(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 556 623**

(51) Int. CI.:

H04L 9/00 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.04.2007 E 07719535 (2)**

(97) Fecha y número de publicación de la concesión europea: **21.10.2015 EP 2005636**

(54) Título: **Método y aparato para proporcionar un nivel de seguridad adaptable en una comunicación electrónica**

(30) Prioridad:

13.04.2006 US 791434 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.01.2016

(73) Titular/es:

CERTICOM CORP. (100.0%)
4701 Tahoe Boulevard, Tahoe A, 6th Floor
Mississauga, Ontario L4W 0B5, CA

(72) Inventor/es:

STRUIK, MARINUS

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Método y aparato para proporcionar un nivel de seguridad adaptable en una comunicación electrónica

Sector técnico de la invención

La presente invención se refiere a un método y un aparato para proporcionar un nivel de seguridad adaptable en una comunicación electrónica.

Descripción de la técnica anterior

En las comunicaciones electrónicas, a menudo es necesario impedir que un espía intercepte un mensaje. Es deseable asimismo tener una indicación de la autenticidad de un mensaje, que es una identificación verificable del emisor. Estos objetivos se consiguen normalmente mediante la utilización de criptografía. La criptografía de clave privada requiere la compartición de una clave secreta antes de iniciar las comunicaciones. En general, se prefiere la criptografía de clave pública dado que no requiere dicha clave secreta compartida. En su lugar, cada interlocutor tiene un par de claves que incluyen una clave privada y una clave pública. La clave pública se puede proporcionar por cualquier medio adecuado, y no es necesario mantenerla secreta.

Existen muchas variaciones en los algoritmos criptográficos, y diversos parámetros que determinan la implementación precisa. En los estándares para comunicaciones inalámbricas, ha sido habitual ajustar previamente estos parámetros para cada tipo de trama. Sin embargo, este enfoque limita la flexibilidad de los parámetros.

El documento US2005/0081032 da a conocer un sistema de comunicaciones seguras en el que se negocia previamente un nivel de seguridad fijo entre las partes en comunicación.

Cuando un dispositivo está comunicando con varios dispositivos, a menudo tiene que establecer parámetros independientes para cada comunicación.

Un objetivo de la presente invención es evitar o mitigar los inconvenientes anteriores.

Compendio de la invención

En un aspecto, se da a conocer un método de preparación y provisión de una serie de tramas para transmisión, tal como se define en la reivindicación independiente 1.

En otro aspecto, se da a conocer un método de recepción de una serie de tramas, tal como se define en la reivindicación independiente 7.

Breve descripción de los dibujos

Se describirá a continuación una realización de la invención solamente a modo de ejemplo, haciendo referencia a los dibujos adjuntos en los cuales:

la figura 1 es una representación esquemática de un sistema de comunicación;

la figura 2 es una representación esquemática de una trama de información intercambiada en el sistema de comunicación de la figura 1;

la figura 3 es una representación esquemática de una parte de control de trama, de la trama de la figura 2;

la figura 4 es una representación esquemática de un método llevado a cabo por un emisor en la figura 1;

la figura 5 es una representación esquemática de un método llevado a cabo por un receptor en la figura 1;

la figura 6 es una representación esquemática de un protocolo de red utilizado en una realización del sistema de comunicación;

la figura 7 es una representación esquemática de una realización del sistema de comunicación;

la figura 8 es una representación esquemática de otra realización del sistema de comunicación;

la figura 9 es una representación esquemática de otra trama;

la figura 10 es una representación esquemática de un método llevado a cabo por un emisor utilizando la trama de la figura 9;

la figura 11 es una representación esquemática de un método llevado a cabo por un receptor utilizando la trama en la figura 9;

la figura 12 es una representación esquemática de otro sistema de comunicación; y

la figura 13 es una representación esquemática de un método llevado a cabo por un interlocutor en la figura 12.

Descripción de las realizaciones preferidas

Haciendo referencia a la figura 1, un sistema de comunicación 10 incluye un par de interlocutores 12, 14 conectados mediante un enlace de comunicación 16. Cada interlocutor 12, 14 incluye una respectiva unidad criptográfica 18, 20.

Cada interlocutor 12, 14 puede incluir un procesador 22, 24. Cada procesador puede estar acoplado a una pantalla y a dispositivos de entrada de usuario, tales como un teclado, un ratón u otros dispositivos adecuados. Si la pantalla es táctil, la propia pantalla se puede utilizar como el dispositivo de entrada del usuario. Un medio de almacenamiento legible por ordenador (no mostrado) está acoplado a cada procesador 22, 24 para proporcionar instrucciones al procesador 22, 24 y/o configurar el procesador 22, 24 para la realización de etapas o algoritmos relacionados con el funcionamiento de cada interlocutor 12, 14, tal como se explica en mayor detalle a continuación. El medio legible por ordenador puede incluir hardware y/o software tal como, solamente a modo de ejemplo, discos magnéticos, cinta magnética, un medio legible ópticamente tal como un CD-ROM y memoria de semiconductor tal como tarjetas PCMCIA. En cada caso, el medio puede adoptar la forma de un producto portátil tal como un disco pequeño, un disco flexible, un casete, o puede adoptar la forma de un producto relativamente grande o inmóvil tal como una unidad de disco duro, una tarjeta de memoria de estado sólido, o RAM dispuesta en un sistema de soporte. Cabe señalar que los medios de ejemplo enumerados arriba pueden ser utilizados por separado o en combinación.

Para transferir datos entre los interlocutores 12, 14, un flujo de paquetes 30 está montado en uno de los interlocutores de acuerdo con un protocolo definido. El flujo de paquetes 30 se muestra esquemáticamente en la figura 2 y se compone de una o varias tramas 31, cada una de las cuales tiene una cabecera 32 y datos 34. En algunos protocolos, el propio paquete puede estar organizado como una trama con una cabecera 32a y los datos 34a que consisten en una colección de tramas individuales. La cabecera 32 se compone de una cadena de bits y contiene información de control en posiciones especificadas en el interior del flujo de bits.

En cada una de las cabeceras 34 están incluidos bits de control de seguridad 33, que incluyen un bit de modo de seguridad 35 y bits de nivel de integridad 36, 37.

En esta realización, el bit de modo de seguridad 35 es utilizado para indicar si el cifrado está activado o desactivado. Los bits de nivel de integridad 36 y 37 se utilizan juntos para indicar cuál de los cuatro niveles de integridad, como son los tamaños de clave de 0, 32, 64 ó 128 bits, se utiliza. El bit de modo de seguridad 35 se puede utilizar para indicar modos alternativos de funcionamiento, tal como autenticación y el número de bits se puede aumentar (o reducir) para adaptarse a diferentes combinaciones. Se reconocerá que disponer bits de seguridad en cada trama 31 del flujo 30 permite que el nivel de seguridad esté en una base trama a trama, en lugar de estar basado en un par de interlocutores, proporcionando por lo tanto mayor flexibilidad en la organización de las comunicaciones.

Para proporcionar seguridad, se pueden utilizar ciertos niveles de seguridad mínimos. Estos niveles deberán ser adoptados entre todos los interlocutores mediante una regla acordada. Esta regla puede ser estática o bien dinámica.

En funcionamiento, el interlocutor 12 lleva a cabo las etapas mostradas en la figura 4 mediante el numeral 100 para enviar información al interlocutor 14. En primer lugar, el interlocutor 12 prepara datos y una cabecera, en la etapa 102. A continuación, selecciona el nivel de seguridad, en la etapa 104. El nivel de seguridad se determina considerando un nivel de seguridad mínimo requerido por el receptor, la naturaleza del receptor y la clase de datos que se están transmitiendo. Si el nivel de seguridad incluye cifrado, entonces el interlocutor 12 cifra los datos en la etapa 106. Si el nivel de seguridad incluye autenticación, entonces el interlocutor 12 firma los datos en la etapa 108. A continuación el interlocutor 12 incluye bits que indican el modo de seguridad y el nivel de seguridad en el control de trama en la etapa 110. El interlocutor 12 envía a continuación la trama al interlocutor 14 en la etapa 112.

