(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 404 175**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **29.10.2008 E 08872189 (9)**

(97) Fecha y número de publicación de la concesión europea: **20.02.2013 EP 2239883**

(54) Título: **Método, dispositivo, sistema, nodo cliente, nodo homólogo y punto de convergencia para evitar la falsificación de identidad de nodos**

(30) Prioridad:

02.02.2008 CN 200810006832

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.05.2013

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building Bantian
Longgang District, Shenzhen
Guangdong 518129 , CN

(72) Inventor/es:

LI, FENG;
JIANG, XINGFENG y
JIANG, HAIFENG

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método, dispositivo, sistema, nodo cliente, nodo homólogo y punto de convergencia para evitar falsificación de identidad de nodos

Campo de la tecnología

La presente invención está relacionada con el campo de la red superpuesta y, más en particular, con un método, un dispositivo, un sistema, un nodo cliente, un nodo homólogo y un punto de convergencia para evitar que un equipo de red falsifique una identidad (ID).

Antecedentes de la invención

Una red superpuesta es una red virtual construida sobre una o más redes subyacentes (por ejemplo, una red física o una red lógica) existentes. La red superpuesta puede implementar ciertas funciones que son difíciles para la red subyacente como, por ejemplo, encaminamiento de mensajes o mantenimiento de la topología.

La red superpuesta entre pares (P2P) (esto es, la red P2P) es una red superpuesta construida en un modo P2P basada en la Internet existente. En la red P2P, se pueden implementar funciones como, por ejemplo, estado equivalente y compartición de recursos entre nodos homólogos (pares) en la red P2P a partir de la Internet actual (por ejemplo nodo cliente/red de servidores).

La red P2P tiene dos tipos de entidades: nodo homólogo y nodo cliente. Además de disponer de la función de compartición de recursos, el nodo homólogo participa en la organización y mantenimiento de la red P2P, incluyendo encaminamiento, almacenamiento y otras funciones. Las funciones del nodo cliente son relativamente simples. Necesita reenviar a la red una petición a través de un nodo homólogo y no tiene ninguna función de encaminamiento, esto es, una ruta de la red no pasa por el nodo cliente.

En una red P2P, cada nodo homólogo y nodo cliente tiene una ID. Para el encaminamiento, en función de la ID del nodo homólogo (ID homóloga) se almacenan o leen los pares de clave/valor y los valores correspondientes a las claves de la red. El nodo cliente recibe servicios proporcionados por el nodo homólogo de acuerdo con la ID del nodo cliente. La ID del nodo homólogo y la ID del nodo cliente se obtienen de acuerdo con ciertas reglas, por ejemplo, el primero se obtiene mediante un algoritmo Hash y el último es asignado por un servidor de gestión.

Un nodo malicioso puede falsificar fácilmente la ID del nodo homólogo y la ID del nodo cliente. El nodo malicioso ataca la red u obtiene ilegalmente recursos de red falsificando la ID del nodo homólogo y evita el coste de utilización de recursos de red falsificando las ID de otros nodos cliente.

Para evitar la falsificación de la ID, se utiliza comúnmente el siguiente método. Antes de que cada nodo cliente se conecte a la red, una entidad u organización externa autentica la ID del nodo cliente, y el nodo cliente que pasa la autenticación puede obtener un certificado para conectarse a la red. El nodo cliente firma el mensaje generado automáticamente de acuerdo con la clave privada del certificado, y autentica y firma el mensaje recibido.

Durante la implementación de la presente invención, los inventores encontraron que la solución técnica anterior tiene los siguientes problemas. Como en el método anterior el certificado y el nodo cliente están asociados, los costes son relativamente altos al margen de la capacidad para evitar la falsificación de la ID. En primer lugar, en el método, es necesario desplegar en la red un sistema de Infraestructura de Clave Pública (PKI), pero los costes de despliegue son altos y, además, los costes del mantenimiento del sistema son altos. En segundo lugar, es necesario que el nodo cliente firme cada mensaje enviado y cada mensaje recibido, lo que da como resultado un retardo relativamente grande en el encaminamiento de mensajes en la red. Como resultado, el método no puede satisfacer necesariamente un servicio de flujos multimedia con altos requisitos en relación con el retardo. En tercer lugar, en ciertos entornos de aplicación sencillos, incluso aunque tanto el nodo cliente como el nodo homólogo dispongan de certificados, los certificados no se utilizan necesariamente para autenticar mensajes, y únicamente se necesita autenticación de la ID.

El documento “Handling identity in peer-to-peer-systems (Administrando la identidad en sistemas entre pares), de HAUSWIRTH M Y OTROS divulga que debido al número limitado de direcciones IP disponibles la mayoría de los ordenadores de Internet utilizan direcciones IP dinámicas, lo cual provoca problemas a las aplicaciones que tienen que mantener las tablas de encaminamiento, por ejemplo, los sistemas entre pares. Para superar esto, nosotros proponemos en las tablas de encaminamiento identificadores homólogos únicos y aplicar el propio sistema entre pares para mantener consistentes las asociaciones entre una id y una IP que se van a utilizar en el proceso de encaminamiento.

El documento “Defending the Sybil Attack in P2P Networks: Taxonomy, Challenges, and a Proposal Self-Registration (Protegerse del Ataque tipo Sybil en Redes P2P: Taxonomía, Retos y una Propuesta de Auto-Registro)” de DINGER J Y OTROS divulga que la robustez de las redes entre pares (P2P), en particular las redes superpuestas basadas en

DHT, sufren de forma significativa cuando se lleva a cabo un ataque de tipo Sybil. Nosotros abordamos el problema de los ataques de tipo Sybil desde dos puntos de vista. En primer lugar clarificamos, analizamos y clasificamos el proceso de asignación del identificador P2P. Separando claramente los participantes de la red de los nodos de la red se convierten en obvios dos retos de las redes P2P bajo un ataque de tipo Sybil: 1) estabilidad a lo largo del tiempo, y 2) diferenciación de identidades. En segundo lugar, como punto de partida para un análisis cuantitativo de la estabilidad en el tiempo de redes P2P bajo ataques de tipo Sybil y bajo algunas suposiciones con respecto a la diferenciación de identidades, proponemos un procedimiento de registro de identidades denominado auto-registro que utiliza los mecanismos de distribución inherentes a una red P2P.

El documento US 2007/097986 A1 divulga un terminal de comunicaciones homólogo programado para operar en una red entre pares. El terminal incluye un transceptor, un controlador acoplado al transceptor y un dispositivo de memoria, y en memoria se almacena una tabla de asociación, en donde la tabla de asociación asocia una identidad del terminal con la correspondiente información de transporte para al menos otro terminal homólogo.

