acceso 1402 que tiene un autentificador integrado. El punto de acceso 1402 puede incluir muchos de los mismos componentes que el punto de acceso 1302 en la figura 13, pero en lugar de comunicarse con un autentificador a través de su interfaz de comunicación 1310, el autentificador 1412 está ubicado junto al punto de acceso 1402. El autentificador 1412 y el punto de acceso 1402 pueden funcionar como se ilustra en las figuras 1-12 y 15-17.

[0097] La figura 15 es un diagrama de flujo que ilustra un procedimiento operativo en un primer punto de acceso para facilitar un traspaso de sesión de comunicación segura desde el primer punto de acceso a un segundo punto de acceso usando un enfoque de gestión distributiva de claves. Al establecer una sesión de comunicación segura, el

primer punto de acceso puede recibir una primera clave maestra provisional de un autentificador, en el que la primera clave maestra provisional se basa en una clave maestra de nivel superior asociada con un terminal de acceso y un primer número de secuencia único asociado con el primer punto de acceso 1502. El primer punto de acceso genera una primera clave de sesión transitoria basada en la primera clave maestra provisional 1504. A continuación, establece una sesión de comunicación segura con el terminal de acceso usando la primera clave de sesión transitoria 1506. Posteriormente, el primer punto de acceso puede recibir una indicación de que la sesión de comunicación debe ser traspasada a un segundo punto de acceso junto con un segundo número de secuencia único asociado con el segundo punto de acceso 1508. El primer punto de acceso genera una segunda clave maestra provisional basada en la primera clave maestra provisional y el segundo número de secuencia 1510 y envía la segunda clave maestra provisional al segundo punto de acceso 1512. A continuación, puede traspasar la sesión de comunicación al segundo punto de acceso 1514. Este proceso de traspaso se puede repetir varias veces con cada punto de acceso actual generando la nueva clave maestra provisional para el próximo punto de acceso basado en la clave maestra provisional actual. El nuevo punto de acceso puede generar una nueva clave de sesión transitoria utilizando la nueva clave maestra provisional.

[0098] La figura 16 es un diagrama de flujo que ilustra un procedimiento operativo en un primer punto de acceso para facilitar un traspaso de sesión de comunicación segura desde el primer punto de acceso a un segundo punto de acceso usando un enfoque de gestión centralizada de claves. El primer punto de acceso recibe una solicitud desde un terminal de acceso para establecer una sesión de comunicación segura con un primer punto de acceso 1602. A continuación, obtiene una primera clave de sesión transitoria desde un autentificador 1604. El primer punto de acceso puede establecer entonces la sesión de comunicación segura con el terminal de acceso usando la primera clave de sesión transitoria 1606. Posteriormente, el primer punto de acceso puede recibir una solicitud desde el terminal de acceso para traspasar la sesión de comunicación segura a un segundo punto de acceso 1608. Esto hace que el primer punto de acceso indique al autentificador que la sesión de comunicación se va a traspasar al segundo punto de acceso 1610. La sesión de comunicación puede ser traspasada al segundo punto de acceso 1612.

[0099] La figura 17 es un diagrama de flujo que ilustra un procedimiento operativo en un terminal de acceso para obtener y/o establecer un conjunto activo de puntos de acceso. El terminal de acceso puede escanear en busca de puntos de acceso 1702. Cuando se identifica un nuevo punto de acceso, el terminal de acceso lo agrega a su conjunto activo de puntos de acceso 1704. El terminal de acceso puede establecer una clave segura con cada punto de acceso a medida que se agrega al conjunto activo 1706.

[0100] En un enfoque de gestión distributiva de claves, la clave segura para cada punto de acceso puede incluir una generación de una clave de sesión transitoria basándose en una clave maestra provisional asociada con otro punto de acceso en el conjunto activo 1708. Dicha clave maestra provisional puede haberse generado como se ilustra en las figuras 1-3 y/u 8, por ejemplo.

[0101] En un enfoque de gestión centralizada de claves, la clave segura para cada punto de acceso puede incluir una generación de una clave de sesión transitoria basada en una clave transitoria maestra y un identificador único de punto de acceso para el punto de acceso en el conjunto activo 1710. Dicha clave transitoria maestra puede haberse generado como se ilustra en las figuras 4-6 y/o 9, por ejemplo.

[0102] El terminal de acceso puede iniciar una sesión de comunicación con un primer punto de acceso en el conjunto activo, en el que una primera clave segura asociada con el primer punto de acceso se usa para asegurar la sesión de comunicación 1712. El punto de acceso puede cambiar posteriormente la sesión de comunicación a un segundo punto de acceso en el conjunto activo, en el que una segunda clave segura asociada con el segundo punto de acceso se usa para asegurar la sesión de comunicación 1714. Incluso después de que el terminal de acceso cambie del primer al segundo punto de acceso, la primera clave segura puede reutilizarse posteriormente si el terminal de acceso vuelve a establecer comunicación con el primer punto de acceso.

[0103] Uno o más de los componentes, pasos y/o funciones que se ilustran en las figuras 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 y/o 17 pueden disponerse de nuevo y/o combinarse en un único componente, paso o función o incluirse en varios componentes, pasos o funciones sin afectar al funcionamiento de la generación de números pseudo-aleatorios. También pueden agregarse elementos, componentes, pasos y/o funciones adicionales sin apartarse de la invención. El aparato, dispositivos y/o componentes que se ilustran en las figuras 1, 4, 7, 10, 13 y/o 14 pueden configurarse para realizar uno o más de los procedimientos, características o pasos que se describen en las figuras 2, 3, 5, 6, 8, 9, 11, 12, 15, 16 y/o 17. Los nuevos algoritmos descritos en el presente documento pueden implementarse eficientemente en software y/o integrarse en hardware.

[0104] Los expertos en la materia apreciarán, además, que los diversos bloques lógicos, módulos, circuitos y pasos de algoritmo ilustrativos descritos en relación con los modos de realización divulgados en el presente documento pueden implementarse como hardware electrónico, software informático o combinaciones de ambos. Para ilustrar claramente esta intercambiabilidad de hardware y software, anteriormente se han descrito diversos componentes, bloques, módulos, circuitos y pasos ilustrativos, en general, en lo que respecta a su funcionalidad. Si dicha funcionalidad se implementa como hardware o software depende de la aplicación particular y de las restricciones de diseño impuestas al sistema global.

[0105] Las diversas características de la invención descritas en el presente documento pueden implementarse en diferentes sistemas sin apartarse de la invención. Por ejemplo, algunas implementaciones de la invención se pueden realizar con un dispositivo de comunicación móvil o estático (por ejemplo, un terminal de acceso) y una pluralidad de estaciones base móviles o estáticas (por ejemplo, puntos de acceso).

[0106] Cabe apreciarse que los modos de realización anteriores son simplemente ejemplos y no han de interpretarse como limitantes de la invención. La descripción de las realizaciones pretende ser ilustrativa, y no limitar el alcance de las reivindicaciones. Como tal, las presentes enseñanzas pueden aplicarse fácilmente a otros tipos de aparatos y muchas alternativas, modificaciones y variaciones serán evidentes para los expertos en la técnica.

MODOS DE REALIZACIÓN ADICIONALES DE LA INVENCIÓN

[0107] La presente invención proporciona un punto de acceso que comprende: una memoria; y un procesador acoplado con la memoria, con el procesador configurado para generar una segunda clave temporal a partir de una clave maestra, y ordenar la transmisión de la segunda clave temporal desde el punto de acceso a un segundo punto de acceso para permitir que el segundo punto de acceso se comunique con un terminal de acceso.

[0108] La clave maestra puede ser una clave maestra por pares.

[0109] El procesador puede generar la segunda clave temporal a partir de la clave maestra cuando se inicia un traspaso de comunicación con el terminal de acceso desde el punto de acceso al segundo punto de acceso.

[0110] El procesador puede configurarse además para: establecer una comunicación segura entre el punto de acceso y el terminal de acceso asegurada por una primera clave temporal, en el que la primera clave temporal se basa al menos parcialmente en una clave maestra diferente; y recibir una solicitud desde el terminal de acceso para traspasar la comunicación segura desde el punto de acceso al segundo punto de acceso, en el que la clave maestra utilizada para generar la segunda clave temporal se basa al menos parcialmente en la clave maestra diferente.

[0111] El procesador puede configurarse adicionalmente para generar una tercera clave temporal, diferente de la segunda clave temporal, a partir de la clave maestra, y ordenar la transmisión de la segunda clave temporal desde el punto de acceso a un tercer punto de acceso para comunicarse con el terminal de acceso.

[0112] La segunda clave temporal también puede basarse en al menos un segundo identificador de punto de acceso único asociado con el segundo punto de acceso y la tercera clave temporal también se basa en al menos un tercer identificador de punto de acceso único asociado con el tercer punto de acceso.

[0113] La segunda clave temporal y la tercera clave temporal pueden ser claves de sesión transitorias.

[0114] La tercera clave temporal también puede basarse en al menos un número pseudoaleatorio obtenido por el segundo punto de acceso.

[0115] La clave maestra puede ser una clave maestra por pares basada en una clave maestra de nivel superior asociada con el terminal de acceso.

[0116] El procesador puede configurarse además para: establecer una comunicación segura entre el punto de acceso y el terminal de acceso asegurada por una primera clave temporal, en el que la primera clave temporal se basa al menos parcialmente en la clave maestra; recibir una solicitud del terminal de acceso para traspasar la comunicación segura desde el punto de acceso al segundo punto de acceso; y traspasar la sesión de comunicación al segundo punto de acceso.

[0117] La presente invención también proporciona un procedimiento que comprende: generar una segunda clave temporal a partir de una clave maestra en un primer punto de acceso, utilizándose la clave maestra para la comunicación entre el primer punto de acceso y un terminal de acceso; y transmitir la segunda clave temporal desde el primer punto de acceso a un segundo punto de acceso para permitir que el segundo punto de acceso se comunique con el terminal de acceso.

[0118] La clave maestra puede ser una clave maestra por pares.

[0119] La generación de la segunda clave temporal puede comprender generar la segunda clave temporal cuando se inicia un traspaso de comunicación con el terminal de acceso desde el primer punto de acceso al segundo punto de acceso.

[0120] El procedimiento puede comprender además: el establecimiento de una comunicación segura entre el primer punto de acceso y el terminal de acceso asegurada por una primera clave temporal, en el que la primera clave temporal se basa al menos parcialmente en una clave maestra diferente; y recibir una solicitud desde el terminal de

acceso para traspasar la sesión de comunicación segura desde el primer punto de acceso al segundo punto de acceso; en el que la clave maestra utilizada para generar la segunda clave temporal se basa al menos parcialmente en la clave maestra diferente.

[0121] Las diferentes claves maestras pueden ser recibidas por el primer punto de acceso desde un tercer punto de acceso con el que el terminal de acceso se comunicó previamente.

[0122] El procedimiento puede comprender además: generar una tercera clave temporal, diferente de la segunda clave temporal, a partir de la clave maestra y transmitir la tercera clave temporal desde el primer punto de acceso a un tercer punto de acceso para comunicarse con el terminal de acceso.

[0123] La segunda clave temporal también puede basarse en al menos un segundo identificador de punto de acceso único asociado con el segundo punto de acceso y la tercera clave temporal también se basa en al menos un tercer identificador de punto de acceso único asociado con el tercer punto de acceso.

[0124] La segunda clave temporal y la tercera clave temporal pueden ser claves de sesión transitorias.

[0125] La clave maestra puede ser una clave maestra por pares basada en una clave maestra de nivel superior asociada con el terminal de acceso.

[0126] El procedimiento puede comprender además: el establecimiento de una comunicación segura entre el primer punto de acceso y el terminal de acceso asegurada por una primera clave temporal, en el que la primera clave temporal se basa al menos parcialmente en la clave maestra; recibir una solicitud desde el terminal de acceso para traspasar la comunicación segura desde el primer punto de acceso al segundo punto de acceso; y traspasar la comunicación segura al segundo punto de acceso.

[0127] La presente invención también proporciona un aparato que comprende: medios para generar una segunda clave temporal a partir de una clave maestra en un primer punto de acceso, utilizándose la clave maestra para la comunicación entre el primer punto de acceso y un terminal de acceso; y medios para transmitir la segunda clave temporal desde el primer punto de acceso a un segundo punto de acceso para permitir que el segundo punto de acceso se comunique con el terminal de acceso.

[0128] El aparato puede comprender además: medios para generar una tercera clave temporal, diferente de la segunda clave temporal, a partir de la clave maestra; y medios para transmitir la tercera clave temporal desde el primer punto de acceso a un tercer punto de acceso para comunicarse con el terminal de acceso.

[0129] La clave maestra puede ser una clave maestra por pares.

[0130] El aparato puede comprender además: medios para iniciar un traspaso de comunicación desde el primer punto de acceso al segundo punto de acceso.

[0131] El aparato puede comprender además: medios para establecer una comunicación segura entre el primer punto de acceso y el terminal de acceso asegurada por una primera clave temporal, en el que la primera clave temporal se basa al menos parcialmente en una clave maestra diferente; y medios para recibir una solicitud desde el terminal de acceso para traspasar la comunicación segura desde el primer punto de acceso al segundo punto de acceso, en el que la clave maestra utilizada para generar la segunda clave temporal se basa al menos parcialmente en la clave maestra diferente.

