(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 377 109**

(51) Int. CI.:
H04W 12/04 (2009.01)
H04W 12/06 (2009.01)
H04W 84/18 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **09784397 .3**
(96) Fecha de presentación: **05.06.2009**
(97) Número de publicación de la solicitud: **2294850**
(97) Fecha de publicación de la solicitud: **16.03.2011**

(54) Título: **Procedimiento para asegurar los intercambios entre un nodo solicitante y un nodo destinatario**

(30) Prioridad:
24.06.2008 FR 0854161

(45) Fecha de publicación de la mención BOPI:
22.03.2012

(45) Fecha de la publicación del folleto de la patente:
22.03.2012

(73) Titular/es:
France Telecom
6 place d'Alleray
75015 Paris, FR

(72) Inventor/es:
MOUSTAFA, Hassnaa y
BOURDON, Gilles

(74) Agente/Representante:
Pérez Barquín, Eliana

DESCRIPCIÓN

Procedimiento para asegurar los intercambios entre un nodo solicitante y un nodo destinatario

La invención se refiere a una técnica de autenticación en una red de comunicación.

Se sitúa en el marco de una red de comunicación de tipo ad-hoc. Una red ad-hoc es una red formada por un conjunto de nodos que pueden comunicarse entre sí sin necesidad de una infraestructura fija. No obstante, la red puede estar ligada a una infraestructura, por ejemplo para el acceso a una red de comunicación de tipo Internet. Los nodos que forman una red de este tipo pueden ser móviles o fijos. Estos nodos interactúan y cooperan entre sí, basándose en una comunicación eventualmente multi-salto. De este modo los intercambios entre nodo solicitante y nodo destinatario pueden, en caso necesario, circular por al menos un nodo intermedio.

El documento titulado “Kerberos Assisted Authentication in Mobile Ad-hoc Networks” de A. Pirzada y C. McDonald, publicado en las actas de la conferencia “27th Australasian Computer Science Conference”, 2004, describe un mecanismo de autenticación de tipo Kerberos en una red ad-hoc. Un nodo solicitante N1 contacta con un servidor para un acceso a otro nodo N2. Una vez conseguida la autenticación, el servidor transmite unos datos, denominados tique o prueba de autenticación, protegidos por medio de un clave secreta KN2 del otro nodo N2, y una clave de sesión KN1N2 protegida por medio de una clave secreta KN1 del nodo solicitante N1. El tique comprende la clave de sesión KN1N2. El nodo solicitante N1 obtiene de este modo la clave de sesión KN1N2 mediante desencriptado por medio de la clave KN1. A continuación, transmite una petición de acceso al otro nodo N2, comprendiendo la petición el tique y un dato firmado con la clave de sesión KN1N2. El otro nodo N2 desencripta el tique por medio de su clave KN2 y obtiene la clave de sesión KN1N2. Por medio de esta última, desencripta el dato firmado y autenticado, así como el nodo solicitante N1. Este mecanismo garantiza la detección de la usurpación de la identidad del nodo solicitante, la detección de ataques de repetición, el establecimiento de canales seguros y una autenticación del nodo solicitante en el otro nodo. Solo se autentica el nodo solicitante ante el otro nodo mediante la presentación de la prueba de autenticación y del dato firmado por medio de la clave de sesión KN1N2. Si el otro nodo no utiliza con posterioridad la clave de sesión KN1N2, obtenida mediante desencriptado por medio de su propia clave secreta KN2 de la prueba de autenticación, el nodo solicitante no tiene ninguna garantía de que el otro nodo es un nodo de confianza. Además, en el caso de una comunicación multi-salto que circula por al menos un nodo intermedio, el nodo intermedio no es obligatoriamente un nodo de confianza.

El documento “Providing Authentication and Access Control in Vehicular Network Environnement” de Hasnaa Moustafa y otros, publicado en las actas de la conferencia “IFIP TC-11 21st International Information Security Conference, SEC, 2006”, páginas 62-73, describe otro mecanismo de autenticación para el establecimiento de las comunicaciones seguras entre vehículos.

Uno de los objetivos de la invención es resolver los inconvenientes del estado de la técnica.

La invención propone, para ello, un procedimiento para preservar la seguridad de los intercambios entre un nodo solicitante y un nodo destinatario, perteneciendo dichos nodos a una red de comunicación, dicho procedimiento comprendiendo las siguientes etapas que lleva a cabo un servidor de seguridad:

- una etapa de recepción de una petición enviada por el nodo solicitante para un acceso al nodo destinatario;
- una etapa de envío de una respuesta a la petición, comprendiendo dicha respuesta una prueba de autenticación, dirigida al nodo destinatario, y una clave de sesión, destinada a utilizarse para los intercambios entre los nodos solicitante y destinatario,

caracterizado porque hay que compartir al menos un secreto con al menos otro nodo solicitante, diferente de la clave de sesión, que está asociado al nodo destinatario, la respuesta enviada al nodo solicitante comprende, además, dicho secreto.

Hay que señalar que la invención obtiene su potencial malicioso en una red de comunicación de tipo ad-hoc. No obstante, la invención se puede aplicar a cualquier red de comunicación en la que sea necesario seguir una ruta segura.

En la respuesta a la petición, el servidor transmite no solo unas informaciones ligadas al intercambio entre el nodo solicitante y el nodo destinatario, como una prueba de autenticación que hay que proporcionar al nodo destinatario y una clave de sesión para los intercambios entre el nodo solicitante y el nodo destinatario, sino también un secreto que hay que compartir con, al menos, un nodo solicitante y asociado al nodo destinatario.

De este modo, en función del nodo destinatario, se constituye un grupo de nodos que comprenden al menos el nodo solicitante y el nodo destinatario. Este grupo de nodos comparte un secreto, que permite mejorar la seguridad de los intercambios dentro del grupo. De este modo se realiza una única petición, que permite así obtener a la vez una autorización de acceso a un servicio proporcionado por el nodo destinatario y el secreto compartido dentro del grupo. El servidor, que juega el papel de un tercero de confianza, permite la puesta en marcha de una autenticación

indirecta del nodo solicitante en nombre del nodo destinatario y proporciona al nodo solicitante el secreto compartido permitiéndole comunicarse con el nodo destinatario mediante un enlace seguro. La unicidad de la petición, y respectivamente de su respuesta, permite obtener una aplicación simple y especialmente eficaz. De este modo se puede distribuir de manera sencilla el secreto compartido en los intercambios para el acceso al nodo destinatario sin que se requiera una nueva autenticación en un tercero de confianza. El hecho de que un nodo del grupo guarde el secreto compartido y sea capaz de probarlo permite que de esto se deduzca que está implícitamente autenticado en el servidor. La utilización de un secreto compartido permite, además, aplicar unas técnicas de autenticación simples y rápidas, basadas en la criptografía simétrica, adaptadas para una aplicación en unos nodos susceptibles de tener unos recursos, como su batería o su capacidad de almacenamiento, limitados.