El documento WO 2007/012083 A2 divulga que en un sistema de autenticación de usuarios de red, un usuario de red es identificado para el propósito de autenticación utilizando el identificador único para una línea de comunicación física dedicada asociada con el edificio en el que está situado el usuario de la red o un certificado digital que está asociado con un componente seguro o una línea de comunicación unida físicamente a un edificio. Para el propósito de la autenticación, un servidor de autenticación verifica inicialmente la identificación a asociar con la línea de comunicación dedicada. El certificado digital se puede almacenar en una pasarela del edificio o en un módulo en el emplazamiento extremo que está conectado a los componentes seguros de una pluralidad de edificios y almacena certificados digitales únicos para cada edificio.

Resumen de la invención

Un modo de realización de la presente invención proporciona un método para evitar que un nodo falsifique una ID en una red P2P, que aborda el problema de que los costes son altos en el despliegue y mantenimiento cuando se despliega una PKI en la solución técnica existente para evitar la suplantación de nodos homólogos y aborda el problema del retardo de encaminamiento de mensajes cuando se lleva a cabo la verificación de firma para cada mensaje enviado y cada mensaje recibido en la solución técnica existente para evitar la suplantación de nodos homólogos.

Para conseguir los objetivos, el método para evitar, de acuerdo con el modo de realización de la presente invención, que un nodo falsifique una ID, incluye los siguientes pasos.

Después de que un nodo cliente encuentre a un nodo homólogo que dé servicio al nodo cliente, al menos uno de entre el nodo cliente y el nodo homólogo actúa como iniciador de la autenticación y autentica a la otra parte.

Después de realizar con éxito la autenticación, el nodo cliente o el nodo homólogo que actúa como iniciador de la autenticación elabora y almacena localmente un listado contra la falsificación de ID de la otra parte, e identifica un nodo malicioso utilizando el listado contra la falsificación de ID,

en donde el nodo que actúa como iniciador de la autenticación es el nodo cliente o el nodo homólogo,

si el nodo que actúa como iniciador de la autenticación es el nodo cliente, el listado contra la falsificación de ID en relación con la otra parte comprende la ID del nodo homólogo, una dirección física del nodo homólogo, y una o más relaciones de asociación entre la ID del nodo homólogo y la dirección física del nodo homólogo;

si el nodo que actúa como iniciador de la autenticación es el nodo homólogo, el listado contra la falsificación de ID en relación con la otra parte comprende la ID del nodo cliente, una dirección física del nodo cliente, y una o más relaciones de asociación entre la ID del nodo cliente y la dirección física del nodo cliente.

En el método, de acuerdo con el modo de realización de la presente invención, para evitar que un nodo falsifique una ID, el nodo homólogo o el nodo cliente almacena localmente un listado contra la falsificación de ID, lo que resuelve el problema de que los costes son altos en el despliegue y mantenimiento cuando se despliega una PKI en la solución técnica existente para evitar la suplantación del nodo homólogo. El proceso de identificación de nodos maliciosos utilizando el listado contra la falsificación de ID es simple, efectivo y los costes de detección son bajos. Se resuelve el problema de que el retardo sea grande en el encaminamiento de los mensajes cuando se lleva a cabo la verificación de firma para cada mensaje enviado y recibido en la solución técnica existente para evitar la suplantación del nodo homólogo. Cuando se identifica el nodo malicioso utilizando el listado contra la falsificación de ID, únicamente es necesario verificar la ID del nodo, mientras que no es necesario llevar a cabo la verificación de firma para cada mensaje enviado y recibido y, de este modo, se reduce el retardo de encaminamiento.

En un modo de realización, la presente invención proporciona, además, un dispositivo para evitar que un nodo falsifique una ID en una red P2P, que aborda el problema de que los costes son altos en el despliegue y mantenimiento cuando se despliega una PKI en la solución técnica existente para evitar la suplantación de nodos

homólogos y aborda el problema de que el retardo de encaminamiento de mensajes es grande cuando se lleva a cabo la verificación de firma para cada mensaje enviado y cada mensaje recibido en la solución técnica existente para evitar la suplantación de nodos homólogos.

Para conseguir los objetivos, para evitar que un nodo falsifique una ID de acuerdo con el modo de realización de la presente invención el dispositivo adopta la siguiente solución técnica. El dispositivo incluye una unidad 1 de autenticación, una unidad 2 de almacenamiento y una unidad 3 de identificación.

La unidad 1 de autenticación está configurada para autenticar la validez de una ID de un nodo.

La unidad 2 de almacenamiento está configurada para elaborar y almacenar un listado contra la falsificación de ID en relación con la ID del nodo autenticado.

La unidad 3 de identificación está configurada para identificar a un nodo malicioso de acuerdo con el listado contra la falsificación de ID,

en donde el dispositivo es un nodo cliente o un nodo homólogo o un punto de convergencia de la red,

si el dispositivo es el nodo cliente, el listado contra la falsificación de ID en relación con el nodo autenticado comprende la ID del nodo homólogo, una dirección física del nodo homólogo, y una o más relaciones de asociación entre la ID del nodo homólogo y la dirección física del nodo homólogo; y

si el dispositivo es el nodo homólogo, el listado contra la falsificación de ID en relación con el nodo autenticado comprende la ID del nodo cliente, una dirección física del nodo cliente y una o más relaciones de asociación entre la ID del nodo cliente y la dirección física del nodo cliente; y

si el dispositivo es el punto de convergencia de la red, el listado contra la falsificación de ID en relación con el nodo autenticado comprende la ID del nodo homólogo, una dirección física del nodo homólogo, y una o más relaciones de correspondencia entre la ID del nodo homólogo y la dirección física del nodo homólogo.

En el dispositivo proporcionado en el modo de realización de la presente invención para evitar que un nodo falsifique una ID, el nodo homólogo o el nodo cliente almacena un listado contra la falsificación de ID en la unidad de almacenamiento local, lo cual resuelve el problema de que los costes son altos en el despliegue y mantenimiento cuando se despliega una PKI en la solución técnica existente para evitar la suplantación del nodo homólogo. El proceso de la unidad de identificación para la identificación de un nodo malicioso utilizando el listado contra la falsificación de ID es simple, efectivo y los costes de detección son bajos. Se resuelve el problema de que el retardo sea grande en el encaminamiento de los mensajes cuando se lleva a cabo la verificación de firma para cada mensaje enviado y recibido en la solución técnica existente para evitar la suplantación del nodo homólogo. Cuando la unidad de identificación identifica un nodo malicioso utilizando el listado contra la falsificación de ID, la unidad de identificación únicamente verifica la ID del nodo, mientras que no es necesario llevar a cabo la verificación de firma para cada mensaje enviado y recibido y, de este modo, se reduce el retardo de encaminamiento.

