(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 596 533**

(21) Número de solicitud: 201530970

(51) Int. Cl.:

H04L 1/22 (2006.01)
H04L 12/00 (2006.01)

(12) PATENTE DE INVENCIÓN B1

(22) Fecha de presentación:

06.07.2015

(43) Fecha de publicación de la solicitud:

10.01.2017

Fecha de concesión:

16.10.2017

(45) Fecha de publicación de la concesión:

23.10.2017

(73) Titular/es:

UNIVERSIDAD DEL PAÍS VASCO / EUSKAL HERRIKO UNIBERTSITATEA (50.0%)
Barrio Sarriena, S/N
48940 Leioa (Bizkaia) ES y
SYSTEM-ON-CHIP ENGINEERING, S.L. (50.0%)

(72) Inventor/es:

LÁZARO ARROTEGUI, Jesús ;
ASTARLOA CUÉLLAR, Armando y
IDIRIN GONZÁLEZ, Mikel

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

(54) Título: **MÉTODO Y SISTEMA DE SEGURIDAD EN ANILLOS ETHERNET REDUNDANTES**

(57) Resumen:
Método y sistema de seguridad en anillos ethernet redundantes.
Método y sistema de seguridad en un anillo ethernet redundante en el que una cabecera de seguridad (3) se encapsula dentro de una cabecera de redundancia (4). A pesar de que la seguridad está introducida dentro de la redundancia, cuando un nodo (10) recibe una trama de la que es destinatario (1), autentica también la cabecera de redundancia (4), mientras que los nodos intermedios pueden no autenticar dicha cabecera de redundancia (4) para evitar retardos en la red.

Aviso: Se puede realizar consulta prevista por el art. 37.3.8 LP 11/1986.

ES 2 596 533 B1

DESCRIPCIÓN

MÉTODO Y SISTEMA DE SEGURIDAD EN ANILLOS ETHERNET REDUNDANTES

Campo de la invención

La presente invención se refiere al campo de la seguridad criptográfica en las telecomunicaciones y, más concretamente, a la seguridad en anillos ethernet redundantes.

Antecedentes de la invención

Las comunicaciones ethernet en anillo son relevantes para un gran número de aplicaciones, tales como dispositivos electrónicos de comunicaciones, sistemas de automatización y redes inteligentes (del inlgés 'Smart-grid'). Muchas de estas aplicaciones requieren securizar criptográficamente la red frente a ataques y escuchas externas. Cuando se quiere dotar de seguridad criptográfica a un enlace de red en capa dos, la trama original se introduce en una nueva trama a la que se añaden datos de control, así como el resultado de las operaciones criptográficas realizadas (firmas digitales, resultado de encriptación, etc). En su gran mayoría, las soluciones propuestas se basan en el intercambio de un paquete especial de red o 'testigo' ('token ring' en inglés).

Por ejemplo, WO 1992/017960 A1 presenta una red de datos en anillo (tal como una red token ring) dividida por una unidad de seguridad en un primer y un segundo segmentos. El primer segmento posee un nivel de seguridad superior al segundo. La lógica de la unidad de seguridad lee campos apropiadas de cada paquete (por lo general las dos direcciones) para determinar si es procedente retransmitir el paquete al siguiente segmento del anillo. Si la trama no debe ser transmitida al siguiente segmento, o no está autorizado para hacerlo, entonces la unidad de seguridad retransmite en su lugar una trama modificada en la que los datos no pueden ser interpretados. En la mayoría de los casos, el contenido de datos de la trama se almacena en la unidad de seguridad. Cuando la trama vuelve modificada a la unidad de seguridad a través de su segundo puerto de entrada, la trama original puede, si es preciso, ser reconstruida mediante la lectura de su contenido desde la memoria en la unidad de seguridad. De esta manera, la trama vuelve al grupo seguro sin modificaciones de tiempo y forma a como lo hubiera hecho si hubiera viajado alrededor del primer segmento del anillo. En todo caso, las estaciones en el primer segmento no pueden recuperar el contenido de los datos de tramas originadas en el segmento seguro.

