(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 776 679**

(51) Int. CI.:

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **18.11.2013 PCT/EP2013/003461**

(87) Fecha y número de publicación internacional: **26.06.2014 WO14094948**

(96) Fecha de presentación y número de la solicitud europea: **18.11.2013 E 13814031 (4)**

(97) Fecha y número de publicación de la concesión europea: **12.02.2020 EP 2936767**

(54) Título: **Procedimientos de aumento de la seguridad en transmisiones de datos y de control de autenticación de nodos de una red ad hoc**

(30) Prioridad:

21.12.2012 FR 1203585

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
31.07.2020

(73) Titular/es:

AIRBUS DS SAS (100.0%)
ZAC de la Clef Saint Pierre, 1 Boulevard Jean Moulin
78990 Elancourt, FR

(72) Inventor/es:

DENIAUD, THIERRY y
CARNUS, ROMAIN

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimientos de aumento de la seguridad en transmisiones de datos y de control de autenticación de nodos de una red ad hoc

Campo técnico

El campo de la invención concierne al aumento de la seguridad en las transmisiones en una red ad hoc y a la autenticación de los nodos tales como equipos de red o terminales. Radica una problemática en la arquitectura de tales redes, en las que la topología es dinámica y en las que se debe proporcionar una gran flexibilidad de configuración y una seguridad máxima. Los enfoques centralizados de los esquemas de confianza y de distribución de las claves no pueden convenir para tales redes. La descentralización de los controles de acceso y de autenticación implica que cada nodo es capaz de poner en práctica como mínimo ciertas exigencias de seguridad para preservar la integridad de la red, para preservar la red de ataques, de intrusiones o de usurpación de identidades, o también de sustitución de direcciones de red.

Estado de la técnica y problemas técnicos a los que se enfrenta

Los protocolos de encaminamiento permiten a los nodos conocer la topología de la red, calcular las rutas para contactar con otros nodos y distribuir a los diferentes nodos de la red las rutas así calculadas. Adicionalmente, un protocolo de encaminamiento puede integrar elementos de seguridad para aumentar la seguridad en la red frente a ataques internos o externos (intrusión no autorizada en la red, usurpación de identidad, corrupción de los datos de un mensaje, etc.). Para preservar la integridad de la red, se necesita el aumento de la seguridad en el protocolo de encaminamiento.

El protocolo OLSR, cuyo acrónimo significa, en la terminología anglosajona, “Optimized Link State Routing Protocol”, resulta especialmente adecuado para las redes ad hoc de tipo móvil e inalámbrica.

Este protocolo estriba en la utilización de repetidores multipunto (MPR) y permite el intercambio de la información de topología (vecindad, estado de los enlaces, lista de los vecinos de un nodo que lo han elegido como MPR) entre los diferentes nodos a través de los mensajes HELLO y TC. Esta información de topología permite construir las tablas de encaminamiento utilizadas en el encaminamiento de los paquetes de datos.

En cambio, el protocolo OLSR no comprende todas las capas de seguridad necesarias para la completa protección de una red ad hoc. A título de ejemplo, el protocolo OLSR no tiene en cuenta las problemáticas relativas a la autenticación, especialmente ante la llegada de un nuevo nodo a la red. Un nodo malicioso también puede usurpar la identidad de un nodo sano. Un nodo malicioso también puede corromper los mensajes del protocolo de encaminamiento para transformar a su antojo la topología de la red vista por todos los nodos (inclusive los nodos sanos).

Para solucionar en parte la problemática de la seguridad y de la prevención contra ataques exteriores e interiores a la red, las autenticaciones de nodos, la distribución de claves y la firma de los mensajes pueden permitir aumentar la seguridad de una red.

Para ello, se han propuesto soluciones para ser compatibles con el protocolo OLSR. Existe el protocolo SOLSR, que designa “Secure OLSR” (basado en firmas para la autenticación de los paquetes OLSR y en la utilización de claves simétricas); la solución denominada “Web-of-trust OLSR extension” (basada en firmas para la autenticación de los paquetes OLSR; efectuándose la distribución de las claves mediante un principio basado en el “PGP web-of-trust”). Estas soluciones se han implementado en forma de módulos de extensión (plug-ins) para el demonio OLSRd. Estas últimas mejoras permiten tener en cuenta ciertas problemáticas de autenticación, en orden a dar respuesta a las exigencias de una red segura.

Otra solución es una solución que, basada en el protocolo OLSR, pone en práctica nuevos tipos de mensajes (mensaje de firma) para autenticar los mensajes HELLO y TC. Estos mensajes permiten distribuir firmas, poner en práctica temporizadores, o también gestionar el número y las secuencias de mensajes para efectuar controles.

Se puede poner en práctica un mecanismo de clave pública y de claves privadas para permitir encriptar datos transmitidos en la red. Un mecanismo de distribución de certificados de autenticación puede asociarse con el mecanismo anterior para garantizar la confianza que un nodo puede conceder a otro nodo. Esta solución permite aumentar el nivel de seguridad de una red ad hoc móvil.

En cambio, tales mecanismos no permiten evitar los ataques internos provenientes de la red, tales como los conocidos con el nombre de “link-spoofing” (suplantación).

En lo referente a la distribución de los elementos de seguridad necesarios para la autenticación de los nodos, existen dos enfoques:

- un enfoque centralizado (ejemplos: Kerberos más bien para redes fijas; “Public Key Infrastructure” que se apoya en una autoridad certificadora, pero que precisa de la presencia constante de una entidad central);
- un enfoque descentralizado (ejemplos: “web-of-trust” de tipo PGP, pero con problemas de distribución de los certificados; “Public Key Infrastructure” distribuida).

Asimismo, existen soluciones descritas en los siguientes documentos de los autores ADNANE A ET AL.: “Trust-Based Countermeasures for Securing OLSR protocol”, de la referencia Computational Science and Engineering, 2009, o también el documento de los autores KHADIDJA ATAD ET AL.: “New efficient mechanisms to secure OLSR protocol”, de la referencia Future Generation Communication Technology (FGCT), 2012 International conference On, IEEE, 12 de diciembre de 2012. Pero estos últimos documentos no permiten solucionar los citados inconvenientes.

Exposición de la invención

La invención permite solucionar los citados inconvenientes.

La invención se da a conocer mediante dos procedimientos alternativos de aumento de la seguridad de transmisión de datos puestos en práctica por un nodo emisor de una red ad hoc, según las reivindicaciones 1 y 3. Procedimiento de control de datos de autenticación puesto en práctica por un segundo nodo receptor de una red ad hoc, según la reivindicación 8. También se reivindica un nodo emisor según la reivindicación 14 y uno nodo receptor según la reivindicación 15 para la implantación del procedimiento de aumento de la seguridad de la invención. Formas de realización suplementarias se describen en las reivindicaciones dependientes.

Breve descripción de las figuras

Otras características y ventajas de la invención se desprenderán de la lectura de la descripción detallada que sigue, con referencia a las figuras que se acompañan, las cuales ilustran:

figura 1: un modelo de autenticación de mensaje de la invención, compartido por los diferentes servicios de red que generan tráfico de control;

figura 2: un esquema de arquitectura centrado en torno a una base de datos denominada ID TABLE, que comprende todos los elementos para permitir la autenticación de los mensajes y el aumento de la seguridad de los protocolos;

figura 3: una defensa frente a la intrusión en la red por usurpación de identidad, según un procedimiento de la invención;

figura 4: una defensa frente a la intrusión en la red por usurpación de la dirección IP, según un procedimiento de la invención;

figura 5: un ejemplo de almacenamiento de datos de autenticación por un nodo de la red, según un procedimiento de control de la invención;

figura 6: un primer ejemplo de intercambios de datos, según el procedimiento de aumento de la seguridad de la invención; y

figura 7: un segundo ejemplo de intercambios de datos, según el procedimiento de aumento de la seguridad de la invención.

Descripción de la invención

Más adelante en la descripción, se denomina un “nodo generador” al primer nodo que envía un mensaje de un protocolo de encaminamiento hacia un nodo destinatario, recorriendo el mensaje una ruta calculada mediante una tabla de encaminamiento y comprendiendo en general una pluralidad de nodos intermedios.

Un “nodo emisor” es un nodo que genera un mensaje o que lo transfiere a un nodo vecino que se halla en una ruta con destino a un nodo destinatario.

Un “nodo receptor” es un nodo que recibe un mensaje que, bien le está, o bien no le está destinado. En este último caso, el nodo receptor, tras un procesamiento de datos, tal como un control de autenticación, autoriza o no la transferencia del mensaje hacia el nodo destinatario o el próximo nodo vecino en la ruta.