En un modo de realización, la presente invención proporciona, además, un sistema para evitar que un nodo falsifique una ID en una red P2P, que aborda el problema de que los costes son altos en el despliegue y mantenimiento cuando se despliega una PKI en la solución técnica existente para evitar la suplantación de nodos homólogos y aborda el problema de que el retardo de encaminamiento de mensajes es grande cuando se lleva a cabo la verificación de firma para cada mensaje enviado y cada mensaje recibido en la solución técnica existente para evitar la suplantación de nodos homólogos.

Para conseguir los objetivos, de acuerdo con el modo de realización de la presente invención, el sistema adopta la siguiente solución técnica para evitar que un nodo falsifique una ID. El sistema incluye un nodo homólogo y un nodo cliente.

El nodo cliente está configurado para localizar el nodo homólogo que da servicio al nodo cliente y establecer una conexión con el nodo homólogo.

El nodo homólogo está configurado para establecer la conexión con el nodo cliente que envía una petición de servicio al nodo homólogo.

Al menos uno entre el nodo cliente y el nodo homólogo actúa como iniciador de la autenticación y autentica a la otra parte.

Después de que la autenticación se realice con éxito, el nodo cliente o el nodo homólogo que actúa como el iniciador de la autenticación elabora y almacena localmente un listado contra la falsificación de ID en relación con la otra parte e identifica el nodo malicioso utilizando el listado contra la falsificación de ID, en donde

si el nodo que actúa como iniciador de la autenticación es el nodo cliente, el listado contra la falsificación de ID en

relación con la otra parte comprende la ID del nodo homólogo, una dirección física del nodo homólogo, y una o más relaciones de asociación entre la ID del nodo homólogo y la dirección física del nodo homólogo; y

si el nodo que actúa como iniciador de la autenticación es el nodo homólogo, el listado contra la falsificación de ID en relación con la otra parte comprende la ID del cliente, una dirección física del nodo cliente y una o más relaciones de asociación entre la ID del nodo cliente y la dirección física del nodo cliente.

En el sistema proporcionado en el modo de realización de la presente invención para evitar que un nodo falsifique una ID, el nodo homólogo o el nodo cliente almacena un listado contra la falsificación de ID en un almacenamiento local, lo cual resuelve el problema de que los costes son altos en el despliegue y mantenimiento cuando se despliega una PKI en la solución técnica existente para evitar la suplantación del nodo homólogo. El proceso para que las unidades de identificación del nodo homólogo y del nodo cliente identifiquen al nodo malicioso utilizando el listado contra la falsificación de ID es simple, efectivo y los costes de detección son bajos.

Se resuelve el problema de que el retardo es grande cuando se lleva a cabo la verificación de firma para cada mensaje enviado y recibido en la solución técnica existente para evitar la suplantación del nodo homólogo. Cuando las unidades de identificación del nodo homólogo y del nodo cliente identifican el nodo malicioso utilizando el listado contra la falsificación de ID, la unidad de autenticación únicamente necesita verificar la ID del nodo, mientras que no es necesario llevar a cabo la verificación de firma para cada mensaje enviado y recibido y, de este modo, se reduce el retardo de encaminamiento.

Breve descripción de los dibujos

La FIG. 1 es un diagrama de flujo de un método, de acuerdo con un modo de realización de la presente invención, para evitar que un nodo falsifique una ID;

la FIG. 2 es una vista esquemática de un método, de acuerdo con un modo de realización de la presente invención, para evitar que un nodo falsifique una ID utilizando un punto de convergencia;

la FIG. 3 es una vista esquemática de la estructura de un dispositivo, de acuerdo con un modo de realización de la presente invención, para evitar que un nodo falsifique una ID; y

la FIG. 4 es una vista esquemática de la estructura de un sistema, de acuerdo con un modo de realización de la presente invención, para evitar que un nodo falsifique una ID;

Descripción detallada de los modos de realización

En un modo de realización de la presente invención se proporciona un método para evitar que un nodo falsifique una ID, de modo que se resuelvan los problemas de los altos costes operativos y grandes retardos del método existente para evitar la suplantación de un nodo homólogo en una red P2P. A continuación se describirá en detalle el método del modo de realización de la presente invención para evitar que un nodo falsifique una ID haciendo referencia a los dibujos adjuntos.

Como se muestra en la FIG. 1, en un modo de realización de la presente invención, el método proporcionado para evitar que un nodo falsifique una ID incluye los siguientes pasos.

En el paso 11, después de que un nodo cliente encuentre un nodo homólogo que dé servicio al nodo cliente, al menos uno de entre el nodo cliente y el nodo homólogo actúa como iniciador de la autenticación y autentica a la otra parte.

La autenticación incluye autenticación en un solo sentido y autenticación recíproca.

La autenticación en un solo sentido es del siguiente modo: el iniciador de la autenticación (bien el nodo cliente o bien el nodo homólogo) autentica la ID de la otra parte, esto es, el nodo cliente autentica la ID del nodo homólogo, o el nodo homólogo autentica la ID del nodo cliente.

La autenticación recíproca es del siguiente modo: el nodo cliente autentica la ID del nodo homólogo, y el nodo homólogo autentica la ID del nodo cliente.

El proceso de autenticación específico está cubierto en la técnica anterior y no se describirá aquí en detalle.

En el paso 12, después de realizar con éxito la autenticación, el nodo cliente o el nodo homólogo que actúa como iniciador de la autenticación elabora y almacena localmente un listado contra la falsificación de ID de la otra parte.

En la autenticación en un solo sentido, si el nodo cliente es el iniciador de la autenticación, el nodo cliente elabora localmente un listado contra la falsificación de ID del nodo homólogo. El listado contra la falsificación de ID incluye la ID del nodo homólogo, una dirección física del nodo homólogo, y una o más relaciones de asociación entre la ID del

nodo homólogo y la dirección física del nodo homólogo.

En la autenticación en un solo sentido, si el nodo homólogo es el iniciador de la autenticación, el nodo homólogo elabora localmente un listado contra la falsificación de ID en relación con el nodo cliente. El listado contra la falsificación de ID incluye la ID del nodo cliente, la dirección física del nodo cliente, y una o más relaciones de asociación entre la ID el nodo cliente y la dirección física del nodo cliente.

En la autenticación recíproca, el nodo homólogo elabora localmente un listado contra la falsificación de ID en relación con el nodo cliente, y el nodo cliente elabora localmente un listado contra la falsificación de ID en relación con el nodo homólogo.

La ID del nodo homólogo incluye la identificación del nodo homólogo, y la ID del nodo cliente incluye la identificación del nodo cliente. La dirección física puede ser una dirección MAC, o una dirección IP, o un Identificador de la Ruta Virtual/Identificador del Canal Virtual del Modo de Transferencia Asíncrono (ATM VPI/VCI), o una ID de la Red de Área Local Virtual (VLAN ID) del nodo, o puede ser una dirección de conexión física entre el nodo cliente y el nodo homólogo. Un nodo homólogo puede tener una relación de asociación con al menos dos direcciones físicas.