En un segundo ejemplo, WO 2013/174578 A1 presenta un método para la generación de paquetes de datos redundantes protegidos criptográficamente. En una primera etapa, una pluralidad de paquetes de datos redundante son generados por medio de una pluralidad de unidades de generación diferentes. A cada unidad de generación se le asigna un código de identificación único. En un segundo paso, la pluralidad de paquetes son protegidos criptográficamente por medio de una función criptográfica individual. La función criptográfica es parametrizada para generar el paquete de datos protegido criptográficamente por una clave criptográfica y por la identificación asignada a la unidad de generación correspondiente. Como la función criptográfica para generar el paquete de datos protegido criptográficamente no sólo está parametrizado por la clave criptográfica sino también por la respectiva identificación, dicha clave criptográfica se puede utilizar por una pluralidad de canales.

Por su parte, US 5,850,515 propone un método para securizar una red frente al acceso no autorizado de estaciones finales. Un puerto en un repetidor multipuerto se puede desactivar automáticamente al detectar una dirección de origen desconocida en un paquete de datos. Además, se proporciona una señal de interrupción que indica la detección de un intruso. La desactivación del puerto puede realizarse inmediatamente para interrumpir incluso la retransmisión de un único paquete. Alternativamente, la desactivación de un puerto se puede ejecutar de forma programable después de haber sido detectado un número predeterminado de paquetes de intrusos, o después de la verificación de la integridad de los paquetes.

Finalmente, US 5,400,334 A presenta un método para contrarrestar la amenaza de espionaje en redes token ring. Se utiliza una red en anillo con cableado en estrella con un controlador central multipuerto que almacena información de un paquete de datos cuando la dirección de la estación no coincide con el destino del paquete de datos. Alternativamente, cuando la dirección de la estación no coincide con el destino del paquete, puede proporcionarse seguridad sustituyendo la información por una versión codificada de la misma.

Sin embargo, cuando se desea utilizar anillos ethernet redundantes, surgen serios problemas para compatibilizar los protocolos de seguridad y de redundancia. En redes en anillo redundantes, cada elemento de la red actúa como enrutador de la información, decidiendo si tiene que enviar cada trama al siguiente elemento de la red y/o utilizar dicha información al ser destinatario de la misma. En este tipo de redes la trama original se introduce dentro de una nueva trama que dota de los elementos de redundancia necesarios. En cada nodo que procesa la información es necesario procesar los datos de redundancia así como las direcciones origen y destino de la información para poder tomar una decisión. Por ejemplo, US 2004/0008722 A1 presenta un dispositivo para red ethernet redundante capaz de conectarse a dos redes (una red primaria y una red secundaria). El dispositivo comprueba continuamente el estado de la red primaria y, en caso de error de la misma, recurre a la red secundaria para la transmisión del mensaje.

US 8,582,426 B2 presenta un método de recepción de tramas redundantes y no redundantes en una red ethernet, que incorpora un protocolo de seguridad, pero dicho protocolo únicamente brinda protección en capa tres, por ejemplo mediante IPSec (Seguridad de Protocolo de Internet, del inglés 'Internet Protocol Security'). Se introduce asimismo un identificador de seguridad en la forma de un campo de longitud de trama. El receptor comprueba el valor del campo de longitud y lo compara con la longitud física del paquete. Si no coinciden, el receptor asume que la trama no forma parte del protocolo de seguridad y la transmite directamente a las capas superiores. Si los valores coinciden, el receptor decodifica el resto de campos asociados a la redundancia de acuerdo con el formato del protocolo de seguridad y actúa en consecuencia.