[0132] El aparato puede comprender además: medios para generar una tercera clave temporal, diferente de la segunda clave temporal, a partir de la clave maestra y transmitir la tercera clave temporal desde el primer punto de acceso a un tercer punto de acceso para comunicarse con el terminal de acceso.

[0133] La segunda clave temporal también puede basarse en al menos un segundo identificador de punto de acceso único asociado con el segundo punto de acceso y la tercera clave temporal también se basa en al menos un tercer identificador de punto de acceso único asociado con el tercer punto de acceso.

[0134] La segunda clave temporal y la tercera clave temporal pueden ser claves de sesión transitorias.

[0135] La clave maestra puede ser una clave maestra por pares basada en una clave maestra de nivel superior asociada con el terminal de acceso.

[0136] El aparato puede comprender además: medios para establecer una comunicación segura entre el primer punto de acceso y el terminal de acceso asegurada por una primera clave temporal, en el que la primera clave temporal se basa al menos parcialmente en la clave maestra; medios para recibir una solicitud desde el terminal de acceso para traspasar la comunicación segura desde el primer punto de acceso al segundo punto de acceso; y medios para traspasar la comunicación segura al segundo punto de acceso.

[0137] La presente invención también proporciona un medio legible por procesador que comprende instrucciones que pueden ser utilizadas por uno o más procesadores, comprendiendo las instrucciones: instrucciones para generar una segunda clave temporal a partir de una clave maestra en un primer punto de acceso, utilizándose la clave maestra para la comunicación entre el primer punto de acceso y un terminal de acceso; e instrucciones para transmitir la clave temporal desde el primer punto de acceso a un segundo punto de acceso para permitir que el segundo punto de acceso se comunique con el terminal de acceso.

[0138] La segunda clave temporal puede generarse para iniciar un traspaso de comunicación desde el primer punto de acceso al segundo punto de acceso.

[0139] El medio legible por procesador puede comprender además instrucciones que comprenden: instrucciones para establecer una comunicación segura entre el primer punto de acceso y el terminal de acceso asegurada por una primera clave temporal, en el que la primera clave temporal se basa al menos parcialmente en una clave maestra diferente; e instrucciones para recibir una solicitud desde el terminal de acceso para traspasar la comunicación segura desde el primer punto de acceso al segundo punto de acceso; en el que la clave maestra utilizada para generar la segunda clave temporal se basa al menos parcialmente en la clave maestra diferente.

[0140] El medio legible por procesador puede comprender además instrucciones que comprenden: instrucciones para generar una tercera clave temporal, diferente de la segunda clave temporal, a partir de la clave maestra, y transmitir la tercera clave temporal desde el primer punto de acceso a un tercer punto de acceso para comunicarse con el terminal de acceso.

[0141] El medio legible por procesador puede comprender además instrucciones que comprenden: instrucciones para establecer una comunicación segura entre el primer punto de acceso y el terminal de acceso asegurada por una primera clave temporal, en el que la primera clave temporal se basa al menos parcialmente en la clave maestra; instrucciones para recibir una solicitud del terminal de acceso para traspasar la comunicación segura desde el primer punto de acceso al segundo punto de acceso; e instrucciones para traspasar la comunicación segura al segundo punto de acceso.

[0142] La presente invención también proporciona un procesador que comprende: un circuito de procesamiento configurado para establecer una comunicación segura entre el primer punto de acceso y el terminal de acceso asegurada por una primera clave temporal, en el que la primera clave temporal se basa al menos parcialmente en una clave maestra diferente; y recibir una solicitud desde el terminal de acceso para traspasar la sesión de comunicación segura desde el primer punto de acceso al segundo punto de acceso; en el que la clave maestra utilizada para generar la segunda clave temporal se basa al menos parcialmente en la clave maestra diferente.

[0143] Las diferentes claves maestras pueden ser recibidas por el primer punto de acceso desde un tercer punto de acceso con el que el terminal de acceso se comunicó previamente.

[0144] El circuito de procesamiento puede configurarse además para generar una tercera clave temporal, diferente de la segunda clave temporal, a partir de la clave maestra y transmitir la tercera clave temporal desde el primer punto de acceso a un tercer punto de acceso para comunicarse con el terminal de acceso; en el que la segunda clave temporal también se basa en al menos un segundo identificador de punto de acceso único asociado con el segundo punto de acceso y la tercera clave temporal también se basa en al menos un tercer identificador de punto de acceso único asociado con el tercer punto de acceso.

[0145] El circuito de procesamiento puede configurarse además para establecer una comunicación segura entre el primer punto de acceso y el terminal de acceso asegurada por una primera clave temporal, en el que la primera clave temporal se basa al menos parcialmente en la clave maestra; recibir una solicitud del terminal de acceso para traspasar la comunicación segura desde el primer punto de acceso al segundo punto de acceso; y traspasar la comunicación segura al segundo punto de acceso.

[0146] La presente invención también proporciona un punto de acceso que comprende: una memoria; y un procesador acoplado con la memoria, el procesador configurado para recibir una primera clave temporal desde otro punto de acceso, y ordenar la comunicación con un terminal de acceso utilizando la primera clave temporal para asegurar la comunicación.

[0147] La primera clave temporal puede funcionar durante un período de tiempo limitado, y el procesador está además configurado para recibir una clave maestra para asegurar la comunicación entre el terminal de acceso y el punto de acceso y para descartar la utilización de la primera clave temporal.

[0148] El procesador puede configurarse además para recibir la primera clave temporal desde el otro punto de acceso cuando se inicia el traspaso al punto de acceso desde el otro punto de acceso para la comunicación con el terminal de acceso.

[0149] El procesador puede configurarse además para recibir una indicación de que la comunicación con el terminal de acceso debe ser traspasada a un segundo punto de acceso; generar una segunda clave temporal basada en la primera clave temporal; y enviar la segunda clave temporal al segundo punto de acceso.

[0150] La presente invención también proporciona un procedimiento que comprende: recibir una primera clave temporal en un primer punto de acceso desde otro punto de acceso; y comunicarse con un terminal de acceso utilizando la primera clave temporal para asegurar la comunicación.

[0151] La primera clave temporal puede funcionar durante un período de tiempo limitado y el procedimiento comprende además: recibir una clave maestra para la comunicación entre el terminal de acceso y el primer punto de acceso y descartar la utilización de la primera clave temporal.

[0152] El procedimiento puede comprender además: recibir la primera clave temporal desde el otro punto de acceso cuando se inicia el traspaso al primer punto de acceso desde el otro punto de acceso para la comunicación con el terminal de acceso.

[0153] El procedimiento puede comprender además: recibir una indicación de que una comunicación con el primer terminal de acceso debe ser traspasada a un segundo punto de acceso; generar una segunda clave temporal basada en la primera clave temporal; y enviar la segunda clave temporal al segundo punto de acceso.

[0154] La presente invención también proporciona un aparato que comprende: medios para recibir una primera clave temporal en un primer punto de acceso, desde otro punto de acceso; y medios para comunicarse con un terminal de acceso utilizando el primer temporal para asegurar la comunicación.

[0155] El aparato puede comprender además: medios para recibir una clave maestra para la comunicación entre el terminal de acceso y el primer punto de acceso; y medios para descartar la utilización de la primera clave temporal.

[0156] El aparato puede comprender además: medios para recibir la primera clave temporal desde el otro punto de acceso cuando se inicia el traspaso al primer punto de acceso desde el otro punto de acceso para la comunicación con el terminal de acceso.

[0157] El aparato puede comprender además: medios para recibir una indicación de que la comunicación con el primer terminal de acceso debe ser traspasada a un segundo punto de acceso; medios para generar una segunda clave temporal basada en la primera clave temporal; y medios para enviar la segunda clave temporal al segundo punto de acceso.

[0158] La presente invención también proporciona un medio legible por procesador que comprende instrucciones que pueden ser utilizadas por uno o más procesadores, comprendiendo las instrucciones: instrucciones para recibir una primera clave temporal en un primer punto de acceso, desde otro punto de acceso; e instrucciones para comunicarse con un terminal de acceso utilizando la primera clave temporal para asegurar la comunicación.

[0159] La primera clave temporal desde el otro punto de acceso puede recibirse cuando se inicia un traspaso al primer punto de acceso desde el otro punto de acceso para la comunicación con el terminal de acceso.

[0160] El medio legible por el procesador puede comprender además instrucciones que comprenden: instrucciones para recibir una indicación de que la comunicación con el primer terminal de acceso debe ser traspasada a un segundo punto de acceso; instrucciones para generar una segunda clave temporal basada en la primera clave temporal; e instrucciones para enviar la segunda clave temporal al segundo punto de acceso.

[0161] La presente invención también proporciona un procesador que comprende: un circuito de procesamiento configurado para recibir una primera clave temporal en un primer punto de acceso desde otro punto de acceso; y comunicarse con un terminal de acceso utilizando la primera clave temporal para asegurar la comunicación.

[0162] La primera clave temporal puede funcionar durante un período de tiempo limitado y el circuito de procesamiento está configurado además para recibir una clave maestra para la comunicación entre el terminal de acceso y el primer punto de acceso y descartar la utilización de la primera clave temporal.

[0163] El circuito de procesamiento puede configurarse además para recibir la primera clave temporal desde el otro punto de acceso cuando se inicia el traspaso al primer punto de acceso desde el otro punto de acceso para la comunicación con el terminal de acceso.

[0164] El circuito de procesamiento puede configurarse además para recibir una indicación de que una comunicación con el primer terminal de acceso debe ser traspasada a un segundo punto de acceso; generar una segunda clave temporal basada en la primera clave temporal; y enviar la segunda clave temporal al segundo punto de acceso.

[0165] La presente invención también proporciona un terminal de acceso que comprende: una memoria; y un procesador acoplado con la memoria, con el procesador configurado para generar una primera clave temporal a partir de una clave maestra utilizada para la comunicación entre un primer punto de acceso y el terminal de acceso, y ordenar la comunicación utilizando la primera clave temporal entre un segundo punto de acceso y el terminal de acceso.

[0166] La clave maestra puede ser una segunda clave temporal utilizada para la comunicación entre un primer punto de acceso y el terminal de acceso.

[0167] El procesador puede configurarse además para ordenar a un servidor de autentificación que proporcione otra clave maestra para la comunicación con el segundo punto de acceso y que interrumpa el uso de la primera clave temporal.

[0168] La clave maestra puede ser una clave maestra por pares.

[0169] El procesador puede configurarse además para proporcionar una indicación de que la comunicación con el segundo punto de acceso debe ser traspasada a un tercer punto de acceso.

[0170] El procesador puede configurarse además para generar una segunda clave temporal a partir de la primera clave temporal utilizada para la comunicación entre el segundo punto de acceso y el terminal de acceso, y ordenar la comunicación utilizando la segunda clave temporal entre un tercer punto de acceso y el terminal de acceso.

[0171] El procesador puede configurarse además para generar una segunda clave temporal a partir de la clave maestra; ordenar la comunicación utilizando la segunda clave temporal entre un tercer punto de acceso y el terminal de acceso.

[0172] El procesador puede configurarse además para escanear en busca de puntos de acceso; agregar puntos de acceso a un conjunto activo de puntos de acceso a medida que se identifican; establecer una clave segura con cada punto de acceso a medida que se agrega al conjunto activo.

[0173] En un sistema de gestión distributiva de claves, el procesador puede configurarse adicionalmente para generar una clave de sesión transitoria para cada punto de acceso a medida que se agrega al conjunto activo, en el que la clave de sesión transitoria se basa en una clave maestra provisional asociada con otro punto de acceso en el conjunto activo.

[0174] En un sistema centralizado de gestión de claves, el procesador puede configurarse adicionalmente para generar una clave de sesión transitoria para cada punto de acceso a medida que se agrega al conjunto activo, en el que la clave de sesión transitoria se basa en una clave transitoria maestra y un identificador de punto de acceso único para el punto de acceso.

[0175] La presente invención también proporciona un procedimiento operativo en un terminal de acceso, que comprende: comunicarse con un primer punto de acceso utilizando una clave maestra; generar una primera clave temporal a partir de la clave maestra; y comunicarse con un segundo punto de acceso utilizando la primera clave temporal.

[0176] La clave maestra puede ser una segunda clave temporal utilizada para asegurar la comunicación entre un primer punto de acceso y el terminal de acceso.

[0177] El procedimiento puede comprender además: ordenar a un servidor de autentificación que proporcione otra clave maestra para la comunicación con el segundo punto de acceso y que interrumpa el uso de la primera clave temporal.

[0178] La clave maestra puede ser una clave maestra por pares compartida con un servidor de autentificación.

[0179] El procedimiento puede comprender además: proporcionar una indicación de que la comunicación con el segundo punto de acceso debe ser traspasada a un tercer punto de acceso.

[0180] El procedimiento puede comprender además: generar una segunda clave temporal a partir de la primera clave temporal utilizada para la comunicación entre el segundo punto de acceso y el terminal de acceso, y ordenar la comunicación utilizando la segunda clave temporal entre un tercer punto de acceso y el terminal de acceso.