Después de recibir la trama, el interlocutor 14 lleva a cabo las etapas mostradas en la figura 5 mediante el numeral 120. El interlocutor 14 recibe en primer lugar la trama en la etapa 122. A continuación extrae los bits de seguridad en la etapa 124. Si los bits de seguridad de modo 34 indican cifrado, entonces el interlocutor 14 descifra los datos en la etapa 126. Si los bits de seguridad indican autenticación, entonces el interlocutor 14 verifica la firma en la etapa 126. Finalmente, el interlocutor 14 comprueba el nivel de seguridad para asegurar que satisface requisitos mínimos predeterminados, en la etapa 128. Si falla el cifrado o la autenticación, o si el nivel de seguridad no satisface los requisitos mínimos, entonces el interlocutor 14 rechaza el mensaje, y si no fallan el cifrado ni la autenticación, y el nivel de seguridad satisface los requisitos mínimos entonces en mensajes acepta, en la etapa 130.

Se reconocerá que proporcionar bits de seguridad y un nivel de seguridad ajustable proporciona flexibilidad en la protección de cada trama de la comunicación. Por lo tanto, es posible para el emisor decidir qué tramas deberá cifrar pero no autenticar. Dado que el autenticación aumenta habitualmente la longitud de un mensaje, esto proporciona un ahorro en entornos limitados donde el ancho de banda es muy preciado.

En otra realización, el interlocutor 12 desea enviar el mismo mensaje a múltiples receptores 14 con requisitos de seguridad mínima variables. En este caso, el interlocutor 12 elige un nivel de seguridad lo suficientemente alto para satisfacer todos los requisitos. El interlocutor 12 procede a continuación tal como en la figura 4 para montar y enviar

un mensaje con el nivel de seguridad. El mensaje será aceptado por cada receptor dado que satisface cada uno de sus requisitos mínimos. Se reconocerá que esta realización proporciona mayor eficiencia que tratar por separado con los requisitos de cada receptor.

En otra realización, se utiliza un número diferente de bits de seguridad. El verdadero número de bits no se limita a ningún valor, sino que puede estar predeterminado para cualquier aplicación dada. Los bits de seguridad deberán indicar los parámetros del algoritmo. Estos pueden ser utilizados para determinar la longitud de una clave como 40 bits o 128 bits, la versión de una clave a utilizar, o cualesquiera otros parámetros del sistema de cifrado.

Se reconocerá que en las realizaciones anteriores, se puede utilizar una pila de red para organizar comunicaciones entre los interlocutores. Haciendo referencia por consiguiente a la figura 6, la pila de red del interlocutor A se muestra mediante el numeral 130. Una pila de red del interlocutor B se muestra mediante el numeral 140. Las pilas de red están organizadas en capas y tienen estructuras similares. La pila de red 130 incluye una capa de aplicación (APL) 132, una capa de red (NWK) 134, una capa de autenticación de mensajes (MAC) 136 y una capa física (PHY) 138. La pila de red 140 incluye componentes similares con numeración similar.

El emisor determina cómo desea proteger la carga útil (y dónde protegerla, es decir, qué capa). Para la capa APL, la seguridad debería ser transparente; su función se limita a indicar en qué nivel desea proteger datos (es decir, servicios de seguridad: ninguno, confidencialidad, autenticidad de datos, o ambos). El verdadero proceso criptográfico se delega entonces a las capas inferiores.

El receptor determina si acepta o no la carga útil protegida, en base a la trama recibida y a información de estado mantenida localmente. El resultado del proceso criptográfico (realizado en la misma capa que la del emisor), que incluye información sobre el nivel de protección ofrecido supuestamente, se traslada a la capa de aplicación, que determina si el nivel de protección ofrecido es adecuado. El receptor puede acusar la recepción correcta de la trama al emisor original, en base a esta "prueba de adecuación".

El acuse de recibo (ACK), si está presente, se devuelve al emisor y se eleva al nivel apropiado (si es un mensaje protegido enviado en la capa APL, entonces el ACK debería asimismo volver a dicho nivel, de manera similar para capas inferiores por supuesto).

El emisor A determina que desea proteger la carga útil m utilizando el nivel de protección indicado mediante SEC (teniendo en cuenta sus propias necesidades de seguridad y, posiblemente, las de su receptor o receptores previstos. La carga útil m y el nivel de protección deseado SEC se trasladan a continuación a una capa inferior (por ejemplo, la capa MAC, según el diagrama) que controla el propio proceso criptográfico. (Este traslado del mensaje podría incluir información de estado adicional que ayuda al procesamiento de la trama, tal como el receptor o receptores previstos, información de fragmentación, etc. Cabe señalar que la delegación del proceso criptográfico a una capa inferior es solamente una etapa conceptual si el proceso criptográfico tiene lugar en la misma capa en la que se origina la carga útil m).

El proceso criptográfico implica proteger la carga útil m y, posiblemente, información asociada tal como cabeceras de trama, utilizando el proceso criptográfico indicado mediante el nivel de protección deseado SEC. La clave utilizada para proteger esta información se obtiene a partir del material de claves compartidas mantenido entre el emisor y el receptor o receptores previstos. Después del proceso criptográfico, la trama protegida, indicada mediante [m]K, SEC en la figura 6, se comunica al receptor o receptores previstos B.

El receptor o receptores previstos recuperan la carga útil m' a partir de la trama protegida recibida, utilizando el proceso criptográfico indicado mediante el nivel de protección observado SEC, utilizando una clave que se obtiene a partir del material de claves compartidas mantenido entre el emisor y el receptor o receptores en cuestión. La carga útil recuperada m' y el nivel de protección observado SEC se trasladan al mismo nivel en el que fue originada la carga útil por el emisor, donde se determina la adecuación del nivel de protección observado. El nivel de protección observado SEC se considera suficiente si cumple o supera el nivel de protección esperado SEC_0, donde el parámetro SEC_0 puede ser un nivel de protección fijo negociado previamente que depende, o no, de la carga útil recuperada m' en cuestión. (Definir SEC_0 de manera dependiente del mensaje permitiría políticas minuciosas de control de acceso, pero generalmente involucra requisitos mayores de almacenamiento y procesamiento.)

El enfoque anterior funciona en contextos donde los niveles de protección esperado y observado se pueden comparar, por ejemplo, cuando el conjunto de niveles de protección es una ordenación parcial o cuando se lleva a cabo una prueba de pertenencia (una de un conjunto de niveles de protección). Un ejemplo es el contexto donde la protección involucra una combinación de cifrado y/o autenticación, tomando como ordenación el producto cartesiano de la ordenación natural para el cifrado (cifrado ACTIVADO < cifrado DESACTIVADO) por el orden natural de autenticación (ordenada según longitud creciente del campo de autenticidad de los datos). Además, si el conjunto de niveles de protección tiene un elemento máximo, entonces el emisor puede utilizar este nivel de protección máximo para asegurar que el mensaje (inalterado) pasa siempre la prueba de adecuación. En otro ejemplo, el nivel de protección observado se compara con SEC_0, donde SEC_0 es un conjunto de niveles de protección y no solamente un nivel de seguridad mínimo. De este modo, si SEC_0 = {ninguno, aut-32, aut-64, aut-128} y SEC = aut-32, entonces podría pasar la prueba de adecuación, mientras que si SEC_0 es igual que antes y SEC = aut-32 + confidencialidad (por ejemplo, cifrado), entonces la prueba de adecuación fallaría.

En las realizaciones anteriores, cada emisor negocia previamente el nivel de protección mínimo esperado SEC_0 con cada receptor previsto. Por lo tanto, el enfoque puede no ser tan adaptativo como es deseable para algunas aplicaciones, y puede involucrar una sobrecarga adicional de protocolo en cada cambio del parámetro SEC_0. Estos inconvenientes se pueden superar utilizando el mecanismo de acuse de recibo (ACK) desde el receptor o receptores al emisor, como un canal de retroalimentación para trasladar la información de SEC_0. Esto se lleva a cabo incorporando en cada mensaje de acuse de recibo una indicación relativa al nivel de protección esperado. Esta información puede ser recopilada a continuación por el emisor original para actualizar el nivel de protección mínimo esperado por su receptor o receptores, tanto si éste depende del mensaje como si no.