Sin embargo, si a los anillos redundantes se les desea añadir seguridad en capa dos (en términos de ciber-seguridad), podemos encontrar dos situaciones en el estado de la técnica: que la redundancia no tenga noción de seguridad o que la seguridad no tenga noción de la redundancia. En el primer caso, la red no está protegida frente a ataques sobre la redundancia ya que las cabeceras de redundancias no quedan securizadas por el protocolo de seguridad. En el segundo caso, la red se ralentiza ya que cada nodo debe resolver el protocolo de seguridad antes de resolver el protocolo de redundancia. La minimización del tiempo de procesamiento de paquetes en cada nodo es una característica técnica y comercial clave en el contexto de las redes de comunicación en anillo, puesto que un procesamiento lento de los paquetes en cada nodo limita drásticamente el número de equipos que pueden conectarse a la red. Una limitación adicional es la imposibilidad de mezclar elementos seguros y no seguros en una misma red. Así mismo, todos los elementos de la red deben compartir los mismos parámetros de seguridad (por ejemplo clave) con lo que la efectividad del mecanismo de seguridad puede verse reducida.

Por lo tanto, sigue existiendo en el estado de la técnica la necesidad de una técnica de seguridad en anillos ethernet redundantes capaz de securizar la información de redundancia sin incrementar el retardo introducido por la red.

Descripción de la invención

La presente invención soluciona los problemas anteriormente descritos al encapsular el protocolo de seguridad dentro del protocolo de redundancia, pero manteniendo la protección mediante autenticación en capa dos de dicho protocolo de redundancia. De esta manera los nodos intermedios no tienen por qué resolver la seguridad, pudiendo dejar dicho procesado en manos del nodo destinatario de cada mensaje. Además la redundancia queda protegida, con lo que los elementos finales pueden resolver la seguridad previamente a resolver la redundancia.

En un primer aspecto de la invención se presenta un método de seguridad en un anillo ethernet redundante que comprende:

i. Recibir en un nodo una trama ethernet que comprende al menos un destinatario, una cabecera de seguridad y una cabecera de redundancia. La cabecera de seguridad está encapsulada dentro de la cabecera de redundancia, lo que permite resolver la información de enrutado comprendida en la cabecera de redundancia sin necesidad de procesar el protocolo de seguridad asociado a la cabecera de seguridad.

   Preferentemente, la cabecera de seguridad es una cabecera de un protocolo MacSec (seguridad de control de acceso al medio, del inglés 'Medium Access Control Security), como el estándar 802.1AE de la IEEE (Instituto de Ingeniería Eléctrica y Electrónica, del inglés 'Institute of Electrical and Electronics Engineers').

   También preferentemente, la cabecera de enrutado es una cabecera de un protocolo de anillo homogéneo de alta disponibilidad (HSR, del inglés 'High-availability Seamless Redundancy').

ii. Si el nodo que recibe la trama es el destinatario de dicha trama, autenticar la cabecera de redundancia. Esta autenticación puede realizarse antes de resolver la propia redundancia. Es decir, a pesar de que la cabecera de seguridad está encapsulada dentro de la cabecera de redundancia, la autenticación proporcionada por el protocolo de seguridad se extiende también a la cabecera de redundancia. Se consigue así que sea decisión de cada nodo que recibe la trama si procesar o no el protocolo de seguridad, pudiendo enrutar el mensaje sin procesar dicho protocolo de seguridad. Como consecuencia, se protege la cabecera de redundancia, sin que ello suponga un procesado excesivo en nodos intermedios que ralentice las comunicaciones en el anillo y limite su tamaño.

iii. Si el nodo que recibe la trama no es el destinatario de dicha trama, es decir, es un nodo intermedio que debe enrutar dicha trama hacia otro nodo del anillo, se contemplan dos opciones preferentes:

   – No autenticar la cabecera de redundancia en ningún nodo intermedio, optimizando así el retardo del

sistema.

- Autenticar la cabecera de redundancia en el nodo intermedio únicamente cuando dicho procesado no incrementa el retardo ocasionado por la autenticación de la trama por encima de un límite predeterminado. Más preferentemente, esta opción comprende iniciar la autenticación de la cabecera de redundancia al recibir la trama, y detener dicha autenticación en caso de que la trama se retransmita antes de haber finalizado la autenticación.

iv. Preferentemente, el método puede comprender desencriptar la trama recibida, añadiendo así al protocolo de seguridad capacidades de encriptado además de las capacidades de autenticación.

