(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 710 279**

(51) Int. CI.:

H04L 12/46 (2006.01)
H04L 12/66 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.12.2011 E 11306713 (6)**

(97) Fecha y número de publicación de la concesión europea: **07.11.2018 EP 2469771**

(54) Título: **Procedimiento y dispositivo de transmisión de datos entre dos redes seguras de tipo Ethernet a través de una red enrutada**

(30) Prioridad:

22.12.2010 FR 1005041

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.04.2019

(73) Titular/es:

THALES (100.0%)
45, rue de Villiers
92200 Neuilly Sur Seine, FR

(72) Inventor/es:

ECH-CHERGUI, BEN YOUCEF

(74) Agente/Representante:

SALVÀ FERRER, Joan

DESCRIPCIÓN

Procedimiento y dispositivo de transmisión de datos entre dos redes seguras de tipo Ethernet a través de una red enrutada

[0001] La presente invención se refiere a un procedimiento de transmisión de datos en un canal de comunicación entre al menos una red de salida y una red de destino a través de una red de tránsito de un nivel de seguridad diferente de las redes de salida y de destino, que comprende, durante una transmisión, la red de salida hacia la red de destino a través de la red de tránsito, de datos comprendidos en al menos una trama de una capa de conexión de datos, la trama comprendiendo al menos un encabezamiento y una carga útil:

- una etapa de encapsulación de la trama en al menos un paquete de una capa de red de nivel 3 del modelo OSI, compatible con la red de tránsito, y
- una etapa de transmisión del o de cada paquete hacia la red de destino a través de la red de tránsito.

[0002] Se aplica en particular a la transmisión de datos entre dos redes conmutadas seguras, por ejemplo, dos redes Ethernet de una empresa, a través de una red enrutada pública, por ejemplo, la red Internet.

[0003] En el seno de una red segura conmutada tal como una red de tipo Ethernet, los datos son intercambiados entre los diferentes terminales en forma de tramas de la capa 2 del modelo OSI, es decir la capa de conexión, por ejemplo, según el protocolo Ethernet. Tales tramas no pueden circular tal cual en una red pública enrutada, por ejemplo en una red de tipo IP, ya que no comprenden ninguna información de nivel 3 del modelo OSI, es decir, de la capa red de este modelo.

[0004] Este aislamiento, aunque permite asegurar que ningún dato sensible salga de la red segura y no transite en una red externa de nivel de seguridad más reducido, impide igualmente el intercambio de datos entre dos redes seguras distantes, por ejemplo, entre dos redes seguras distantes de una misma empresa, a través de una red de tránsito enrutada.

[0005] Se conoce, a partir del documento WO 2008/039468 A2, un procedimiento de encapsulación de tramas Ethernet en unas tramas Ethernet seguras, de manera que se asegure el intercambio de estas tramas Ethernet entre dos redes de tipo Ethernet a través de una red de tránsito igualmente de tipo Ethernet.

[0006] No obstante, este procedimiento no permite el intercambio de tramas Ethernet a través de una red enrutada, ya que las tramas Ethernet seguras obtenidas no comprenden ninguna información de nivel 3. Además, la protección aportada a las tramas Ethernet por este procedimiento no permite suministrar una anonimización de los intercambios entre las dos redes Ethernet, las identidades de los terminales fuente y destino de estos intercambios permanecen visibles. Este procedimiento ya no permite proteger las tramas intercambiadas contra unos ataques procedentes de la red de tránsito, especialmente contra unos ataques sobre el encabezamiento de encapsulación que comprende unos datos de seguridad. Tales ataques pueden accionar una indisponibilidad en los flujos impidiendo así que dos redes protegidas se intercambien datos.

[0007] Para permitir un intercambio seguro entre dos redes conmutadas seguras a través de una red enrutada pública, se conoce la colocación, en cada una de las redes conmutadas, de un encriptador y la colocación entre estos dos encriptadores de una arquitectura específica, destinada a crear una subred virtual entre estos dos encriptadores, comunicándose los dos encriptadores como si estuviesen en una misma red Ethernet. No obstante, esta solución es muy restrictiva en términos de empleo y muy costosa. Especialmente, tal arquitectura permite únicamente crear una conexión punto-a-punto entre dos encriptadores como máximo e impone la creación de una infraestructura específica entre estos dos encriptadores.

[0008] La invención tiene por tanto como objeto permitir un intercambio seguro entre al menos dos redes conmutadas distantes a través de una red enrutada de nivel de seguridad más reducido, cuya colocación sea a la vez menos costosa y más flexible que los intercambios según el estado de la técnica.

[0009] Con este fin, la invención tiene como objeto un procedimiento de transmisión del tipo precitado, caracterizado porque el o cada paquete es un paquete seguro y porque la etapa de encapsulación comprende las etapas siguientes:

- generación de al menos un encabezamiento de encapsulación de seguridad,
- formación de al menos un paquete de encapsulación que comprende al menos el o uno de los encabezamiento(s) de encapsulación de seguridad y dicha trama o un fragmento de dicha trama,
- formación del o de cada paquete seguro por aplicación de al menos una protección criptográfica al o a cada paquete de encapsulación.

[0010] El procedimiento de transmisión según la invención consta igualmente de las características

siguientes, tomadas de forma separada o en combinación:

- la etapa de encapsulación comprende además una etapa de anonimización del o de cada paquete seguro, que comprende un ajuste de la longitud del o de cada paquete seguro (P_{sec}) a una longitud predefinida,
- el procedimiento de transmisión comprende, además, durante una transmisión de al menos una trama de una capa de conexión de datos de la red de salida hacia la red de destino a través de la red de tránsito, antes de dicha etapa de encapsulación:

  - una comparación de un tamaño de la trama con un tamaño máximo predefinido,
  - si el tamaño de la trama es superior al tamaño máximo predefinido, una fragmentación de la trama en al menos dos fragmentos de trama, siendo el tamaño de cada fragmento de trama inferior o igual al tamaño máximo predefinido,

- el procedimiento de transmisión comprende además la generación de al menos un campo de fin, comprendiendo el o cada paquete de encapsulación al menos el o uno de los encabezamiento(s) de encapsulación de seguridad, la trama o un fragmento de la trama y el o uno de los campo(s) de fin,
- el o cada campo de fin comprende unos datos de atasco, siendo escogida la longitud de los datos de atasco de tal modo que la longitud del o de cada paquete seguro sea igual a dicha longitud predefinida,
- el procedimiento de transmisión comprende, además, durante una transmisión de al menos un paquete seguro de la red de tránsito hacia la red de destino, al menos una etapa de recepción del o de cada paquete seguro y una etapa de transmisión de dichos datos a dicha red de destino, comprendiendo la o cada etapa de recepción:

  - una verificación criptográfica del paquete de encapsulación comprendido en dicho paquete seguro,
  - una extracción de la trama o del fragmento de trama comprendido en dicho paquete de encapsulación,
  - el procedimiento de transmisión comprende, si al menos dos paquetes de encapsulación comprenden un fragmento de dicha trama, un ensamblaje de los fragmentos de la trama comprendido en los paquetes de encapsulación, antes de la etapa de transmisión de dichos datos a dicha red de destino,
  - dicha trama es una trama Ethernet, y
  - dicho paquete seguro comprende un paquete seguro según un protocolo IPsec.