Para una aplicación de una red ad-hoc, el nodo destinatario proporciona, por ejemplo, un servicio en una zona geográfica determinada. Los nodos, que han obtenido el secreto compartido y de este modo se han autenticado de manera implícita en el servidor, forman así un grupo de confianza que preserva la seguridad de los intercambios dirigidos al nodo destinatario en un enlace eventualmente multi-salto. El nodo destinatario puede, por su parte, obtener el secreto mediante una relación privilegiada con el servidor.

De este modo, se puede mejorar la preservación de la seguridad de los intercambios entre un nodo solicitante y un nodo destinatario en una red de comunicación de tipo ad-hoc.

En un modo de realización, la respuesta contiene, además, un intervalo de tiempo de validez asociado a dicho secreto.

De este modo, se puede distribuir una multitud de secretos compartidos a los que se asocian unos intervalos de validez respectivos. El nodo solicitante determina a continuación, en función de un reloj actual el secreto que hay que utilizar. Esto permite limitar las peticiones hacia el servidor con el fin de obtener secretos válidos y evitar una simultaneidad de las peticiones cuando los secretos ya no son válidos. Al renovarse de manera frecuente el secreto compartido, esto permite evitar casos de robo del secreto compartido.

La invención se refiere, además, a un procedimiento para que se pongan en contacto un nodo solicitante y un nodo destinatario, perteneciendo dichos nodos a una red de comunicación, comprendiendo dicho procedimiento las siguientes etapas que lleva a cabo el nodo solicitante:

- una etapa de envío de una petición a un servidor de seguridad para un acceso al nodo destinatario;
- una etapa de recepción de una respuesta a la petición, que comprende una prueba de autenticación dirigida al nodo destinatario y una clave de sesión, destinada a utilizarse para los intercambios entre los nodos solicitante y destinatario,

caracterizado porque la respuesta comprende, además, un secreto y porque dicho procedimiento comprende, además, una etapa de autenticación de, al menos, otro nodo por medio de dicho al menos un secreto, siendo apto este otro nodo para comunicarse con el nodo destinatario.

El nodo solicitante obtiene de este modo un secreto, asociado a un nodo destinatario, compartido dentro de un grupo de nodos, denominado grupo de confianza. De este modo puede autenticar los nodos con los que está en contacto directo, es decir, sus vecinos inmediatos, por medio de este secreto compartido y dar preferencia a los nodos vecinos autenticados en los intercambios con el nodo destinatario. Se obtiene de este modo la garantía de que un nodo malicioso no responde en lugar del nodo destinatario y también de que ningún nodo malicioso se introduce en la cadena de nodos que conectan el nodo solicitante y el nodo destinatario.

En un modo de realización, en el que la respuesta comprende, además, un intervalo de tiempo de validez asociado a dicho secreto, el nodo solicitante selecciona un secreto válido en función de un momento actual.

De este modo, los nodos del grupo comparten un secreto común con independencia del momento en el que estos han transmitido una petición al servidor.

En otro modo de realización, la etapa de envío de una petición de acceso a un nodo destinatario se realiza una vez que se ha detectado una ausencia de secreto válido.

Cada vez que el nodo solicitante ya no tiene secretos en vigor, contacta de nuevo con el servidor, con el fin de que se pueda mantener el grupo de confianza formado.

Además, el nodo solicitante y el nodo destinatario se ponen en contacto a continuación mediante una ruta formada por nodos autenticados por medio del secreto.

La invención también se refiere a un servidor para preservar la seguridad de los intercambios entre un nodo solicitante y un nodo destinatario en una red de comunicación, que comprende:

– unos medios de recepción de una petición enviada por un nodo solicitante para un acceso a un nodo destinatario;
– unos medios de envío de una respuesta a la petición, comprendiendo dicha respuesta una prueba de autenticación, dirigida al nodo destinatario, y una clave de sesión, destinada a utilizarse para los intercambios entre los nodos solicitante y destinatario,

caracterizado porque los medios de envío están, además, preparados para incluir en la respuesta un secreto, dicho secreto, que hay que compartir con al menos otro nodo solicitante, diferente de la clave de sesión, estando asociado al nodo destinatario.

La invención se refiere, además, a un nodo de una red de comunicación, que comprende:

– unos medios de envío de una petición a un servidor para un acceso a un nodo destinatario;
– unos medios de recepción de una respuesta a la petición, comprendiendo la respuesta una prueba de autenticación, dirigida a un nodo destinatario, y una clave de sesión, destinada a utilizarse para los intercambios entre el nodo y el nodo destinatario,

caracterizado porque los medios de recepción están, además, preparados para recibir una respuesta que comprende, al menos, un secreto y porque dicho nodo comprende, además, unos medios de autenticación de, al menos, otro nodo por medio de dicho, al menos, un secreto, siendo apto este otro nodo para comunicarse con el nodo destinatario.

La invención también se refiere a un sistema de comunicación en una red de comunicación, que comprende un servidor como el que se ha descrito con anterioridad y una multitud de nodos como los que se han descrito con anterioridad.

La invención se refiere, además, a un programa de ordenador que consta de unas instrucciones para la puesta en marcha del procedimiento para preservar la seguridad de los intercambios tal y como se ha descrito con anterioridad mediante un servidor de una red de comunicación, cuando este programa lo ejecuta un procesador.

La invención también se refiere a un programa de ordenador que consta de unas instrucciones para la puesta en marcha del procedimiento para comunicarse con un nodo destinatario tal y como se ha descrito con anterioridad mediante un nodo solicitante de una red de comunicación, cuando este programa lo ejecuta un procesador.

La invención se refiere, además, a una señal que lleva una respuesta a una petición de acceso a un nodo destinatario emitida por un nodo solicitante, siendo emitida dicha respuesta por un servidor en el nodo solicitante y que comprende una prueba de autenticación, dirigida al nodo destinatario, y una clave de sesión, destinada a utilizarse para los intercambios entre los nodos solicitante y destinatario, caracterizada porque dicha respuesta comprende, además, al menos un secreto, dicho secreto, que hay que compartir con al menos otro nodo solicitante, diferente de la clave de sesión, estando asociado al nodo destinatario.

La invención se entenderá mejor con la siguiente descripción de un modo de realización particular de los procedimientos de la invención, en referencia a los dibujos que se anexan, en los que:

- la figura 1 representa una red de comunicación;
- la figura 2 representa una parte de las etapas de los procedimientos de acuerdo con un modo particular de realización de la invención;
- la figura 3 representa otra parte del procedimiento para comunicar de acuerdo con el modo particular de realización de la invención;
- la figura 4 representa una petición para un acceso de acuerdo con el modo particular de realización de la invención;
- la figura 5 representa una respuesta a la petición para un acceso de acuerdo con el modo particular de realización de la invención;
- la figura 6 representa de manera más detallada un campo de la respuesta de acuerdo con el modo particular de realización de la invención;
- la figura 7 representa un dispositivo para preservar la seguridad de los intercambios de acuerdo con el modo particular de realización de la invención;
- la figura 8 representa un nodo de la red de comunicación de acuerdo con el modo particular de realización de la invención.