En un segundo aspecto de la invención se presenta un sistema de seguridad en un anillo ethernet redundante que comprende, en al menos un nodo del anillo:

- Un controlador de redundancia configurado para implementar un protocolo de redundancia, siendo dicho protocolo de redundancia preferentemente un protocolo HSR.

- Una pluralidad de elementos de autenticación conectados al controlador de redundancia y a una pluralidad de puertos de un nodo del anillo. Los elementos de autenticación están configurados para implementar un protocolo de seguridad, dotando de seguridad criptográfica a un enlace de la red. El protocolo de seguridad es preferentemente un protocolo MacSec. También preferentemente, los elementos de seguridad pueden implementar un protocolo de seguridad que comprende encriptado además de autenticación.

  La pluralidad de elementos de autenticación están configurados para recibir tramas ethernet que comprenden un destinatario, una cabecera de seguridad y una cabecera de redundancia, así como cualquier otro campo requerido por el enlace ethernet. La cabecera de seguridad está encapsulada dentro de la cabecera de redundancia, por lo que cada elemento de seguridad se encuentra ubicado entre un puerto del nodo y el controlador de redundancia.

  Si el nodo en el que se implementan los elementos de autenticación es el nodo destinatario de la trama recibida, dichos elementos de autenticación están configurados para autenticar la cabecera de seguridad. Si el nodo no es el destinatario, se contemplan dos opciones preferentes: los elementos de autenticación pueden bien ser evitados para no aumentar el retardo del enlace, o bien pueden ser utilizados para autenticar la cabecera de seguridad selectivamente cuando el retardo acumulado no supera un determinado umbral. Esta segunda opción puede implementarse autenticando las tramas recibidas, pero deteniendo o descartando dicha autenticación en caso de que la trama deba ser retransmitida antes de que la autenticación haya terminado, evitando así que ralentice la red.

Finalmente, en un tercer aspecto de la invención se presenta un programa de ordenador que comprende medios de código de programa de ordenador adaptados para implementar el método descrito, al ejecutarse en un procesador digital de la señal, un circuito integrado específico de la aplicación, un microprocesador, un microcontrolador o cualquier otra forma de hardware programable. Nótese que cualquier opción preferente e implementación particular del dispositivo de la invención puede ser aplicado al método y al programa de ordenador de la invención, y viceversa.

El método, sistema y programa de ordenador de la invención proporcionan por lo tanto redundancia y seguridad a una red ethernet en anillo, minimizando el retardo en las comunicaciones como consecuencia de proteger la cabecera de redundancia. Es decir, el método protege tanto el mensaje como la información necesaria para garantizar la redundancia, sin penalizar el tiempo en la red respecto a opciones sin securizar. Adicionalmente, al no ser necesario resolver la seguridad en todos los nodos del anillo para acceder a la información de enrutado, todos los aspectos de la invención pueden ser implementados en anillos que combinen nodos con capacidades de seguridad y modos que no implementen dichas capacidades de seguridad. Es decir, la invención es compatible con elementos no securizados, así como con protocolos de alto nivel que requieren la modificación de las tramas en cada elemento enrutador intermedio. Asimismo, no requiere compartir secretos entre elementos del anillo para su correcto funcionamiento, pero permite que todos los elementos de la red puedan poseer los diferentes parámetros de seguridad, aumentándose la resistencia de red frente a potenciales ciber ataques. Todas éstas y otras ventajas de la invención serán aparentes a la luz de la descripción detallada de la misma.