El nodo elabora y almacena un listado contra la falsificación de ID en relación con la otra parte, e identifica el nodo malicioso utilizando el listado contra la falsificación de ID. Cuando el nodo cliente elabora y almacena localmente el listado contra la falsificación de ID en relación con la otra parte, el proceso específico para que el nodo cliente identifique el nodo malicioso es del siguiente modo.

Después de recibir el mensaje enviado por el nodo homólogo, el nodo cliente actúa como el iniciador de autenticación y autentica la relación o relaciones de asociación entre la ID del nodo homólogo y la dirección física del nodo homólogo.

Si la relación o relaciones de asociación entre la ID del nodo homólogo y la dirección física del nodo homólogo es consistente con el registro del listado contra la falsificación de ID que posee el iniciador, el nodo homólogo no es un nodo malicioso; si la relación o relaciones de asociación entre la ID del nodo homólogo y la dirección física del nodo homólogo es inconsistente con el registro del listado contra la falsificación de ID que posee el iniciador, el nodo homólogo es un nodo malicioso.

Cuando el nodo homólogo elabora y almacena localmente el listado contra la falsificación de ID en relación con la otra parte, el proceso específico para que el nodo homólogo identifique el nodo malicioso es como sigue.

Después de recibir el mensaje enviado por el nodo cliente, el nodo homólogo actúa como el iniciador de la autenticación y autentica la relación o relaciones de asociación entre la ID del nodo cliente y la dirección física del nodo cliente.

Si la relación o relaciones de asociación entre la ID del nodo cliente y la dirección física del nodo cliente es consistente con el registro del listado contra la falsificación de ID que posee el iniciador, el nodo cliente no es un nodo malicioso; si la relación o relaciones de asociación entre la ID del nodo cliente y la dirección física del nodo cliente es inconsistente con el registro del listado contra la falsificación de ID que posee el iniciador, el nodo cliente no es un nodo malicioso, el nodo cliente es un nodo malicioso.

En el método proporcionado en el modo de realización de la presente invención para evitar que un nodo falsifique una ID, el nodo homólogo o el nodo cliente almacena localmente un listado contra la falsificación de ID, lo que resuelve el problema de que los costes son altos en el despliegue y mantenimiento cuando se despliega una PKI en la solución técnica existente para evitar la suplantación del nodo homólogo. El proceso de identificación de nodos maliciosos utilizando el listado contra la falsificación de ID es simple, efectivo y los costes de detección son bajos. Se resuelve el problema de que el retardo sea grande en el encaminamiento de los mensajes cuando se lleva a cabo la verificación de firma para cada mensaje enviado y recibido en la solución técnica existente para evitar la suplantación del nodo homólogo. Cuando se identifica el nodo malicioso utilizando el listado contra la falsificación de ID, únicamente es necesario verificar la ID del nodo, mientras que no es necesario llevar a cabo la verificación de firma para cada mensaje enviado y recibido y, de este modo, se reduce el retardo de encaminamiento.

Si cambia la dirección física del nodo homólogo, el nodo cliente borra un registro contra la falsificación de ID del nodo homólogo del listado contra la falsificación de ID.

Después de que el nodo homólogo obtenga la nueva dirección física, el nodo cliente vuelve a autenticar al nodo homólogo.

Después de que tenga éxito la autenticación, el nodo cliente almacena en el listado contra la falsificación de ID la relación o relaciones de asociación entre la ID del nodo homólogo y la nueva dirección física del nodo homólogo.

Cuando el nodo homólogo que da servicio al nodo cliente deja la red P2P, el nodo homólogo notifica a un nodo homólogo sustituto la relación o relaciones entre la ID del nodo cliente y la dirección física del nodo cliente, y notifica

al nodo cliente que el nodo homólogo sustituto continúa dando servicio al nodo cliente.

Antes de aceptar el servicio proporcionado por el nodo homólogo sustituto, el nodo cliente autentica primero una ID del nodo homólogo sustituto.

Después de que tenga éxito la autenticación, el nodo cliente añade al listado contra la falsificación de ID local la relación o relaciones de asociación entre la ID del nodo homólogo sustituto y la dirección física del nodo homólogo sustituto.

A continuación, el nodo cliente acepta el servicio proporcionado por el nodo homólogo sustituto.

Tal y como se muestra en la FIG. 2, en algunos escenarios de aplicación, en la red P2P se conectan puntos de convergencia que pueden detectar el mensaje en la red P2P. Cada nodo homólogo está conectado a la red P2P a través del punto de convergencia, y los nodos homólogos también se pueden conectar con nodos cliente. El mensaje entre los nodos homólogos es reenviado a la red P2P a través de cierto punto de convergencia. Estos puntos de convergencia tienen una función básica de análisis de mensajes. Los puntos de convergencia analizan el mensaje recibido mediante una inspección profunda de paquetes (DPI) para obtener el contenido del mensaje, extraer la relación o relaciones de correspondencia entre la ID del nodo homólogo y la dirección física del nodo homólogo del mensaje, y elaborar un listado contra la falsificación de ID en relación con el nodo homólogo.

El modo de realización de la presente invención proporciona, además, un dispositivo para evitar que un nodo falsifique una ID en una red P2P. Tal y como se muestra en la FIG. 3, el dispositivo incluye una unidad 1 de autenticación, una unidad 2 de almacenamiento, y una unidad 3 de identificación

La unidad 1 de autenticación está configurada para autenticar la validez de una ID de un nodo.

La unidad 2 de almacenamiento está configurada para elaborar y almacenar un listado contra la falsificación de ID en relación con el nodo autenticado.

La unidad 3 de identificación está configurada para identificar a un nodo malicioso de acuerdo con el listado contra la falsificación de ID.

Los nodos incluyen un nodo cliente o un nodo homólogo. Si un nodo es un nodo cliente, el listado contra la falsificación de ID del nodo incluye: la ID del nodo homólogo, la dirección física del nodo homólogo, y la relación o relaciones de asociación entre la ID del nodo homólogo y la dirección física. La ID del nodo homólogo incluye la identificación del nodo homólogo. Si un nodo es un nodo homólogo, el listado contra la falsificación de ID del nodo incluye la ID del nodo cliente, la dirección física del nodo cliente y la relación o relaciones de asociación entre la ID del nodo cliente y la dirección física del nodo cliente.

El proceso de identificación de un nodo malicioso de acuerdo con el listado contra la falsificación de ID se ha descrito en detalle en el método del modo de realización y no se describirá aquí de nuevo.