En la figura 1 se representa una red ad-hoc 2. Esta comprende una multitud de nodos, designados N1 a N8. Estos nodos son aptos para comunicarse entre sí a través de conexiones inalámbricas. Una comunicación entre dos nodos de la red ad-hoc 2 puede circular a través de otros nodos; se trata en este caso de comunicación multi-salto. A título de ejemplo, una comunicación entre los nodos N1 y N4 circula a través del nodo N3 y se materializa en la figura 1 con una línea de puntos. Del mismo modo, la comunicación entre los nodos N2 y N8 circula a través de los nodos

N5 y N7, y la comunicación entre los nodos N2 y N6 circula por el nodo N5. Estos nodos pueden ser móviles o bien fijos.

Cada nodo N1-N8 de la red ad-hoc 2 posee una clave secreta propia KN1-KN8.

A continuación, los nodos N1 y N2 desempeñan un papel particular de nodo proveedor de aplicación. Se trata de un nodo de la red ad-hoc 2, que se mantiene, por ejemplo, fijo, con el cual los otros nodos de la red ad-hoc pueden comunicarse con el fin de tener acceso a un servicio determinado o a una aplicación determinada. A título de ejemplos no excluyentes, se trata de la descarga de contenidos audiovisuales, de aplicación de contenido vídeo o "video streaming", de impresión…

Un servidor de seguridad Serv pertenece a una red centralizada 1 de un operador de comunicación. Este servidor de seguridad Serv está preparado para autenticar unos nodos de la red ad-hoc y proporcionarle una prueba de su autenticación con el fin de que estos puedan acceder a las aplicaciones propuestas por los nodos N1 y N2 proveedores de aplicación. El servidor de seguridad Serv está preparado para memorizar los identificadores de los nodos autorizados para acceder a la red ad-hoc. A cada identificador de nodo se le asocia la clave secreta de este. A continuación, el servidor Serv de seguridad pone en marcha el protocolo Kerberos, tal y como se especifica en el documento de la Internet Engineering Task Force RFC 4120, titulado "The Kerberos Network authentication Service". Este desempeña la función de un tercero de confianza. Comprende dos entidades: una primera entidad que desempeña la función de una entidad de autenticación, designada AS para "Authentication Server", y una segunda entidad que desempeña la función de un servicio de emisión de tiques, designada TGS para "Ticket Grant Service".

Un punto AP de acceso permite a los nodos de la red ad-hoc 2 acceder a la red centralizada 1 y de este modo comunicarse con el servidor de seguridad Serv. A continuación el punto AP de acceso está preparado para desempeñar la función de un Proxy Kerberos, tal y como se especifica en el documento del IETF "draft-ietf-krb-wg-iakerb-00".

El procedimiento para preservar la seguridad de los intercambios, tal y como lo lleva a cabo el servidor de seguridad, se va a describir a continuación en relación con la figura 2.

El procedimiento para comunicarse, tal y como lo lleva a cabo un nodo solicitante, se va a describir, por su parte, en relación con las figuras 2 y 3.

En el ejemplo que se describe, el usuario del nodo solicitante N4 quiere comunicarse con el nodo N1 proveedor de aplicación.

El nodo solicitante N4 detecta en una primera etapa E1, designada "S_RAS(NF)" en la figura 2, que no tiene un secreto válido para comunicar en la red ad-hoc 2 o que no tiene una prueba de autenticación válida para el nodo N1 proveedor de aplicación. El secreto está asociado al nodo N1 proveedor de aplicación y destinado a compartirse en el grupo de nodos de la red ad-hoc que se comunica con este último. La prueba de autenticación está destinada a que se la proporcionen al nodo N1 proveedor de aplicación y le aporta a este una prueba de que el nodo solicitante N4 se ha autenticado en el servidor de seguridad Serv.

Aun en esta etapa E1, el nodo solicitante N4 transmite una petición M1 al servidor de seguridad Serv para un acceso al nodo N1 proveedor de aplicación. Se trata, en el protocolo Kerberos, de un mensaje AS-REQ.

Los intercambios se realizan a través del punto AP de acceso que pone en marcha un mecanismo de delegación (o función de "Proxy Kerberos" en inglés). No obstante, con el fin de simplificar la descripción y la figura 2, no se han analizado los diferentes intercambios.

Esta petición M1 la recibe el servidor de seguridad Serv, de manera más precisa la entidad AS, en una etapa F1 de recepción, designada "R_RAS(NF)" en la figura 2.

Una vez verificado el identificador del nodo solicitante N4, la entidad AS del servidor de seguridad Serv transmite en una etapa F2, designada "S_RepAS" en la figura 2, un mensaje M2 de respuesta a la petición para un acceso al nodo N1 proveedor de aplicación que comprende, de acuerdo con el protocolo Kerberos:

- un primer tique $T_{TGS.}$ y
- una primera clave de sesión Ksession encriptada por medio de la propia clave secreta KN4 del nodo solicitante N4.

En el protocolo Kerberos, se trata de un mensaje AS-REP.

Este primer tique T_{TGS} lo cifra la entidad AS del servidor de seguridad Serv por medio de una clave Ktgs. Contiene en particular datos sobre el nodo solicitante N4, pero también la primera clave de sesión Ksession destinada a que la utilice este último para obtener una prueba de autenticación.

El mensaje M2 de respuesta a la petición para un acceso al nodo N1 proveedor de aplicación lo recibe el nodo solicitante N4 en una etapa E2, designada “R_RepAS” en la figura 2.

Al término de estos intercambios de mensajes M1 y M2, el nodo solicitante N4 tiene el primer tique T_{TGS}. que no puede desencriptar, y la primera clave de sesión Ksession. Si el nodo solicitante N4 no es el que dice ser, no le es posible desencriptar la primera clave de sesión Ksession, ya que solo el verdadero nodo solicitante N4 tiene la clave secreta KN4 que permite desencriptar la primera clave de sesión Ksession.

En una etapa E3, designada “S_RTGA” en la figura 2, el nodo solicitante N4 transmite a la entidad TGS del servidor de seguridad una petición M3 de prueba de autenticación. En el protocolo Kerberos, se trata de un mensaje TGS-REQ. Esta petición M3 comprende el primer tique T_{TGS} transmitido por la entidad AS del servidor Serv en el mensaje M2 de respuesta a la petición para un acceso al nodo N1 proveedor de aplicación así como de los datos protegidos por medio de la primera clave de sesión Ksession.

La petición M3 de prueba de autenticación se representa en la figura 4.

Una petición 100 de este tipo comprende, de acuerdo con la RFC 4120:

- un campo 102, que indica la versión del protocolo Kerberos;
- un campo 104 que indica el tipo de mensaje;
- un campo 106 que comprende un dato para pre-autenticar;
- un campo 108 que comprende el cuerpo del mensaje.