Más adelante en la descripción, las funciones de autenticación comprenden las funciones utilizadas habitualmente para los servicios de autenticación y, asimismo, comprenden los procedimientos de la invención que constituyen servicios que mejoran la seguridad de las transferencias de datos en una red ad hoc.

La figura 1 representa una arquitectura que representa los componentes esenciales para la puesta en práctica de los procedimientos de la invención. De acuerdo con una forma de realización, el componente OLSR permite procesar los mensajes entrantes y salientes relativos al protocolo de encaminamiento OLSR. Las funciones que permiten la

gestión de la interfaz del nodo para la recepción y la emisión de los mensajes de control se representan mediante un componente “CONT. MESS” en la figura 1. Las interacciones entre los componentes OLSR y CONT. MESS se representan mediante el enlace 12. Un nodo generador visto por un nodo receptor puede tomar parte en la topología de la red, y la información y los datos relativos al nodo generador se pueden guardar a continuación en la tabla “ID TABLE” que se describe seguidamente cuando los mensajes OLSR han sido aceptados, previo control de autenticación.

Un componente DDHCP permite procesar los mensajes entrantes y salientes relativos al protocolo DDHCP. Las interacciones entre los componentes DDHCP y CONT. MESS se representan mediante el enlace 10. La dirección IP obtenida por el protocolo se puede guardar a continuación en la tabla “ID TABLE” que se describe seguidamente cuando los mensajes han sido aceptados, previo control de autenticación.

Un componente suplementario “DIST SE” permite procesar los mensajes entrantes y salientes relativos a un servicio distribuido que no sea DDHCP y OLSR. Las interacciones entre los componentes DIST SE y CONT. MESS se representan mediante el enlace 11.

Un componente AUTH MOD se hace cargo de las operaciones para verificar la validez de la autenticación (verificación de firma) para los mensajes entrantes asociados a los protocolos DDHCP (enlace 14), OLSR (enlace 13) o a cualquier otro servicio distribuido (enlace 15). Este componente AUTH MOD también se hace cargo del cálculo de las firmas de los mensajes salientes asociados a los protocolos DDHCP (enlace 14), OLSR (enlace 13) o a cualquier otro servicio distribuido (enlace 15) cuando el nodo es el nodo generador del mensaje. El método de autenticación para proteger el tráfico de control está basado en la criptografía de clave pública. Los servicios distribuidos deben estar adaptados para que los mensajes de protocolos transporten firma e identificador.

El componente CERT DB permite la gestión de los certificados de autenticación del nodo y de los certificados de autenticación conocidos por el nodo que los almacena. Los certificados de autenticación se pueden guardar en una base que se actualiza regularmente. Una interfaz 16 permite a las funciones de control y de gestión de los datos de autenticación acceder a los certificados de autenticación CERT DB.

El componente O SSL permite almacenar los útiles criptográficos que sirven para las funciones de autenticación del componente AUTH MOD. Puede tratarse de una biblioteca de funciones tal como, por ejemplo, una función resumen o también una función cifrado de datos. El componente AUTH MOD accede a los servicios del componente O SSL por medio de una interfaz 17.

Finalmente, el componente AUTH MOD con el componente CERT DB permiten la copia de datos de autenticación y su organización, en orden a garantizar la autenticación de los nodos que entran en comunicación con el nodo de que se trata en la figura 1. Adicionalmente, el componente AUTH MOD permite asegurar un elevado grado de seguridad, especialmente en lo referente a las intrusiones exteriores y las sustituciones en el propio seno de la red. Los componentes AUTH MOD y CERT DB permiten la ejecución de los procedimientos de la invención y se detallan seguidamente.

La figura 2 permite describir con mayor detalle las diferentes funciones necesarias para la realización de los procedimientos de la invención. El componente CERT DB comprende una tabla de datos que reúne diferentes datos de autenticaciones almacenados en un nodo. Los datos de autenticaciones conciernen a los datos de nodos conocidos por un nodo dado de la red, especialmente los almacenados en la tabla de encaminamiento, señalada con ROU PROT, en la figura 2. En especial, los datos de autenticación son guardados en una tabla 26, señalada con ID TABLE, en la figura 2. La tabla ID TABLE permite asociar, a un identificador de un nodo conocido, un certificado de autenticación correspondiente. Esta asociación permite controlar la autenticación de un mensaje recibido proveniente de un nodo conocido de la tabla de encaminamiento. La tabla ID TABLE puede estar almacenada en el componente CERT DB.

El procedimiento de control de la invención permite la actualización de la ID TABLE por medio de un protocolo de intercambio de certificados representado con el bloque CERT EXCH PROT y el enlace 20. Las funciones de autenticación realizadas por el componente AUTH MOD permiten realizar operaciones que utilizan los datos almacenados en la ID TABLE y los datos extraídos de los mensajes entrantes (verificación de firma).

En especial, la autenticación de los mensajes entrantes relativos al protocolo DDHCP se puede realizar en el componente que se encarga de la puesta en práctica del protocolo de direccionamiento DDHCP por intermedio del componente AUTH MOD mediante la verificación de la firma de mensajes entrantes. Utilizando el identificador contenido en la firma, el servicio puede recuperar los correspondientes certificados de la ID TABLE del componente CERT DB para la verificación de firma, y puede verificar que la dirección IP se corresponde con la del nodo generador. Los enlaces 21 y 22 entre la ID TABLE y la función autenticación AUTH1 del componente AUTH MOD que utiliza su interfaz con el componente DDHCP se ilustran en la figura 2.

En especial, la autenticación de los mensajes entrantes relativos al protocolo OLSR se puede realizar en el dominio del protocolo de encaminamiento OLSR por intermedio del componente AUTH MOD mediante la verificación de la firma de mensajes entrantes. Utilizando el identificador contenido en la firma, el servicio puede recuperar los

correspondientes certificados de la ID TABLE del componente CERT DB para la verificación de firma, y puede verificar que la dirección IP se corresponde con la del nodo generador. El enlace 24 entre la ID TABLE y la función autenticación AUTH2 del componente AUTH MOD que utiliza el componente OLSR se ilustra en la figura 2.

Una ventaja de la arquitectura que permite la realización de los procedimientos de la invención es que las funciones de autenticación se realizan independientemente del protocolo de intercambio de certificados.

La tabla de encaminamiento de un nodo, señalada con ROUT PROT, se representa en la figura 2. Ésta establece interfaz necesariamente con la capa OLSR que permite implementar las funciones relativas al protocolo de encaminamiento de la red ad hoc. Esta interfaz se representa mediante el enlace 25 de la figura 2.

Una interfaz 23 entre la tabla de encaminamiento ROUT PROT y la ID TABLE permite efectuar controles y sincronizaciones entre la tabla de encaminamiento y la tabla ID TABLE.

Se podría utilizar, no obstante, otro protocolo de encaminamiento distinto a OLSR, de la misma familia que OLSR (protocolo de encaminamiento proactivo) con tal de que las etapas de los procedimientos de la invención puedan apoyarse en las funciones necesarias de tal protocolo de encaminamiento.

Las figuras 3 y 4 representan, respectivamente, un caso de una usurpación de identidad de un nodo (figura 3) y un caso de una usurpación de dirección IP (figura 4). Los procedimientos de la invención permiten evitar tales ataques en el seno de la red.

En especial, la ID TABLE permite hacer corresponder de manera biyectiva: un identificador de un nodo, una dirección IP y un certificado de autenticación.

Un objetivo de la tabla ID TABLE es el de permitir la construcción de una tabla segura que comprenda la lista de los nodos que tienen certificaciones de autenticación validadas y que incluya datos de confianza frente a los nodos conocidos por la tabla de encaminamiento. De este modo, un primer nodo que es autenticado por un segundo nodo después de un control de autenticación mediante intercambios de certificados según el procedimiento de la invención podrá transmitir mensajes provenientes de este nodo a otro nodo. De esta manera, la confianza de un nodo se propaga de grado en grado mediante un control de nodo a nodo.

Otro objetivo de la tabla ID TABLE es el de almacenar la información relativa a los datos de autenticación de los demás nodos, a fin de poder actualizar constantemente estos datos.

Cuando un nodo se une a la red por primera vez, posiblemente aún no se le ha asignado su dirección IP cuando trata de contactar con un nodo de la red. En este último caso, la ID TABLE no tiene en cuenta el campo de dirección IP del nodo en la tabla ID TABLE, por lo que no compara esta entrada con el campo vacío de dirección IP de los mensajes recibidos. La dirección IP se añadirá, en lo sucesivo, a los datos de autenticación en la tabla cuando se reconozca la identificación del nodo en cuestión.