En otra realización, se muestra un método de sincronización de niveles de seguridad. Haciendo referencia a la figura 7, se muestra en general otra realización del sistema de comunicación mediante el numeral 160. El sistema incluye un emisor A 162 y receptores 168 en un grupo designado como G. El emisor incluye parámetros SEC_A 164 y SEC_G 166.

El emisor A desea comunicar de forma segura un mensaje m a un grupo G de dispositivos. El emisor A tiene acceso a los dos parámetros, por ejemplo, (1) el nivel mínimo SEC_A con el que desearía proteger este mensaje (en general, SEC_A puede depender del grupo al que envía información y del propio mensaje, de manera que una notación apropiada podría ser SEC_A (m,G)); (2) el nivel de protección mínimo SEC_G que espera el grupo G de receptores (de nuevo, la notación apropiada podría ser SEC_G (m,A) si este nivel depende del emisor y asimismo del propio mensaje). En este caso, el nivel mínimo de expectativa de un grupo es el nivel máximo sobre todos los elementos del grupo del nivel mínimo de expectativa para cada elemento del grupo.

Inicialización:

El emisor A asume que cada parámetro SEC_G está configurado al nivel de protección máximo (para cada grupo G con el que comunica de manera segura).

Uso operacional:

El emisor A determina el nivel de protección mínimo SEC_A con el que desea proteger el mensaje m. El verdadero nivel de protección SEC aplicado al mensaje m satisface tanto su propia prueba de adecuación (es decir, $SEC \geq SEC_A$) como el nivel mínimo esperado por el grupo G (es decir, $SEC \geq SEC_G$).

Cada receptor B que está en el grupo G de receptores (es decir, $B \in G$) indica en su mensaje seguro de acuse de recibo el nivel de protección mínimo esperado (para el emisor A y el mensaje m) en dicho instante de tiempo particular.

A actualiza el parámetro SEC_G de tal modo que es consistente con todos los niveles de protección mínimos indicados en cada uno de los mensajes de acuse de recibo que recibe de vuelta (es decir, $SEC_G \geq SEC_B$ para todos los dispositivos B que responden).

Cabe señalar que el procedimiento descrito anteriormente envía mensajes con un nivel de protección que satisface tanto las necesidades del emisor como las expectativas del receptor o receptores, y es adaptable a cambios en el mismo con el tiempo. Alternativamente, el emisor puede tener en cuenta solamente sus propias necesidades de protección, al precio de enviar potencialmente mensajes que serán rechazados por uno o varios receptores debido a un nivel de protección insuficiente (al ser menor que el esperado).

El procedimiento descrito anteriormente se puede generalizar en un procedimiento general de auto-sincronización para información de estado entre dispositivos en cualquier topología de red, donde la información de retroalimentación sobre información de estado se puede procesar parcialmente a lo largo del trayecto de retroalimentación desde el receptor o receptores hacia el emisor, en lugar de solamente en el propio emisor (en el ejemplo anterior, el gráfico es un árbol siendo A la raíz, y las hojas el receptor o receptores, y la sincronización involucra un parámetro de seguridad específico).

Tal como se ve en la figura 8, A envía a una carga útil asegurada con el nivel de protección SEC a un grupo de dispositivos que consisten en B1 hasta B4. Los receptores B1 a B4 proporcionan retroalimentación al emisor A sobre el nivel de protección esperado (indicado en el diagrama como los números enteros 1, 3, 2, 5, donde estos enteros están numerados en orden de nivel de protección creciente). La retroalimentación se comunica de vuelta a A por medio de nodos intermedios C1 y C2, que reúnen las retroalimentaciones respectivas de los dispositivos en sus grupos respectivos G1 y G2 y las procesan, antes de devolver al emisor A un mensaje de acuse de recibo condensado que representa ambos grupos. Las retroalimentaciones condensadas proporcionadas por estos dispositivos intermedios proporcionan a A la misma información sobre el nivel de protección mínimo que satisface las expectativas de todos los receptores, de la que hubiera sido el caso si esta información se hubiera transmitido a A sin el proceso intermedio. (En este caso, se asume que los dispositivos intermedios son fieles en sus cálculos).

En otra realización, cada trama en la comunicación está estructurada tal como se muestra en la figura 9 y se indica en general mediante el numeral 170. La trama 170 comprende en general una cabecera 172, una carga útil 174 y un

pie 176. El pie 176 comprende habitualmente uno o varios bits que representan un código de error. La carga útil 174 incluye los datos que deben ser enviados en dicha trama particular 170, por ejemplo un mensaje.

Se muestra asimismo una cabecera 172a a modo de ejemplo en mayor detalle en la figura 9. La cabecera 172a incluye un identificador 178 de clave, una representación 180 de una clave, un tipo de trama 182, un nivel de seguridad 184 (como antes) y una indicación del originador 186 del mensaje, por ejemplo el emisor 12.

Cada parte de la cabecera 172a contiene uno o varios bits que representan un cierto atributo de la transmisión o incluyen una pieza de información. El identificador 178 de la clave y la representación 180 de la clave se utilizan habitualmente para determinar, no solamente qué clave se debe utilizar sino asimismo cómo debe ser utilizada la clave, por ejemplo para comunicaciones de difusión o de unidifusión.

El tipo de trama 182 proporciona una indicación sobre qué tipo de transmisión está siendo enviada en dicha trama particular 172a. Los tipos de trama habituales 182 incluyen tramas del tipo de datos, de comando, de acuse de recibo y de baliza. Las tramas de tipo datos transmiten datos, las tramas de tipo comando transmitan comandos, las tramas de tipo acuse de recibo transmiten información de vuelta al emisor, por ejemplo un acuse de recibo procedente del receptor indicando que una trama se ha recibido adecuadamente, y las tramas de baliza se utilizan habitualmente para dividir una transmisión en intervalos de tiempo.

Para proporcionar seguridad, además de proporcionar un nivel de seguridad mínimo para el receptor 14, el emisor 12 incluye el tipo de trama 182 en la cabecera 172a. El tipo de trama 182 es utilizado por el receptor 14 para llevar a cabo una verificación de políticas con el fin de determinar si el nivel de seguridad, la clave, la utilización de la clave, etc., son adecuadas para el tipo de trama que está siendo transmitida. Por ejemplo, se rechazaría una seguridad inadecuada para un tipo de trama que debería incluir normalmente alta seguridad.

En funcionamiento, el emisor 12 lleva a cabo las etapas mostradas en la figura 10 mediante el numeral 200 para enviar información al receptor 14. En primer lugar, el emisor 12 prepara la trama en la etapa 202 en función de las etapas 102 a 110 explicadas anteriormente. Se apreciará que estas etapas incluirían asimismo la preparación de la cabecera 172a para incluir la representación de los bits mostrada en la figura 9. En la etapa 204, el emisor 12 determina el tipo de trama 182 e incluye uno o varios bits en la cabecera 172a para indicar el tipo de trama 182. El emisor 12 envía a continuación la trama 170 al receptor 14, en la etapa 206.

Tras la recepción de la trama 170, el receptor 14 lleva a cabo las etapas mostradas en la figura 11 mediante el numeral 208. El receptor 14 recibe en primer lugar la trama en la etapa 210, y a continuación lleva a cabo en la etapa 212 las etapas 124 a 126 descritas anteriormente. El receptor 14 extrae a continuación el tipo de trama 182 desde la cabecera 172a, en la etapa 214. El tipo de trama 182 se correlaciona a continuación con una política para llevar a cabo una verificación de políticas, en la etapa 216. En particular, el receptor accede a una tabla de consulta que indica una o varias políticas para cada tipo de trama. El receptor 14 determina a continuación si la política se cumple, en la etapa 218, y rechaza o bien acepta la trama 170 en la etapa 220 en base a si se cumple o no dicha política.