En el dispositivo proporcionado en el modo de realización de la presente invención para evitar que un nodo falsifique una ID, el nodo almacena un listado contra la falsificación de ID en una unidad de almacenamiento local, lo cual resuelve el problema de que los costes son altos en el despliegue y mantenimiento cuando se despliega una PKI en la solución técnica existente para evitar la suplantación del nodo homólogo. El proceso de la unidad de identificación para la identificación de un nodo malicioso utilizando el listado contra la falsificación de ID es simple, efectivo y los costes de detección son bajos. Se resuelve el problema de que el retardo es grande cuando se lleva a cabo la verificación de firma para cada mensaje enviado y recibido en la solución técnica existente para evitar la suplantación del nodo homólogo. Cuando la unidad de identificación identifica al nodo malicioso utilizando el listado contra la falsificación de ID, la unidad de autenticación únicamente tiene que verificar la ID del nodo, mientras que no es necesario llevar a cabo la verificación de firma para cada mensaje enviado y recibido y, de este modo, se reduce el retardo de encaminamiento.

El modo de realización de la presente invención proporciona, además, un nodo cliente, el cual incluye una unidad de autenticación, una unidad de almacenamiento y una unidad de identificación.

La unidad de autenticación está configurada para autenticar la validez de una ID de un nodo homólogo.

La unidad de almacenamiento está configurada para elaborar y almacenar un listado contra la falsificación de ID en relación con el nodo homólogo de acuerdo con un resultado de la autenticación de la unidad de autenticación.

La unidad de identificación está configurada para identificar un nodo homólogo malicioso de acuerdo con la información del nodo homólogo que envía un mensaje y el listado contra la falsificación de ID almacenado por la unidad de almacenamiento.

El listado contra la falsificación de ID en relación con el nodo homólogo incluye la ID del nodo homólogo, la dirección

física del nodo homólogo, y la relación o relaciones de asociación entre la ID del nodo homólogo y la dirección física del nodo homólogo.

El nodo cliente puede identificar un nodo homólogo malicioso, y en el método del modo de realización se ha descrito en detalle el proceso específico de identificación de un nodo homólogo malicioso, y no se describirá aquí de nuevo.

El nodo cliente proporcionado en el modo de realización de la presente invención almacena un listado contra la falsificación de ID en un almacenamiento local, lo cual resuelve el problema de que los costes son altos en el despliegue y mantenimiento cuando se despliega una PKI en la solución técnica existente para evitar la suplantación del nodo homólogo. El proceso de la unidad de identificación del nodo cliente para la identificación de un nodo malicioso utilizando el listado contra la falsificación de ID es simple, efectivo y los costes de detección son bajos. Se resuelve el problema de que el retardo en el encaminamiento de los mensajes es grande cuando se lleva a cabo la verificación de firma para cada mensaje enviado y recibido en la solución técnica existente para evitar la suplantación del nodo homólogo. Cuando la unidad de identificación del nodo cliente identifica el nodo homólogo malicioso utilizando el listado contra la falsificación de ID, la unidad de autenticación del nodo cliente únicamente tiene que verificar la ID del nodo homólogo, mientras que no es necesario llevar a cabo la verificación de firma para cada mensaje enviado y recibido y, de este modo, se reduce el retardo de encaminamiento.

El modo de realización de la presente invención proporciona un nodo homólogo de red, el cual incluye una unidad de autenticación, una unidad de almacenamiento y una unidad de identificación.

La unidad de autenticación está configurada para autenticar la validez de una ID de un nodo cliente.

La unidad de almacenamiento está configurada para elaborar y almacenar un listado contra la falsificación de ID en relación con el nodo cliente de acuerdo con un resultado de la autenticación de la unidad de autenticación.

La unidad de identificación está configurada para identificar un nodo cliente malicioso de acuerdo con la información del nodo cliente que envía un mensaje y el listado contra la falsificación de ID almacenado por la unidad de almacenamiento.

El listado contra la falsificación de ID en relación con el nodo cliente incluye la ID del nodo cliente, la dirección física del nodo cliente, y la relación o relaciones de asociación entre la ID del nodo cliente y la dirección física del nodo cliente.

El nodo homólogo puede identificar el nodo cliente malicioso, y en el método del modo de realización se ha descrito en detalle el proceso de identificación de un nodo cliente malicioso, y no se describirá aquí de nuevo.

El nodo homólogo de red proporcionado en el modo de realización de la presente invención almacena un listado contra la falsificación de ID en un almacenamiento local, lo cual resuelve el problema de que los costes son altos en el despliegue y mantenimiento cuando se despliega una PKI en la solución técnica existente para evitar la suplantación del nodo homólogo. El proceso de la unidad de identificación del nodo homólogo para la identificación de un nodo malicioso utilizando el listado contra la falsificación de ID es simple, efectivo y los costes de detección son bajos. Se resuelve el problema de que el retardo en el encaminamiento de los mensajes es grande cuando se lleva a cabo la verificación de firma para cada mensaje enviado y recibido en la solución técnica existente para evitar la suplantación del nodo homólogo. Cuando la unidad de identificación del nodo homólogo identifica el nodo cliente malicioso utilizando el listado contra la falsificación de ID, la unidad de autenticación del nodo homólogo únicamente tiene que verificar la ID del nodo cliente, mientras que no es necesario llevar a cabo la verificación de firma para cada mensaje enviado y recibido y, de este modo, se reduce el retardo de encaminamiento.

El modo de realización de la presente invención proporciona un punto de convergencia de red, el cual incluye una unidad de autenticación, una unidad de almacenamiento y una unidad de identificación.

La unidad de autenticación está configurada para autenticar la validez de una ID de un nodo homólogo autenticado.

La unidad de almacenamiento está configurada para elaborar y almacenar un listado contra la falsificación de ID en relación con el nodo homólogo autenticado de acuerdo con un resultado de la autenticación de la unidad de autenticación.

La unidad de identificación está configurada para identificar un nodo malicioso de acuerdo con la información de un nodo que envía un mensaje y el listado contra la falsificación de ID almacenado por la unidad de almacenamiento.

El listado contra la falsificación de ID en relación con el nodo homólogo incluye la ID del nodo homólogo, la dirección física del nodo homólogo, y la relación o relaciones de asociación entre la ID y la dirección física.

El punto de convergencia puede identificar un nodo malicioso, y en el método del modo de realización se ha descrito en detalle el proceso específico, y no se describirá aquí de nuevo.

El punto de convergencia de red proporcionado en el modo de realización de la presente invención almacena un listado contra la falsificación de ID en un almacenamiento local, lo cual resuelve el problema de que los costes son altos en el despliegue y mantenimiento cuando se despliega una PKI en la solución técnica existente para evitar la suplantación del nodo homólogo. El proceso de la unidad de identificación del punto de convergencia para la identificación del nodo malicioso utilizando el listado contra la falsificación de ID es simple, efectivo y los costes de detección son bajos. Se resuelve el problema de que el retardo en el encaminamiento de los mensajes es grande cuando se lleva a cabo la verificación de firma para cada mensaje enviado y recibido en la solución técnica existente para evitar la suplantación del nodo homólogo. Cuando la unidad de identificación del punto de convergencia identifica el nodo malicioso utilizando el listado contra la falsificación de ID, la unidad de autenticación del punto de convergencia únicamente tiene que verificar la ID del nodo, mientras que no es necesario llevar a cabo la verificación de firma para cada mensaje enviado y recibido y, de este modo, se reduce el retardo de encaminamiento.