[0181] El procedimiento puede comprender además: generar una segunda clave temporal a partir de la clave maestra; ordenar la comunicación utilizando la segunda clave temporal entre un tercer punto de acceso y el terminal de acceso.

[0182] El procedimiento puede comprender además: escanear en busca de puntos de acceso; agregar puntos de acceso a un conjunto activo de puntos de acceso a medida que se identifican; establecer una clave segura con cada punto de acceso a medida que se agrega al conjunto activo.

[0183] En un sistema de gestión distributiva de claves, puede comprender además generar una clave de sesión transitoria para cada punto de acceso a medida que se agrega al conjunto activo, en el que la clave de sesión transitoria se basa en una clave maestra provisional asociada con otro punto de acceso en el conjunto activo.

[0184] En un sistema centralizado de gestión de claves, el procedimiento puede comprender además generar una clave de sesión transitoria para cada punto de acceso a medida que se agrega al conjunto activo, en el que la clave de sesión transitoria se basa en una clave transitoria maestra y un identificador de punto de acceso único para el punto de acceso.

[0185] La presente invención también proporciona un terminal de acceso que comprende: medios para comunicarse con un primer punto de acceso utilizando una clave maestra; medios para generar una primera clave temporal a partir de la clave maestra; y medios para comunicarse con un segundo punto de acceso utilizando la primera clave temporal.

[0186] La clave maestra puede ser una segunda clave temporal utilizada para asegurar la comunicación entre un primer punto de acceso y el terminal de acceso.

[0187] El terminal de acceso puede comprender además: medios para ordenar a un servidor de autentificación que proporcione otra clave maestra para la comunicación con el segundo punto de acceso y que interrumpa el uso de la primera clave temporal.

[0188] La clave maestra puede ser una clave maestra por pares compartida con un servidor de autentificación.

[0189] El terminal de acceso puede comprender además: medios para proporcionar una indicación de que la comunicación con el segundo punto de acceso debe ser traspasada a un tercer punto de acceso.

[0190] El terminal de acceso puede comprender además: medios para generar una segunda clave temporal a partir de la primera clave temporal utilizada para la comunicación entre el segundo punto de acceso y el terminal de acceso, y medios para ordenar la comunicación utilizando la segunda clave temporal entre un tercer punto de acceso y el terminal de acceso.

[0191] El terminal de acceso puede comprender además: medios para generar una segunda clave temporal a partir de la clave maestra; medios para ordenar la comunicación utilizando la segunda clave temporal entre un tercer punto de acceso y el terminal de acceso.

[0192] La presente invención también proporciona un medio legible por procesador que comprende instrucciones que pueden ser utilizadas por uno o más procesadores, comprendiendo las instrucciones: instrucciones para la comunicación con un primer punto de acceso desde un terminal de acceso utilizando una clave maestra; instrucciones para generar una primera clave temporal a partir de la clave maestra; e instrucciones para comunicarse con un segundo punto de acceso utilizando la primera clave temporal.

[0193] El medio legible por procesador puede comprender además instrucciones que comprenden: instrucciones para proporcionar una indicación de que la comunicación con el segundo punto de acceso debe ser traspasada a un tercer punto de acceso.

[0194] El medio legible por procesador puede comprender además instrucciones que comprenden: instrucciones para generar una segunda clave temporal a partir de la primera clave temporal utilizada para la comunicación entre el segundo punto de acceso y el terminal de acceso, e instrucciones para ordenar la comunicación utilizando la segunda clave temporal entre un tercer punto de acceso y el terminal de acceso.

[0195] El medio legible por procesador puede comprender además instrucciones que comprenden: instrucciones para generar una segunda clave temporal a partir de la clave maestra; instrucciones para ordenar la comunicación utilizando la segunda clave temporal entre un tercer punto de acceso y el terminal de acceso.

[0196] La presente invención también proporciona un procesador que comprende: un circuito de procesamiento configurado para comunicarse con un primer punto de acceso utilizando una clave maestra; generar una primera clave temporal a partir de la clave maestra; y comunicarse con un segundo punto de acceso utilizando la primera clave temporal.

[0197] La clave maestra puede ser una segunda clave temporal utilizada para asegurar la comunicación entre un primer punto de acceso y el terminal de acceso.

[0198] El circuito de procesamiento puede configurarse además para ordenar a un servidor de autentificación que proporcione otra clave maestra para la comunicación con el segundo punto de acceso y que interrumpa el uso de la primera clave temporal.

[0199] El circuito de procesamiento puede configurarse además para generar una segunda clave temporal a partir de la primera clave temporal utilizada para la comunicación entre el segundo punto de acceso y el terminal de acceso, y ordenar la comunicación utilizando la segunda clave temporal entre un tercer punto de acceso y el terminal de acceso.

[0200] El circuito de procesamiento puede configurarse adicionalmente para generar una segunda clave temporal a partir de la clave maestra; ordenar la comunicación utilizando la segunda clave temporal entre un tercer punto de acceso y el terminal de acceso.

[0201] El circuito de procesamiento puede configurarse además para escanear en busca de puntos de acceso; agregar puntos de acceso a un conjunto activo de puntos de acceso a medida que se identifican; y establecer una clave segura con cada punto de acceso a medida que se agrega al conjunto activo.

REIVINDICACIONES

1. Un procedimiento de traspaso seguro, que comprende:

un terminal de acceso que se comunica de forma segura con un primer punto de acceso utilizando una primera clave de sesión transitoria, en el que la primera clave de sesión transitoria se genera basándose en una primera clave maestra provisional y en la que la primera clave maestra provisional se genera basada en una clave maestra de nivel superior y un primer número de secuencia asociado con el primer punto de acceso;

el terminal de acceso que asocia un segundo número de secuencia con un segundo punto de acceso;

el terminal de acceso que inicia un traspaso seguro desde el primer punto de acceso al segundo punto de acceso, en el que el segundo número de secuencia se reenvía al primer punto de acceso;

el terminal de acceso que genera una segunda clave maestra provisional basada en la primera clave maestra provisional y el segundo número de secuencia;

el terminal de acceso que genera una segunda clave de sesión transitoria basada en la segunda clave maestra provisional; y

el terminal de acceso que se comunica de forma segura con el segundo punto de acceso usando la segunda clave de sesión transitoria.

2. El procedimiento para traspaso seguro como se define en la reivindicación 1, en el que el terminal de acceso que genera una segunda clave de sesión transitoria basada en la segunda clave maestra provisional comprende el terminal de acceso que genera la segunda clave de sesión transitoria basada en un número aleatorio y la segunda clave maestra provisional.

3. El procedimiento para traspaso seguro como se define en la reivindicación 2, en el que el número aleatorio es generado por el terminal de acceso.

4. El procedimiento para traspaso seguro como se define en la reivindicación 2, en el que el número aleatorio es del primer punto de acceso.

5. El procedimiento para traspaso seguro como se define en la reivindicación 2, en el que el número aleatorio es del segundo punto de acceso.

6. El procedimiento para traspaso seguro como se define en la reivindicación 1, que comprende además:

el terminal de acceso que mantiene una lista de números de secuencia para asociar cada punto de acceso con un número de secuencia único.

7. El procedimiento para traspaso seguro como se define en la reivindicación 1, que comprende además:

el terminal de acceso que asocia un tercer número de secuencia con un tercer punto de acceso;

el terminal de acceso que inicia un traspaso seguro desde el segundo punto de acceso al tercer punto de acceso, en el que el tercer número de secuencia se reenvía al segundo punto de acceso;

el terminal de acceso que genera una tercera clave maestra provisional basada en la segunda clave maestra provisional y el tercer número de secuencia;

el terminal de acceso que genera una tercera clave de sesión transitoria basada en la tercera clave maestra provisional; y

el terminal de acceso que se comunica de forma segura con el tercer punto de acceso usando la tercera clave de sesión transitoria.

8. El procedimiento para traspaso seguro como se define en la reivindicación 7, en el que el terminal de acceso que genera una tercera clave de sesión transitoria basada en la tercera clave maestra provisional comprende el terminal de acceso que genera la tercera clave de sesión transitoria basada en un segundo número aleatorio y la tercera clave maestra provisional.

9. Un aparato, que comprende:

medios para comunicarse de forma segura con un primer punto de acceso utilizando una primera clave de sesión transitoria, en el que la primera clave de sesión transitoria se genera basándose en una primera clave maestra provisional y en el que la primera clave maestra provisional se genera basándose en una clave maestra de nivel superior y un primer número de secuencia asociado con el primer punto de acceso;

medios para asociar un segundo número de secuencia con un segundo punto de acceso;

medios para iniciar un traspaso seguro desde el primer punto de acceso al segundo punto de acceso, en el que el segundo número de secuencia se reenvía al primer punto de acceso;

medios para generar una segunda clave maestra provisional basada en la primera clave maestra provisional y el segundo número de secuencia;

medios para generar una segunda clave de sesión transitoria basada en la segunda clave maestra provisional; y

medios para comunicarse de forma segura con el segundo punto de acceso usando la segunda clave de sesión transitoria.

10. Un medio legible por procesador no transitorio que comprende instrucciones que pueden ser utilizadas por uno o más procesadores, con las instrucciones que comprenden:

instrucciones para realizar el procedimiento de cualquiera de las reivindicaciones 1 a 8.

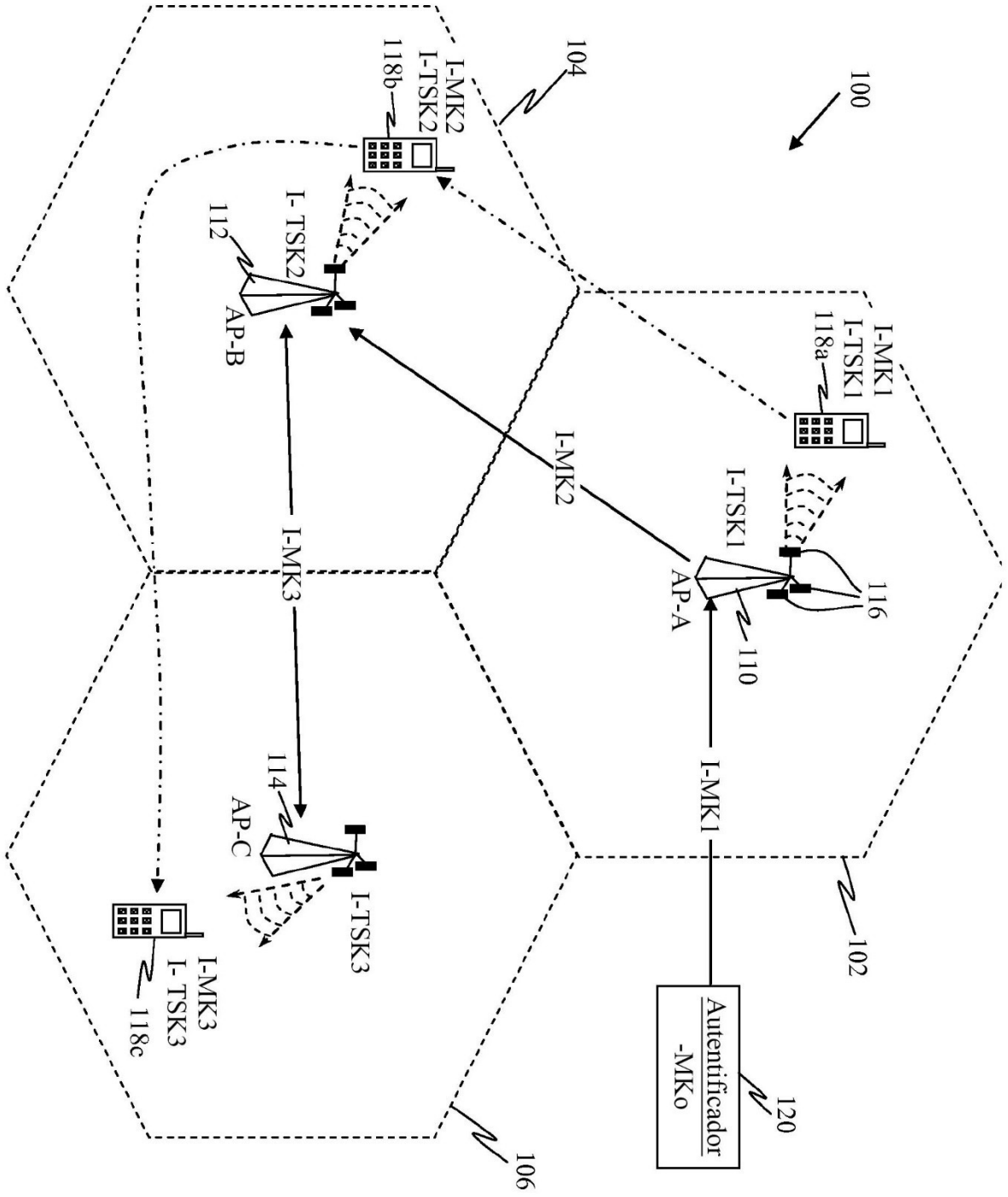
100
102
104
106
I-MK1
I-TSK1
118a
I-MK2
I-TSK2
118b
I-MK3
I- TSK3
118c
AP-A
110
AP-B
112
AP-C
114
116
I-TSK1
I- TSK2
I-TSK3
I-MK1
I-MK2
I-MK3
Autentificador
-MKo
120