Breve descripción de las figuras

Para complementar la descripción y con objeto de ayudar a una mejor comprensión de las características de la invención, de acuerdo con un ejemplo de realización práctica de la misma, se acompaña como parte integrante de la descripción, un juego de figuras en el que con carácter ilustrativo y no limitativo, se ha representado lo siguiente:

La figura 1 representa esquemáticamente una primera trama de un anillo ethernet redundante en el que el protocolo de redundancia se introduce dentro del protocolo de seguridad, de acuerdo con lo conocido en el estado de la técnica.

La figura 2 muestra esquemáticamente una segunda trama de un anillo ethernet redundante en el que el protocolo de seguridad se introduce dentro del protocolo de redundancia, de acuerdo con lo conocido en el estado de la técnica.

La figura 3 ilustra una tercera trama de un anillo ethernet redundante de acuerdo con una implementación particular de la presente invención.

La figura 4 ejemplifica los bloques lógicos comprendidos en un nodo de un anillo ethernet redundante de acuerdo con una implementación particular de la presente invención.

Descripción de un modo de realización de la invención

En este texto, la palabra “comprende” y sus variantes (como “comprendiendo”, etc.) no deben interpretarse de forma excluyente, es decir, no excluyen la posibilidad de que lo descrito incluya otros elementos, pasos etc.

Por otra parte, la invención no está limitada a las realizaciones concretas que se han descrito sino abarca también, por ejemplo, las variantes que pueden ser realizadas por el experto medio en la materia (por ejemplo, en cuanto a la elección de materiales, dimensiones, componentes, configuración, etc.), dentro de lo que se desprende de las reivindicaciones.

Nótese en particular, que si bien algunas realizaciones concretas de la invención han sido descritas utilizando HSR como protocolo de redundancia y MacSec como protocolo de seguridad, la invención puede realizarse con cualquier otro protocolo de seguridad y/o redundancia conocido en el estado de la técnica para anillos ethernet redundantes. Como ejemplos no limitativos, el protocolo de redundancia también puede ser un protocolo de anillo abierto (del inglés 'Open Ring'), un protocolo de redundancia en paralelo (PRP, del inglés 'Parallel Redundancy Protocol'), un protocolo Ethernet/IP (del inglés 'Ethernet Industrial Protocol'), un protocolo de anillo a nivel de dispositivo (DLR, del inglés 'Device Level Ring'), un protocolo de redundancia de medios (MRP, del inglés 'Media Redundancy Protocol'), un protocolo Profinet, o un protocolo Ethercat, entre otros. Asimismo, como ejemplos no limitativos, el protocolo de seguridad también puede ser un protocolo de tunelado de capa 2 (L2PT, del inglés 'Layer 2 Protocol Tunneling'), un protocolo de privacidad equivalente a cableado (WEP, del inglés ' Wired Equivalent Privacy ') o un protocolo de acceso wi-fi protegido (WPA, del inglés 'Wi-fi Protected Access'), entre otros.

La figura 1 presenta una primera trama de ejemplo en un anillo ethernet que combina redundancia y seguridad de acuerdo con lo conocido en el estado de la técnica previo a la presente invención. La primera trama comprende un destinatario (1), una fuente (2), una cabecera de seguridad (3), una cabecera de redundancia (4) que comprende la información de enrutado, una carga útil (en inglés 'payload') (5), un valor de comprobación de integridad (ICV, del inglés 'integrity check value') (6) y una secuencia de comprobación de trama (FCS, del inglés 'frame check sequence) (7). Nótese que la cabecera de seguridad (3) aparece antes de la cabecera de redundancia (4), estando por lo tanto el protocolo de enrutado encapsulado dentro del protocolo de seguridad. Se ha representado también con un indicador (8) los elementos de la trama securizados, es decir: el destinatario (1), la fuente (2), la cabecera de seguridad (3), la cabecera de redundancia (4) y la carga útil (5). En consecuencia, todo el mensaje queda protegido, pero para poder acceder a la cabecera de redundancia (4), es necesario resolver primero el protocolo de seguridad. Puesto que la cabecera de redundancia (4) debe ser accedida en todos los nodos intermedios, esto supone un retardo de las comunicaciones dentro del anillo que limita el tamaño del mismo.