[0011] La invención tiene igualmente como objeto un dispositivo de transmisión de datos en un canal de comunicación entre al menos una red de salida y una red de destino a través de una red de tránsito de un nivel de seguridad diferente de las redes de salida y de destino, que comprende:

- unos medios de encapsulación, aptos para encapsular una trama de una capa de conexión de datos, que comprenden al menos un encabezamiento y una carga útil, en al menos un paquete de una capa de red compatible con la red de tránsito, y
- unos medios para transmitir el o cada paquete hacia la red de destino a través de la red de tránsito,

estando el dispositivo caracterizado porque el o cada paquete es un paquete seguro y porque dichos medios de encapsulación comprenden:

- unos medios para generar al menos un encabezamiento de encapsulación de seguridad,
- unos medios para formar al menos un paquete de encapsulación que comprende al menos el o uno de los encabezamiento(s) de encapsulación de seguridad y dicha trama o un fragmento de dicha trama,
- unos medios para formar el o cada paquete seguro por aplicación de al menos una protección criptográfica al o a cada paquete de encapsulación.

[0012] La invención se comprenderá mejor con respecto a ejemplos de realización de la invención que se van a describir ahora haciendo referencia a las figuras anexas entre las que:

- la figura 1 es un esquema que ilustra la arquitectura global de redes adaptadas a la aplicación del procedimiento según la invención;
- la figura 2 es un esquema de un dispositivo de transmisión según un modo de realización de la invención;
- la figura 3 es un esquema sinóptico que ilustra unas etapas de procedimiento según un modo de realización de la invención, aplicadas por el dispositivo de transmisión de la figura 2;
- la figura 4 es un esquema que ilustra la estructura de un paquete seguro tal como ha sido emitido por el dispositivo de transmisión de la figura 2; y
- la figura 5 es un esquema sinóptico que ilustra otras etapas del procedimiento según un modo de realización de la invención, aplicadas por un dispositivo de transmisión tal como se representa en la figura 2.

[0013] Se ha representado en la figura 1 la arquitectura global de redes adaptadas a la aplicación del procedimiento según un modo de realización de la invención.

[0014] Unas redes de telecomunicación seguras N1 y N3, denominadas posteriormente respectivamente

redes de salida y de destino, son aptas para comunicar a través de una red de tránsito N2, de nivel de seguridad más reducido que las redes seguras N1 y N3.

[0015] Las redes seguras N1 y N3 son por ejemplo unas redes internas de empresa, es decir unas redes locales, que comprenden cada una varios equipos informáticos. En el seno de cada una de estas redes, estos equipos son aptos para intercambiarse datos de manera segura, según un protocolo de red local de la capa 2 de conexión del modelo OSI, por ejemplo, según el protocolo Ethernet.

[0016] La red de tránsito N2 es una red enrutada de nivel de seguridad más reducido que las redes seguras N1 y N3, por ejemplo, una red pública como Internet, en la que los datos transitan según un protocolo de la capa red 3 del modelo OSI, por ejemplo, según el protocolo IP.

[0017] Se considerará posteriormente que las redes seguras N1 y N3 son unas redes Ethernet y que la red de tránsito N2 es una red IP.

[0018] La red de salida N1 comprende al menos un terminal emisor 3 y un dispositivo de seguridad 5, conectado por una conexión 7 alámbrica o inalámbrica al terminal emisor 3.

[0019] El terminal emisor 3, por ejemplo un ordenador, es apto para intercambiar unos datos con la red de salida N1 y, en particular, con el dispositivo de transmisión 5, con la red de tránsito N2, y con la red de destino N3, por medio del dispositivo de trasmisión de datos 5. El terminal emisor 3 comprende especialmente una tarjeta de red, apta para intercambiar unos daos con la red de salida N1, en particular con el dispositivo de transmisión 5 y con la red de tránsito N2.

[0020] El dispositivo de transmisión de datos 5 está en desconexión entre la red de salida N1 y la red de tránsito N2, de tal modo que todos los datos intercambiados entre el terminal emisor 3 y la red de tránsito N2 pasen obligatoriamente por el dispositivo 5.

[0021] El dispositivo de transmisión 5 es apto para encapsular una trama de una capa de conexión de datos de la red de salida N1, que comprende al menos un encabezamiento y una carga útil, en al menos un paquete seguro de una capa de red compatible con la red de tránsito N2, y para transmitir este o estos paquete(s) seguros hacia la red de destino N3 a través de la red de tránsito N2.

[0022] Este dispositivo de transmisión 5 se describirá más en detalle en referencia a la figura 2.

[0023] La red de destino N3 comprende al menos un terminal receptor 9 y un dispositivo de seguridad 11, conectado por una conexión 13 alámbrica o inalámbrica al terminal receptor 9.

[0024] El terminal receptor 9, por ejemplo un ordenador, es apto para intercambiar unos datos con la red de destino N3 y, en particular, con el dispositivo de transmisión 11, con la red de tránsito N2, y con la red de salida N1, por medio del dispositivo de transmisión 11. El terminal receptor 9 comprende especialmente una tarjeta de red, apta para intercambiar unos datos con la red de destino N3, en particular con el dispositivo de transmisión 11 y con la red de tránsito N2.

[0025] El dispositivo de transmisión 11 está instalado en desconexión entre la red de tránsito N2 y la red de destino N3. Es de estructura y de funcionamiento idéntico al dispositivo de transmisión 5 de la red de salida N1.

[0026] La red de tránsito N2 comprende especialmente varios enrutadores R_1, R_2, R_3, R_n, interconectados por una red de enlaces 13, que son por ejemplo unos enlaces alámbricos o unos enlaces radios. Por otro lado, al menos un enrutador R_1 está conectado al dispositivo de transmisión 5 de la red de salida N1, y al menos un enrutador R_n está conectado al dispositivo de transmisión 11 de la red de destino N3.

[0027] De manera conocida, los enrutadores R_1, R_2, R_3, R_n son aptos para hacer transitar unos datos entre los dispositivos 5, 11 de transmisión de las redes N1, N3 de salida y de destino.

[0028] La figura 2 ilustra, de manera simplificada, la arquitectura de un dispositivo de transmisión 5, colocado en desconexión entre el terminal emisor 3 y el enrutador R_1 de la red de tránsito N2, los dos representados de manera esquemática.

[0029] El dispositivo de transmisión 5 consta de un primer módulo de análisis 20, un módulo de encapsulación y de protección 22 y un módulo de fragmentación 24, así como un módulo de verificación criptográfica 26, un módulo de desencapsulación 28 y un módulo de reensamblaje 30.

[0030] El dispositivo 5 consta de una primera entrada 5a conectada al terminal emisor 3 por el enlace 7, una segunda entrada 5b conectada al enrutador R_1, una primera y una segunda salidas 5c y 5d conectadas al terminal

emisor 3 por el enlace 7, y una tercera salida 5e conectada al enrutador R_1.

[0031] El módulo de análisis 20 comprende una entrada 20a, conectada a la primera entrada 5a del dispositivo 5, y una primera y una segunda salidas 20b, 20c.

[0032] El módulo de fragmentación comprende una entrada 24a, conectada a la segunda salida 20c del módulo de análisis 20 y una salida 24b.

[0033] El módulo de encapsulación y de seguridad 22 comprende una primera entrada 22a, conectada a la primera salida 20b del módulo de análisis 20, una segunda entrada 22b, conectada a la salida 24b del módulo de fragmentación y una salida 22c, conectada a la tercera salida 5e del dispositivo 5.

[0034] El módulo de verificación criptográfica 26 comprende una entrada 26a, conectada a la segunda entrada 5b del dispositivo 5 y una salida 26b.