El campo 108 comprende, entre otros, un identificador del nodo solicitante N4 y unas marcas 110 que permiten indicar el soporte o no de opciones del protocolo. En el modo particular de realización de la invención, una marca permite al nodo solicitante N4 señalar que su petición también busca obtener un secreto asociado al nodo N1 proveedor de aplicación. Esto permite garantizar la compatibilidad con un servidor que pone en marcha el protocolo Kerberos clásico y también diferenciar los nodos que soportan esta opción de los nodos que no la soportan.

Esta petición M3 de prueba de autenticación la recibe la entidad TGS del servidor de seguridad Serv en una etapa F3, designada “R_RTGS” en la figura 2.

En una etapa F4, designada “Auth” en la figura 2, la entidad TGS del servidor de seguridad desencripta el primer tique T_{TGS} con su propia clave secreta Ktgs. Esta obtiene entonces la primera clave de sesión Ksession y puede desencriptar de este modo los datos transmitidos por el nodo solicitante N4. Esto le permite autenticar de manera implícita al nodo solicitante N4 ya que este último le aporta la prueba de que efectivamente tiene la clave KN4. La entidad TGS determina a continuación una segunda clave KN1N4 de sesión, destinada a utilizarse, en caso necesario, para los intercambios posteriores entre el nodo N1 proveedor de aplicación y el nodo solicitante N4. La entidad TGS determina también una prueba de autenticación, que permite un acceso al nodo N1 proveedor de aplicación. Esta prueba de autenticación comprende la segunda clave KN1N4 de sesión y se protege por medio de la clave secreta KN1 del nodo N1 proveedor de aplicación.

En una etapa de prueba F5, designada “Prueba_F” en la figura 2, la entidad TGS verifica si la petición M3 comprende en el campo 110 una marca que indica que la petición también busca obtener un secreto compartido.

Si está presente una marca de este tipo, en una etapa F6, designada “Det_Kad” en la figura 2, la entidad TGS determina un secreto Kad, asociado al nodo N1 proveedor de aplicación al que el nodo solicitante N4 desea acceder, y destinado a compartirse en un grupo de nodos de la red ad-hoc 2.

En una etapa F7, designada “S_RepTGS” en la figura 2, la entidad TGS transmite al nodo solicitante N4 una respuesta M4 a la petición que comprende:

- la prueba de autenticación que hay que proporcionar al nodo N1 proveedor de aplicación, determinada en la etapa F4, protegida por medio de la clave secreta KN1 del nodo N1 proveedor de aplicación;
- la segunda clave de sesión, KN1N4, destinada a utilizarse para los intercambios entre el nodo solicitante N4 y el nodo N1 proveedor de aplicación y determinada en la etapa F4, protegida por medio de la primera clave de sesión Ksession;
- si la marca que indica que la petición también busca obtener un secreto estaba presente en la petición M3, el secreto compartido Kad determinado en la etapa F6, protegido por medio de la primera clave de sesión Ksession.

Una respuesta M4 de este tipo a la petición de prueba de autenticación se representa en la figura 5. En el protocolo Kerberos, se trata de un mensaje TGS-REP.

Una respuesta 200 de este tipo comprende, de acuerdo con la RFC 4120:

- un campo 202, que indica la versión del protocolo Kerberos;
- un campo 204, que indica el tipo de mensaje;
- un campo 206, que comprende un dato para pre-autenticar;
- un campo 208, que comprende un dominio del nodo solicitante;
- un campo 210, que comprende un nombre del nodo solicitante;
- un campo 212, que comprende la prueba de autenticación que hay que proporcionar al nodo N1 proveedor de aplicación;
- un campo 214, que comprende unos datos protegidos mediante encriptado por medio de la primera clave de sesión Ksession conocida a la vez por la entidad TGS y el nodo solicitante N4.

Los datos encriptados comprendidos en el campo 214 se representan en la figura 6. Estos comprenden, en particular:

- la segunda clave KN1N4 216 de sesión;
- un campo 218 que comprende unas marcas que permiten indicar el soporte o no de opciones del protocolo; en el modo particular de realización de la invención, una marca permite al servidor de seguridad Serv indicar que un secreto está comprendido en los siguientes datos 214;
- un campo 222 que comprende el secreto Kad en función del valor de la marca relativa al secreto compartido, que se ha citado con anterioridad.

En una variante de realización, a un secreto Kad se le asocia un intervalo de tiempo de validez de secreto, transmitido en un campo 220.

La respuesta M4 la recibe el nodo solicitante N4 en una etapa E4, designada “R_RepTGS” en la figura 2.

Al final de los intercambios de los mensajes M3 y M4, el nodo solicitante N4 tiene una prueba de autenticación que tiene que proporcionar al nodo N1 proveedor de aplicación, que él no puede desencriptar, la segunda clave KN1N4 de sesión y el secreto compartido Kad en el grupo de nodos de la red ad-hoc.

Hay que señalar también que en el caso de una comunicación multi-salto, cuando el nodo solicitante N4 transmite la prueba de autenticación al nodo N1 proveedor de aplicación, ninguno de los nodos intermedios, que contribuyen al envío de la prueba de autenticación, puede desencriptar esta y no pueden, por lo tanto, obtener la segunda clave KN1N4 de sesión. En efecto, la prueba de autenticación está protegida mediante encriptado por medio de la clave secreta KN1 del nodo N1 proveedor de aplicación y no lo puede desencriptar un nodo cualquiera.

Al nodo solicitante N4 que tiene el secreto compartido Kad, le resulta entonces posible poner en marcha una etapa de autenticación para cada uno de los nodos con los que está en relación directa, es decir, los nodos vecinos. Se entiende por nodo vecino un nodo localizado en una zona de cobertura de radio del nodo solicitante N4. El nodo solicitante N4 presenta el secreto compartido Kad a un nodo vecino como prueba de autenticidad y el nodo vecino prueba también su autenticidad presentando la misma clave. Se trata, por ejemplo, de una autenticación mutua EAP-PSK por medio del secreto compartido Kad. Este tipo de autenticación presenta la ventaja de necesitar unos recursos de tratamiento limitados.

Este mecanismo de autenticación se describe en el documento RFC 4764 del IETF. Se describe sucintamente en relación con la figura 3.