La figura 2 presenta una segunda trama de ejemplo en un anillo ethernet que combina redundancia y seguridad de acuerdo con lo conocido en el estado de la técnica previo a la presente invención. La segunda trama comprende los mismos campos que la primera trama, con la diferencia de que la cabecera de redundancia (4) aparece antes que la cabecera de seguridad (3). En consecuencia, no es necesario resolver la seguridad para acceder a la información de redundancia, pero la cabecera de redundancia (4) no queda protegida, como se aprecia en el indicador (8). Dicha cabecera de redundancia (4) puede por lo tanto ser atacada convirtiéndose en una brecha de seguridad.

La figura 3 presenta una tercera trama de ejemplo en un anillo ethernet, utilizada por el método, sistema y programa de ordenador de la presente invención. La disposición de los campos es la misma que en el caso de la segunda trama de ejemplo, pero la protección de seguridad abarca a la cabecera de redundancia (4), como se aprecia en el indicador (8). Es decir, a pesar de que la cabecera de redundancia (4) está encapsulada dentro de la cabecera de seguridad (3), el protocolo de seguridad se ejecuta sobre el destinatario (1), la fuente (2), la cabecera de seguridad (3), la cabecera de enrutado (4) y la carga útil (5). Para poder acceder a la cabecera de redundancia (4) no es necesario resolver la seguridad, pero dicha cabecera de redundancia (4) está

completamente protegida.

La figura 4 presenta los elementos principales de un nodo (10) de un anillo ethernet redundante en el que se implementa una realización preferente del sistema de la invención, que a su vez ejecuta los pasos de una realización preferente del método de la invención. El nodo (10) está conectado a dos enlaces ethernet (20) a través de dos puertos (11) que actúan como interfaz físico, si bien pueden existir otras implementaciones con un mayor número de enlaces y de sus correspondientes puertos (11). Cada puerto (11) está conectado a un controlador ethernet (12), que a su vez está conectado a un elemento de autenticación (13) (que puede comprender asimismo capacidades de desencriptado) y a un autenticador (14) (que puede comprender asimismo capacidades de encriptado). Nótese que en el presente texto se entiendo como elemento de autenticación (13) a los medios que realizan la comprobación de autenticación, y por autenticador (14) a los medios que introducen en la trama los elementos necesarios para permitir dicha autenticación. Es decir, el elemento de autenticación (13) actúa en recepción y el autenticador (14) actúa en transmisión. Común a ambos puertos (11), el nodo comprende además un controlador de redundancia (15) que transmite las tramas cuyo destinatario sea el propio nodo (10) a las capas superiores (16) del mismo.

Cuando el nodo (10) recibe una trama a través de un puerto (11), el controlador ethernet (12) comprueba la presencia de un carácter que delimita el inicio de trama y transmite la capa completa al elemento de autenticación (13). El controlador ethernet (12) también calcula la secuencia de comprobación de trama (FCS, del inglés 'Frame Check Sequence'. Si la trama está encriptada y el nodo (10) es el destinatario final del mensaje, el elemento de autenticación (13) realiza el procesamiento de seguridad correspondiente. Nótese que el nodo (10) puede ser el destinatario único del mensaje, o ser uno de múltiples destinatarios en un mensaje de difusión (del inglés 'broadcast') o multidifusión (del inglés 'multicast'). El procesamiento de seguridad comprende la autenticación del destinatario (1), la fuente (2), la cabecera de seguridad (3), la cabecera de enrutado (4) y la carga útil (5). El procesamiento de seguridad puede comprender adicionalmente el desencriptado del mensaje. Una vez realizado el procesamiento de seguridad, el mensaje se traslada al controlador de redundancia (15) junto con la validación FCS y la validación de la integridad criptográfica. Al tratarse de un destinatario de la trama, el controlador de redundancia (15) transmite el mensaje a las capas superiores (16).