[0035] El módulo de desencapsulación 28 comprende una entrada 28a, conectada a la salida 26b del módulo 26 de verificación criptográfica, una primera salida 28b, conectada a la segunda salida 5d del dispositivo 5 y una segunda salida 28c.

[0036] El módulo de reensamblaje 30 comprende una entrada 30a, conectada a la segunda salida 28c del módulo 28 de desencapsulación y una salida 30b, conectada a la primera salida 5c del dispositivo 5.

[0037] El módulo de análisis 20 es apropiado para recibir una trama de una capa de conexión de la red N1 emitida por el terminal emisor 3, para analizar esta trama para determinar si una fragmentación de esta trama es necesaria antes de su transmisión en la red de tránsito N2. El módulo de análisis 20 es igualmente apropiado para transmitir esta trama al módulo de fragmentación 24 si una fragmentación es necesaria, o al módulo de encapsulación y de seguridad 22 en el caso contrario.

[0038] El módulo de fragmentación 24 comprende unos medios para fragmentar una trama recibida del módulo de análisis 20 en tantas porciones de trama como sea necesario, y para formar a partir de cada una de estas porciones un fragmento de trama, que comprende una de las porciones de trama procedentes de la fragmentación y un campo que indica la posición de esta porción en la trama de origen y que permite identificar esta trama de origen. El módulo de fragmentación 24 es igualmente apto para transmitir los fragmentos de trama así formados al módulo de encapsulación y de seguridad 22.

[0039] El módulo de encapsulación y de seguridad 22 es apto para encapsular cada trama o fragmento de trama que recibe en un paquete seguro de nivel 3. En particular, el módulo de encapsulación 22 es apto para generar al menos un encabezamiento de encapsulación de seguridad, para formar al menos un paquete de encapsulación que comprende al menos un encabezamiento de encapsulación de seguridad, la trama o un fragmento de la trama y un campo de fin y para aplicar al menos una protección criptográfica a cada paquete de encapsulación, formando así al menos un paquete seguro.

[0040] El módulo de encapsulación y de seguridad 22 es por otro lado apto para transmitir el o los paquete(s) seguro(s) así formado(s) a través de la red de tránsito N2, con destino al dispositivo de transmisión 11.

[0041] El módulo de verificación criptográfica 26 es apto para recibir unos paquetes seguros de datos que hayan transitado a través de la red de tránsito N2, para analizar estos paquetes para verificar su autenticidad y su integridad y para descifrar las partes de estos paquetes que hayan sido eventualmente objeto de un cifrado.

[0042] El módulo de desencapsulación 28 comprende unos medios para extraer de un paquete seguro una trama o un fragmento de trama contenido en este paquete por desencapsulación de este paquete, es decir, por supresión de un encabezamiento y de un campo de fin previamente añadidos a esta trama o a este fragmento de trama. El módulo de desencapsulación 28 es por otro lado apropiado para analizar los datos procedentes de la desencapsulación, para determinar si se trata de una trama entera o de un fragmento de trama, para transmitir las tramas enteras en la red N1, hacia el terminal de destino de estas tramas y los fragmentos de trama al módulo de reensamblaje 30.

[0043] El módulo de reensamblaje 30 comprende unos medios para reformar, a partir de al menos dos fragmentos de trama recibidos del módulo de desencapsulación 28, la trama a partir de la que estos fragmentos hayan sido generados y para transmitir esta trama reconstituida en la red N1, hacia el terminal de destino de esta trama.

[0044] El dispositivo de transmisión 5 está instalado preferiblemente en un espacio controlado, por ejemplo, en un recinto de la red N1, a fin de proteger físicamente sus entradas y salidas contra unos atacantes potenciales. El dispositivo de transmisión 5 está por ejemplo físicamente blindado, especialmente para evitar los ataques por

canales auxiliares, a través especialmente del análisis de la corriente eléctrica consumida por este dispositivo o la radiación electromagnética emitida por este dispositivo.

[0045] Se han representado en la figura 3 las etapas aplicadas por el dispositivo de transmisión 5 cuando recibe unos datos emitidos por el terminal emisor 3 con destino al terminal receptor 9, siendo emitidos estos datos según un protocolo de la capa de conexión del modelo OSI, en el caso presente en forma de tramas Ethernet.

[0046] Cada una de estas tramas comprende un encabezamiento Ethernet, una carga útil CU y un campo de fin. El encabezamiento comprende especialmente la dirección MAC de la fuente de la trama, es decir de la tarjeta Ethernet del terminal emisor 3, la dirección MAC del destinatario de la trama, es decir de la tarjeta Ethernet del terminal receptor 9 y un campo «Tipo» que indica el tipo de protocolo utilizado. La carga útil, de tamaño comprendido entre 46 y 1.500 bytes, corresponde a los datos efectivamente transmitidos por la trama y comprende por tanto los datos o una parte de los datos emitidos por el terminal emisor 3 con destino al terminal receptor 9. El campo de fin es un campo de control FCS (para «Frame Check Sequence», es decir secuencia de control de trama). Se trata de un código de detección de errores, que permite al receptor de la trama detectar ciertos errores aparecidos durante la transmisión de la trama.

[0047] La carga útil de una trama Ethernet que tiene un tamaño máximo limitado a 1.500 bytes, los datos emitidos por el terminal emisor 3 con destino al terminal receptor 9 son generalmente transmitidos en forma de una pluralidad de tramas.

[0048] La figura 3 ilustra las etapas del procedimiento de transmisión según la invención aplicadas por el dispositivo de transmisión 5, durante la transmisión de cada una de estas tramas.

[0049] Tales tramas n pueden ser transmitidas a través de la red de tránsito N2, ya que no están adaptadas a una transmisión en una red IP, no comprendiendo ninguna información de nivel 3 del modelo OSI. Además, estas tramas no están protegidas, de tal modo que la transmisión de estas tramas tal cual a través de la red de tránsito N2 permitiría a un atacante colocado en esta red de tránsito N2 acceder a todos los datos transmitidos y atacar a la red N1 y/o la red N3.

[0050] Cada trama TR emitida por el terminal emisor 3 es recibida por el módulo de análisis 20 del dispositivo 5 de transmisión. En una etapa 40, el módulo de análisis 20 analiza la trama TR para determinar si el tamaño de esta trama autoriza la transmisión de esta trama, después de la protección por el procedimiento según la invención en la red de tránsito N2.

[0051] Se define en efecto en toda la red tal como una red IP o una red Ethernet un tamaño máximo autorizado por el protocolo de esta red, llamado PMTU, para «Path Maximum Transmission Unit». En el caso de una red IP, este tamaño máximo corresponde al número máximo de bytes del conjunto constituido por el encabezamiento IP y unos datos IP transmitidos por este paquete. En el caso de una red de nivel inferior, por ejemplo, una red Ethernet, este tamaño máximo corresponde al número máximo de bytes de la carga útil, por defecto 1.500 si se trata de una trama Ethernet.

[0052] Como se describirá posteriormente, la transmisión de una trama TR desde la red N1 hacia la red de tránsito N2 comprende una encapsulación de esta trama en un paquete IP seguro de encapsulación. Así, el paquete IP transmitido por el dispositivo de transmisión 5 a través de la red de tránsito N2 tiene un tamaño más importante que la trama TR de origen, emitida por el terminal emisor 3, de tal modo que el tamaño de este paquete IP podría ser superior al valor PMTU de la red de tránsito N2, impidiendo una transmisión de este paquete IP en esta red N2.