La figura 3 representa una red en la que se ilustran los siguientes nodos con sus datos de direccionamiento y de identificadores:

- un primer nodo N_A tiene una dirección IP .2 y un identificador ID_A;
- un segundo nodo N_B tiene una dirección IP .12 y un identificador ID_B;
- un tercer nodo N_C tiene una dirección IP .6 y un identificador ID_C.

Un nodo tercero, señalado con Att1, intenta un ataque usurpando el identificador del nodo N_A: ID_A y una dirección IP .4.

El procedimiento de control de la invención permite especialmente organizar los datos de autenticación de nodos vecinos, a los efectos de que un único identificador de un nodo quede asociado a una única dirección IP y a un único certificado de autenticación del mismo nodo.

De este modo, la configuración representada en la figura 3 puede ser detectada merced a las funciones de autenticación que aprovechan los datos almacenados y actualizados en la ID TABLE mediante la comparación de los datos de los mensajes entrantes y de los datos almacenados en la ID TABLE.

La figura 4 representa una red en la que se ilustran los siguientes nodos con sus datos de direccionamiento y de identificadores:

- un primer nodo N_A tiene una dirección IP .2 y un identificador ID_A;
- un segundo nodo N_B tiene una dirección IP .12 y un identificador ID_B;
- un tercer nodo N_C tiene una dirección IP .6 y un identificador ID_C;

- un cuarto nodo N_D tiene una dirección IP .4 y un identificador ID_D;
- un quinto nodo N_E tiene una dirección IP .2 y un identificador ID_E.

El quinto nodo N_E intenta un ataque desde el interior de la red por usurpación de la dirección IP .2 del primer nodo N_A.

El procedimiento de control de la invención permite especialmente organizar los datos de autenticación de nodos vecinos, a los efectos de que una única dirección IP de un nodo quede asociada a un único certificado de autenticación del mismo nodo y a su identificador.

De este modo, la configuración representada en la figura 4 puede ser detectada merced a las funciones de autenticación que aprovechan los datos almacenados y actualizados en la ID TABLE mediante la comparación de los datos de los mensajes entrantes y de los datos almacenados en la ID TABLE.

Cuando un mensaje es recibido y autenticado por un nodo, el componente de autenticación AUTH MOD procesa los datos de autenticación a fin de registrarlos en la ID TABLE, bien creando una nueva entrada para un nuevo nodo, o bien actualizando datos ya registrados.

Cuando los datos controlados son idénticos a datos ya presentes en la ID TABLE, la ID TABLE no se actualiza. En cambio, una comparación de datos permite verificar la autenticación de mensajes provenientes de un nodo conocido por la tabla de encaminamiento y, por tanto, por la ID TABLE.

Los mensajes recibidos, cuando están firmados, se pueden verificar merced a los certificados registrados en la tabla ID TABLE. En este caso, la consulta de la base puede efectuarse comparando la dirección IP del mensaje recibido y la correspondiente dirección IP almacenada en la ID TABLE.

Otra posible entrada es la de los identificadores de los nodos.

La figura 5 representa una tabla ID TABLE 26 que incluye:

- los identificadores ID de los nodos conocidos por la tabla de encaminamiento ROUT PROT de un nodo: ID_A, ID_B, ID_C;
- las direcciones IP de los nodos conocidos por los datos referenciados en el componente DDHCP: IP_A, IP_B, IP_C;
- los certificados C_i, señalados con CERT (K) en la figura 5, de las claves públicas K_i de los nodos i conocidos por la tabla de encaminamiento de un nodo, estando dichas claves firmadas por una autoridad certificadora CA, los certificados se señalan asimismo con K_i/K_{CA},
- los certificados C_{ti}, señalados con CERT TEMP (K_t) en la figura 5, de las claves públicas temporales K_{ti} de nodos i conocidos por la tabla de encaminamiento de un nodo, estando dichas claves públicas temporales firmadas con la clave privada ki del nodo i, estos certificados se señalan asimismo con K_{ti}/k_i.

De entre las funciones de autenticación de la invención, una de ellas comprende un procedimiento de aumento de la seguridad de transmisión de los datos en la red. El procedimiento se pone en práctica para el aumento de la seguridad en las transmisiones de los datos de dos nodos adyacentes que se comunican a través de la red.

De esta manera, se asegura el aumento de la seguridad en las transmisiones mediante la puesta en práctica del procedimiento, de grado en grado, de un primer nodo generador de mensajes hacia un nodo destinatario. Entre el nodo generador y el nodo destinatario, los nodos cooperan de grado en grado transfiriendo los datos después de un control de los datos que han de transmitirse.

La figura 6 representa una transmisión de mensajes de un protocolo de encaminamiento de un nodo N_A hacia un nodo N_B. El nodo N_A es un nodo generador de mensajes. El nodo N_E es el nodo destinatario de los mensajes provenientes del nodo N_A.

Los nodos N_B, N_C, N_D representan nodos que transfieren, según una ruta calculada, los mensajes del nodo N_A hacia el nodo N_E.

El procedimiento de aumento de la seguridad de los datos transmitidos permite aumentar la seguridad en la transferencia de un primer nodo en la ruta calculada hacia su nodo aguas abajo, y así sucesivamente, hasta el nodo destinatario.

El procedimiento de aumento de la seguridad estriba en la explotación de datos de autenticación que han sido distribuidos en los nodos de la red. De entre estos datos distribuidos, se ha distribuido a cada nodo N_i una clave privada ki, una clave pública Ki. Los datos de autenticación pueden ser distribuidos por una autoridad certificadora.

Adicionalmente, un certificado es generado especialmente con la clave pública Ki y es firmado por la autoridad certificadora CA. Se puede transmitir, asimismo, un certificado autofirmado por la autoridad certificadora CA, en orden a distribuir la firma de la autoridad certificadora. Este certificado permite especialmente efectuar los controles de las firmas en la recepción de mensajes firmados.

La figura 6 representa, pues, una primera transmisión del nodo N_A hacia el nodo N_B. El nodo N_A transmite un mensaje al nodo N_B de un protocolo de encaminamiento, por ejemplo OLSR, que puede ser, por ejemplo, un mensaje HELLO o TC.

De acuerdo con una primera forma de realización del procedimiento de la invención, al menos un mensaje M_1 transmitido está firmado con la clave privada del nodo N_A, el mensaje firmado se señala con M_1/k_A.

Consiste una etapa preliminar en comparar el identificador ID del nodo generador N_A con la lista de los identificadores ID de los nodos conocidos y comprendidos en la tabla ID TABLE. El identificador ID se puede transmitir por mediación de los mensajes del protocolo OLSR, tal como el mensaje M_1, que puede ser, bien un mensaje HELLO, o bien un mensaje TC.

Si el identificador es conocido y está autenticado merced a la firma, entonces el mensaje M_1 se transfiere al próximo nodo que está situado en la ruta calculada por el protocolo de encaminamiento. Si el identificador es desconocido o incluye datos de autenticación incompletos o no actualizados, entonces se puede activar el procedimiento de aumento de la seguridad de los datos transmitidos.

En este último caso, cuando el nodo N_B recibe el primer mensaje M_1, una función de autenticación puede almacenar la firma del mensaje M_1. Un segundo mensaje M_2 es emitido del nodo N_B hacia el nodo N_A en orden a solicitar un tercer mensaje M_3.

Por lo tanto, a instancias del nodo N_B, se genera un tercer mensaje por el nodo N_A hacia el nodo N_B. El tercer mensaje M_3 permite transmitir datos de autenticación del nodo N_A para aumentar la seguridad en la transferencia de los mensajes a través de la red. El mensaje M_3 comprende unos datos ENS_1 que incluyen:

- un primer certificado que comprende la clave pública K_A del primer nodo N_A firmado por la autoridad certificadora CA, señalado con K_A/k_{CA} ;
- un conjunto de datos ENS_2 que incluye:
  - la dirección IP_A del primer nodo N_A;
  - el primer certificado asociado a la dirección IP_A del primer nodo N_A.

Adicionalmente, el conjunto de datos ENS_2/k_A, también señalado con $\{IP_A; K_A/K_{CA}\}/k_A$, está firmado con la clave privada k_A del primer nodo N_A.

Cuando el nodo N_A todavía no tiene dirección IP, la dirección IP_A no se envía entre los datos ENS_2. Los datos se almacenan en el nodo N_B.

La comparación de los datos del mensaje M_1 y M_3 permite autenticar el generador de mensajes M_1 y establecer un nexo de confianza entre los dos nodos. La firma de los certificados por la autoridad certificadora permite reforzar este nexo de confianza entre los dos nodos.

Los datos de autenticación del nodo N_A se guardan en la tabla ID TABLE del nodo N_B: el identificador del nodo N_A, la dirección IP del nodo N_A y el certificado del nodo N_A cuando estos últimos no se hallan presentes en la tabla ID TABLE o cuando los valores no son idénticos a aquellos descodificados de los mensajes.