Figura 1

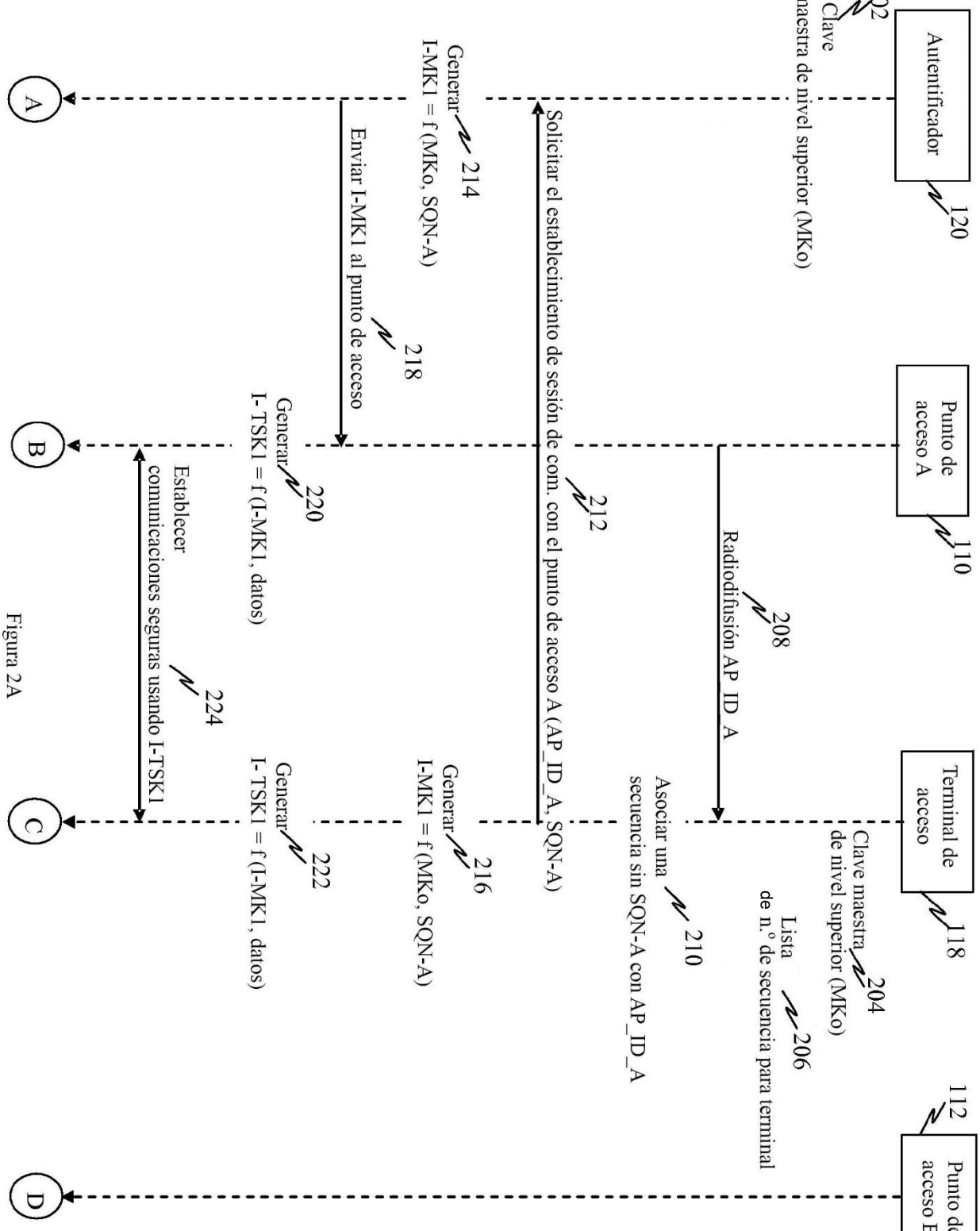
Autentificador
120
Punto de acceso A
110
Terminal de acceso
118
Punto de acceso B
112
202
Clave maestra de nivel superior (MKo)
208
Radiodifusión AP_ID_A
Clave maestra de nivel superior (MKo)
204
Lista de n.º de secuencia para terminal
206
210
Asociar una secuencia sin SQN-A con AP_ID_A
212
Solicitar el establecimiento de sesión de com. con el punto de acceso A (AP_ID_A, SQN-A)
214
Generar I-MK1 = f (MKo, SQN-A)
216
Generar I-MK1 = f (MKo, SQN-A)
218
Enviar I-MK1 al punto de acceso
220
Generar I- TSK1 = f (I-MK1, datos)
222
Generar I- TSK1 = f (I-MK1, datos)
224
Establecer comunicaciones seguras usando I-TSK1
A
B
C
D

Figura 2A

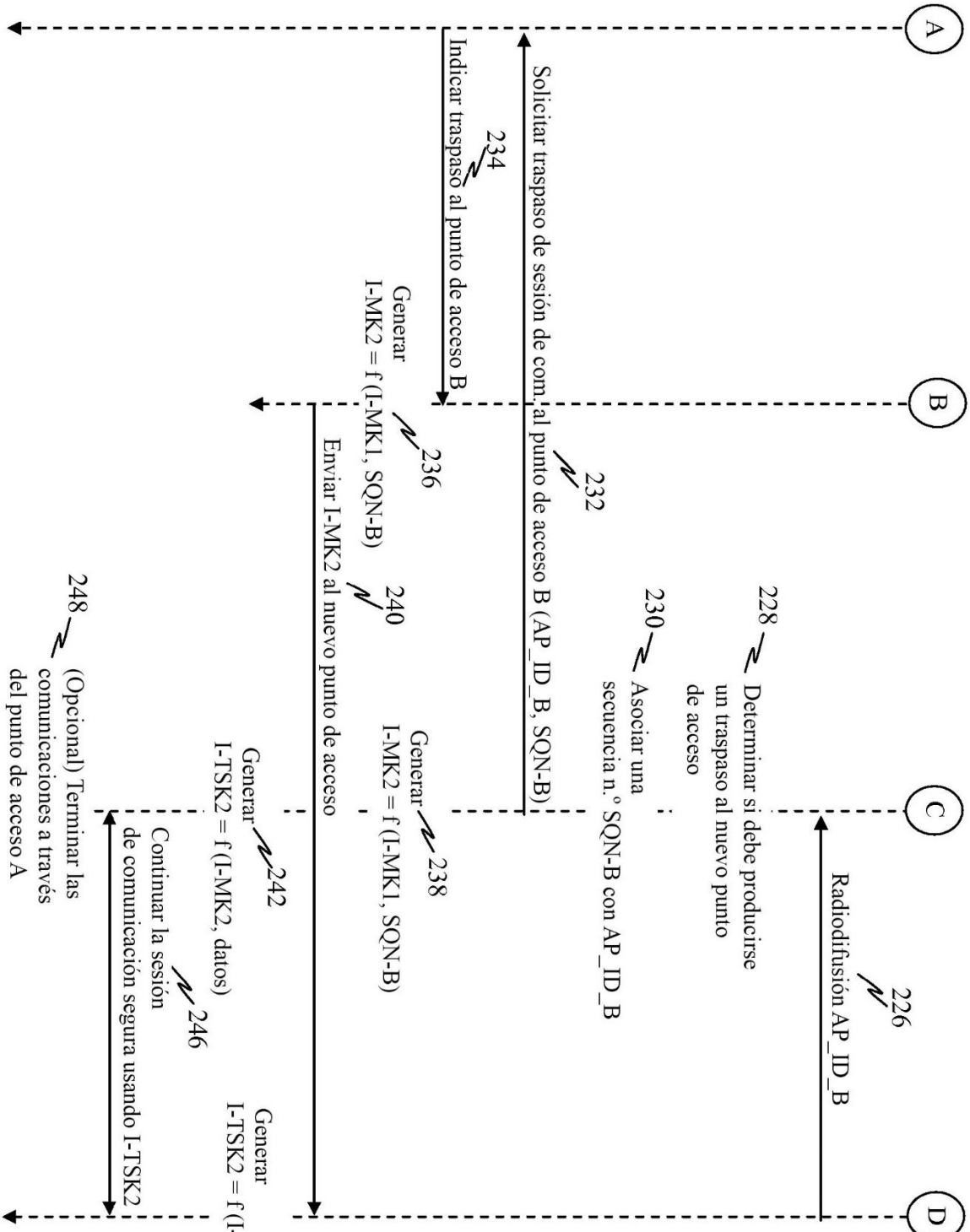
A
B
C
D
226
Radiodifusión AP_ID_B
228
Determinar si debe producirse un traspaso al nuevo punto de acceso
230
Asociar una secuencia n.º SQN-B con AP_ID_B
232
Solicitar traspaso de sesión de com. al punto de acceso B (AP_ID_B, SQN-B)
234
Indicar traspaso al punto de acceso B
236
Generar I-MK2 = f (I-MK1, SQN-B)
238
Generar I-MK2 = f (I-MK1, SQN-B)
240
Enviar I-MK2 al nuevo punto de acceso
242
Generar I-TSK2 = f (I-MK2, datos)
244
Generar I-TSK2 = f (I-MK2, datos)
246
Continuar la sesión de comunicación segura usando I-TSK2
248
(Opcional) Terminar las comunicaciones a través del punto de acceso A

Figura 2B

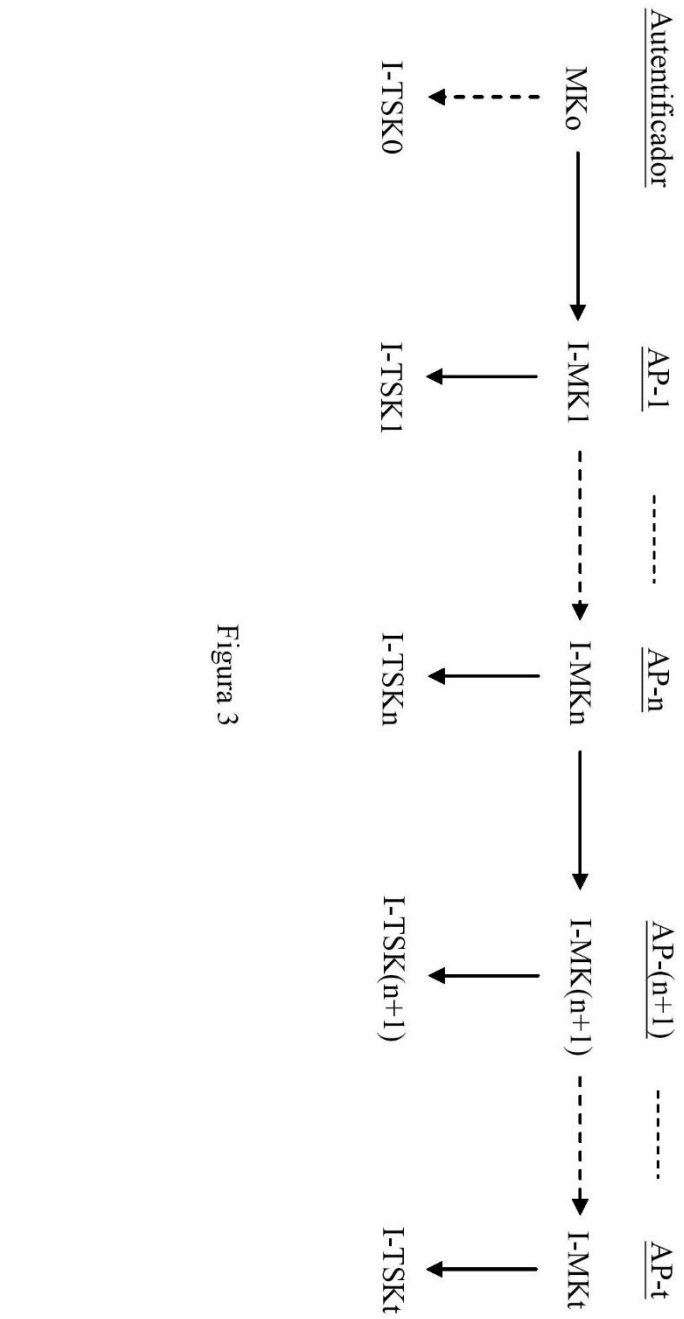
Autentificador
AP-1
AP-n
AP-(n+1)
AP-t
MKo
I-MK1
I-MKn
I-MK(n+1)
I-MKt
I-TSK0
I-TSK1
I-TSKn
I-TSK(n+1)
I-TSKt