[0053] Durante la etapa 40, el módulo de análisis 20 compara el tamaño T_{TR} de la trama TR con el tamaño máximo T_{max} que esta trama podría tener sin que el paquete IP obtenido por encapsulación de esta trama Ethernet supere el valor PMTU de la red N2. Este tamaño máximo T_{max} es igual así al valor PMTU de la red N2 menos el número de bytes añadidos a esta trama durante su encapsulación en un paquete IP.

[0054] Si el tamaño T_{TR} de la trama TR es superior a este tamaño máximo T_{max}, se transmite por el módulo de análisis 20 al módulo 24 de fragmentación. Si el tamaño T_{TR} de la trama TR es inferior o igual a este tamaño máximo T_{max}, se transmite por el módulo de análisis 20 al módulo de encapsulación y de protección 22.

[0055] Durante una etapa 42, aplicada únicamente si la trama TR es transmitida al módulo 24 de fragmentación, la trama TR es fragmentada por el módulo 24 de fragmentación en al menos dos porciones, siendo cada una de estas porciones de tamaño inferior o igual a un segundo tamaño máximo $T'_{max} < T_{max}$ predefinido, y pudiendo la trama TR de origen estar reconstituida por concatenación de estas porciones.

[0056] Después, el módulo de fragmentación 24 genera, a partir de las N porciones creadas, N fragmentos de trama FTR, comprendiendo cada uno de estos fragmentos una porción de la trama TR de origen y un campo de fragmentación. Este campo de fragmentación comprende un identificador de trama, que permite identificar de

manera única la trama TR de la que resulta la porción de trama y un identificador de fragmento, que indica la posición de esta porción en la trama Ethernet, con respecto a las otras porciones de la trama procedentes de esta fragmentación. Este campo de fragmentación tiene un tamaño T_f. La definición de un segundo tamaño máximo $T'_{max} < T_{max}$ permite asegurar así que el tamaño de cada fragmento FTR siga siendo inferior al tamaño máximo T_{max}, a pesar de la adición del campo de fragmentación a cada porción de trama.

[0057] Cada uno de los fragmentos de trama FTR es transmitido a continuación por el módulo de fragmentación 24 al módulo de encapsulación y de protección 22.

[0058] Durante una etapa 44, el módulo de encapsulación y de protección 22 genera, a partir de la trama TR recibida del módulo de análisis 20 o de cada fragmento FTR de trama recibido del módulo de fragmentación 22, un paquete $\hat{P}_{enc}$ de encapsulación seguro de la capa red del modelo OSI, por ejemplo según un protocolo IPsec en modo Tunnel (para Internet Protocol Security, es decir, Seguridad del Protocolo Internet), especialmente según el protocolo ESP (para Encapsulating Security Payload, o encapsulación de carga útil segura).

[0059] Con este fin, durante una etapa 46, el módulo de encapsulación 22 y de protección genera un encabezamiento de encapsulación de seguridad E_{enc} y un primer campo de fin CF_{enc}, igualmente llamado «trailer» y genera un paquete de encapsulación P_{enc}, por concatenación del encabezamiento E_{enc}, de la trama TR o del fragmento de trama FTR que se va a encapsular y del campo de fin CF_{enc}.

[0060] El encabezamiento de encapsulación de seguridad E_{enc}, llamado igualmente encabezamiento de seguridad, es un encabezamiento de seguridad de nivel 3 del modelo OSI, por ejemplo, un encabezamiento de tipo ESP.

[0061] El encabezamiento E_{enc} comprende por ejemplo un encabezamiento IP que indica una dirección fuente del paquete, es decir la dirección red del dispositivo de transmisión 5 en la red N2, por ejemplo, su dirección IP, así como una dirección de destino del paquete, es decir la dirección red del dispositivo de transmisión 11 en la red N2, por ejemplo, su dirección IP.

[0062] Este encabezamiento E_{enc} comprende además un identificador que permite a un equipo homólogo destinatario del paquete, en el caso presente el dispositivo 11, identificar la política de seguridad aplicada al paquete seguro y, si todo o parte de este paquete es objeto posteriormente de un cifrado, identificar la clave que permite al dispositivo 11 descifrarlo.

[0063] Si el encabezamiento E_{enc} es un encabezamiento de tipo ESP, este identificador es por ejemplo un campo SPI (para Security Parameters Index, o índice de parámetros de seguridad), que indica la asociación de seguridad (SA) utilizada para la protección del paquete seguro P_{enc}.

[0064] El encabezamiento E_{enc} comprende igualmente uno o varios campos de seguridad que permiten al destinatario, es decir al dispositivo 11, controlar la repetición de los paquetes que recibe y evitar así que un atacante intercepte ciertos de los paquetes para reenviarlos más tarde. Por ejemplo, si el encabezamiento E_{enc} es un encabezamiento de tipo ESP, comprende un campo SEQ o «Secuencia», que contiene el número de secuencia de la asociación de seguridad utilizada, estando tal número incrementado entre cada paquete seguro.

[0065] El campo de fin CF_{enc} comprende especialmente unos datos que permiten hacer anónimo el paquete transmitido en la red de tránsito N2, en particular ajustar la longitud de este paquete a una longitud predefinida, de tal modo que todos los paquetes emitidos por el dispositivo 5 en la red de tránsito N2 tengan la misma longitud.

[0066] Este campo de fin CF_{enc} comprende por ejemplo un campo de fin de tipo ESP, que comprende unos datos de atasco, cuya longitud es escogida de tal modo que la longitud del paquete seguro sea igual a una longitud predefinida, un campo «Longitud» o «Pad length», que indica la longitud de los datos de atasco, y un campo «Next Header», es decir «Encabezamiento siguiente», que indica el tipo de datos llevados por el paquete de encapsulación P_{enc}, por ejemplo se trata de una trama Ethernet entera o de un fragmento de trama.

[0067] Después, durante una etapa de protección criptográfica en confidencialidad 48, el módulo de encapsulación y de protección 22 aplica una protección criptográfica en confidencialidad a una parte del paquete de encapsulación P_{enc} que comprende la trama TR o el fragmento de trama FTR encapsulado y, eventualmente, el campo de fin CF_{enc}. Esta protección criptográfica es por ejemplo un cifrado, que permite proteger en confidencialidad la trama TR o el fragmento de trama FTR antes de su transmisión en la red de tránsito N2. La parte del paquete cifrada puede ser descifrada posteriormente por medio de la clave identificada en el encabezamiento E_{enc}.

[0068] Durante una etapa de protección criptográfica en integridad 50, el módulo de encapsulación y de protección 28 aplica una protección criptográfica en integridad al conjunto del paquete de encapsulación P_{enc} a excepción del encabezamiento IP, incluso al conjunto del paquete de encapsulación P_{enc}. Esta protección tiene como

objeto proteger en integridad el paquete de encapsulación P_{enc}, es decir evitar una modificación de este paquete por un atacante colocado en la red de tránsito N2. Esta protección en integridad es por ejemplo una firma o la aplicación de una función hash.

[0069] El módulo 22 de encapsulación y de protección añade entonces un campo de fin CF_2 al paquete obtenido, comprendiendo este campo de fin un código de autentificación, procedente de la protección criptográfica en integridad, que permite proceder a la autentificación del paquete y verificar la integridad, durante la recepción de este paquete por el dispositivo 11, después de la transmisión de este paquete en la red de tránsito N2.

[0070] Este campo de fin CF_2 es por ejemplo un campo ICV («Integrity Check Value», es decir valor de control de integridad).

[0071] Así, al final de la etapa 50, la trama o el fragmento de trama es encapsulado en un paquete de encapsulación protegido, que forma un paquete seguro P_{sec}.