El nodo solicitante N4 transmite un mensaje L1 de petición de identidad del nodo vecino N3, por ejemplo “EAP-Request Identity”. El nodo vecino N3 transmite su identidad Idv al nodo solicitante N4 en un mensaje L2, por ejemplo “EAP-Response Identity”. En un mensaje L3, por ejemplo “EAP-Request/PSK”, el nodo solicitante N4 transmite su propia identidad Idd, así como una variable aleatoria Rd que ha generado al nodo vecino N3. El nodo vecino N3 determina una variable aleatoria Rv, calcula un primer código de autenticación MAC para el conjunto de los datos (Idv, Rv, Idd, Rd) firmado por el secreto compartido Kad y transmite al nodo solicitante N4 su identificador Idv, la variable aleatoria Rv y el primer código de autenticación MAC en un mensaje L4, por ejemplo “EAP-Response/PSK”. El nodo solicitante N4 verifica el primer código de autenticación MAC por medio del secreto compartido Kad para autenticar al nodo vecino N3. A continuación, el nodo solicitante N4 transmite en un mensaje L5, por ejemplo “EAP-Request/PSK”, al nodo vecino N3 la variable aleatoria Rd, así como un segundo código MAC calculado para el conjunto formado por su identidad Idd y por la variable aleatoria Rv, firmada con el secreto compartido Kad. El nodo vecino N3 verifica el segundo código de autenticación MAC por medio del secreto compartido Kad y transmite al nodo solicitante N4 un mensaje L6, por ejemplo “EAP-Response/PSK”, que comprende la variable aleatoria Rd. Un mensaje L7, por ejemplo “EAP_Success” en caso de éxito, transmitido desde el nodo solicitante N4 al nodo vecino N3, termina la etapa de autenticación.

Se puede entonces dar preferencia, para el envío de los mensajes entre el nodo solicitante N4 y el nodo N1 proveedor de aplicación, unos nodos de la red ad-hoc 2 pertenecientes al grupo que comparte el secreto Kad. Es en

efecto posible construir unas rutas utilizadas por un protocolo de envío utilizando una métrica de seguridad. Un mecanismo de este tipo se describe, por ejemplo, en el artículo titulado “Secure Routing for Mobile Ad-hoc Networks” de P. Argyroudis y D. O’Mahony, publicado en la revista IEEE Communications Survey, 3rd quarter, 2005. Este artículo describe un mecanismo SAR para “Secure Ad-hoc Routing”, aplicable a los protocolos de envío reactivo como el protocolo AODV, para “Ad-hoc On-Demand Distance Vector”, o el protocolo DSR, para “Dynamic Source Routing”, que integra una métrica de seguridad en los mensajes de Route Request, con el fin de construir unas rutas entre los nodos que tienen un nivel de seguridad definido.

El nodo solicitante N4 transmite, por lo tanto, su petición de acceso al nodo proveedor de aplicación presentando su prueba de autenticación, que, a título de indicación, está protegida por medio de la clave secreta KN1 del nodo N1 proveedor de aplicación. La petición de acceso se transfiere entonces mediante el protocolo de envío al nivel de la capa 3 OSI. Un nodo intermedio N3 que recibe la petición de acceso no puede desencriptar la prueba de autenticación y transmite esta petición seleccionando, a su vez, un nodo vecino en función el estado de autenticidad de sus vecinos. Esto se repite hasta el nodo N1 proveedor de aplicación que, al desencriptar la prueba de autenticación por medio de su propia clave secreta KN1, obtiene la segunda clave KN1N4 de sesión. La prueba de autenticación prueba que el nodo solicitante N4 se ha autenticado efectivamente en el servidor de seguridad Serv. La prueba de autenticación se envía de este modo al nodo N1 proveedor de aplicación por una ruta formada por nodos autenticados por medio del secreto compartido. El nodo N1 proveedor de aplicación puede entonces proporcionar el servicio solicitado protegiendo el tráfico por medio de la segunda clave KN1N4 de sesión. Los intercambios posteriores entre el nodo solicitante N4 y el nodo N1 proveedor de aplicación toman también esta ruta o cualquier otra ruta formada por nodos autenticados por medio del secreto compartido.

En otro modo de realización de la invención, tras la recepción de una petición enviada por el nodo solicitante N4 en la etapa F1, la entidad TGS determina en la etapa F6 una multitud de secretos compartidos y le asocia a cada secreto compartido un intervalo de tiempo de validez del secreto. Cada secreto compartido Kad tiene de este modo un tiempo útil limitado D. El servidor transmite en la etapa F7, en la respuesta, un conjunto de secretos compartidos válidos para los periodos siguientes.

La respuesta se recibe en la etapa E4 mediante el nodo solicitante N4.

A continuación, cuando debe autenticar a uno de sus vecinos, el nodo solicitante N4 selecciona un secreto compartido válido en función de un instante actual.

De este modo, al distribuir el servidor de seguridad Serv una multitud de claves en la petición para un acceso al nodo destinatario, los nodos solicitan con menor frecuencia al servidor y, además, estas peticiones se realizan de forma desincronizada.

Se va a describir a continuación un servidor para preservar la seguridad de los intercambios entre un nodo solicitante y un nodo destinatario en una red de comunicación en relación con la figura 7.

Un servidor 300 de este tipo comprende:

- unos medios 308 de memorización, designados “KN” en la figura 7, preparados para memorizar unas claves secretas respectivamente asociadas a unos nodos de la red de comunicación;
- un módulo 302 de recepción de una petición, designado “Rec_S” en la figura 7, la petición enviándola un nodo solicitante para un acceso a un nodo destinatario;
- un módulo 310 de determinación de datos para el acceso a un nodo destinatario, designado “Det_PK” en la figura 7, preparado para determinar una prueba de autenticación dirigida al nodo solicitante y una clave de sesión destinada a utilizarse en los intercambios entre el nodo solicitante y el nodo destinatario;
- un módulo 306 de obtención de, al menos, un secreto compartido, designado “Det_Kad” en la figura 7, el secreto estando asociado a un nodo destinatario y que hay que compartir en un grupo de nodos que comprenden al menos un nodo solicitante, diferente de la clave de sesión;
- un módulo de encriptado/desencriptado 312, designado “C/D_S” en la figura 7, preparado para encriptar unos datos destinados a un nodo en función de su clave secreta respectiva extraída de los medios 308 de memorización o en función de una clave de sesión compartida entre un nodo y el servidor, y para desencriptar unos datos recibidos por medio de la clave de sesión;
- un módulo 304 de envío de una respuesta a la petición, designada “S_S” en la figura 7, comprendiendo dicha respuesta la prueba de autenticación dirigida al nodo destinatario, la clave de sesión, destinada a utilizarse para los intercambios entre los nodos solicitante y destinatario, y al menos un secreto obtenido.

En un modo particular de realización de la invención, el módulo 310 de determinación de datos para el acceso a un nodo destinatario lleva a cabo las etapas del protocolo Kerberos.

En una variante del modo de realización descrito, el módulo 306 de obtención de un secreto compartido obtiene, además, un intervalo de tiempo de validez asociado. En este caso, el módulo 304 de envío también transmite en la

respuesta el intervalo de tiempo de validez asociado.

Se va a describir a continuación un nodo de una red de comunicación en relación con la figura 8.