La verificación de políticas incluye una correlación del tipo de trama 182 con algunos otros datos, preferentemente algunos incluidos en la trama. Por ejemplo, la política puede incluir ciertas correlaciones entre tipos de clave y tipos de trama, de tal modo que en base a la representación de la clave 160 la trama se acepta o se rechaza en función de si la clave es o no aceptable para su utilización con el tipo de trama particular 182. Como resultado, se requiere un cierto tipo de clave (o de utilización de clave) para que se cumpla la política. Si la clave no es del tipo correcto, entonces la trama 170 no es aceptada por el receptor 14. Si se utiliza una única cabecera 32a para múltiples tramas 34a, tal como se muestra en la figura 2, entonces la política aplicará asimismo a las tramas restantes del mensaje.

En otro ejemplo, la política se establece en base al nivel de seguridad 184 que está incluido en la trama 170, por ejemplo el nivel de seguridad mínimo SEC_0 explicado anteriormente. La trama 170 incluye un cierto nivel de seguridad mínimo que se ha incluido en el momento en que la cabecera 172 es preparada por el emisor 12, y este nivel de seguridad mínimo se correlaciona con el tipo de trama particular 162. Si el nivel de seguridad 184 es adecuado para el tipo de trama 162, entonces la trama 170 es trasladada por el receptor en la etapa 220, y si no es rechazada. Se apreciará que la política se puede adaptar para correlacionar con cualquier información adecuada incluida en la trama con el tipo de trama 182.

Los principios anteriores permiten adaptar las verificaciones de seguridad a diversos mensajes, tipos de trama, etc., para protección frente a combinaciones de características de seguridad que son más susceptibles a un ataque. Por ejemplo, una política puede provocar que un receptor rechace una trama por no utilizar cifrado sino tan sólo autenticación, cuando dicho tipo de trama es particularmente vulnerable a un ataque cuando no se utiliza cifrado.

En general, existen tres verificaciones de nivel de seguridad que poseen diferentes niveles de granularidad. La primera es cuando SEC_0 es independiente del mensaje. En este caso, se establece una vez el nivel mínimo de seguridad, y solamente es necesario almacenar localmente un valor para llevar a cabo una verificación de políticas. Sin embargo, cuando SEC_0 es independiente del mensaje, se proporciona una granularidad mínima debido a que hay solamente un nivel de seguridad mínimo para todos los mensajes y tipos de mensajes.

La segunda es cuando SEC_0 es completamente dependiente del mensaje. En este caso, se proporciona un alto nivel de granularidad dado que cada mensaje tiene su propio nivel de seguridad mínimo. Sin embargo, esto requiere la numeración de todos los mensajes y que los correspondientes niveles de seguridad mínimos se almacenen localmente en una tabla.

La tercera es cuando SEC_0 es dependiente parcialmente del mensaje, es decir, tal como se ha comentado haciendo referencia a las figuras 9 a 11, los mensajes se dividen en diferentes tipos (por ejemplo, por tipo de trama) y se asigna un nivel de seguridad mínimo a cada tipo de mensaje. Este caso compensa los requisitos de espacio en competencia y la granularidad de llevar a cabo una verificación de políticas basada en el nivel de seguridad mínimo. Habitualmente, el número de mensajes/tipos de trama es significativamente menor que el número de mensajes/tipos de trama y por lo tanto es más factible para su implementación en una tabla.

En otra realización mostrada en la figura 12, una red N comprende uno o varios interlocutores (por ejemplo, A, B) que comunican por medio de un interlocutor central C. El interlocutor A comunica sobre la red N mediante transmitir tramas 150 al interlocutor central C utilizando, por ejemplo, cualquiera de los principios descritos anteriormente. Cuando el interlocutor A desea en primer lugar acoplarse con la red N, estos no tienen una clave y por lo tanto no se pueden autenticar para comunicar en la red N. Las etapas generales para un procedimiento de inicialización se muestran en la figura 13. El interlocutor C obtiene en primer lugar una indicación de que A desea unirse a la red N, en la etapa 224. Esta indicación se puede proporcionar por medio de un procedimiento de registro adecuado. El interlocutor C incluye a continuación a A en una tabla que indica su estado, y establece el estado para el interlocutor A como "Exento" en la etapa 226. El estado exento tiene en cuenta que se requiere un procedimiento de inicialización, de tal modo que el interlocutor puede comunicar de manera insegura hasta que ha sido inicializado en la red N.

En la etapa 228, el interlocutor A envía una trama al interlocutor central C. El interlocutor C verifica la tabla en la etapa 230. En esta primera comunicación, el estado del interlocutor A es exento y se lleva a cabo un intercambio de claves u otro procedimiento de inicialización en la etapa 232, y a continuación el estado del interlocutor A se cambia a "no exento" (o se elimina un indicador de exento, se pone a cero, etc.) en la etapa 234. El interlocutor A envía a continuación tramas al interlocutor C sometiéndose a las reglas normales de seguridad. En la etapa 230 el estado para el interlocutor A se establecerá a continuación como no exento y se aplican las reglas ordinarias de seguridad en la etapa 236, por ejemplo verificando el nivel de seguridad, el tipo de trama, etc. Se puede apreciar que A podría asimismo eximir a C de tal modo que se inviertan las funciones y A permita a C comunicar con el mismo (por ejemplo, cuando A forma parte de otra red).

En un ejemplo de implementación de la red N mostrada en la figura 12, la anterior verificación del nivel de seguridad mínimo tiene en cuenta la trama 150 y asimismo el originador 186. En este caso, el emisor es el interlocutor A y el receptor es el interlocutor B. Una verificación para el nivel de seguridad mínimo sería por lo tanto $SEC \geq SEC_B(m, A)$. Si el nivel de seguridad mínimo es independiente del originador A, esto se reduce a $SEC \geq SEC_B (m)$, tal como se ha explicado anteriormente. Se utilizarían entonces las mismas consideraciones de almacenamiento que con la verificación del nivel de seguridad original (caso 1).

Si el nivel de seguridad mínimo depende completamente del originador A, se numera una tabla de niveles de seguridad mínimos (en función de la trama m, del tipo de trama de m, o dependiendo del mensaje (tal como se ha descrito anteriormente)), pero en este caso para cada originador (caso 2). Si el nivel de seguridad mínimo es independiente del originador A, excepto cuando el originador está en un conjunto explícitamente numerado de dispositivos exentos, por ejemplo indicado mediante Conjunto Exento ("ExemptSet") en la tabla, se implementa un único nivel de seguridad mínimo para dispositivos fuera del Conjunto Exento (que potencialmente dependen del tipo de trama, etc.) y, adicionalmente, se implementa una tabla de niveles de seguridad mínimos para cada elemento individual del Conjunto Exento (caso 3). Por lo tanto, si un interlocutor (y el dispositivo asociado con el mismo) es parte de la tabla Conjunto Exento, se utiliza el caso 2, y sin ningún dispositivo está en la tabla Conjunto Exento, se utiliza el caso 1.

El caso 3 se puede hacer de implementación más amigable si para los interlocutores en la tabla Conjunto Exento, se utiliza una tabla de niveles de seguridad mínimos que es independiente del dispositivo particular en el Conjunto Exento. Esto requiere que se implemente una tabla de niveles de seguridad para dispositivos que no están en la tabla de Conjunto Exento, y que se implemente una tabla para los dispositivos que están en la tabla del Conjunto Exento (caso 4).

Otra optimización adicional de este caso 4 es cuando, para todos los dispositivos de la tabla Conjunto Exento, el nivel de seguridad mínimo (que potencialmente depende del mensaje o del tipo de mensaje (tal como se ha explicado anteriormente)) se configura al nivel de seguridad mínimo que aplica a todos los dispositivos que están fuera del Conjunto Exento o bien se configura a un valor especificado previamente que puede aplicar a todos los dispositivos en el interior del Conjunto Exento. Dado que esto conduciría a solamente dos opciones (por ejemplo, por trama, tipo de trama, global), esto se puede indicar utilizando un parámetro booleano.