[0072] El paquete seguro P_{sec} es entonces transmitido en una etapa 54 por el dispositivo 5 en la red de tránsito N2, con destino al dispositivo 11 de transmisión.

[0073] La figura 4 ilustra de manera esquemática la estructura del paquete seguro P_{sec} emitido en la red de tránsito N2, en un modo particular de realización de la invención. En este modo de realización, la trama TR es una trama Ethernet, el paquete seguro P_{sec} es un paquete IP, obtenido por encapsulación de la trama TR según el protocolo IPsec en modo túnel ESP.

[0074] Como se ha descrito anteriormente, el paquete seguro P_{sec} comprende, en este orden, el encabezamiento E_{enc} de encapsulación de seguridad, unos datos cifrados CH que comprenden la trama TR y el primer campo se fin CF_{enc} y el segundo campo de fin CF_2.

[0075] El encabezamiento E_{enc} comprende un encabezamiento E_{IP} que indica las direcciones IP fuente y destino, un campo SPI, que indica la asociación de seguridad (SA) utilizada y un campo SEQ de control de la repetición.

[0076] La trama TR comprende un encabezamiento que indica la dirección MAC de la tarjeta de red del terminal fuente 3, indicado como MAC_3, la dirección MAC de la tarjeta de red del terminal destinatario 9, indicada como MAC_9 y el tipo de protocolo utilizado, un campo útil CU que comprende los datos que se van a transmitir y un campo de control FCS.

[0077] El primer campo de fin CF_{enc} comprende los datos de atasco Bo, un campo «Longitud» PL que indica el tamaño de los datos de atasco y un campo «Encabezamiento siguiente» NH, que indica que el paquete de encapsulación P_{sec} comprende una trama entera.

[0078] La trama TR y el primer campo de fin CF_{enc} están así presentes en forma cifrada en el paquete seguro P_{sec}, siendo identificada la clave que permite el desciframiento de estos datos en el campo SPI del encabezamiento E_{enc}. Además, los campos SPI y SEQ del encabezamiento E_{enc}, la trama TR y el primer campo de fin CF_{enc} son protegidos íntegramente, comprendiendo el campo de fin de tipo ICV unos datos que permiten verificar la integridad de estos datos, durante su recepción por el dispositivo 11.

[0079] Así, durante la transmisión del paquete seguro P_{sec} en la red de tránsito N2, ni las direcciones MAC de la fuente y del destino, ni los datos llevados por la trama TR no son accesibles en abierto.

[0080] La figura 5 ilustra las etapas del procedimiento de transmisión según la invención aplicadas por el dispositivo de transmisión 11, durante la recepción de un paquete seguro P_{sec} que comprende una trama TR o un fragmento de trama FTR y emitido por el dispositivo de transmisión 5, después del tránsito de este paquete en la red N2.

[0081] En una etapa de verificación criptográfica 60, el módulo de verificación criptográfica 26 del dispositivo 11 analiza el paquete seguro P_{sec} para verificar su autenticidad y su integridad y descifra la trama TR o el fragmento de trama FTR y el primer campo de fin CF_{enc}, si estos no son objeto de un cifrado.

[0082] Con este fin, en una etapa de análisis 62, el módulo de verificación criptográfica 26 analiza el encabezamiento E_{enc} del paquete P_{enc} de encapsulación, por ejemplo, su campo SPI si se trata de un encabezamiento ESP e identifica la política de seguridad aplicada al paquete seguro P_{sec}. Si la trama TR o el fragmento de trama FTR y el primer campo de fin CF_{enc} están cifrados, el módulo de verificación 26 criptográfica identifica a partir de este encabezamiento E_{enc} la clave que permite descifrarlos. Por otro lado, si este encabezamiento E_{enc} comprende un campo de control anti-repetición, por ejemplo, un número de secuencia SEQ, el módulo de verificación criptográfica 26 identifica este número.

[0083] En una etapa 64, el módulo de verificación criptográfica 26 verifica la autenticidad y la integridad del paquete seguro P_{sec}. Para ello, el módulo de verificación criptográfica 26 compara el código de autentificación, por ejemplo, el campo ICV, del segundo campo de fin CF_2, con el código que se obtendría a partir del paquete recibido, permitiendo esta comparación detectar eventuales modificaciones aportadas a este paquete. El módulo de verificación criptográfica 26 compara igualmente el campo de control anti-repetición del encabezamiento E_{enc} con unos campos de control procedentes de paquetes previamente recibidos por el dispositivo 11. Esta comparación permite determinar si el paquete P_{sec} ha sido emitido por un adversario, que habría interceptado este paquete durante su transmisión inicial. Así, si el campo de control anti-repetición del encabezamiento E_{enc} es inferior o igual a un campo de control de un paquete previamente recibido, el módulo de verificación criptográfica 26 rechaza este paquete en una etapa 66.

[0084] Después, en una etapa de desciframiento 68, aplicada si la trama TR o el fragmento de trama FTR y el primer campo de fin CF_{enc} están cifrados, el módulo de verificación criptográfica 26 descifra estos por medio de la clave identificada en el encabezamiento E_{enc}.

[0085] Al final de la etapa de verificación criptográfica 60, el paquete seguro descifrado es transmitido a continuación al módulo de desencapsulación 28.

[0086] En una etapa de desencapsulación 70, el módulo de desencapsulación 28 extrae del paquete seguro descifrado la trama TR o el fragmento de trama FTR contenido en este paquete, por supresión del encabezamiento de encapsulación de seguridad E_{enc} y de los campos de fin CF_{enc} y CF_2.

[0087] En una etapa 72, el módulo de desencapsulación 28 analiza los datos extraídos del paquete seguro, para determinar si se trata de una trama entera o de un fragmento de trama.

[0088] Si se trata de una trama entera TR, el dispositivo 11 transmite en una etapa 74 esta trama en la red N3, con destino al terminal receptor 9, y más precisamente de la tarjeta de red del terminal receptor 9 cuya dirección MAC está indicada en el encabezamiento de la trama TR.

[0089] Si se trata de un fragmento de trama FTR, el módulo de desencapsulación 28 transmite en una etapa 76 este fragmento al módulo de reensamblaje 30.

[0090] Como se ha descrito anteriormente, un fragmento de trama DTR comprende un campo de fragmentación y una porción de una trama TR de origen. En una etapa de reensamblaje 78, el módulo de reensamblaje 30 analiza el campo de fragmentación del fragmento de trama FTR, e identifica a partir de este campo la trama TR de origen de la que procede esta porción de trama, así como la posición de esta porción en la trama de origen. El módulo de reensamblaje 30 memoriza esta porción, así como su posición en la trama de origen hasta que haya recibido el conjunto de las porciones de trama procedentes de la fragmentación de la trama de origen. El módulo de reensamblaje 30 concatena entonces estas porciones de trama para reconstituir esta trama de origen.

[0091] Después, en una etapa 80, el dispositivo 11 transmite la trama TR reconstituida en la red N3, con destino al terminal receptor 9, y más precisamente a la tarjeta de red del terminal receptor 9 cuya dirección MAC está indicada en el encabezamiento de la trama TR.

[0092] Se comprende de la descripción anterior cómo el procedimiento y el dispositivo de transmisión según la invención permiten transmitir de manera segura unos datos comprendidos en una trama de una capa de conexión de datos, entre dos redes seguras conmutadas, a través de una red enrutada no segura o de nivel de seguridad diferente de las redes seguras.