El modo de realización de la presente invención proporciona, además, un sistema para evitar que un nodo falsifique una ID en una red P2P. Tal y como se muestra en la FIG. 4, el sistema incluye un nodo homólogo y un nodo cliente.

El nodo cliente está configurado para localizar el nodo homólogo que da servicio al nodo cliente y establecer una conexión con el nodo homólogo.

El nodo homólogo está configurado para establecer la conexión con el nodo cliente que envía una petición de servicio al nodo homólogo.

Al menos uno entre el nodo cliente y el nodo homólogo actúa como iniciador de la autenticación y autentica una ID de la otra parte.

Después de que la autenticación se realice con éxito, el nodo cliente o el nodo homólogo que actúa como el iniciador de la autenticación elabora y almacena localmente un listado contra la falsificación de ID en relación con la otra parte.

El listado contra la falsificación de ID en relación con el nodo homólogo incluye la ID del nodo homólogo, la dirección física del nodo homólogo, y una o más relaciones de asociación entre la ID del nodo homólogo y la dirección física del nodo homólogo. El listado contra la falsificación de ID en relación con el nodo cliente incluye la ID del nodo cliente, una dirección física del nodo cliente y una o más relaciones de asociación entre la ID del nodo cliente y la dirección física del nodo cliente.

En algunos escenarios de aplicación, el sistema para evitar que un nodo falsifique una ID en una red P2P proporcionado en el modo de realización de la presente invención incluye, además, un punto de convergencia, el cual se conecta con, al menos, un nodo homólogo, y el nodo homólogo se conecta con el nodo cliente.

El nodo homólogo está configurado para localizar el punto de convergencia que da servicio al nodo homólogo y establecer una conexión con el punto de convergencia.

El punto de convergencia está configurado para establecer la conexión con el nodo homólogo que envía una petición de servicio al punto de convergencia.

El punto de convergencia actúa como un iniciador de la autenticación y autentica una ID del nodo homólogo.

Después de que se realice con éxito la autenticación, el punto de convergencia que actúa como el iniciador de la autenticación elabora y almacena localmente un listado contra la falsificación de ID en relación con el nodo homólogo.

Un nodo es un nodo cliente o un nodo homólogo. Si un nodo es un nodo cliente, el listado contra la falsificación de ID del nodo incluye: la ID del nodo homólogo, la dirección física del nodo homólogo, y la relación o relaciones de asociación entre la ID del nodo homólogo y la dirección física del nodo cliente. Si un nodo es un nodo homólogo, el listado contra la falsificación de ID del nodo incluye la ID del nodo cliente, la dirección física del nodo cliente y la relación o relaciones de asociación entre la ID del nodo cliente y la dirección física del nodo cliente.

El sistema puede identificar un nodo malicioso cuyo proceso específico se ha descrito en detalle en el método del modo de realización y no se describirá aquí de nuevo.

En el sistema proporcionado en el modo de realización de la presente invención para evitar que un nodo falsifique una ID, el nodo homólogo, el nodo cliente o el punto de convergencia almacena un listado contra la falsificación de ID en un almacenamiento local, lo cual resuelve el problema de que los costes son altos en el despliegue y mantenimiento cuando se despliega una PKI en la solución técnica existente para evitar la suplantación del nodo homólogo. El proceso para que el nodo homólogo, el nodo cliente o el punto de convergencia identifique el nodo malicioso utilizando el listado contra la falsificación de ID es simple, efectivo y los costes de detección son bajos. Se resuelve el problema de que el retardo en el encaminamiento de los mensajes es grande cuando se lleva a cabo la

verificación de firma para cada mensaje enviado y recibido en la solución técnica existente para evitar la suplantación del nodo homólogo. Cuando el nodo homólogo, el nodo cliente, o el punto de convergencia identifica el nodo malicioso utilizando el listado contra la falsificación de ID, únicamente es necesario verificar la ID del nodo, mientras que no es necesario llevar a cabo la verificación de firma para cada mensaje enviado y recibido y, de este modo, se reduce el retardo de encaminamiento.

Aquellos experimentados en la técnica pueden entender que todos o parte de los pasos del método de acuerdo con los modos de realización de la presente invención se pueden implementar mediante un programa que controle un hardware relevante. El programa puede estar almacenado en un medio de almacenamiento legible por un ordenador como, por ejemplo, una Memoria de Solo Lectura (ROM), una Memoria de Acceso Aleatorio (RAM), un disco magnético o una Memoria de Solo Lectura de Disco Compacto (CD-ROM).

Las descripciones de más arriba son únicamente algunos ejemplos de modos de realización de la presente invención, pero no pretenden limitar el alcance de la presente invención. Cualquier modificación, sustitución equivalente, o mejora realizada sin apartarse del principio de la presente invención debería encontrarse dentro del alcance de la presente invención. Por lo tanto, el alcance de protección de la presente invención está sujeto a las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método para evitar que un nodo falsifique una identidad, ID, en una red Entre Pares, P2P, en donde la red de pares comprende un nodo homólogo y un nodo cliente, en donde el método comprende:

después de que el nodo cliente localice el nodo homólogo que da servicio al nodo cliente, actuar, por parte de al menos uno entre el nodo cliente y el nodo homólogo, como un iniciador de la autenticación, y autenticar (11) una ID de la otra parte; y

después de que se realice con éxito la autenticación, elaborar y almacenar (12) localmente, por parte del nodo cliente o del nodo homólogo que actúa como el iniciador de la autenticación, un listado contra la falsificación de ID en relación con la otra parte, e identificar un nodo malicioso utilizando el listado contra la falsificación de ID, en donde el nodo que actúa como un iniciador de la autenticación es el nodo cliente o el nodo homólogo,

si el nodo que actúa como un iniciador de la autenticación es el nodo cliente, el listado contra la falsificación de ID en relación con la otra parte comprende la ID del nodo homólogo, una dirección física del nodo homólogo, y una o más relaciones de asociación entre la ID del nodo homólogo y la dirección física del nodo homólogo;

si el nodo que actúa como un iniciador de la autenticación es el nodo homólogo, el listado contra la falsificación de ID en relación con la otra parte comprende la ID del nodo cliente, una dirección física del nodo cliente, y una o más relaciones de asociación entre la ID del nodo cliente y la dirección física del nodo cliente.