Un nodo 400 de este tipo comprende:

- un módulo 402 de envío, designado “S_N” en la figura 8, de una petición a un servidor para un acceso a un nodo destinario;
- un módulo 404 de recepción de una respuesta a la petición, designado “Rec_N” en la figura 8, comprendiendo la respuesta una prueba de autenticación dirigida al nodo destinatario, una clave de sesión destinada a utilizarse para los intercambios entre el nodo y el nodo destinatario, y al menos un secreto compartido;
- un módulo 410 de encriptado/desencriptado, designado “C/D_N” en la figura 8, preparado para desencriptar unos datos en función de su clave secreta respectiva o en función de una clave de sesión compartida entre el nodo y un servidor, y para cifrar unos datos por medio de la clave de sesión;
- un módulo 406 de autenticación, designado “Auth” en la figura 8, de al menos otro nodo por medio de dicho al menos un secreto, siendo apto este otro nodo para comunicarse con el nodo destinatario;
- un módulo 408 de determinación de rutas en una red de comunicación, designado “Det_R” en la figura 8, preparado para determinar una ruta con destino en el nodo destinatario que da preferencia a los nodos autenticados.

En la variante del modo de realización descrito, el módulo 404 de recepción está preparado para recibir un intervalo de tiempo de validez asociado a un secreto compartido y el módulo 406 de autenticación está preparado para determinar en función de un momento actual un secreto compartido válido.

Los módulos 302, 304, 306 del servidor de seguridad están preparados para poner en marcha el procedimiento para preservar la seguridad de los intercambios que se han descrito con anterioridad. Se trata, de preferencia, de módulos de programas que comprenden unas instrucciones informáticas para que se ejecuten las etapas del procedimiento de protección descrito con anterioridad, llevadas a cabo por un servidor de la red de comunicación.

La invención también se refiere, por lo tanto, a:

- un programa para servidor de una red de comunicación, que comprende unas instrucciones de programa destinadas a ordenar la ejecución de las etapas del procedimiento para preservar la seguridad de los intercambios descritos con anterioridad, cuando dicho programa lo ejecuta un procesador;
- un soporte de grabación legible por un servidor de una red de comunicación en el que se graba el programa para un servidor de una red de comunicación.

Los módulos 402, 404, 406 del nodo de la red de comunicación están preparados para poner en marcha el procedimiento para comunicar con otro nodo descrito con anterioridad. Se trata, de preferencia, de módulos de programas que comprende unas instrucciones informáticas para que se ejecuten las etapas del procedimiento para comunicar descritas con anterioridad, llevadas a cabo por un nodo de la red de comunicación.

La invención también se refiere, por lo tanto, a:

- un programa para nodo de una red de comunicación, que comprende unas instrucciones de programa destinadas a ordenar la ejecución de las etapas del procedimiento para comunicar descrito con anterioridad, cuando dicho programa lo ejecuta un procesador;
- un soporte de grabación legible por un nodo de una red de comunicación en el que se graba el programa para nodo de una red de comunicación.

Los módulos de programa se pueden almacenar en o transmitir por un soporte de datos. Este puede ser un soporte material de almacenamiento, por ejemplo un CD-ROM, un disquete magnético o un disco duro, o bien un soporte de transmisión como una señal eléctrica, óptica o de radio, o una red de telecomunicación.

La invención también se refiere a un sistema de comunicación en una red de comunicación, que comprende un servidor para preservar la seguridad de los intercambios y una multitud de nodos como los que se han descrito con anterioridad.

La descripción se ha hecho con un secreto compartido asociado a un nodo N1 proveedor de aplicación. En otra variante, también se puede compartir un secreto de este tipo en el conjunto de la red ad-hoc 2 y asociarlo al conjunto de los nodos proveedores de aplicación.

La descripción se ha hecho en el caso particular de un servidor de seguridad que comprende las dos entidades AS y TGS. También se puede prever un servidor por entidad.

La descripción también se ha hecho en el caso particular de un nodo proveedor de aplicación. Por supuesto, los

procedimientos de acuerdo con la invención se aplican a cualquier nodo destinatario con el que un nodo solicitante desea comunicarse.

La invención también se puede aplicar por medio de otros tipos de mecanismos, en los que un servidor de seguridad transmite una prueba de autenticación que hay que proporcionar mediante un nodo solicitante a un nodo proveedor de aplicación.

Los intercambios de mensajes se han descrito de forma secuencial. También se pueden disociar en el tiempo los intercambios de los mensajes M1 (petición para un acceso al nodo N1 proveedor de aplicación) y M2 (respuesta a la petición M1) de los de los mensajes M3 (petición M3 de prueba de autenticación) y M4 (respuesta a la petición M4).

En otra variante más, también se puede, si la primera clave de sesión Ksession tiene una duración de validez asociada, enviar directamente la petición M3 de prueba de autenticación.

La descripción también se ha hecho en el marco de una red ad-hoc. La aplicación de la invención no se debe restringir a este tipo de red. También se puede aplicar a cualquier tipo de red de comunicación, en el que un nodo desea establecer una ruta a través de nodos de confianza.

REIVINDICACIONES

1. Procedimiento para preservar la seguridad de los intercambios entre un nodo solicitante (N4) y un nodo destinatario (N1), perteneciendo dichos nodos a una red (2) de comunicación, comprendiendo dicho procedimiento las siguientes etapas llevadas a cabo por un servidor de seguridad (Serv):

– una etapa (F1) de recepción de una petición (M1, M3) enviada por el nodo solicitante para un acceso al nodo destinatario;

– una etapa (F7) de envío de una respuesta (M4) a la petición, comprendiendo dicha respuesta una prueba de autenticación, dirigida al nodo destinatario, y una clave de sesión, destinada a utilizarse para los intercambios entre los nodos solicitante y destinatario,

caracterizado porque, al menos un secreto, que hay que compartir con al menos otro nodo solicitante, diferente de la clave de sesión, está asociado al nodo destinatario, la respuesta enviada al nodo solicitante comprende, además, dicho secreto.

2. Procedimiento de acuerdo con la reivindicación 1, en el que la respuesta contiene, además, un intervalo de tiempo de validez asociado a dicho secreto.

3. Procedimiento para poner en contacto un nodo solicitante (N4) y un nodo destinatario (N1), perteneciendo dichos nodos a una red (2) de comunicación, comprendiendo dicho procedimiento las siguientes etapas que lleva a cabo el nodo solicitante:

– una etapa (E1) de envío de una petición (M1) a un servidor de seguridad para un acceso al nodo destinatario;

– una etapa (E4) de recepción de una respuesta (M1) a la petición, que comprende una prueba de autenticación, dirigida al nodo destinatario, y una clave de sesión, destinada a utilizarse para los intercambios entre los nodos solicitante y destinatario,

caracterizado porque la respuesta comprende, además, al menos un secreto y porque dicho procedimiento comprende, además, una etapa de autenticación de al menos otro nodo por medio de dicho al menos un secreto, siendo apto este otro nodo para comunicarse con el nodo destinatario.