[0093] En particular, la encapsulación de una trama de una capa de conexión de datos que se va a transmitir a través de la red de tránsito en un paquete seguro de una capa red, por ejemplo, la encapsulación de una trama Ethernet en un paquete IPsec, permite obtener un paquete que puede ser transmitido en todos los tipos de redes, contrariamente a la trama de origen.

[0094] La seguridad de los datos es especialmente asegurada por la protección criptográfica en integridad aplicada al paquete de encapsulación P_{enc} y por la protección criptográfica en confidencialidad aplicada de preferencia a la trama o al fragmento de trama encapsulada y al primer campo de fin CF_{enc}.

[0095] En efecto, la protección criptográfica en integridad aplicada al paquete de encapsulación P_{enc} permite controlar, durante la recepción del paquete seguro, que este paquete no sea objeto de una modificación durante su tránsito en la red N2 e impedir la repetición de este paquete. La protección en integridad aplicada en particular al encabezamiento de encapsulación E_{enc} permite protegerse contra unos ataques en el formato de encapsulación, susceptibles de impedir que las redes N1 y N3 intercambien datos.

[0096] Además, la aplicación de una protección criptográfica en confidencialidad a la trama o al fragmento de trama encapsulado(a) y al primer campo de fin CF_{enc} permite garantizar la confidencialidad de los datos intercambiados y de las identidades de los terminales emisor 3 y receptor 9. En particular, cuando el paquete seguro P_{sec} comprende un fragmento de trama, el cifrado del campo de fragmentación permite evitar que un atacante perturbe el funcionamiento del dispositivo de transmisión 11 interceptando uno o varios paquete(s) seguro(s) y modificando los valores de campo. Tal modificación tendría por ejemplo como consecuencia conducir un almacenamiento de los fragmentos recibidos por el dispositivo de transmisión 11 a fin de esperar un hipotético último fragmento.

[0097] Además, puesto que solo las direcciones red de los dispositivos 5 y 11 de transmisión son indicados en el encabezamiento del paquete seguro, solo estas direcciones pueden ser vistas en la red de tránsito N2. No es por tanto posible, a partir de esta red N2, saber qué terminales protegidos se intercambian datos.

[0098] La anonimización de los datos transmitidos es por otro lado reforzada gracias a la adición de datos de atasco Bo en el paquete de encapsulación, garantizando la adición de tales datos que el conjunto de los paquetes emitidos en la red de tránsito N2 sean de la misma longitud. No es por tanto posible para un adversario colocado en la red N2 determinar cuál es el tipo de datos intercambiados entre las redes N1 y N3 por simple análisis de la longitud de los paquetes intercambiados.

[0099] Además, la aplicación de tal procedimiento es menos costosa que la de los procedimientos según el estado de la técnica, puesto que permite explotar unos protocolos existentes tal como un protocolo IPsec.

[0100] Deberá comprenderse no obstante que los ejemplos de realización presentados más arriba no son limitativos.

[0101] Especialmente, según otros modos de realización, el procedimiento de transmisión es aplicado en un modo punto-a-multi-punto entre más de dos redes seguras, a través de varias redes de niveles de seguridad más reducidos, estando equipada cada una de las redes seguras con al menos un dispositivo de transmisión según la invención.

REIVINDICACIONES

1. Procedimiento de transmisión de datos en un canal de comunicación entre al menos una red de salida (N1) y una red de destino (N3) a través de una red de tránsito (N2) de un nivel de seguridad diferente de las redes de salida (N1) y de destino (N3), que comprende, durante una transmisión, la red de salida (N1) hacia la red de destino (N3) a través de la red de tránsito (N2), de datos comprendidos en al menos una trama (TR) de una capa de conexión de datos, la trama (TR) comprendiendo al menos un encabezamiento y una carga útil (CU):

- una etapa de encapsulación (44) de la trama (TR) en al menos un paquete (P_{sec}) de una capa de red de nivel 3 del modelo OSI, compatible con la red de tránsito (N2), y
- una etapa de transmisión (54) del o de cada paquete (P_{sec}) hacia la red de destino (N3) a través de la red de tránsito (N2),

estando el procedimiento **caracterizado porque** el o cada paquete (P_{sec}) es un paquete seguro y **porque** la etapa (44) de encapsulación comprende las etapas siguientes:

- generación (46) de al menos un encabezamiento de encapsulación de seguridad (E_{enc}),
- formación de al menos un paquete de encapsulación (P_{enc}) que comprende al menos el o uno de los encabezamiento(s) de encapsulación de seguridad (E_{enc}) y dicha trama (TR) o un fragmento de dicha trama (FTR),
- formación del o de cada paquete seguro (P_{sec}) por aplicación (48, 50) de al menos una protección criptográfica al o a cada paquete de encapsulación (P_{enc}).

2. Procedimiento de transmisión según la reivindicación 1, **caracterizado porque** la etapa de encapsulación (44) comprende además una etapa de anonimización del o de cada paquete seguro (P_{sec}), que comprende un ajuste de la longitud del o de cada paquete seguro (P_{sec}) a una longitud predefinida.

3. Procedimiento de transmisión según una de las reivindicaciones 1 o 2, **caracterizado porque** comprende, además, durante una transmisión de al menos una trama (TR) de una capa de conexión de datos de la red de salida (N1) hacia la red de destino (N3) a través de la red de tránsito (N2), antes de dicha etapa de encapsulación (44):

- una comparación (40) de un tamaño (T_{TR}) de dicha trama (TR) con un tamaño máximo predefinido (T_{max}),
- si el tamaño (T_{TR}) de dicha trama (TR) es superior a dicho tamaño máximo predefinido (T_{max}), una fragmentación (42) de dicha trama (TR) en al menos dos fragmentos (FTR) de trama, siendo el tamaño de cada fragmento (FTR) de trama inferior o igual al tamaño máximo predefinido (T_{max}).

4. Procedimiento de transmisión según cualquiera de las reivindicaciones anteriores, **caracterizado porque** comprende además la generación (46) de al menos un campo de fin (CF_{enc}), comprendiendo el o cada paquete de encapsulación (P_{enc}) al menos dicho o uno de dichos encabezamiento(s) de encapsulación de seguridad(E_{enc}), dicha trama (TR) o un fragmento de dicha trama (FTR) y el o uno de dichos campo(s) de fin (CF_{enc}).

5. Procedimiento de transmisión según la reivindicación 4 tomada en combinación con la reivindicación 2, **caracterizado porque** el o cada campo de fin (CF_{enc}) comprende unos datos de atasco (Bo), siendo escogida la longitud de los datos de atasco (Bo) de tal modo que la longitud del o de cada paquete seguro (P_{sec}) sea igual a dicha longitud predefinida.

6. Procedimiento de transmisión según cualquiera de las reivindicaciones anteriores, **caracterizado porque** comprende, además, durante una transmisión de al menos un paquete seguro (P_{sec}) de dicha red de tránsito (N2) hacia dicha red de destino (N3), al menos una etapa de recepción del o de cada paquete seguro (P_{sec}) y una etapa de transmisión (74, 80) de dichos datos a dicha red de destino (N3), comprendiendo la o cada etapa de recepción:

- una verificación criptográfica (62, 64, 68) del paquete de encapsulación (P_{enc}) comprendido en dicho paquete seguro (P_{sec}),
- una extracción (70) de la trama (TR) o del fragmento de trama (FTR) comprendido en dicho paquete de encapsulación (P_{enc}).