Figura 3

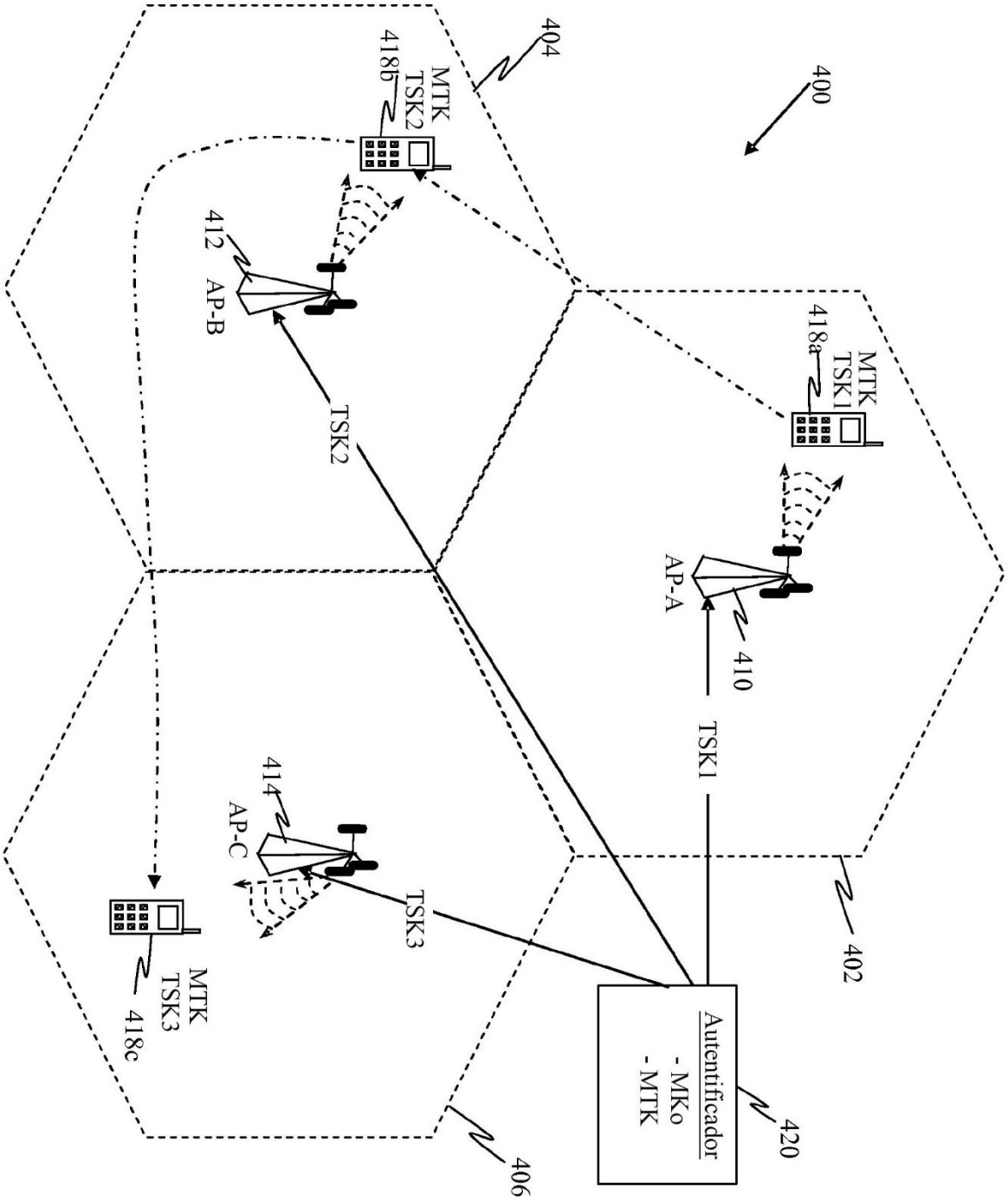
400
404
MTK
TSK2
418b
412
AP-B
TSK2
MTK
TSK1
418a
AP-A
410
TSK1
414
AP-C
TSK3
MTK
TSK3
418c
402
406
Autentificador
- MKo
- MTK
420

Figura 4

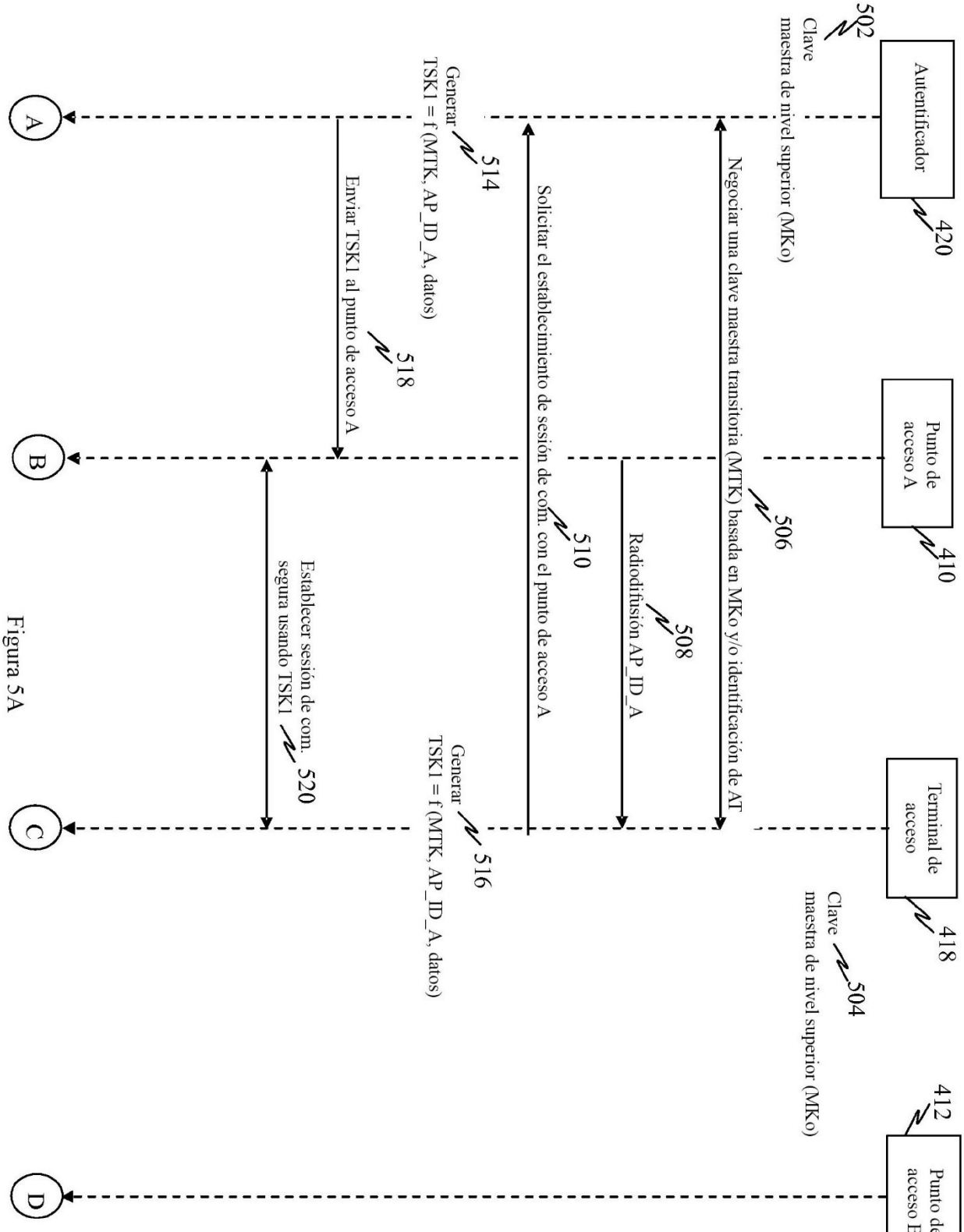
Autentificador
420
Punto de acceso A
410
Terminal de acceso
418
Punto de acceso B
412
502
Clave maestra de nivel superior (MKo)
504
Clave maestra de nivel superior (MKo)
Negociar una clave maestra transitoria (MTK) basada en MKo y/o identificación de AT
506
Radiodifusión AP_ID_A
508
Solicitar el establecimiento de sesión de com. con el punto de acceso A
510
Generar TSK1 = f (MTK, AP_ID_A, datos)
514
Generar TSK1 = f (MTK, AP_ID_A, datos)
516
Enviar TSK1 al punto de acceso A
518
Establecer sesión de com. segura usando TSK1
520
A
B
C
D

Figura 5A

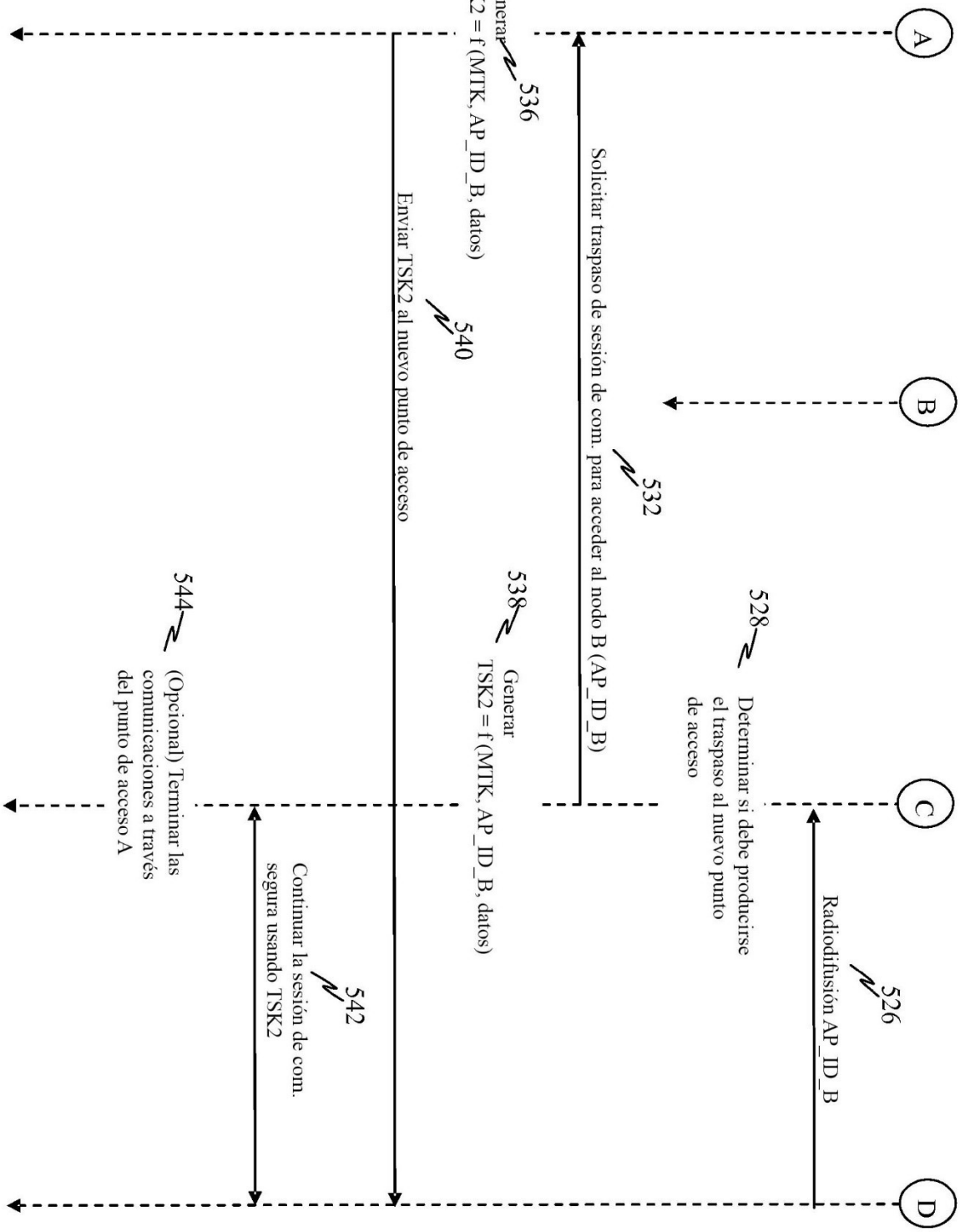
A
B
C
D
526
Radiodifusión AP_ID_B
528
Determinar si debe producirse el traspaso al nuevo punto de acceso
532
Solicitar traspaso de sesión de com. para acceder al nodo B (AP_ID_B)
536
Generar TSK2 = f (MTK, AP_ID_B, datos)
538
Generar TSK2 = f (MTK, AP_ID_B, datos)
540
Enviar TSK2 al nuevo punto de acceso
542
Continuar la sesión de com. segura usando TSK2
544
(Opcional) Terminar las comunicaciones a través del punto de acceso A