4. Procedimiento de acuerdo con la reivindicación 3, en el que la respuesta contiene, además, un intervalo de tiempo de validez asociado a dicho secreto, el nodo solicitante selecciona un secreto válido en función de un momento actual.

5. Procedimiento de acuerdo con la reivindicación 3, en el que la etapa de envío de una petición de acceso a un nodo destinatario se realiza una vez detectada una ausencia de secreto válida.

6. Procedimiento de acuerdo con la reivindicación 3, en el que el nodo solicitante y el nodo destinatario se ponen en contacto mediante una ruta formada por nodos autenticados por medio del secreto.

7. Servidor (300) para preservar la seguridad de los intercambios entre un nodo solicitante y un nodo destinatario en una red de comunicación, que comprende:

– unos medios (302) de recepción de una petición enviada por un nodo solicitante para un acceso a un nodo destinatario;

– unos medios (304) de envío de una respuesta a la petición, comprendiendo dicha respuesta una prueba de autenticación, dirigida al nodo destinatario, y una clave de sesión, destinada a utilizarse para los intercambios entre los nodos solicitante y destinatario,

caracterizado porque los medios de envío están, además, preparados para incluir en la respuesta un secreto, dicho secreto, que hay que compartir con al menos otro nodo solicitante, diferente de la clave de sesión, estando asociado al nodo destinatario.

8. Nodo (400) de una red de comunicación, que comprende:

– unos medios (402) de envío de una respuesta a un servidor para un acceso a un nodo destinatario;

– unos medios (404) de recepción de una respuesta a la petición, comprendiendo la respuesta una prueba de autenticación, dirigida al nodo destinatario, y una clave de sesión, destinada a utilizarse para los intercambios entre el nodo y el nodo destinatario,

caracterizado porque los medios de recepción están, además, preparados para recibir una respuesta que comprende al menos un secreto y porque dicho nodo comprende, además, unos medios (406) de autenticación de, al menos, otro nodo por medio de dicho al menos un secreto, siendo apto este otro nodo para comunicarse con el nodo destinatario.

9. Sistema de comunicación en una red de comunicación, que comprende un servidor de acuerdo con la reivindicación 7 y una multitud de nodos de acuerdo con la reivindicación 8.

10. Programa de ordenador que consta de unas instrucciones para la puesta en marcha del procedimiento para preservar la seguridad de los intercambios de acuerdo con la reivindicación 1 mediante un servidor de una red de comunicación, cuando este programa lo ejecuta un procesador.

11. Programa de ordenador que consta de unas instrucciones para la puesta en marcha del procedimiento para comunicarse con un nodo destinatario de acuerdo con la reivindicación 3 mediante un nodo solicitante de una red de comunicación, cuando este programa lo ejecuta un procesador.

12. Señal que lleva una respuesta a una demanda de acceso a un nodo destinatario emitida por un nodo solicitante, siendo emitida dicha respuesta por un servidor en el nodo solicitante y que comprende una prueba de autenticación, dirigida al nodo destinatario, y una clave de sesión, destinada a utilizarse para los intercambios entre los nodos solicitante y destinatario, caracterizada porque dicha respuesta comprende, además, al menos un secreto, dicho secreto, que hay que compartir con al menos otro nodo solicitante, diferente de la clave de sesión, estando asociado al nodo destinatario.