El mensaje M_3, que comprende el conjunto de datos ENS_2 que incluye la dirección IP del nodo A y la clave pública firmada, permite:

- por una parte, garantizar que el primer mensaje M_1 realmente es un mensaje con origen en el nodo N_A; y
- por otra, asociar una dirección IP del nodo N_A a un único certificado de autenticación; y
- finalmente, garantizar que el nodo N_A está realmente en poder de la clave privada k_A.

De este modo, el nodo N_B ha establecido un enlace seguro con el nodo N_A, en orden a procesar todos los mensajes firmados del nodo N_A como consecuencia de esta fase de autenticación.

Asimismo, se puede tratar otra forma de realización de la invención, bien en oposición a esta primera realización, o bien de manera complementaria.

En esta segunda realización, al menos un mensaje M_1 transmitido por el nodo N_A está firmado con una clave privada

temporal del nodo N_A, el mensaje firmado se señala con M_1/k_{tA}.

Una clave privada temporal de un nodo dado la genera el propio nodo a partir de los datos de autenticación que han sido transmitidos y certificados por una autoridad certificadora. De este modo, a partir de estos datos de autenticación, se delega en cada nodo una parte de la gestión de la seguridad.

La petición contenida en el mensaje M_2 es similar en la segunda forma de realización a la primera forma de realización. Cuando el nodo N_B recibe el primer mensaje M_1, una función de autenticación puede almacenar la firma del mensaje M_1. Un segundo mensaje M_2 es emitido del nodo N_B hacia el nodo N_A en orden a solicitar un tercer mensaje M_3.

Por lo tanto, a instancias del nodo N_B, se genera un tercer mensaje por el nodo N_A hacia el nodo N_B. El tercer mensaje M_3 comprende unos datos ENS_1 que incluyen:

- un primer certificado que comprende la clave pública K_A del primer nodo N_A firmado por la autoridad certificadora CA, señalado con K_A/k_{CA} ;
- un segundo certificado, señalado con K_{tA}/k_A, que comprende la clave pública temporal K_{tA} del primer nodo N_A firmada con la clave privada k_A del nodo N_A;
- un conjunto de datos ENS_2 que incluye:
    - la dirección IP_A del primer nodo N_A;
    - el primer certificado asociado a la dirección IP_A del primer nodo N_A.

Adicionalmente, el conjunto de datos ENS_2/k_A, también señalado con $\{IP_A; K_A/K_{CA}\}/k_A$, está firmado con la clave privada k_A del primer nodo N_A.

- un conjunto de datos ENS_3 que incluye:
    - la dirección IP_A del primer nodo N_A;
    - el segundo certificado asociado a la dirección IP_A del primer nodo N_A.

Adicionalmente, el conjunto de datos ENS_3/k_{tA}, también señalado con $\{IP_A; K_{tA}/K_A\}/k_{tA}$, está firmado con la clave privada temporal k_{tA} del primer nodo N_A.

El nodo N_B puede solicitar tan solo, por intermedio del mensaje M_2, el segundo certificado y el conjunto ENS_3 si ya conoce al nodo N_A (el nodo N_A ya aparece en la ID TABLE).

Esta forma de realización permite no utilizar demasiadas veces las claves maestras distribuidas por la autoridad certificadora CA. Solo se utilizan las claves temporales para firmar los mensajes, en orden a evitar los ataques en la red.

Las dos formas de realización son complementarias, por cuanto que se puede efectuar una primera autenticación con la firma de la autoridad certificadora entre dos nodos. Y luego, en lo sucesivo, se pueden utilizar claves temporales en orden a limitar la utilización de las claves maestras distribuidas por la autoridad certificadora CA. Una ventaja de esta utilización complementaria de estas dos formas de realización es la de poder cambiar con frecuencia de claves temporales, a fin de garantizar un alto nivel de seguridad en la red ad hoc, al propio tiempo que se limita el tráfico generado por estos mensajes.

Otra ventaja es la de gestionar un aumento de la seguridad en las transmisiones de grado en grado, es decir, de un nodo a otro.

A cada recepción de un mensaje OLSR firmado, el nodo receptor del mensaje M_1 emprende el procedimiento de control a fin de validar la firma y la autenticidad del mensaje del nodo emisor y/o del nodo generador antes de procesar el mensaje o de transferirlo.

Cada nodo emite mensajes OLSR, tal como mensajes TC, en la red. La propagación de los mensajes OLSR en la red permite a los nodos que descubren un nuevo nodo o un nodo que ha cambiado de datos de autenticación, tal como un nuevo certificado, emprender un procedimiento de aumento de la seguridad en las transmisiones con ese nuevo nodo.

La figura 7 ilustra este funcionamiento de despliegue del aumento de la seguridad en las transmisiones de grado en grado a través de la red.

El nodo N_C transmite el mensaje M_1 al nodo N_D. El mensaje M_1 tiene origen en el nodo N_A y destino al nodo N_E. Los nodos entre el nodo N_A y el nodo N_E son nodos de transición que persiguen controlar la autenticación del nodo N_A y

transferir luego los mensajes provenientes de este nodo, si es de confianza, hacia un nodo destinatario. El aumento de la seguridad en la transferencia se efectúa de grado en grado.

Si, por ejemplo, el nodo N_D carece de entrada en la tabla ID TABLE del nodo N_A, entre dos nodos consecutivos se producirá un funcionamiento análogo al descrito anteriormente.

El mensaje M_1 está firmado con la clave privada del nodo N_A, bien la clave privada maestra, o bien la clave privada temporal, según la forma de realización. Se genera un mensaje M_2 del nodo N_D hacia el nodo N_C a la recepción del mensaje M_1 por el nodo N_D.

El nodo N_C, que con anterioridad ha autenticado al nodo N_A como un nodo “seguro”, puede transmitir el mensaje M_1 y transferir los datos contenidos en el mensaje M_3, ya que el propio nodo N_C ha guardado esta información en su tabla ID TABLE.

Por lo tanto, el mensaje M_3 se envía del nodo N_C hacia el nodo N_D, a instancias del nodo N_D. El tercer mensaje M_3 comprende unos datos ENS_1 que incluyen, según la forma de realización adoptada:

- el primer certificado o el primer y el segundo certificados, como anteriormente se ha definido;
- un conjunto de datos ENS_2 o los conjuntos de datos ENS_2 y ENS_3 que incluyen:
    - la dirección IP_A del primer nodo N_A;
    - el primer o el segundo certificado asociado a la dirección IP_A del primer nodo N_A, según que se trate del conjunto de datos ENS_2 o ENS_3.

Adicionalmente, el conjunto de datos ENS_2/k_A o ENS_3/k_{tA} está firmado, respectivamente, bien con la clave privada del nodo N_A, o bien con la clave privada temporal del nodo N_A.

La tabla ID TABLE puede almacenar cada entrada, es decir, por cada nodo de nueva autenticación: su dirección IP, su identificador, un primer certificado que comprende la clave pública del nodo firmado por la autoridad certificadora CA, un segundo certificado que comprende la clave pública temporal del nodo firmado con la clave privada del nodo. La tabla ID TABLE puede comprender, además:

- un primer conjunto de datos firmado con la clave privada del nodo generador del mensaje, considerado asimismo como una primera asociación que incluye:
    - la dirección IP del nodo generador del mensaje, esto es, N_A en el ejemplo.
    - el primer certificado.
- un segundo conjunto de datos firmado con la clave privada temporal del nodo generador del mensaje, N_A, considerado asimismo como una segunda asociación que incluye:
    - la dirección IP del nodo generador del mensaje, esto es, N_A en el ejemplo.
    - el segundo certificado.