En resumen:

$SEC \geq SEC_B (m, A))$, donde

- SEC_B (m, A))= SEC_B (m) si A no es un elemento del Conjunto Exento.
- SEC_B (m, A))= SEC_B (m) si A es un elemento del Conjunto Exento y el parámetro de anular OverrideSEC(m) para el mensaje M está configurado a FALSO.
- SEC_B (m, A))= $ExemptSEC_B$ (m) si A es un miembro del Conjunto Exento y el parámetro de anular OverrideSEC(m) para el mensaje m está configurado a VERDADERO.

En general, el escenario más práctico es cuando $ExemptSEC_B$(m) está configurado a 'sin seguridad'.

Cabe señalar que un escenario permite que los dispositivos que todavía no tienen una clave (por ejemplo, debido a que se acaban de unir a la red y aún tienen que configurar una clave, por ejemplo, mediante un protocolo de acuerdo de claves o de transporte de claves o PIN o cualquier otro mecanismo) "omitan" la verificación del nivel de seguridad mínimo (es decir, la verificación de seguridad siempre tiene éxito), si estos han sido etiquetados mediante el receptor B como pertenecientes al Conjunto Exento (y $ExemptSEC_B$(m) se configura como 'sin seguridad').

La omisión de las verificaciones del nivel de seguridad mínimo puede depender del mensaje m recibido, del tipo de trama del mensaje m (que es visible para el receptor si el tipo de trama de m está incluido en la trama transmitida (normalmente los tipos de trama y otra información de control de tramas no está cifrada)), o de un parámetro que se puede configurar a través del parámetro de anulación OverrideSEC(m).

Cabe señalar asimismo que las operaciones en el Conjunto Exento mediante el receptor dirigen de manera efectiva el funcionamiento de la verificación del nivel de seguridad mínimo (la inclusión de un dispositivo en dicho conjunto puede permitir la omisión, o requisitos de seguridad rebajados, mientras que la exclusión de un dispositivo respecto de dicho conjunto restablece la verificación ordinaria del nivel de seguridad mínimo y la hace aplicable (posiblemente de nuevo) al dispositivo de origen en cuestión).

Por lo tanto, lo anterior permite un mecanismo flexible para tener en cuenta el comportamiento transitorio de un interlocutor (y su dispositivo) durante el tiempo de vida del sistema, y facilita la transgresión de un dispositivo desde alguna fase inicial en la que todavía no tiene una clave, hasta la fase en la que ha establecido una clave y puede ser forzado a adherirse a las políticas estrictas normales del nivel de seguridad mínimo.

El parámetro de anulación OverrideSEC(m) permite el ajuste fino de la "omisión" de la verificación del nivel de seguridad mínimo, y la hace dependiente del mensaje m recibido (o del tipo de mensaje (obviamente, se puede hacer la granularidad tan fina como sea posible, al precio del coste de implementación de las tablas)). Como ejemplo, en el escenario en el que un dispositivo se une a una red y todavía tiene que configurar una clave, se podría poner el parámetro de anular a VERDADERO solamente para aquellos mensajes o tipos de mensajes mínimos necesarios para que el dispositivo de origen A establezca una clave con el dispositivo receptor B (o con algún otro dispositivo T en la red que podría notificar a B una vez que ha sido establecida la clave), limitando de ese modo el comportamiento permisible del dispositivo A, pero no descartando todos los comportamientos. Esto se puede utilizar asimismo para cualquier otro procedimiento de inicialización o procedimiento de establecimiento y no se deberá limitar al establecimiento de claves.

De nuevo, las operaciones sobre el parámetro de anulación Anular(m) mediante el receptor B permiten un ajuste fino de políticas de control de seguridad, muy flexible y a coste reducido. A modo de ejemplo, poniendo todos los parámetros de anular a FALSO se cierran de manera efectiva todas las operaciones en la red a los dispositivos que no tienen una clave (dado que todos los mensajes no seguros criptográficamente hacia el receptor B serán rechazados en última instancia) (el denominado modo oculto) mientras que poner a VERDADERO todos los parámetros de anular permite flujos ilimitados de información no segura hacia el dispositivo B, dado que esto puede tener como resultado que se omita de manera efectiva la prueba de nivel de seguridad mínimo.

Se reconocerá que las reglas de seguridad se pueden adaptar para proporcionar flexibilidad no sólo trama a trama, sino asimismo en base al tipo de trama, de tal modo que una verificación de políticas puede determinar si pueden ser utilizadas ciertas reglas de seguridad o tipos de clave con un tipo de trama particular.

Aunque la invención se ha descrito haciendo referencia a ciertas realizaciones específicas, algunas modificaciones de las mismas resultarán evidentes para los expertos en la materia.

REIVINDICACIONES

1. Un método, comprendiendo el método:

un dispositivo de comunicación (12) que prepara una serie de tramas para su transmisión a un dispositivo receptor (14), teniendo cada trama una cabecera (32), datos (34) y una serie de características de seguridad;

que dicho dispositivo de comunicación procese trama a trama cada trama mediante:

determinar un tipo de trama de dicha trama en base a un tipo de transmisión que se está enviando en dicha trama, donde dicho tipo de trama tiene asociada con el mismo una política que indica características de seguridad adecuadas para dicho tipo de trama; e

incluir datos del tipo de trama en dicha cabecera, indicando los datos de tipo de trama, en base a dicho tipo de trama, el tipo de transmisión;

donde dicho tipo de trama es uno de una serie de tipos de trama predeterminados, incluyendo la serie de tipos de trama predeterminados dos o más de tipo de datos, tipo de comandos, tipo de acuse de recibo y tipo de baliza, incluyendo la cabecera una representación de una clave y una indicación de un nivel de seguridad; y

dotar a dicha trama de dichas características de seguridad, y proporcionando dicho dispositivo de comunicación la serie de tramas para su transmisión al dispositivo receptor.

2. El método según la reivindicación 1, en el que el dispositivo de comunicación proporciona la serie de tramas para transmisión, por lo menos, a un dispositivo receptor, la política comprende una política de dicho por lo menos un dispositivo receptor, y el método comprende además que dicho por lo menos un dispositivo receptor:

reciba la serie de tramas;

para cada trama, determine dicho tipo de trama a partir de dicha cabecera de dicha trama; y

para cada trama, correlacione el tipo de trama con una política y determine si se cumple la política.

3. El método según cualquier reivindicación anterior, en el que dicha preparación comprende, para cada trama, seleccionar un nivel de seguridad para dicha trama, e incorporar uno o varios bits de seguridad en dicha trama indicativos de dicha seguridad.

4. El método según la reivindicación 3, que comprende alguno o ambos de: cifrar dichos datos de dicha trama, y firmar dichos datos de dicha trama, según dicho nivel de seguridad.

5. El método según cualquier reivindicación anterior, en el que cada trama comprende además un pie que comprende uno o varios bits que representan un código de error.

6. El método según cualquier reivindicación anterior, en el que dicha cabecera para cada trama comprende un identificador de clave, una representación de una clave correspondiente a dicho identificador de clave, un nivel de seguridad y un originador para determinar la aceptabilidad de dicho tipo de trama.

7. Un método, comprendiendo dicho método:

un dispositivo receptor (14) que recibe una serie de tramas, teniendo cada trama una cabecera (32), datos (34) y una serie de características de seguridad, incluyendo la cabecera de cada trama:

datos de tipo de trama que indican un tipo de transmisión enviada en dicha trama;

una representación de una clave; y

una indicación de un nivel de seguridad; y

para cada trama, que dicho dispositivo receptor:

identifique un tipo de trama de la trama en base al tipo de transmisión indicada mediante los datos del tipo de trama en la cabecera de la trama, donde dicho tipo de trama es uno de una serie de tipos de trama predeterminados, incluyendo la serie de tipos de trama predeterminados dos o más de tipo de datos, tipo de orden, tipo de acuse de recibo y tipo de baliza; y

correlacione el tipo de trama con una política y determine si la política se cumple.