Figura 5B

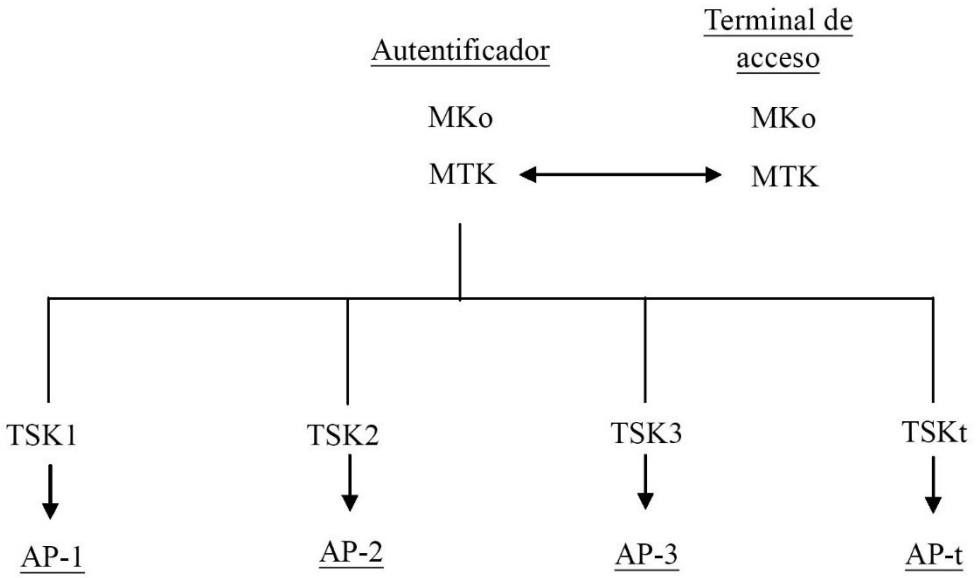

Figura 6

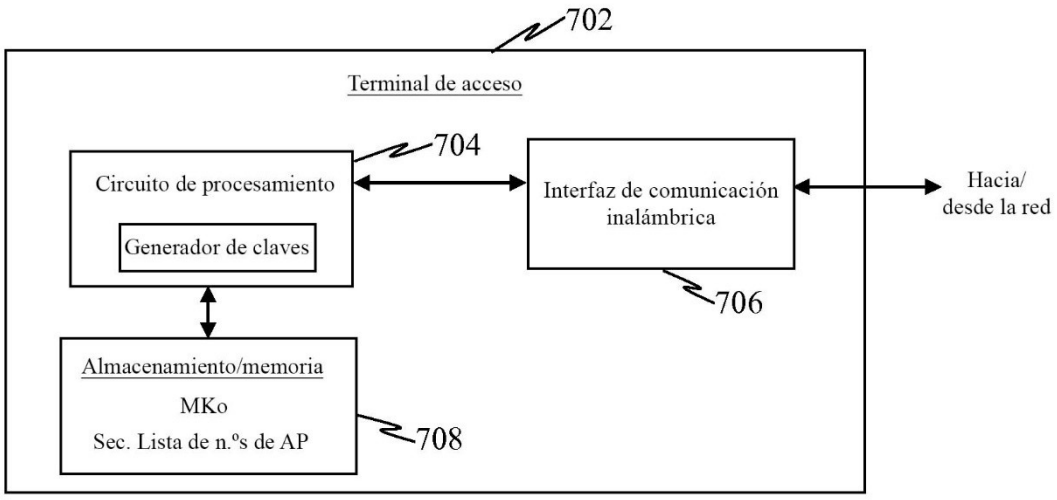

Figura 7

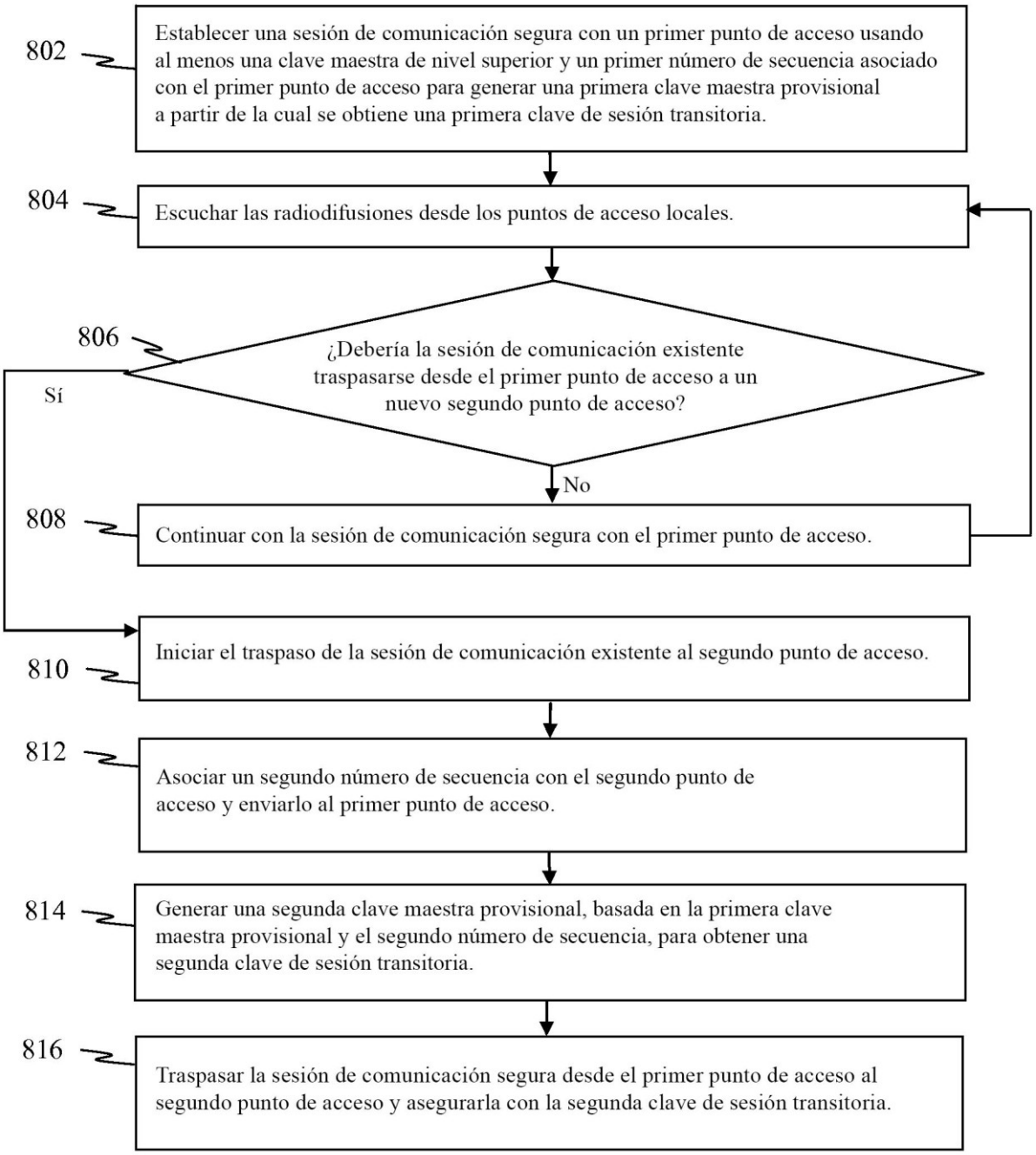
802
Establecer una sesión de comunicación segura con un primer punto de acceso usando al menos una clave maestra de nivel superior y un primer número de secuencia asociado con el primer punto de acceso para generar una primera clave maestra provisional a partir de la cual se obtiene una primera clave de sesión transitoria.
804
Escuchar las radiodifusiones desde los puntos de acceso locales.
806
¿Debería la sesión de comunicación existente traspasarse desde el primer punto de acceso a un nuevo segundo punto de acceso?
Sí
No
808
Continuar con la sesión de comunicación segura con el primer punto de acceso.
810
Iniciar el traspaso de la sesión de comunicación existente al segundo punto de acceso.
812
Asociar un segundo número de secuencia con el segundo punto de acceso y enviarlo al primer punto de acceso.
814
Generar una segunda clave maestra provisional, basada en la primera clave maestra provisional y el segundo número de secuencia, para obtener una segunda clave de sesión transitoria.
816
Traspasar la sesión de comunicación segura desde el primer punto de acceso al segundo punto de acceso y asegurarla con la segunda clave de sesión transitoria.

Figura 8

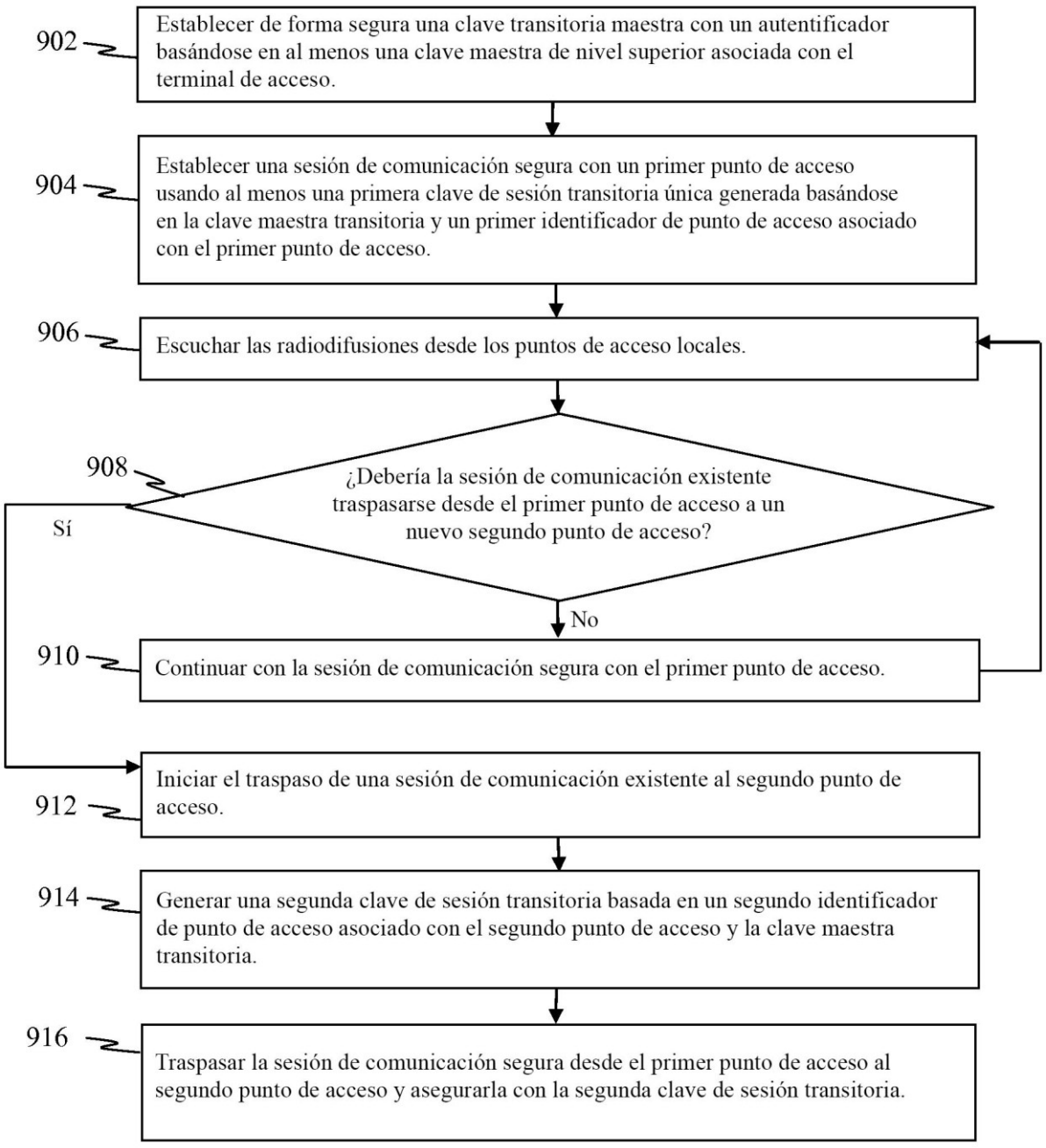
902
Establecer de forma segura una clave transitoria maestra con un autentificador basándose en al menos una clave maestra de nivel superior asociada con el terminal de acceso.
904
Establecer una sesión de comunicación segura con un primer punto de acceso usando al menos una primera clave de sesión transitoria única generada basándose en la clave maestra transitoria y un primer identificador de punto de acceso asociado con el primer punto de acceso.
906
Escuchar las radiodifusiones desde los puntos de acceso locales.
908
¿Debería la sesión de comunicación existente traspasarse desde el primer punto de acceso a un nuevo segundo punto de acceso?
Sí
No
910
Continuar con la sesión de comunicación segura con el primer punto de acceso.
912
Iniciar el traspaso de una sesión de comunicación existente al segundo punto de acceso.
914
Generar una segunda clave de sesión transitoria basada en un segundo identificador de punto de acceso asociado con el segundo punto de acceso y la clave maestra transitoria.
916
Traspasar la sesión de comunicación segura desde el primer punto de acceso al segundo punto de acceso y asegurarla con la segunda clave de sesión transitoria.