Adicionalmente, cada nodo puede contar con una lista de revocación de los certificados:

- Los segundos certificados tienen una vida útil limitada y son renovados periódicamente. Los segundos certificados obsoletos se revocan. Los nuevos segundos certificados se transmiten de grado en grado mediante los mecanismos ilustrados a través de las figuras 6 y 7. Cada nodo actualiza su lista de revocación de los certificados cuando reemplaza en ID TABLE el certificado antiguo por el nuevo.
- El primer certificado puede ser revocado por el nodo que lo posee.
    - Si posee un nuevo primer certificado firmado por la autoridad certificadora, reemplaza el primer certificado obsoleto por el nuevo primer certificado, modifica el segundo certificado (ahora firmado con la nueva clave privada), modifica en consecuencia los conjuntos ENS_2 y ENS_3. Los nuevos primeros y segundos certificados se transmiten de grado en grado mediante los mecanismos ilustrados a través de las figuras 6 y 7. Cada nodo actualiza su lista de revocación de los certificados cuando reemplaza en ID TABLE el certificado antiguo por el nuevo.
    - Si no posee un nuevo primer certificado firmado por la autoridad certificadora, debe transmitir un mensaje M_4 firmado con la clave privada en vigor hacia los nodos de confianza más próximos que conoce (por intermedio de ID TABLE y tabla de encaminamiento) indicando que desea revocar todos sus certificados. A la recepción de un mensaje M_4 y previo control de su autenticidad, el nodo receptor actualiza su tabla ID TABLE suprimiendo la entrada relativa al nodo generador del mensaje M_4 y su

lista de revocación de los certificados y envía una confirmación M_5 firmada con su clave privada temporal hacia el nodo generador del mensaje M_4. El nodo generador suprime definitivamente sus elementos de seguridad en cuanto ha recibido suficientes mensajes M_5 cuya autenticidad ha controlado. Se hace constar que, fuera de la red, la autoridad certificadora debe ser informada de la revocación de un certificado que había firmado para que pueda actualizar su propia lista de revocación.

Se puede introducir un estado intermedio “pendiente” entre no revocado y revocado para que un nodo anuncie un comportamiento errático de otro nodo. Esta información se introduce en la lista de revocación de los certificados del nodo que haya hecho esta observación. La revocación de los certificados del nodo en cuestión no puede llevarla a cabo sino el nodo en cuestión o la autoridad certificadora.

La lista de revocación de los certificados gestionada por un nodo se puede transmitir a los demás nodos ante modificación y periódicamente por mediación de un mensaje M_6 firmado con su clave privada temporal. La revocación de un certificado por mediación de los mensajes M_6 tan solo es tomada en cuenta por un nodo (modificación de su lista de revocación de los certificados) si éste recibe y autentica la revocación del certificado de suficientes nodos de confianza.

La lista de revocación de los certificados gestionada por la autoridad certificadora se puede transmitir a los nodos a través de nodos de la red por mediación de un mensaje M_7 firmado por la autoridad certificadora. La revocación de un certificado por mediación de los mensajes M_7 es tomada en cuenta inmediatamente por un nodo previa autenticación del mensaje (modificación de su lista de revocación de los certificados).

REIVINDICACIONES

1. Procedimiento de aumento de la seguridad de transmisión de datos puesto en práctica por un nodo emisor de una red ad hoc, incluyendo dicha red una pluralidad de nodos (N_i), transmitiéndose los datos según un protocolo de encaminamiento de un primer nodo (N_A) hacia un segundo nodo (N_B), incluyendo cada nodo (N_i) una clave privada (ki), una clave pública (Ki), un certificado (Ci) de la clave pública (Ki) firmado por una autoridad certificadora (CA), caracterizado por que el primer nodo (N_A) transmite al segundo nodo (N_B):

- al menos un primer mensaje (M_1) firmado (M_1/k_A) con la clave privada del primer nodo (N_A);

- al menos un tercer mensaje (M_3) hacia el segundo nodo (N_B) cuando es recibido por el primer nodo (N_A) un segundo mensaje (M_2) proveniente del segundo nodo (N_B) a consecuencia de la emisión del primer mensaje (M_1), incluyendo el tercer mensaje (M_3) un primer conjunto de datos de inicialización (ENS_1) que incluye:

  - un primer certificado que comprende la clave pública (K_A) del primer nodo (N_A) firmado por la autoridad certificadora (CA), señalado con K_A/k_{CA};

  - un segundo conjunto de datos (ENS_2) que incluye:

    - la dirección IP (IP_A) del primer nodo (N_A);

    - el primer certificado asociado a la dirección IP (IP_A) del primer nodo (N_A);

    estando firmado el segundo conjunto de datos (ENS_2/k_A) con la clave privada (k_A) del primer nodo (N_A).

2. Procedimiento de aumento de la seguridad según la reivindicación 1, caracterizado por que cada nodo incluye, además, una clave privada temporal (k_{ti}) y una clave pública temporal (K_{ti}), contando las claves temporales con una vida útil predefinida, incluyendo además el primer conjunto de datos (ENS_1):

- un segundo certificado que comprende la clave pública temporal (K_{tA}) del primer nodo (N_A) firmado con la clave privada (k_A) del primer nodo (N_A), señalado con K_{tA}/k_A;

- un tercer conjunto de datos (ENS_3) que incluye:

  - la dirección IP (IP_A) del primer nodo (N_A);

  - el segundo certificado asociado a la dirección IP (IP_A) del primer nodo (N_A);

  estando firmado el tercer conjunto de datos (ENS_3/k_{tA}) con la clave privada temporal (k_{tA}) del primer nodo (N_A).

3. Procedimiento de aumento de la seguridad de transmisión de datos puesto en práctica por un nodo emisor de una red ad hoc, incluyendo dicha red una pluralidad de nodos (N_i), transmitiéndose los datos según un protocolo de encaminamiento de un primer nodo (N_A) hacia un segundo nodo (N_B), contando cada nodo (N_i) con una clave privada (ki), una clave pública (Ki), un certificado (Ci) de la clave pública (Ki) firmado por una autoridad certificadora (CA), una clave privada temporal (k_{ti}) y una clave pública temporal (K_{ti}), contando las claves temporales con una vida útil predefinida, generándose un nuevo par al final de vida del par precedente, caracterizado por que el primer nodo (N_A) transmite al segundo nodo (N_B):

- al menos un primer mensaje (M_1) firmado (M_1/k_{tA}) con la clave privada temporal del primer nodo (N_A);

- al menos un tercer mensaje (M_3) hacia el segundo nodo (N_B) cuando es recibido por el primer nodo (N_A) un segundo mensaje (M_2) proveniente del segundo nodo (N_B) a consecuencia de la emisión del primer mensaje (M_1), incluyendo el tercer mensaje (M_3) un primer conjunto de datos de inicialización (ENS_1) que incluye:

  - un segundo certificado que comprende la clave pública temporal (K_{tA}) del primer nodo (N_A) firmado con la clave privada (k_A) del primer nodo (N_A), señalado con K_{tA}/k_A;

  - un tercer conjunto de datos (ENS_3) que incluye:

    - la dirección IP (IP_A) del primer nodo (N_A);

    - el segundo certificado asociado a la dirección IP (IP_A) del primer nodo (N_A),

  estando firmado el tercer conjunto de datos (ENS_3/k_{tA}) con la clave privada temporal (k_{tA}) del primer nodo (N_A).

4. Procedimiento de aumento de la seguridad de transmisión de datos puesto en práctica por un nodo emisor de una red ad hoc, incluyendo dicha red una pluralidad de nodos (N_i), transmitiéndose los datos según un protocolo de encaminamiento de un primer nodo (N_A) hacia un segundo nodo (N_B), caracterizado por que el procedimiento según una de las reivindicaciones 1 a 2 se efectúa con anterioridad al procedimiento según la reivindicación 3.

5. Procedimiento de aumento de la seguridad de transmisión de datos puesto en práctica por un nodo emisor de una red ad hoc, incluyendo dicha red una pluralidad de nodos (N_i), transmitiéndose los datos según un protocolo de encaminamiento de un $p^{ésimo}$ nodo (N_P) hacia un $q^{ésimo}$ nodo (N_Q), contando cada nodo (N_i) con una clave privada (ki), una clave pública (Ki), un certificado (Ci) de la clave pública (Ki) firmado por una autoridad certificadora (CA), una clave privada temporal (k_{ti}) y una clave pública temporal (K_{ti}), contando las claves temporales con una vida útil predefinida, generándose un nuevo par al final de vida del par precedente, caracterizado por que un $p^{ésimo}$ nodo transmite a un $q^{ésimo}$ nodo unos datos de encaminamiento provenientes del primer nodo (N_A), llamado “nodo generador” del mensaje, siendo los nodos $p^{ésimo}$ y $q^{ésimo}$ nodos calculados en la ruta que permite encaminar un mensaje del nodo generador hacia un nodo destinatario, incluyendo dichos datos transmitidos:

- al menos un primer mensaje (M_1) firmado (M_1/k_{tA}) con la clave privada temporal del primer nodo (N_A);
- al menos un tercer mensaje (M_3) cuando es recibido por el primer nodo un segundo mensaje (M_2) proveniente del segundo nodo a consecuencia de la emisión del primer mensaje (M_1), incluyendo el tercer mensaje (M_3):
  - bien un primer conjunto de datos de inicialización (ENS_1) según una cualquiera de las reivindicaciones 1 ó 2;
  - o bien un primer conjunto de datos de inicialización (ENS_1) según la reivindicación 3.