8. El método según las reivindicaciones 2 ó 7, que comprende además, para cada trama, que dicho dispositivo receptor acepte dicha trama si se cumple dicha política, y rechace dicha trama de lo contrario.

9. El método según cualquier reivindicación anterior cuando depende de la reivindicación 2 ó 7, en el que dicha política indica tipos de trama vulnerables a un ataque donde están presentes una o varias combinaciones de características de seguridad de dicha trama, comprendiendo dicho método rechazar dicha trama si se encuentra una de dichas combinaciones.

10. El método según las reivindicaciones 2 ó 7, en el que dicho nivel de seguridad proporciona una indicación de un nivel de seguridad mínimo aceptable y dicho nivel de seguridad mínimo aceptable es independiente de dichos datos de dicha trama.

11. El método según las reivindicaciones 2 ó 7, en el que dicho nivel de seguridad proporciona una indicación de un nivel de seguridad mínimo aceptable y dicho nivel de seguridad mínimo aceptable depende de dichos datos de dicha trama.

12. El método según las reivindicaciones 2 ó 7, en el que dicho nivel de seguridad proporciona una indicación de un nivel de seguridad mínimo aceptable, y dicho nivel de seguridad mínimo aceptable depende parcialmente de los datos, de tal modo que dicho nivel de seguridad mínimo aceptable puede diferir según dicho tipo de trama para dicha trama.

13. El método según las reivindicaciones 2 ó 7, en el que cada trama incluye datos de seguridad indicativos de un nivel de seguridad, y dicho método comprende que dicho dispositivo receptor utilice dichos bits de datos de seguridad para determinar dicho nivel de seguridad, donde dicha política indica si dicho tipo de trama para dicha trama es o no aceptable para dicho nivel de seguridad.

14. El método según la reivindicación 13, en el que dichos datos para dicha trama han sido uno o ambos de cifrados y firmados, comprendiendo dicho método que dicho dispositivo receptor descifre dichos datos y/o autentique dichos datos, para dicha trama según dichos bits de seguridad.

15. El método según las reivindicaciones 2 ó 7, en el que dicha política comprende una tabla de consulta que correlaciona dichos tipos de trama con atributos de dicha serie de tramas.

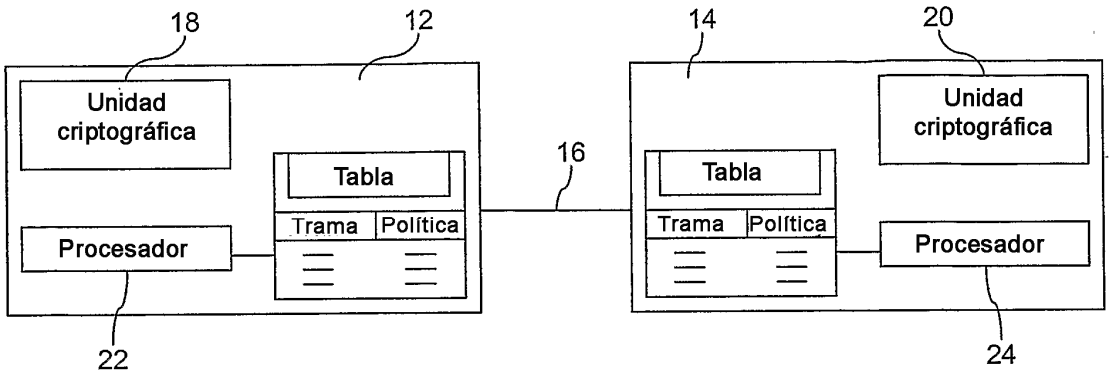

Figura 1

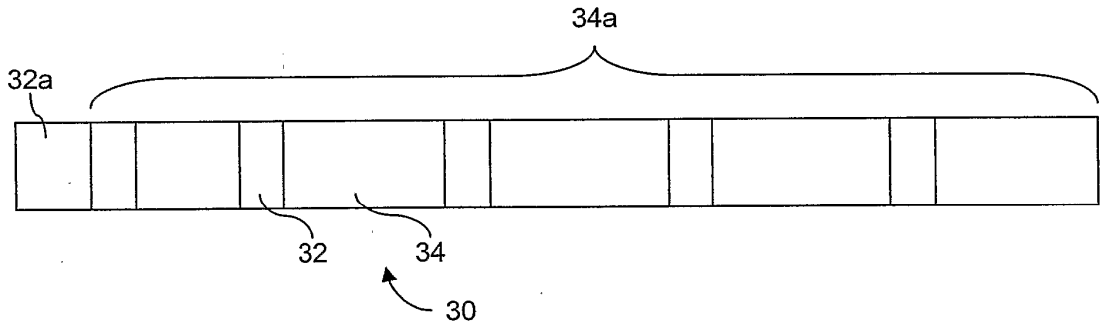

Figura 2

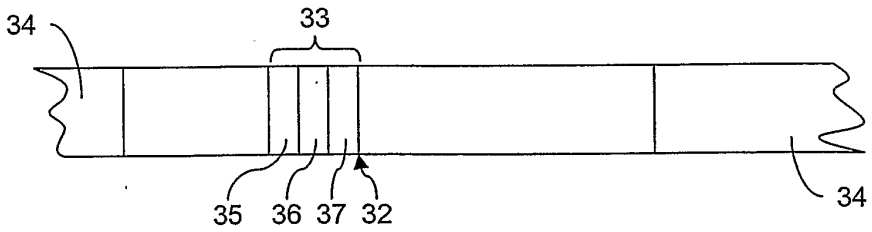

Figura 3

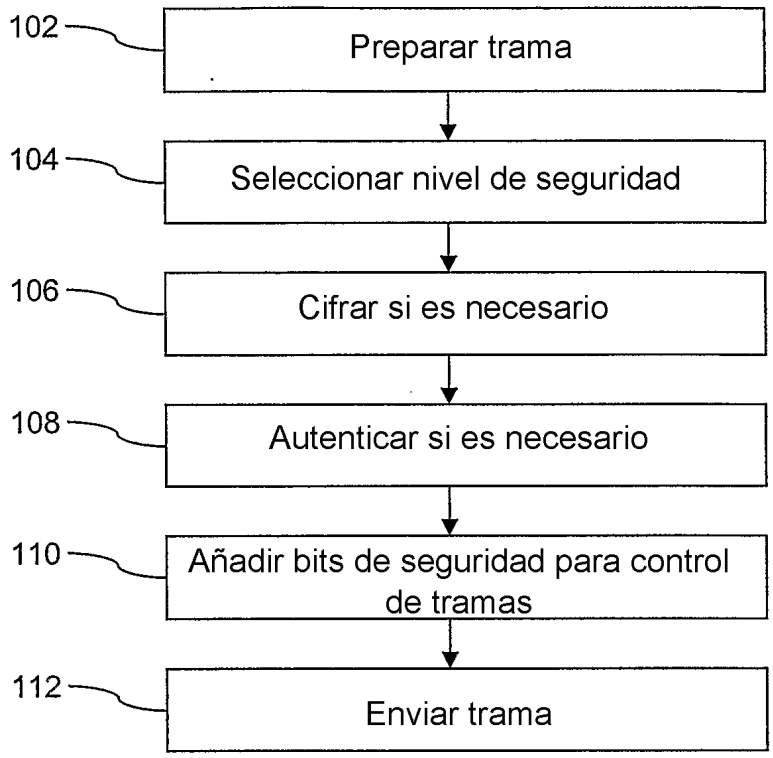
102
Preparar trama
104
Seleccionar nivel de seguridad
106
Cifrar si es necesario
108
Autenticar si es necesario
110
Añadir bits de seguridad para control de tramas
112
Enviar trama
110