Figura 9

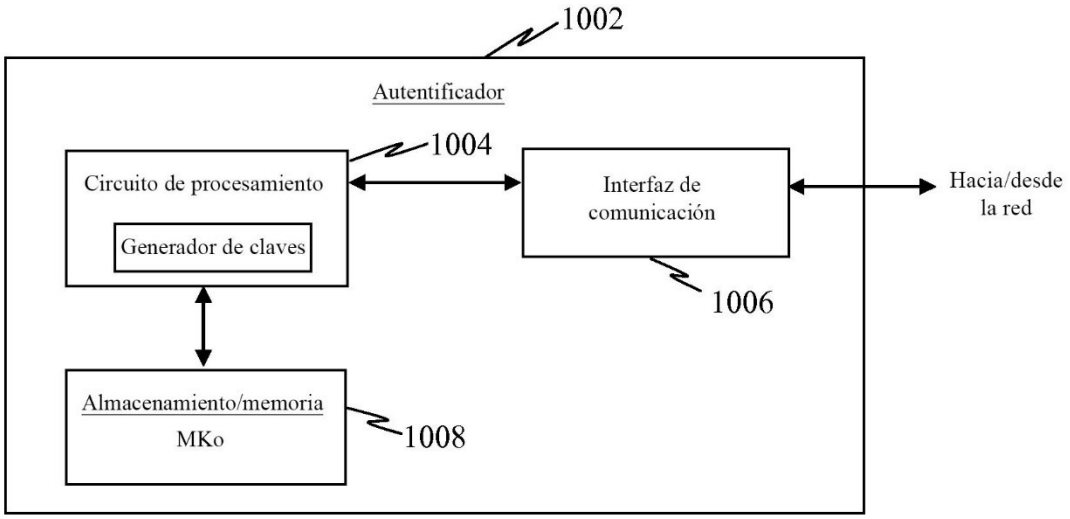
1002
Autentificador
1004
Circuito de procesamiento
Generador de claves
Interfaz de comunicación
Hacia/desde la red
1006
Almacenamiento/memoria
MKo
1008

Figura 10

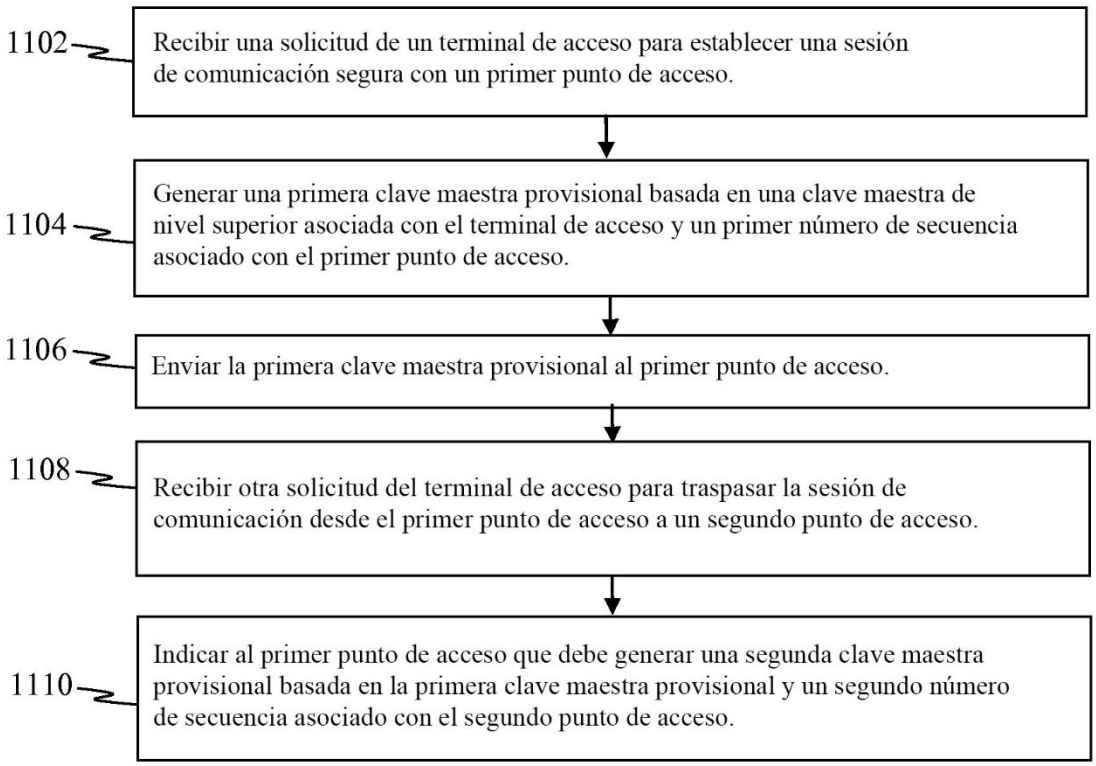
1102
Recibir una solicitud de un terminal de acceso para establecer una sesión de comunicación segura con un primer punto de acceso.
1104
Generar una primera clave maestra provisional basada en una clave maestra de nivel superior asociada con el terminal de acceso y un primer número de secuencia asociado con el primer punto de acceso.
1106
Enviar la primera clave maestra provisional al primer punto de acceso.
1108
Recibir otra solicitud del terminal de acceso para traspasar la sesión de comunicación desde el primer punto de acceso a un segundo punto de acceso.
1110
Indicar al primer punto de acceso que debe generar una segunda clave maestra provisional basada en la primera clave maestra provisional y un segundo número de secuencia asociado con el segundo punto de acceso.

Figura 11

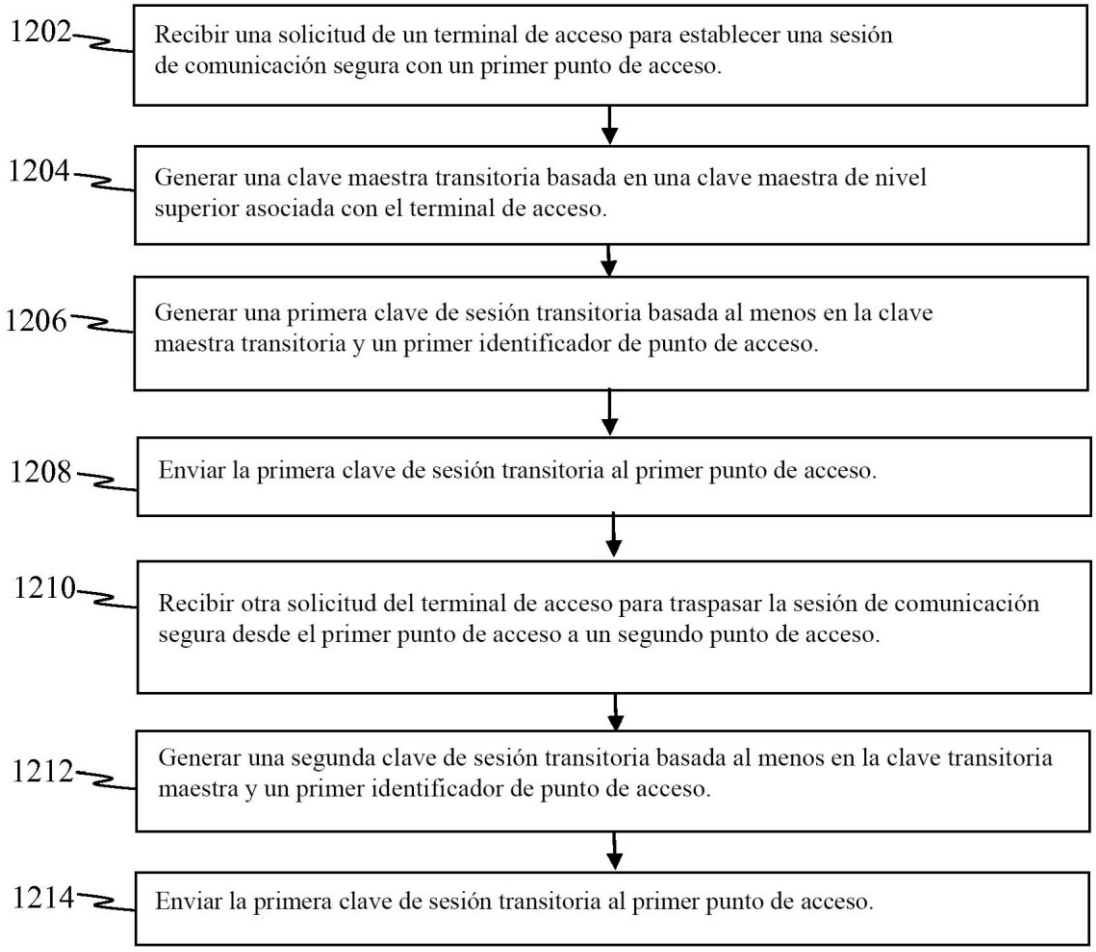
1202
Recibir una solicitud de un terminal de acceso para establecer una sesión de comunicación segura con un primer punto de acceso.
1204
Generar una clave maestra transitoria basada en una clave maestra de nivel superior asociada con el terminal de acceso.
1206
Generar una primera clave de sesión transitoria basada al menos en la clave maestra transitoria y un primer identificador de punto de acceso.
1208
Enviar la primera clave de sesión transitoria al primer punto de acceso.
1210
Recibir otra solicitud del terminal de acceso para traspasar la sesión de comunicación segura desde el primer punto de acceso a un segundo punto de acceso.
1212
Generar una segunda clave de sesión transitoria basada al menos en la clave transitoria maestra y un primer identificador de punto de acceso.
1214
Enviar la primera clave de sesión transitoria al primer punto de acceso.