6. Procedimiento de aumento de la seguridad según una cualquiera de las reivindicaciones 2 a 5, caracterizado por incluir, además, un procedimiento de transmisión de los certificados revocados tal que:

- Si dicho procedimiento de transmisión es iniciado por el nodo propietario del primer certificado:
  - El nodo propietario del primer certificado transmite un mensaje M_4 firmado con su clave privada en vigor hacia los nodos de confianza más próximos, estipulando la revocación de sus certificados;
  - El nodo propietario del primer certificado suprime definitivamente sus elementos de seguridad en cuanto ha recibido suficientes mensajes de confirmación M_5 cuya autenticidad ha controlado;
- Si dicho procedimiento de transmisión es iniciado por la autoridad certificadora:
  - La autoridad certificadora pone a uno o varios nodos a cargo de transmitir su lista de certificados revocados por mediación de un mensaje M_7 firmado por la autoridad certificadora;
- Si dicho procedimiento de transmisión es mantenido por los nodos de la red:
  - Un nodo transmite periódicamente su lista de certificados revocados por mediación de un mensaje M_6 firmado con su clave privada temporal.

7. Procedimiento de aumento de la seguridad según una cualquiera de las reivindicaciones 2 a 5, caracterizado por incluir, además, un procedimiento de gestión de una lista de revocación de los certificados gestionados por un nodo, tal que:

- el nodo integra en su lista los primeros y segundos certificados obsoletos cuando son renovados por los nodos generadores (en poder de estos certificados) y transmitidos según una cualquiera de las reivindicaciones 1 a 5;
- el nodo integra en su lista los certificados revocados primero y segundo extraídos de un mensaje M_4 autenticado, procedente del nodo del cual son propiedad y firmado con la clave privada temporal de este nodo, y transmite una confirmación M_5 firmada con su clave temporal hacia el nodo generador propietario de los certificados revocados;
- el nodo integra en su lista los certificados revocados extraídos de suficientes mensajes M_6 autenticados, procedentes de varios nodos y firmados con la clave privada temporal de estos nodos;
- el nodo integra en su lista los certificados revocados extraídos de un mensaje M_7 autenticado, firmado por la autoridad certificadora y transmitido por nodos terceros.

8. Procedimiento de control de datos de autenticación puesto en práctica por un segundo nodo receptor (N_B) de una red ad hoc, permitiendo los datos de autenticación asegurar el aumento de la seguridad en intercambios de

datos útiles que transitan de un primer nodo emisor (N_A) hacia el segundo nodo receptor (N_B), siendo transmitidos los datos de autenticación por el primer nodo emisor (N_A) según un procedimiento de una de las reivindicaciones anteriores, caracterizado por que el procedimiento comprende:

- una extracción de datos recibidos por el segundo nodo (N_B), entre ellos:
  - el identificador del nodo generador extraído de la cabecera de la firma del primer mensaje enviado por el primer nodo (N_A); y
  - la firma del primer mensaje enviado por el primer nodo (N_A); y
  - el primer certificado (K_A/k_{CA}) extraído del tercer mensaje (M_3) enviado por el primer nodo (N_A); y
  - el segundo conjunto de datos (ENS_2/k_A) firmado con la clave privada (k_A) del primer nodo (N_A) del tercer mensaje (M_3);
- una generación de una petición de elementos de seguridad (M_2) a la recepción del primer mensaje (M_1) hacia el primer nodo (N_A) si el nodo N_A es desconocido para N_B o si el mensaje M_1 no está autenticado por el nodo N_B;
- un registro de los datos extraídos en una memoria del segundo nodo (N_B);
- una verificación de la firma asociada al primer certificado firmada por la autoridad certificadora también conocida por el nodo B;
- una verificación de la posesión del juego de claves k_A/K_A por el nodo N_A de dirección IP IP_A verificando la firma del conjunto ENS_2 firmado con la clave privada k_A del nodo N_A;
- una comparación de las direcciones IP y de los identificadores del nodo N_A respectivamente contenidos en los mensajes primero y tercero, permitiendo una verificación de la autenticación del primer nodo (N_A);
- una verificación de la firma del mensaje M_1 a partir de la clave pública K_A firmada por la autoridad certificadora.

9. Procedimiento de control según la reivindicación anterior, caracterizado por que el registro de los datos se realiza a fin de hacer corresponder los tres siguientes datos:

- una única identificación del primer nodo (N_A);
- una dirección IP (IP_A) del primer nodo (N_A);
- un primer certificado de la clave pública del primer nodo firmado por la autoridad certificadora.

10. Procedimiento de control según una cualquiera de las reivindicaciones 8 a 9, caracterizado por que:

- la extracción de datos recibidos por el segundo nodo (N_B) comprende, además:
  - el segundo certificado (K_{tA}/k_{CA}) del tercer mensaje (M_3);
  - el tercer conjunto de datos (ENS_3/k_{tA}) firmado con la clave temporal privada (k_{tA}) del primer nodo (N_A) del tercer mensaje (M_3);
- el procedimiento comprende, además, una verificación de la firma del segundo certificado a partir de la clave pública K_A firmada por la autoridad certificadora;
- el procedimiento comprende, además, una verificación de la posesión del juego de claves k_{tA}/K_{tA} por el nodo N_A de dirección IP IP_A verificando la firma del conjunto ENS_3 firmado con la clave privada k_{tA} del nodo N_A;
- el procedimiento comprende una verificación de la firma del mensaje M_1 a partir de la clave pública K_{tA} firmada con la clave privada k_A del nodo N_A, en lugar de una verificación de la firma del mensaje M_1 a partir de la clave pública K_A firmada por la autoridad certificadora.

11. Procedimiento de control según la reivindicación anterior, caracterizado por que el registro de los datos se realiza a fin de hacer corresponder los cuatro siguientes datos:

- una única identificación del primer nodo (N_A);
- una dirección IP (IP_A) del primer nodo (N_A);

- un primer certificado (K_A/k_{CA}) de la clave pública del primer nodo firmado por la autoridad certificadora;

- un segundo certificado (K_{tA}/k_A) de la clave pública temporal (K_{tA}) del primer nodo (N_A) firmado con la clave privada (k_A) del primer nodo (N_A).

12. Procedimiento de aumento de la seguridad según una cualquiera de las reivindicaciones 1 a 7 y procedimiento de control según una cualquiera de las reivindicaciones 8 a 11, caracterizado por que el protocolo de encaminamiento es el protocolo OLSR y el primer mensaje M_1 es un mensaje de tipo HELLO o TC.

13. Procedimiento de aumento de la seguridad según una cualquiera de las reivindicaciones 1 a 7 y procedimiento de control según una cualquiera de las reivindicaciones 8 a 11, caracterizado por que al menos un nodo comprende un terminal móvil.

14. Nodo emisor de una red ad hoc, caracterizado por permitir aumentar la seguridad en una transmisión de datos mediante la puesta en práctica del procedimiento de aumento de la seguridad de una cualquiera de las reivindicaciones 1 a 7 y 12 a 13.

15. Nodo receptor de una red ad hoc, caracterizado por permitir controlar los datos de autenticación de un nodo emisor mediante la puesta en práctica del procedimiento de control de una cualquiera de las reivindicaciones 8 a 13.