Figura 4

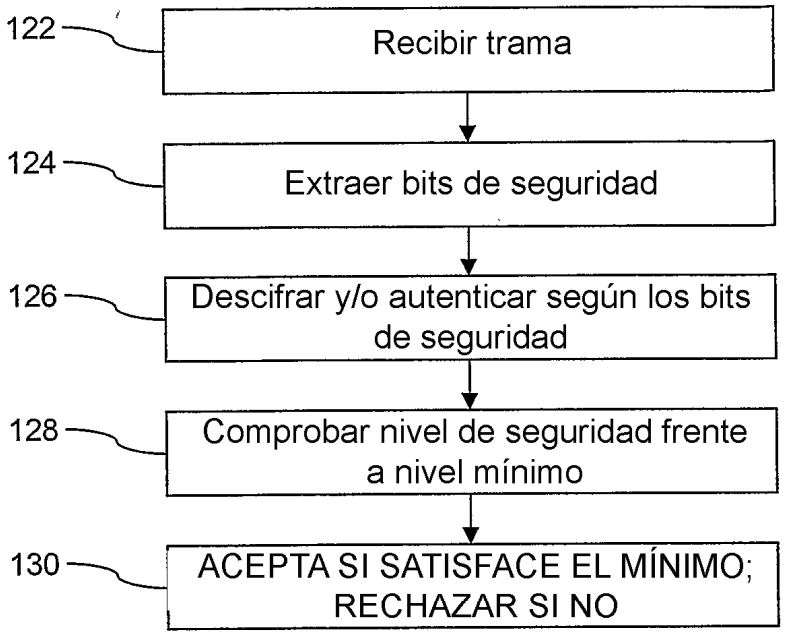
122
Recibir trama
120
124
Extraer bits de seguridad
126
Descifrar y/o autenticar según los bits de seguridad
128
Comprobar nivel de seguridad frente a nivel mínimo
130
ACEPTA SI SATISFACE EL MÍNIMO; RECHAZAR SI NO