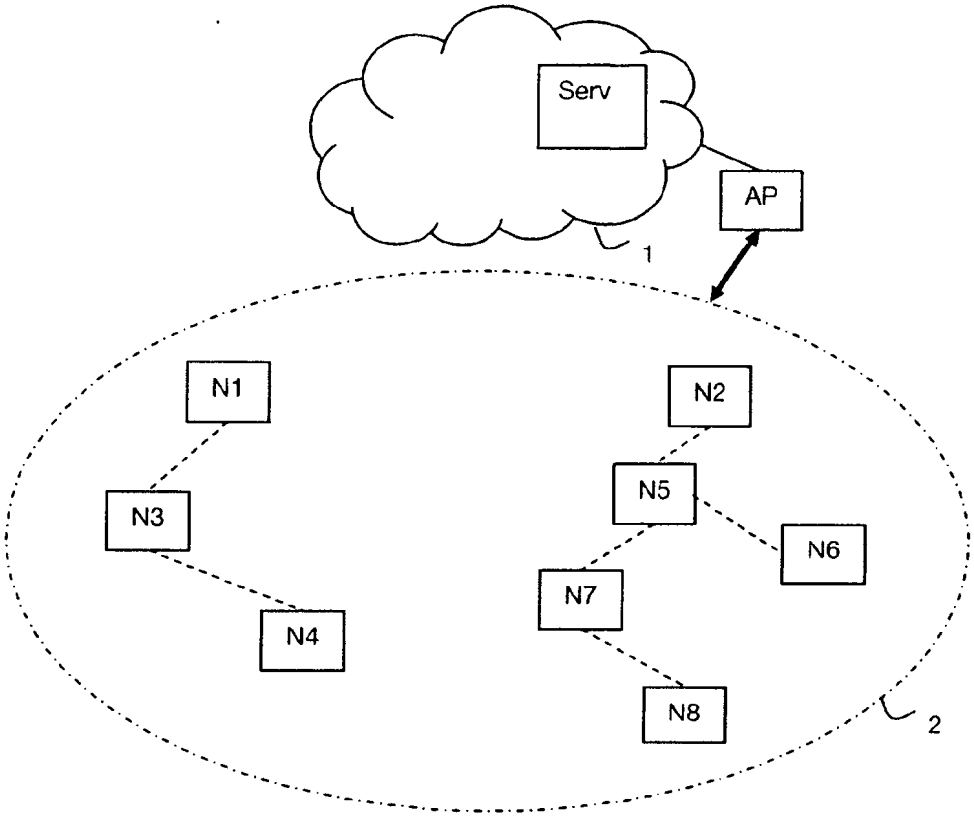

Fig 1

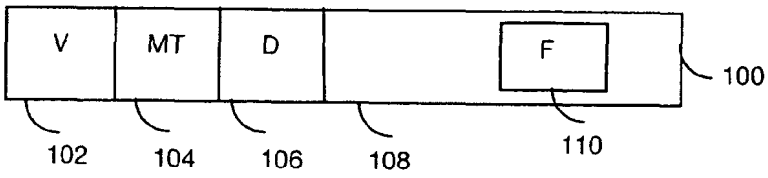

Fig 4

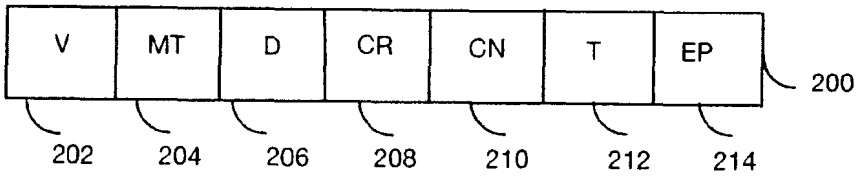

Fig 5

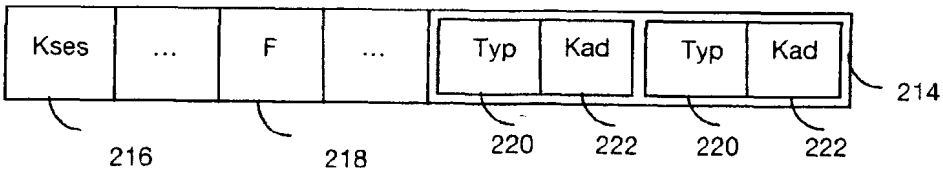

Fig 6

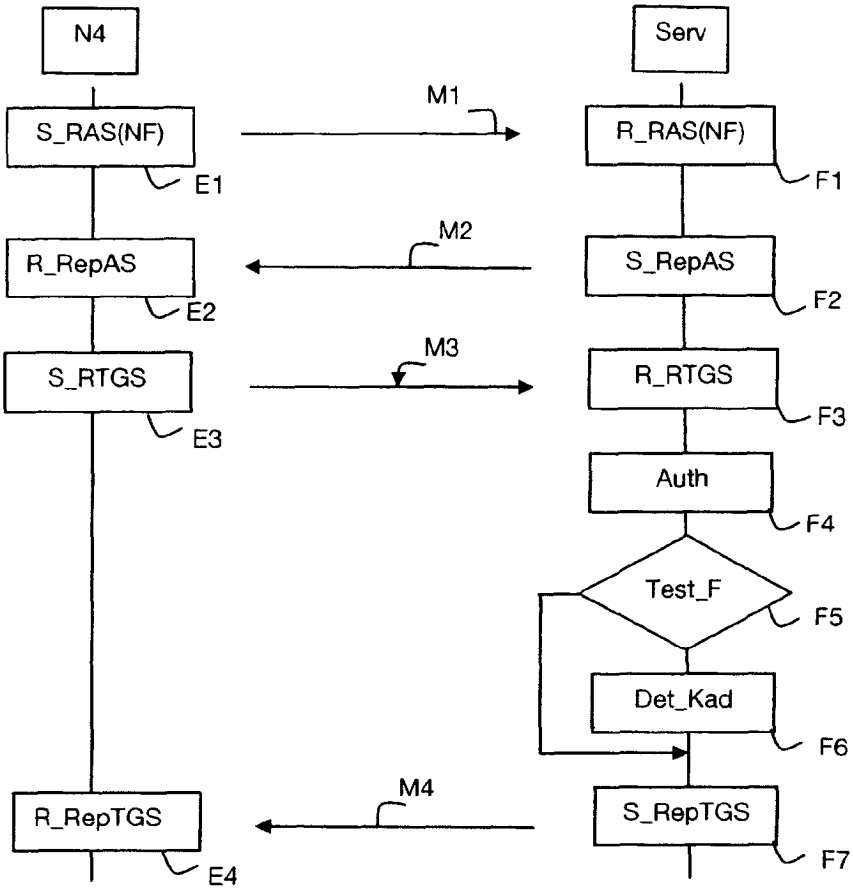
N4
Serv
M1
S_RAS(NF)
R_RAS(NF)
E1
F1
M2
R_RepAS
S_RepAS
E2
F2
M3
S_RTGS
R_RTGS
E3
F3
Auth
F4
Test_F
F5
Det_Kad
F6
M4
R_RepTGS
S_RepTGS
E4
F7

Fig 2

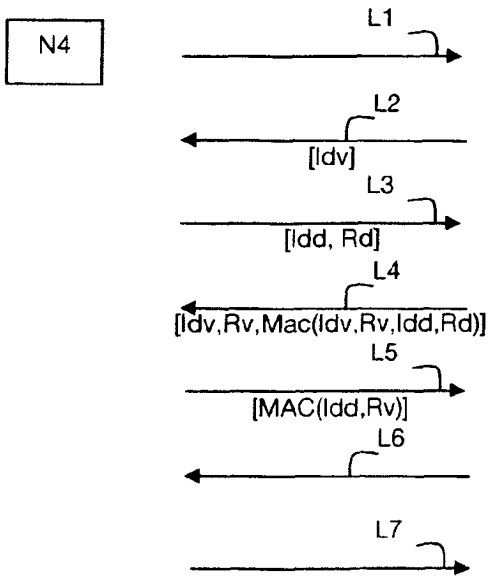
N4
N1
L1
L2
[Idv]
L3
[Idd, Rd]
L4
[Idv,Rv,Mac(Idv,Rv,Idd,Rd)]
L5
[MAC(Idd,Rv)]
L6
L7

Fig 3

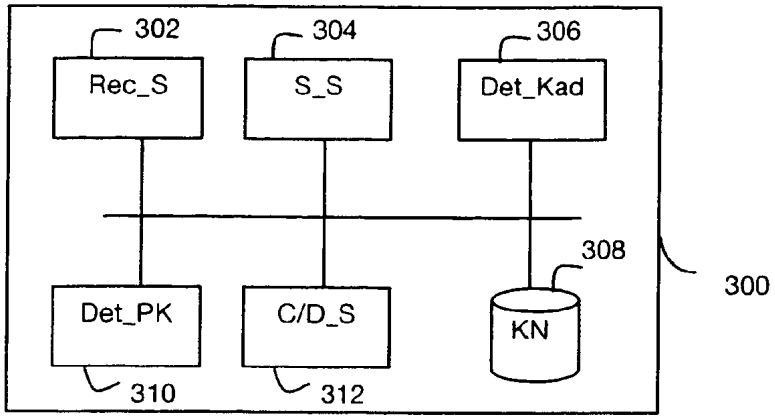
302
304
306
Rec_S
S_S
Det_Kad
308
300
Det_PK
C/D_S
KN
310
312

Fig 7

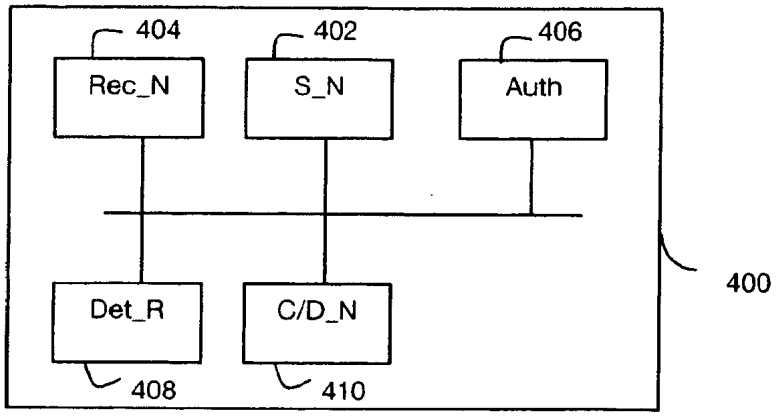
404
402
406
Rec_N
S_N
Auth
400
Det_R
C/D_N
408
410

Fig 8