2. El método para evitar que un nodo falsifique una ID en una red P2P de acuerdo con la reivindicación 1, en donde

si el nodo que actúa como un iniciador de la autenticación es el nodo cliente, el método comprende, además:

después de recibir un mensaje enviado por el nodo homólogo, actuar, por parte del nodo cliente, como el iniciador de la autenticación, y autenticar la relación o relaciones de correspondencia entre la ID del nodo homólogo y la dirección física del nodo homólogo; y

si la relación o relaciones de correspondencia entre la ID del nodo homólogo y la dirección física del nodo homólogo es consistente con un registro en el listado contra la falsificación de ID propiedad del nodo cliente, considerar el nodo homólogo como un nodo no malicioso; si la relación o relaciones de correspondencia entre la ID del nodo homólogo y la dirección física del nodo homólogo es inconsistente con un registro en el listado contra la falsificación de ID propiedad del nodo cliente, considerar el nodo homólogo como un nodo malicioso;

si el nodo que actúa como un iniciador de la autenticación es el nodo homólogo, el método comprende, además:

después de recibir un mensaje enviado por el nodo cliente, actuar, por parte del nodo homólogo, como el iniciador de la autenticación, y autenticar la relación o relaciones de correspondencia entre la ID del nodo cliente y la dirección física del nodo cliente; y

si la relación o relaciones de correspondencia entre la ID del nodo cliente y la dirección física del nodo cliente es consistente con un registro en el listado contra la falsificación de ID propiedad del nodo homólogo, considerar el nodo cliente como un nodo no malicioso; si la relación o relaciones de correspondencia entre la ID del nodo cliente y la dirección física del nodo cliente es inconsistente con un registro en el listado contra la falsificación de ID propiedad del nodo homólogo, considerar el nodo cliente como un nodo malicioso.

3. El método para evitar que un nodo falsifique una ID en una red P2P de acuerdo con la reivindicación 1 ó 2, en donde el método comprende, además:

si el nodo que actúa como un iniciador de la autenticación comprende el nodo cliente, y cambia la dirección física del nodo homólogo, borrar, por parte del nodo cliente, un registro contra la falsificación de ID en relación con el nodo homólogo;

volver a autenticar, por parte del nodo cliente, el nodo homólogo; y

después de que se realice con éxito la autenticación, almacenar la relación o relaciones de asociación entre la ID del nodo homólogo y la nueva dirección física del nodo homólogo en el listado contra la falsificación de ID.

4. El método para evitar que un nodo falsifique una ID en una red P2P de acuerdo con la reivindicación 1, que comprende, además:

si el nodo que actúa como un iniciador de la autenticación comprende el nodo homólogo, y el nodo homólogo que da servicio al nodo cliente deja la red P2P, notificar, por parte del nodo homólogo, la relación o relaciones de

asociación entre la ID del nodo cliente y la dirección física del nodo cliente a un nodo homólogo sustituto, y notificar al nodo cliente que el nodo homólogo sustituto continúa proporcionando un servicio al nodo cliente;

autenticar, por parte del nodo cliente, una ID del nodo homólogo sustituto;

después de que se realice con éxito la autenticación, añadir, por parte del nodo cliente, la relación o relaciones de asociación entre la ID del nodo homólogo sustituto y la dirección física del nodo homólogo sustituto al listado contra la falsificación de ID; y

aceptar, por parte del nodo cliente, el servicio proporcionado por el nodo homólogo sustituto.

5. El método para evitar que un nodo falsifique una ID en una red P2P de acuerdo con la reivindicación 1, en donde la relación o relaciones de correspondencia entre la ID del nodo homólogo y la dirección física del nodo homólogo es/son la relación o relaciones de asociación entre un nodo homólogo y al menos dos direcciones físicas del nodo homólogo.

6. El método para evitar que un nodo falsifique una ID en una red P2P de acuerdo con la reivindicación 1, en donde la red de pares comprende, además, un punto de convergencia conectado a al menos un nodo homólogo, comprendiendo el método, además:

después de que el nodo homólogo localice el punto de convergencia que da servicio al nodo homólogo, autenticar, por parte del punto de convergencia, una ID del nodo homólogo; y

después de que se realice con éxito la autenticación, elaborar y almacenar localmente, por parte del punto de convergencia, el listado contra la falsificación de ID en relación con el nodo homólogo.

7. El método para evitar que un nodo falsifique una ID en una red P2P de acuerdo con la reivindicación 6, en donde el nodo que actúa como un iniciador de autenticación es el nodo cliente o el nodo homólogo,

si el nodo que actúa como un iniciador de la autenticación es el nodo cliente, el listado contra la falsificación de ID en relación con la otra parte comprende la ID del nodo homólogo, la dirección física del nodo homólogo, y la relación o relaciones de asociación entre la ID del nodo homólogo y la dirección física del nodo homólogo; y

si el nodo que actúa como un iniciador de la autenticación es el nodo homólogo, el listado contra la falsificación de ID en relación con la otra parte comprende la ID del nodo cliente, la dirección física del nodo cliente, y la relación o relaciones de asociación entre la ID del nodo cliente y la dirección física del nodo cliente.

8. El método para evitar que un nodo falsifique una ID en una red P2P de acuerdo con la reivindicación 6, en donde después de que el nodo homólogo localice el punto de convergencia que da servicio al nodo homólogo, la autenticación, por parte del punto de convergencia, de la ID del nodo comprende:

después de recibir un mensaje enviado por el nodo homólogo, autenticar, por parte del punto de convergencia, un mensaje mediante una inspección profunda de paquetes, DPI; y

extraer la ID del nodo homólogo y la dirección física del nodo homólogo.

9. Un dispositivo para evitar que un nodo falsifique una identidad, ID, en una red Entre Pares, P2P, que comprende una unidad (1) de autenticación, una unidad (2) de almacenamiento y una unidad (3) de identificación, en donde

la unidad (1) de autenticación está configurada para autenticar la validez de una ID del nodo;

la unidad (2) de almacenamiento está configurada para elaborar y almacenar un listado contra la falsificación de ID en relación con el nodo autenticado, y

la unidad (3) de identificación está configurada para identificar un nodo malicioso de acuerdo con el listado contra la falsificación de ID, en donde el dispositivo es un nodo cliente o un nodo homólogo o un punto de convergencia de red,

si el dispositivo es el nodo cliente, el listado contra la falsificación de ID en relación con el nodo autenticado comprende la ID del nodo homólogo, una dirección física del nodo homólogo y una o más relaciones de asociación entre la ID del nodo homólogo y la dirección física del nodo homólogo; y

si el dispositivo es el nodo homólogo, el listado contra la falsificación de ID en relación con el nodo autenticado comprende la ID del nodo cliente, una dirección física del nodo cliente y una o más relaciones de asociación entre la ID del nodo cliente y la dirección física del nodo cliente; y

si el dispositivo es el punto de convergencia de red, el listado contra la falsificación de ID en relación con el

nodo autenticado comprende la ID del nodo homólogo, una dirección física del nodo homólogo y una o más relaciones de asociación entre la ID del nodo homólogo y la dirección física del nodo homólogo.