7. Procedimiento de transmisión según la reivindicación 6 tomada en combinación con la reivindicación 3, **caracterizado porque** comprende, si al menos dos paquetes de encapsulación (P_{enc}) comprenden un fragmento de dicha trama (FTR), un ensamblaje (78) de los fragmentos de la trama (FTR) comprendido en los paquetes de encapsulación (P_{enc}), antes de la etapa de transmisión (74, 80) de dichos datos a dicha red de destino (N3).

8. Procedimiento de transmisión según cualquiera de las reivindicaciones anteriores, **caracterizado porque** dicha trama (TR) es una trama Ethernet.

9. Procedimiento de transmisión según cualquiera de las reivindicaciones anteriores, **caracterizado porque** dicho paquete seguro (P_{sec}) comprende un paquete seguro según un protocolo IPsec.

10. Dispositivo de transmisión (5, 11) de datos en un canal de comunicación entre al menos una red de salida (N1) y una red de destino (N3) a través de una red de tránsito (N2) de un nivel de seguridad más reducido que las redes de salida (N1) y de destino (N3), que comprende:

- unos medios de encapsulación (22), aptos para encapsular una trama (TR) de una capa de conexión de datos, que comprenden al menos un encabezamiento y una carga útil, en al menos un paquete (P_{sec}) de una capa de red compatible con la red de tránsito (N2), y
- unos medios para transmitir el o cada paquete (P_{sec}) hacia la red de destino (N3) a través de la red de tránsito,

estando el dispositivo **caracterizado porque** el o cada paquete (P_{sec}) es un paquete seguro y **porque** dichos medios de encapsulación (22) comprenden:

- unos medios para generar al menos un encabezamiento de encapsulación de seguridad (E_{enc}),
- unos medios para formar al menos un paquete de encapsulación (P_{enc}) que comprende al menos el o uno de los encabezamiento(s) de encapsulación de seguridad (E_{enc}) y dicha trama (TR) o un fragmento de dicha trama (FTR),
- unos medios para formar el o cada paquete seguro (P_{sec}) por aplicación de al menos una protección criptográfica al o a cada paquete de encapsulación(P_{enc}).

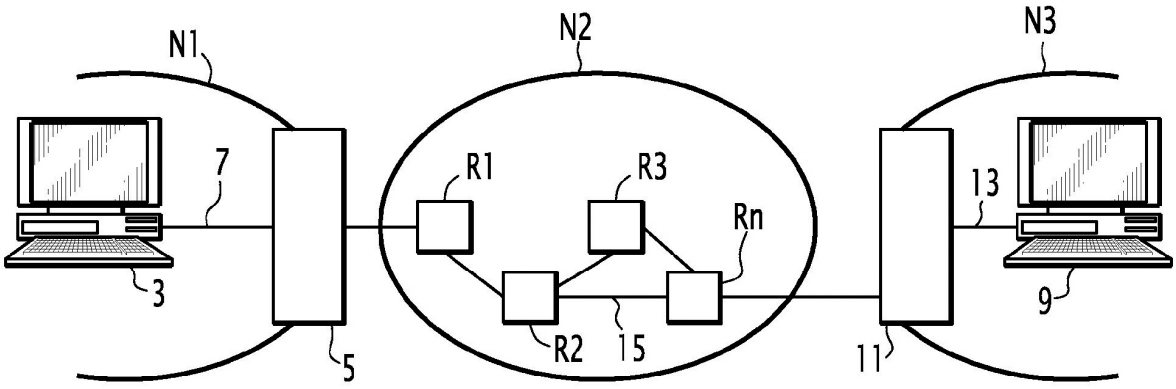
N1
N2
N3
7
R1
R3
Rn
13
3
9
R2
15
5
11

FIG.1

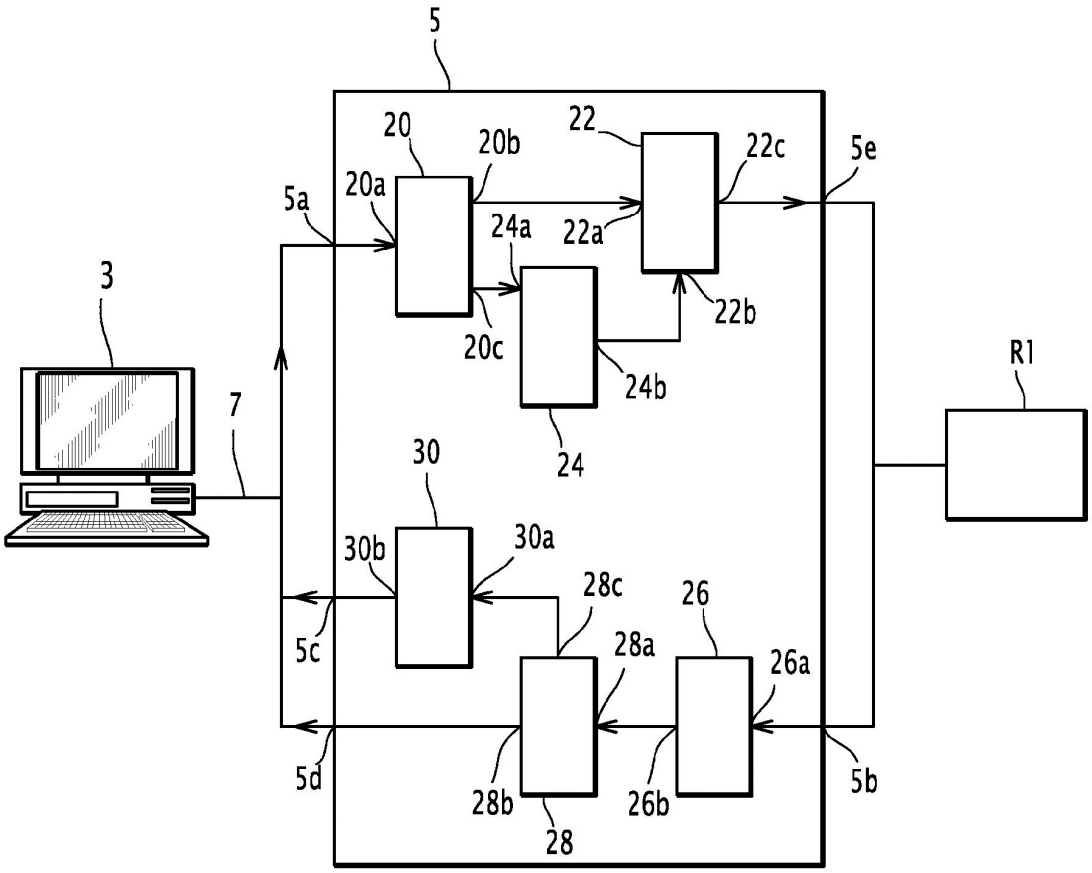
5
20
20b
22
22c
5e
5a
20a
24a
22a
3
22b
20c
24b
R1
7
24
30
30b
30a
28c
26
5c
28a
26a
5d
28b
26b
5b
28