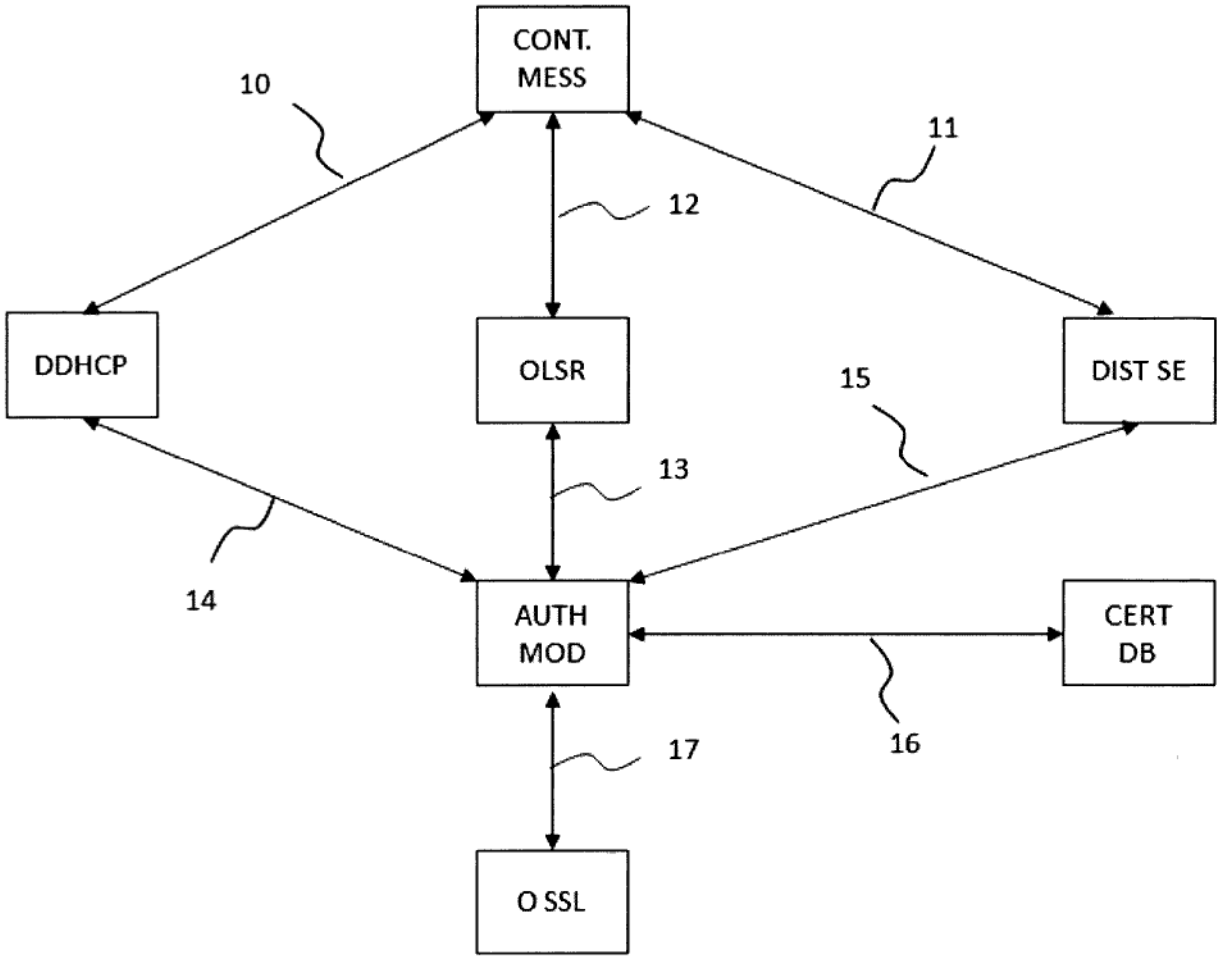

CONT.
MESS
10
11
12
DDHCP
OLSR
DIST SE
15
13
14
AUTH
MOD
CERT
DB
16
17
O SSL

FIG. 1

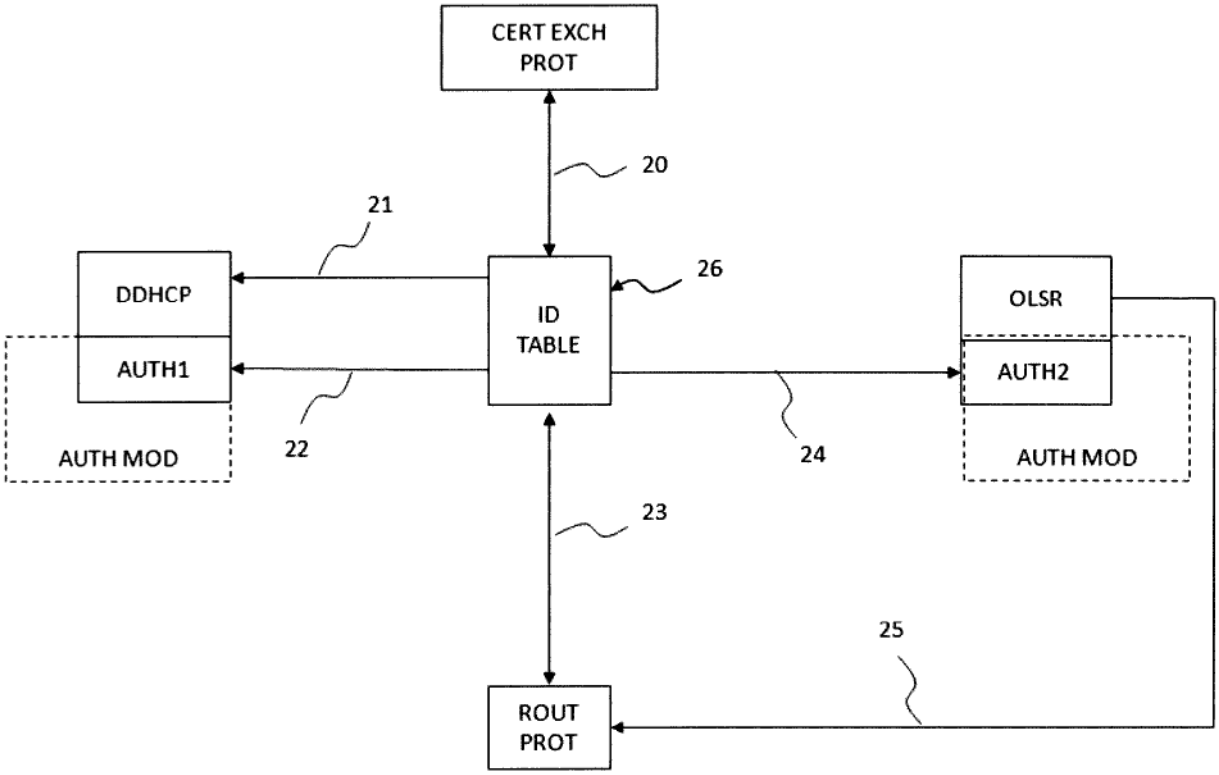

CERT EXCH PROT
20
21
DDHCP
AUTH1
AUTH MOD
22
ID TABLE
26
24
OLSR
AUTH2
AUTH MOD
23
25
ROUT PROT

FIG. 2

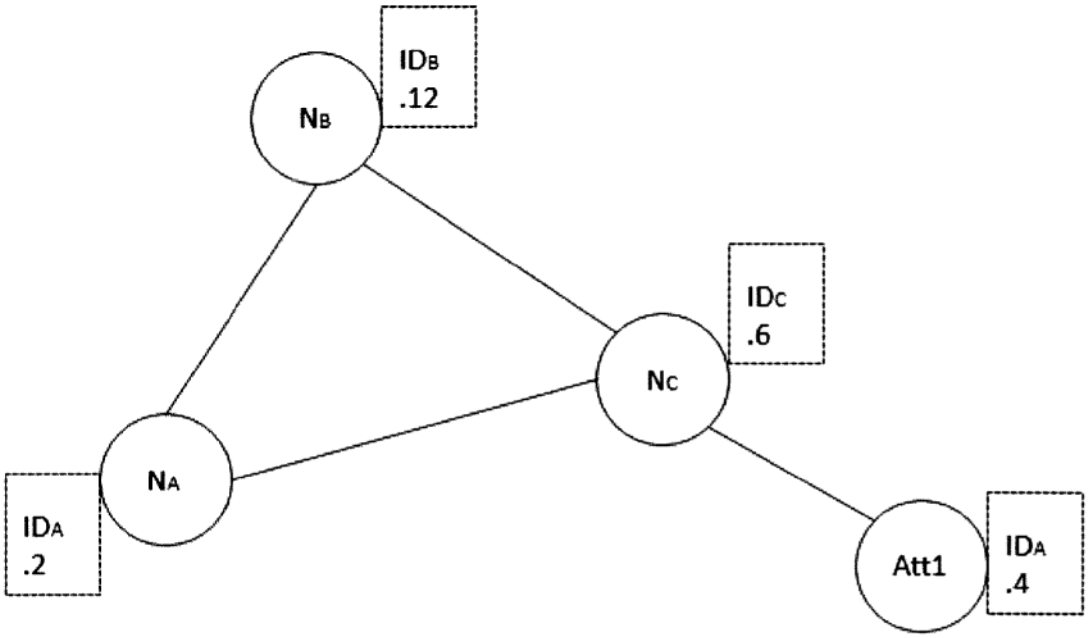


FIG. 3

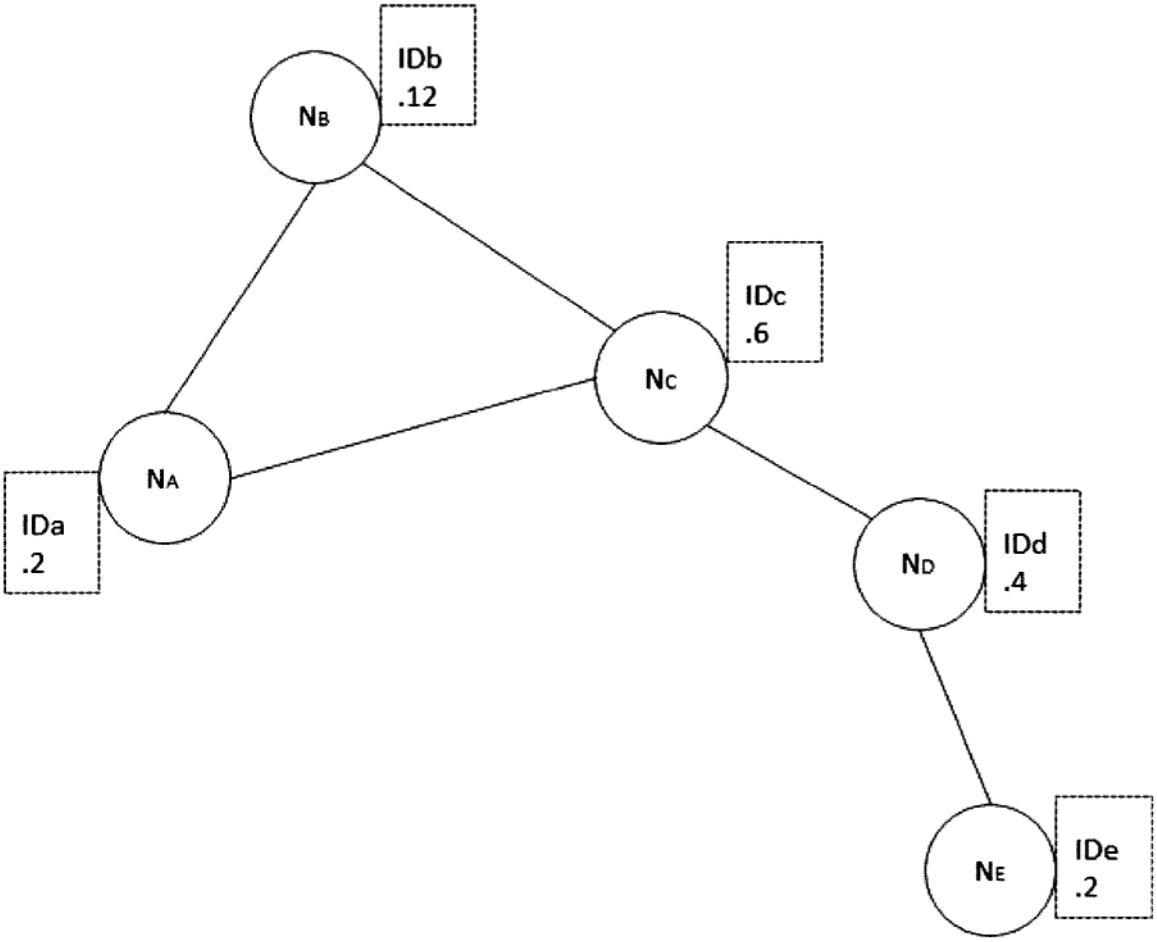