10. Un sistema para evitar que un nodo falsifique una identidad, ID, en una red Entre Pares, P2P, que comprende un nodo homólogo y un nodo cliente, en donde

el nodo cliente está configurado para localizar el nodo homólogo que da servicio al nodo cliente y establecer una conexión con el nodo cliente;

el nodo homólogo está configurado para establecer la conexión con el nodo cliente que envía una petición de servicio al nodo homólogo;

al menos uno entre el nodo cliente y el nodo homólogo actúa como un iniciador de la autenticación y autentica a la otra parte; y

después de que se realice con éxito la autenticación, el nodo cliente o el nodo homólogo que actúa como el iniciador de la autenticación elabora y almacena localmente un listado contra la falsificación de ID en relación con la otra parte e identifica un nodo malicioso utilizando el listado contra la falsificación de ID, en donde

si el nodo que actúa como iniciador de la autenticación es el nodo cliente, el listado contra la falsificación de ID en relación con la otra parte comprende la ID del nodo homólogo, una dirección física del nodo homólogo y una o más relaciones de asociación entre la ID del nodo homólogo y la dirección física del nodo homólogo; y

si el nodo que actúa como iniciador de la autenticación es el nodo homólogo, el listado contra la falsificación de ID en relación con la otra parte comprende una ID del cliente, una dirección física del nodo cliente y una o más relaciones de asociación entre la ID del nodo cliente y la dirección física del nodo cliente.

11. Un sistema para evitar que un nodo falsifique una ID en una red P2P de acuerdo con la reivindicación 15 que comprende, además, un punto de convergencia conectado en la red P2P, en donde el punto de convergencia está conectado a al menos un nodo homólogo,

el nodo homólogo está configurado para localizar el punto de convergencia que da servicio al nodo homólogo y para establecer una conexión con el punto de convergencia;

el punto de convergencia está configurado para establecer la conexión con el nodo homólogo que envía una petición de servicio al nodo de convergencia;

el punto de convergencia actúa como un iniciador de la autenticación y autentica una ID del nodo homólogo; y

después de que se realice con éxito la autenticación, el punto de convergencia que actúa como el iniciador de la autenticación elabora y almacena localmente un listado contra la falsificación de ID en relación con el nodo homólogo.

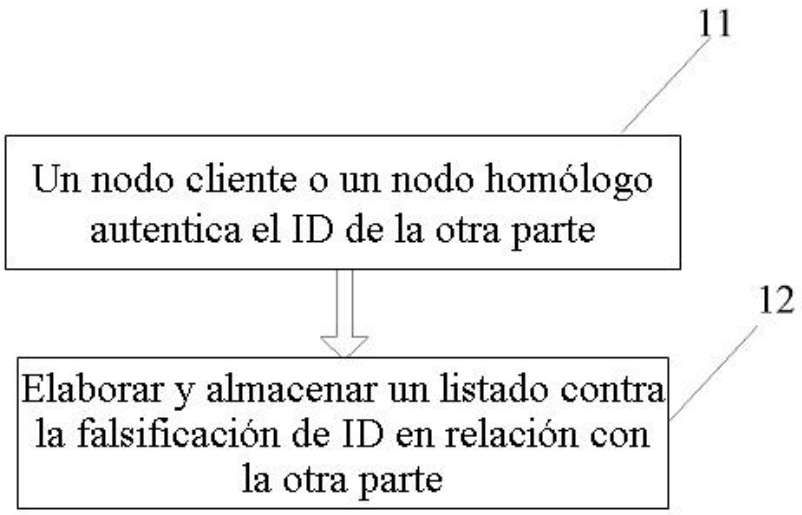
11
Un nodo cliente o un nodo homólogo autentica el ID de la otra parte
12
Elaborar y almacenar un listado contra la falsificación de ID en relación con la otra parte

FIG. 1


Nodo
Punto de convergencia
Nodo cliente
Nodo cliente

FIG. 2

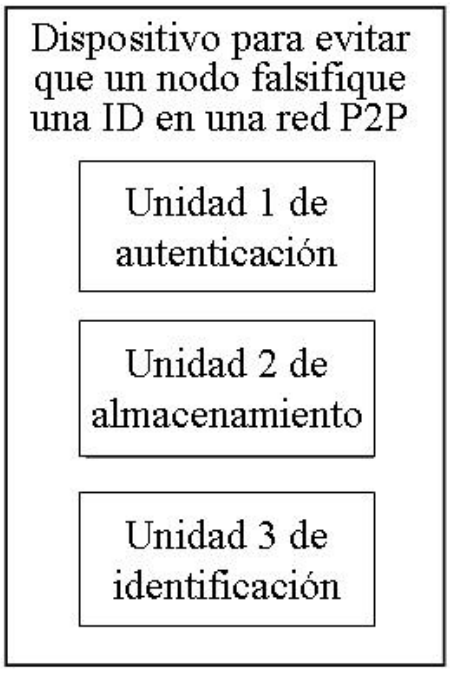
Dispositivo para evitar que un nodo falsifique una ID en una red P2P
Unidad 1 de autenticación
Unidad 2 de almacenamiento
Unidad 3 de identificación

FIG. 3

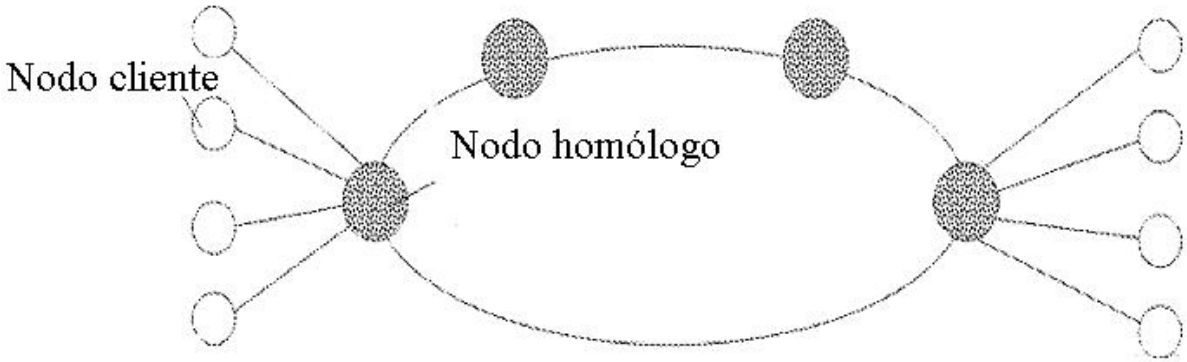
Nodo cliente
Nodo homólogo

FIG. 4