FIG.2

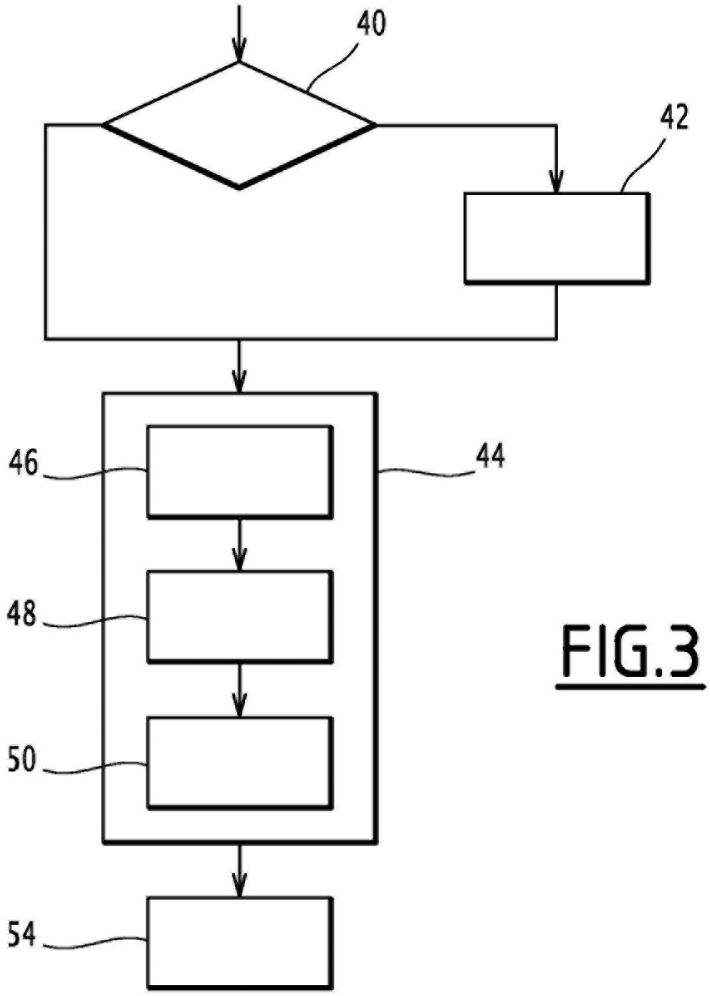
40
42
46
44
48
50
54

FIG.3

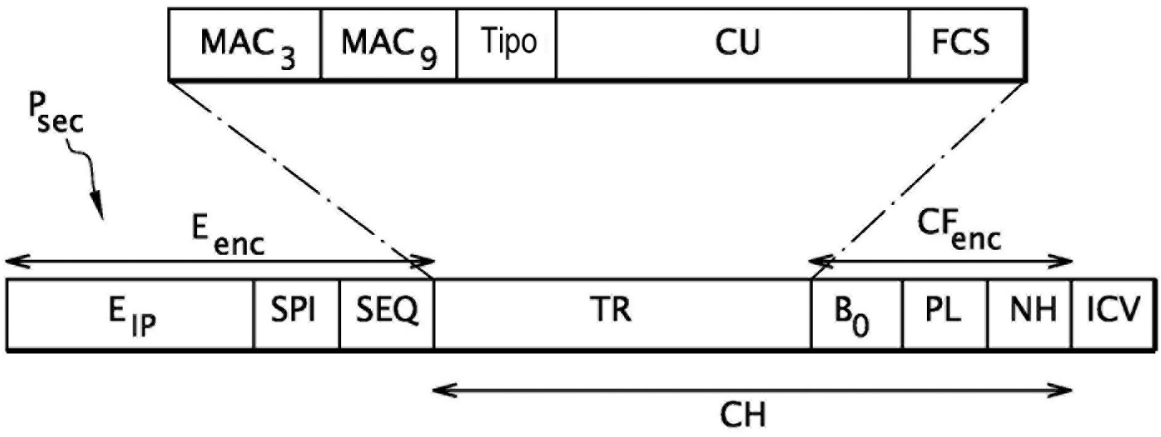
MAC 3
MAC 9
Tipo
CU
FCS
P sec
E enc
CF enc
E IP
SPI
SEQ
TR
B 0
PL
NH
ICV
CH

FIG.4

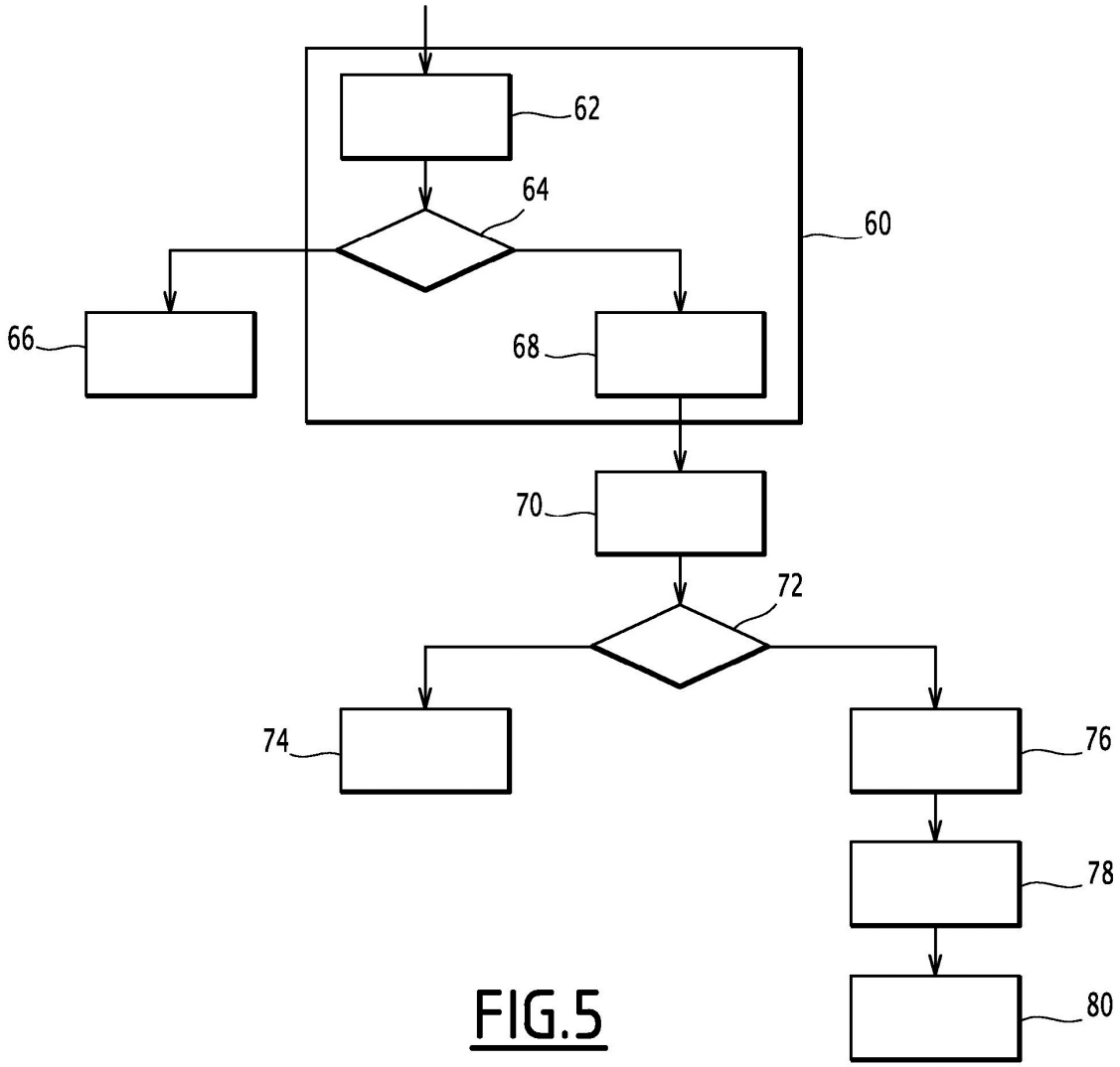

FIG.5