Figura 5

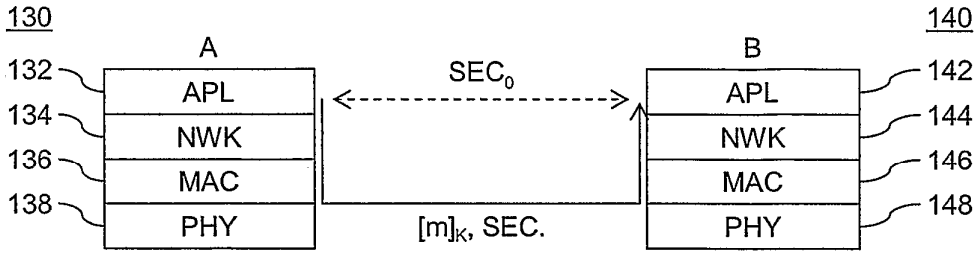

Figura 6

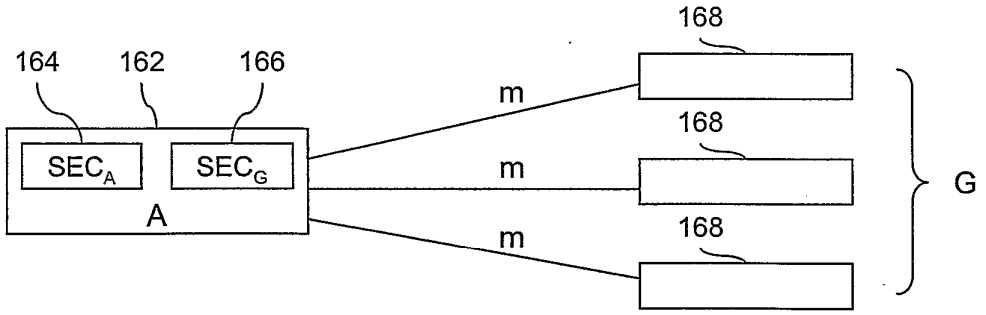

Figura 7

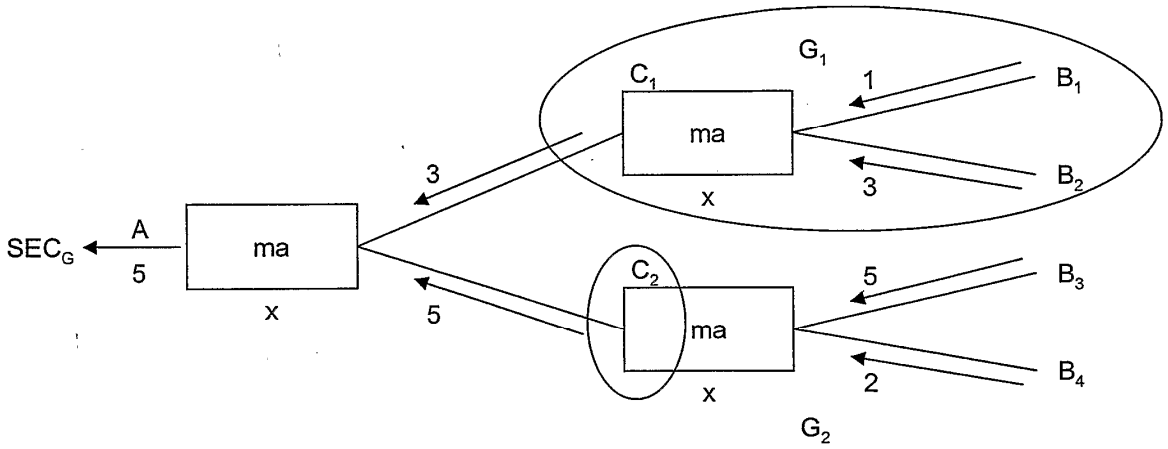

Figura 8

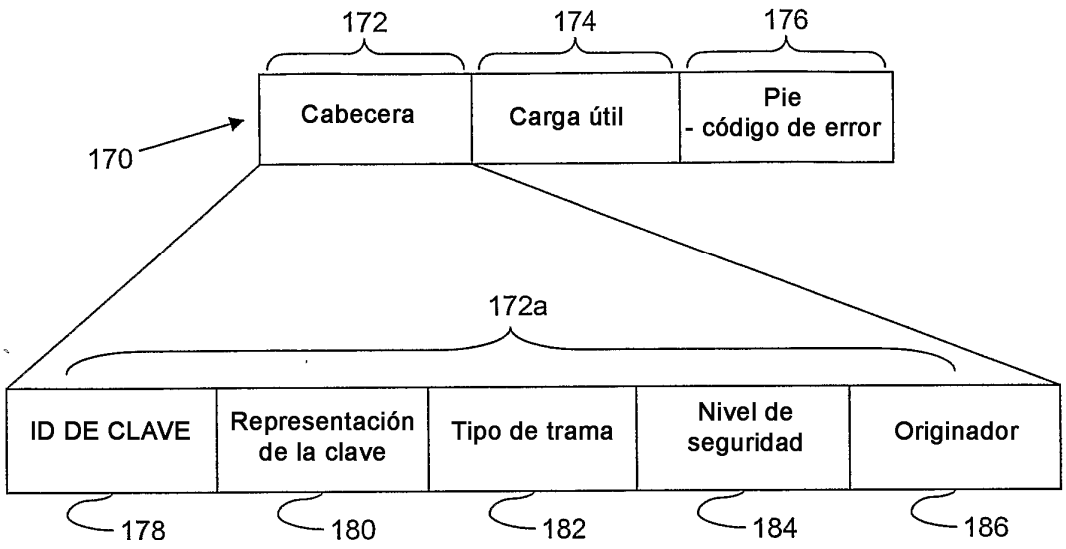

Figura 9

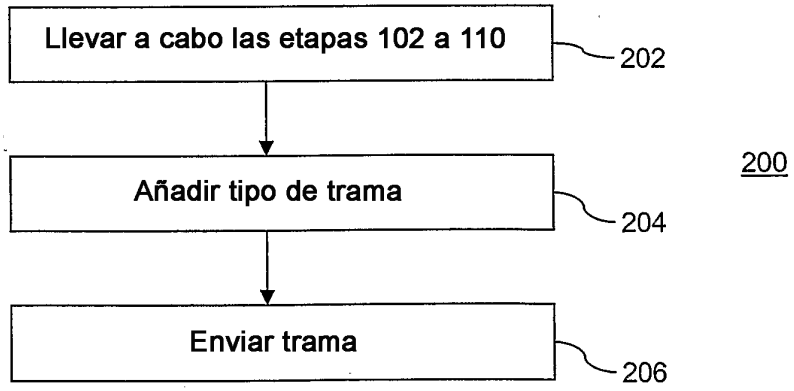

Figura 10

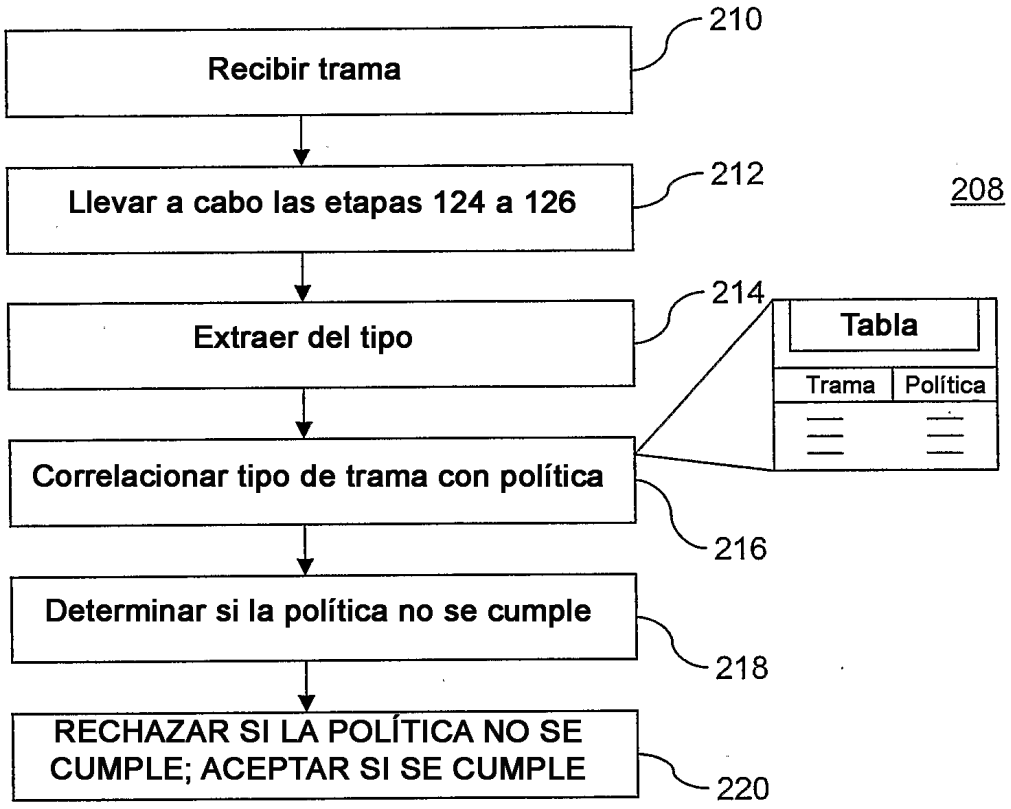
Recibir trama
210
Llevar a cabo las etapas 124 a 126
212
208
Extraer del tipo
214
Tabla
Trama
Política
Correlacionar tipo de trama con política
216
Determinar si la política no se cumple
218
RECHAZAR SI LA POLÍTICA NO SE CUMPLE; ACEPTAR SI SE CUMPLE
220

Figura 11

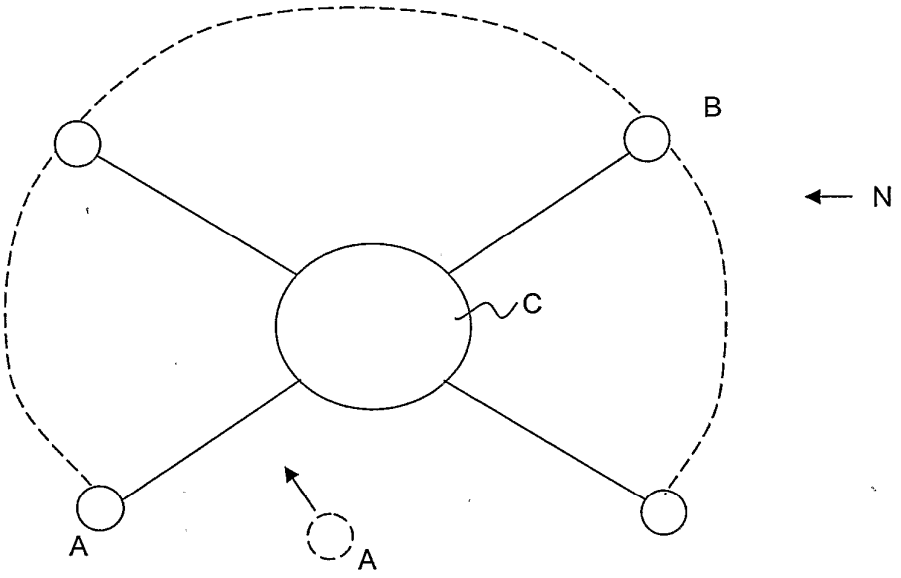

Figura 12

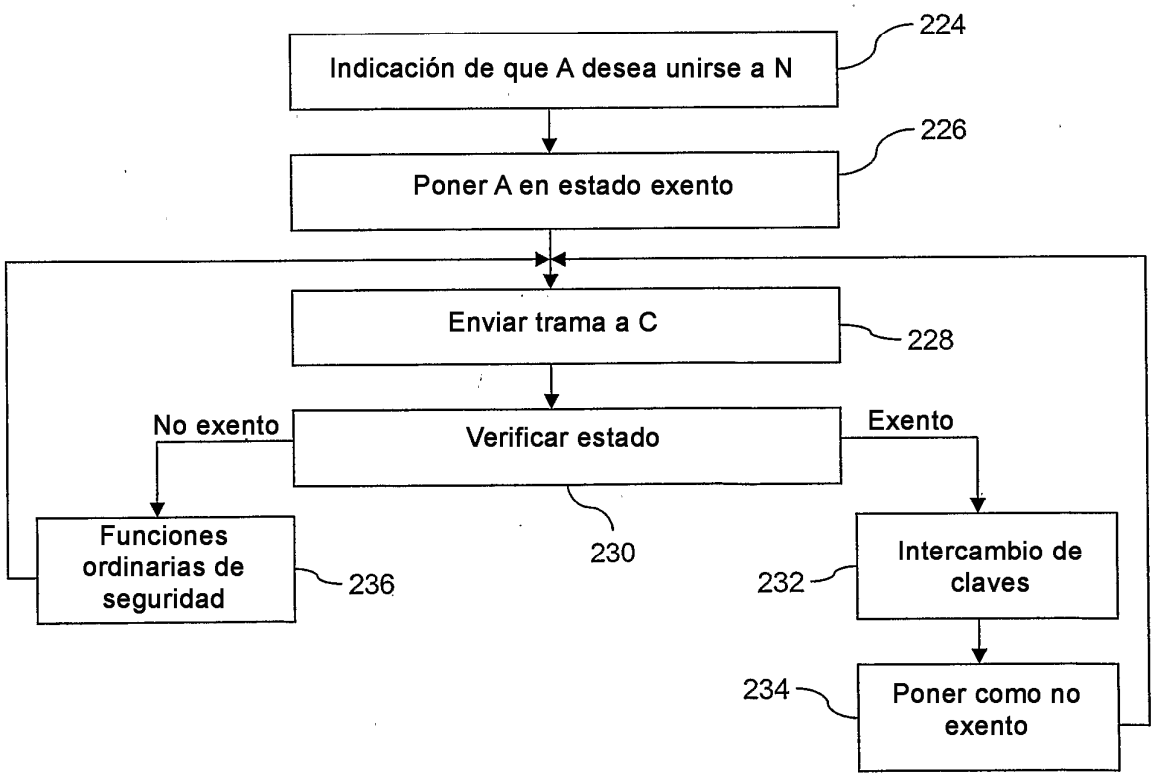

Figura 13