Figura 12

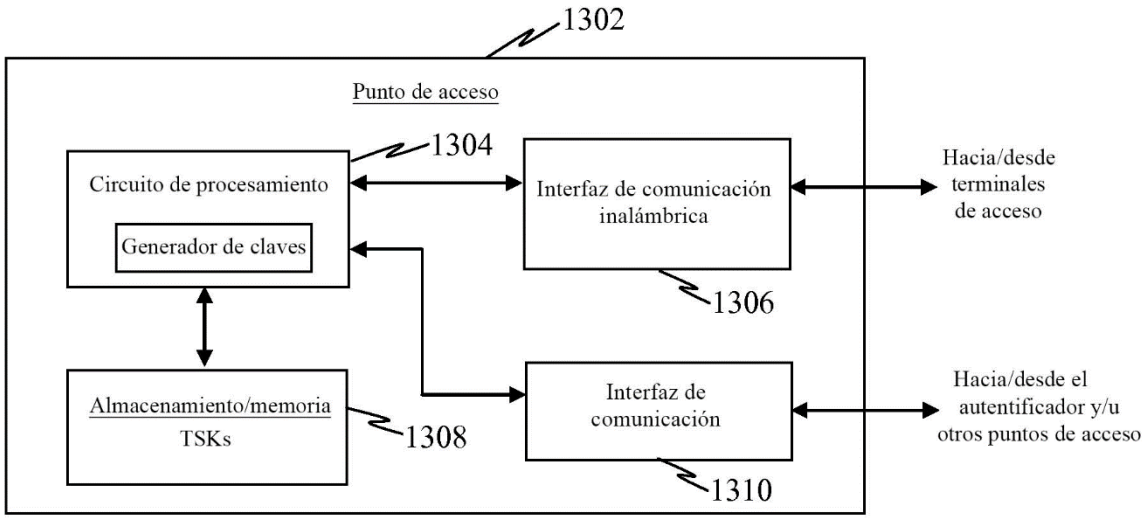

Figura 13

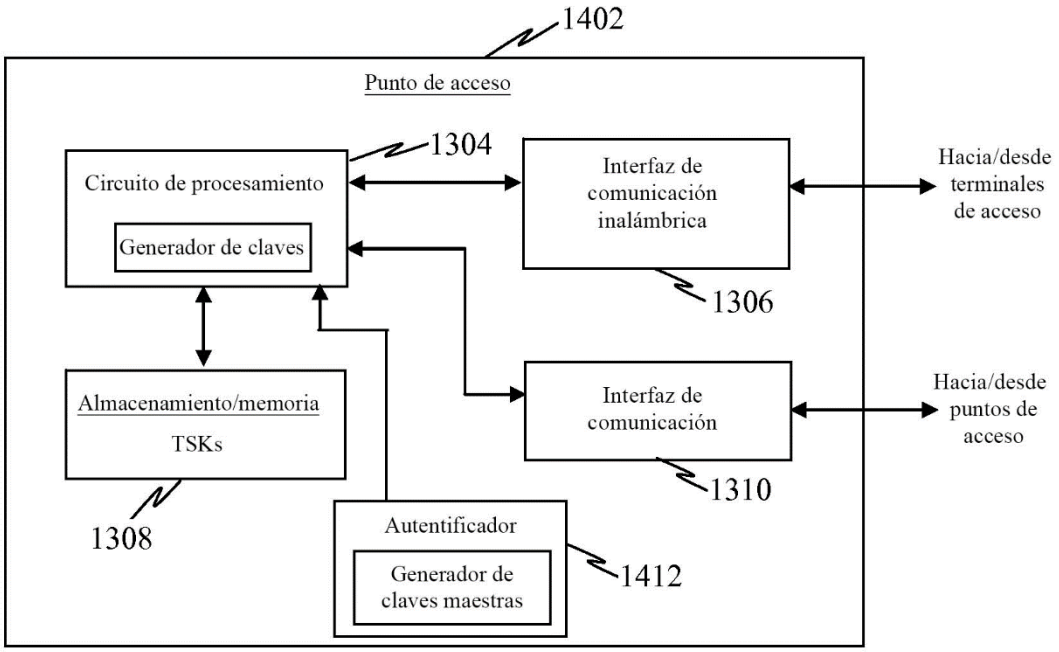

Figura 14

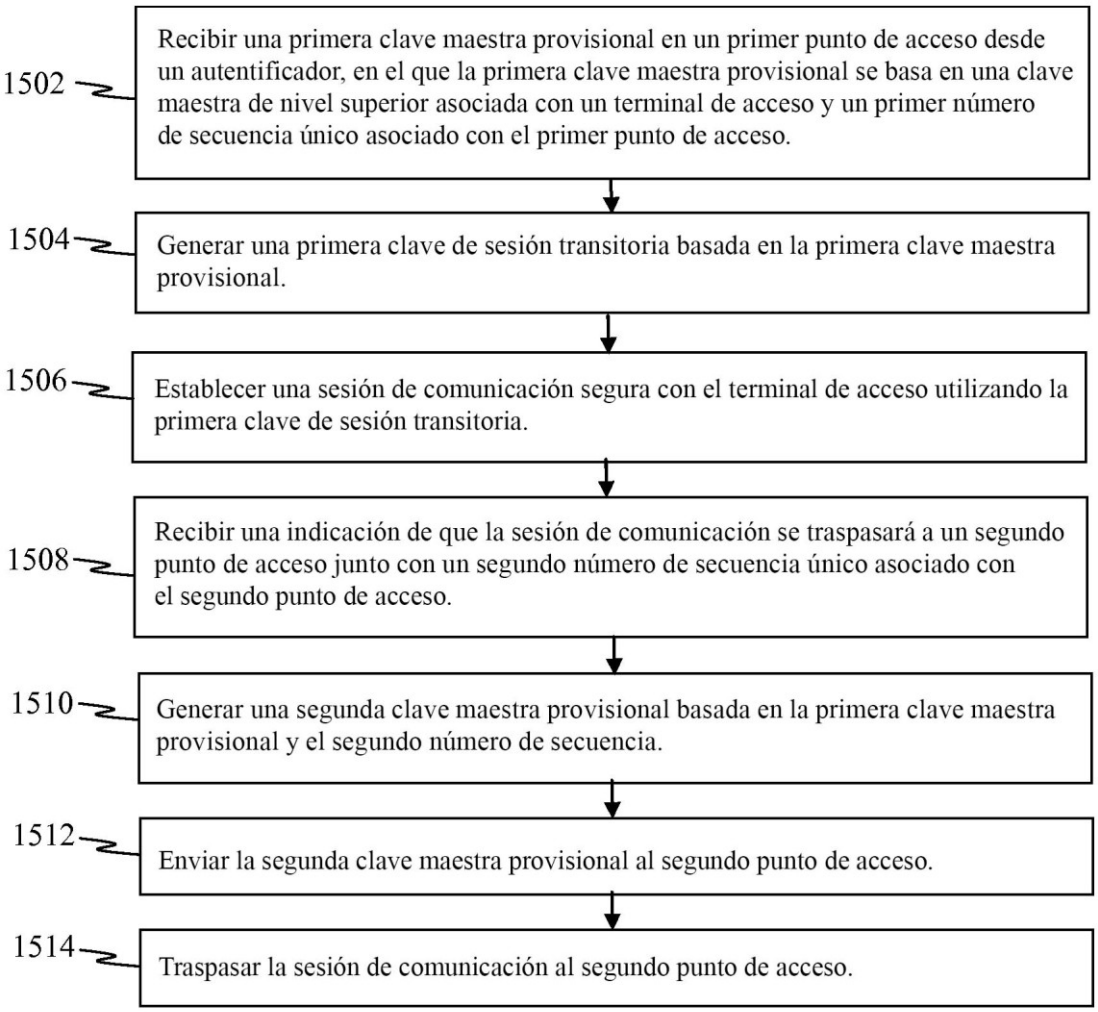
1502
Recibir una primera clave maestra provisional en un primer punto de acceso desde un autentificador, en el que la primera clave maestra provisional se basa en una clave maestra de nivel superior asociada con un terminal de acceso y un primer número de secuencia único asociado con el primer punto de acceso.
1504
Generar una primera clave de sesión transitoria basada en la primera clave maestra provisional.
1506
Establecer una sesión de comunicación segura con el terminal de acceso utilizando la primera clave de sesión transitoria.
1508
Recibir una indicación de que la sesión de comunicación se traspasará a un segundo punto de acceso junto con un segundo número de secuencia único asociado con el segundo punto de acceso.
1510
Generar una segunda clave maestra provisional basada en la primera clave maestra provisional y el segundo número de secuencia.
1512
Enviar la segunda clave maestra provisional al segundo punto de acceso.
1514
Traspasar la sesión de comunicación al segundo punto de acceso.

Figura 15

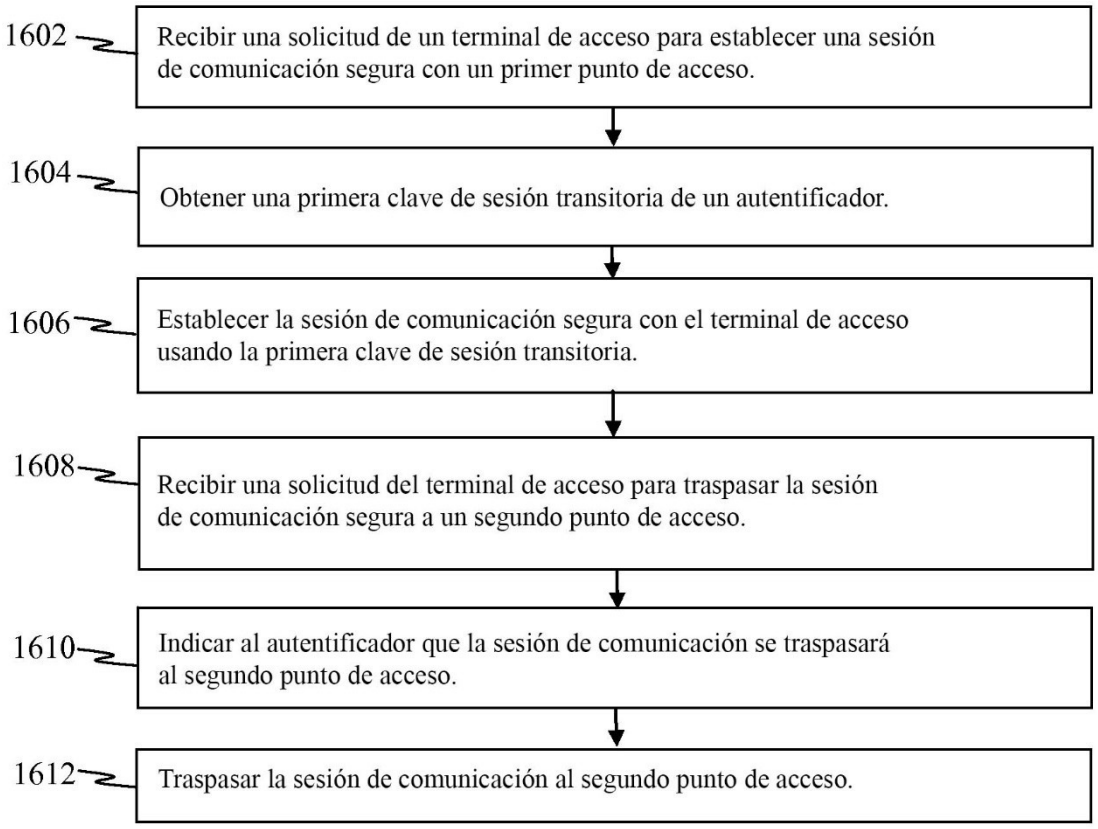
1602
Recibir una solicitud de un terminal de acceso para establecer una sesión de comunicación segura con un primer punto de acceso.
1604
Obtener una primera clave de sesión transitoria de un autentificador.
1606
Establecer la sesión de comunicación segura con el terminal de acceso usando la primera clave de sesión transitoria.
1608
Recibir una solicitud del terminal de acceso para traspasar la sesión de comunicación segura a un segundo punto de acceso.
1610
Indicar al autentificador que la sesión de comunicación se traspasará al segundo punto de acceso.
1612
Traspasar la sesión de comunicación al segundo punto de acceso.

Figura 16

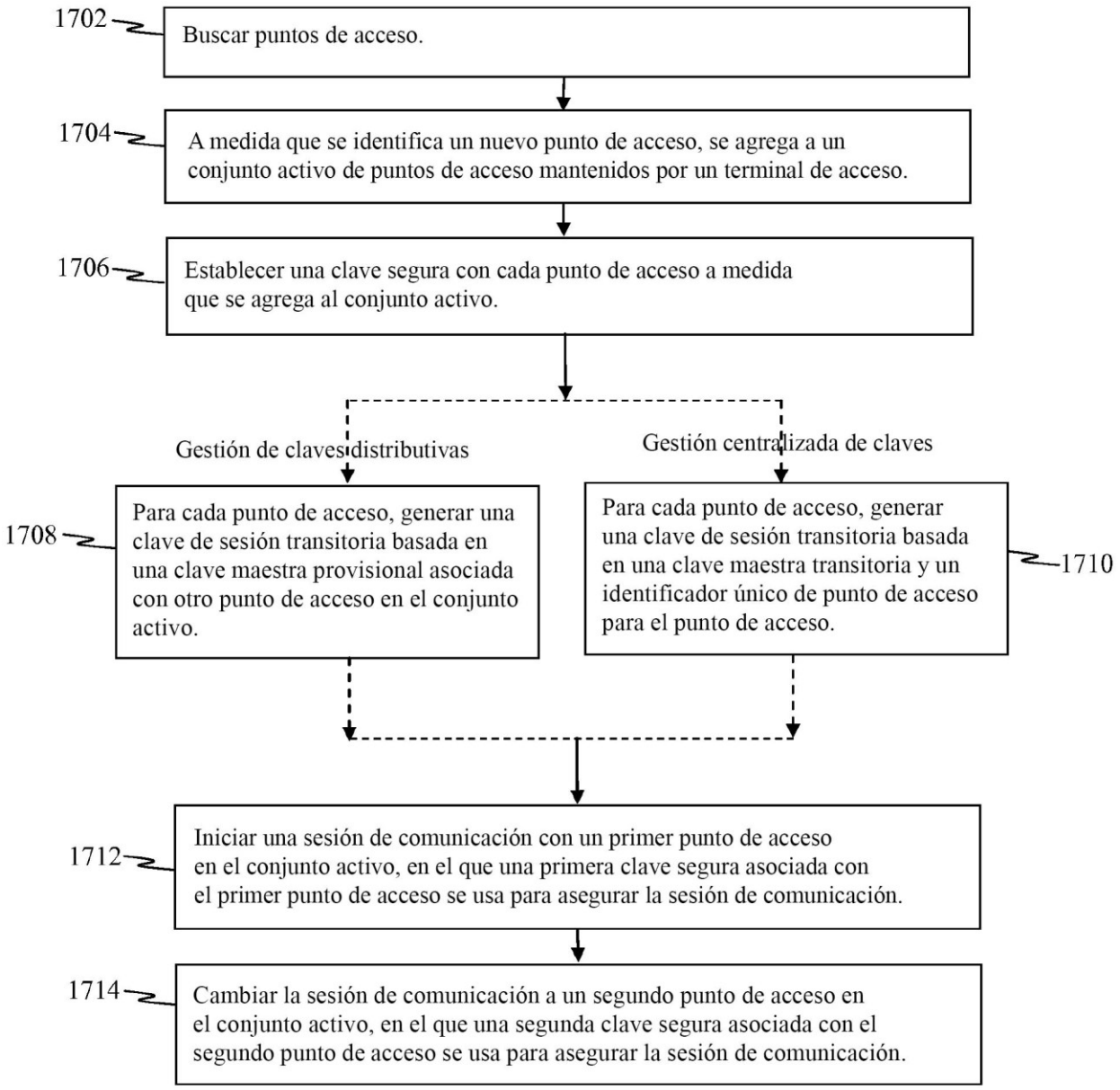
1702
Buscar puntos de acceso.
1704
A medida que se identifica un nuevo punto de acceso, se agrega a un conjunto activo de puntos de acceso mantenidos por un terminal de acceso.
1706
Establecer una clave segura con cada punto de acceso a medida que se agrega al conjunto activo.
Gestión de claves distributivas
Gestión centralizada de claves
1708
Para cada punto de acceso, generar una clave de sesión transitoria basada en una clave maestra provisional asociada con otro punto de acceso en el conjunto activo.
Para cada punto de acceso, generar una clave de sesión transitoria basada en una clave maestra transitoria y un identificador único de punto de acceso para el punto de acceso.
1710
1712
Iniciar una sesión de comunicación con un primer punto de acceso en el conjunto activo, en el que una primera clave segura asociada con el primer punto de acceso se usa para asegurar la sesión de comunicación.
1714
Cambiar la sesión de comunicación a un segundo punto de acceso en el conjunto activo, en el que una segunda clave segura asociada con el segundo punto de acceso se usa para asegurar la sesión de comunicación.

Figura 17