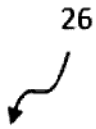


FIG. 4



ID	@IP	CERT (K)	CERT TEMP (K_t)
ID_A	IP_A	C_A (K_A/k_{CA})	Cta (K_{tA}/k_A)
ID_B	IP_B	C_B (K_B/k_{CA})	Ctb (K_{tB}/k_B)
ID_C	IP_C	C_C (K_C/k_{CA})	Ctc (K_{tC}/k_C)
...	...	...	...

FIG. 5

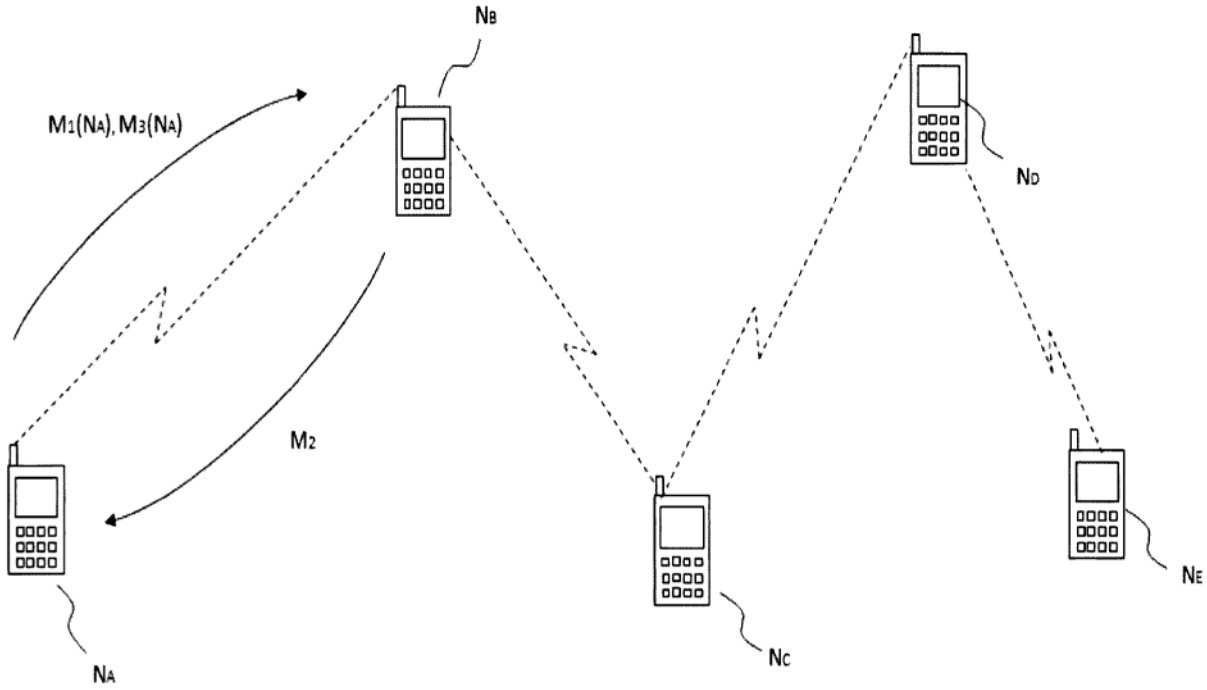


FIG. 6

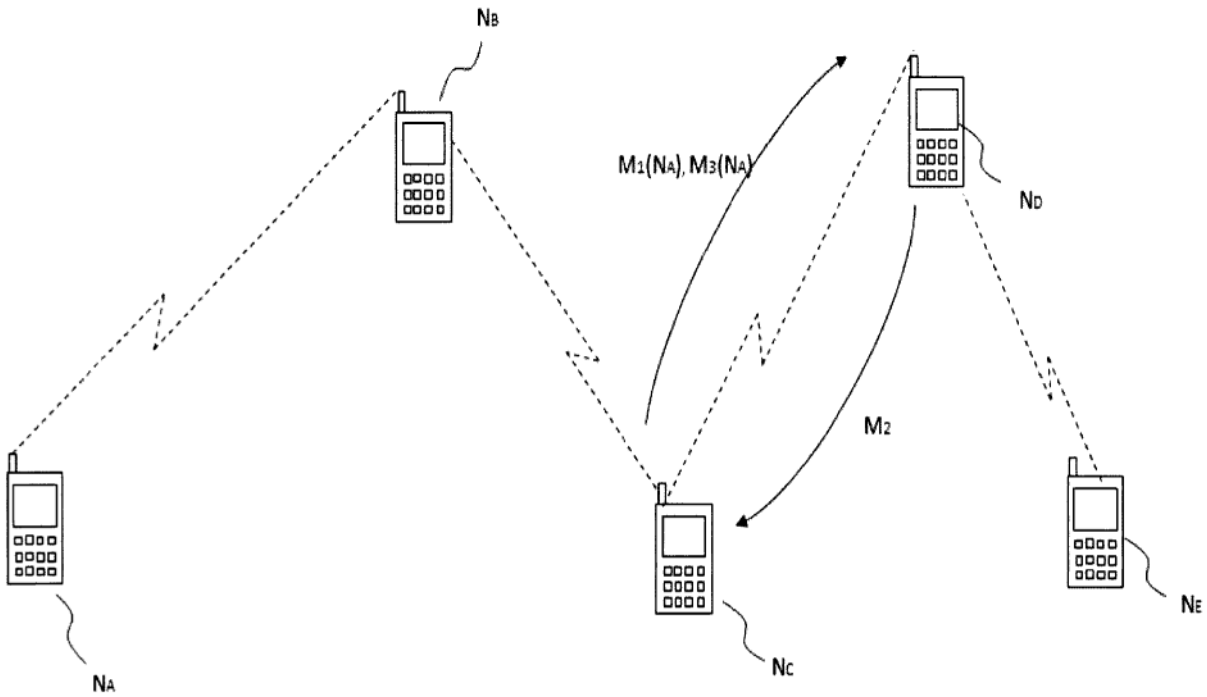


FIG. 7