Cuando la trama no está dirigida al nodo (10), no es necesario que el elemento de autenticación (13) realice el procesamiento de seguridad, evitando así retardos innecesarios en la transmisión. La trama se transmite al controlador de redundancia (15) que decide si transmitir la trama por un enlace ethernet (20) diferente a aquél por el que se ha recibido. En caso afirmativo, la trama se transmite al autenticador (14), que decide si procesar dicha trama. Si la trama ha sido modificada en el interior del sistema, el autenticador (14) realiza de nuevo la autenticación. Si la trama procede del propio nodo (10), el autenticador (14) realiza la autenticación y/o encriptación atendiendo a las reglas de seguridad definidas por los protocolos involucrados. Según vaya obteniendo la trama final, el autenticador (14) la pasa al controlador ethernet (12) que prepara la trama para ser enviada añadiendo el preámbulo, comienzo de trama y anexando la secuencia de comprobación de trama. El puerto (11) traduce la información digital en señales analógicas propias del medio (10).

En el caso en el que falle la autenticación de una trama, el nodo (10) la desecha y, si está instruido para ello, informa a niveles superiores de un posible ataque. Si la trama ha comenzado a transmitirse y, por tanto, no puede interrumpirse su transmisión, se modifica su secuencia de comprobación de trama para que, cualquier nodo, aún sin conocimiento del proceso de seguridad, la pueda detectar como errónea.

Finalmente, de acuerdo con una implementación preferente, un nodo intermedio que no es destinatario de la trama puede configurarse para realizar el proceso de seguridad cuando no ralentiza la red. Para ello, se comprueba la seguridad de cada trama recibida en los elementos de autenticación (13). Si el proceso de seguridad acaba antes de que la trama haya empezado a retransmitirse, se aplica todo el procesamiento de seguridad sin aumentar la latencia. Esto puede ocurrir cuando el puerto (11) de salida está ocupado por una trama que todavía no ha terminado de transmitirse, por ejemplo en el caso de que desde el nodo local se envíe una trama a la vez que llega una segunda trama desde otro puerto. En caso de que la trama recibida esté lista para ser retransmitida antes de que finalice la autenticación, el procesado de seguridad se desecha y se transmite directamente.

REIVINDICACIONES

1.- Método de seguridad en un anillo ethernet redundante que comprende recibir una trama en un nodo (10), comprendiendo dicha trama un destinatario (1) y una cabecera de un protocolo de seguridad (3) encapsulada dentro de una cabecera de un protocolo de redundancia (4), caracterizado por que el método comprende:
comprobar si el nodo (10) es o no destinatario (1);
-si el nodo (10) es destinatario (1), autenticar la cabecera de redundancia (4) mediante el protocolo de seguridad.

2. Método según la reivindicación 1 caracterizado por que comprende además, si el nodo (10) no es el destinatario (1) de la trama, no autenticar la cabecera del protocolo de redundancia (4).

3. Método según la reivindicación 1 caracterizado por que comprende además si el nodo (10) no es el destinatario (1) de la trama, autenticar la cabecera del protocolo de redundancia (4) solamente si el retardo ocasionado por la autenticación es menor que un umbral.

4. Método según la reivindicación 3 caracterizado por que comprende, si el nodo (10) no es el destinatario (1) de la trama:
- iniciar la autenticación de la cabecera del protocolo de redundancia (4) al recibir la trama;
- Detener la autenticación de la cabecera del protocolo de redundancia (4) si la trama puede ser retransmitida antes de haber finalizado la autenticación.

5. Método según cualquiera de las reivindicaciones anteriores caracterizado por que el protocolo de seguridad es un estándar de seguridad de control de acceso al medio.

6. Método según cualquiera de las reivindicaciones anteriores caracterizado por que el protocolo de redundancia es un protocolo de anillo homogéneo de alta disponibilidad.

7. Método según cualquiera de las reivindicaciones anteriores caracterizado por que comprende desencriptar la trama recibida de acuerdo con el protocolo de seguridad.

8. Sistema de seguridad en un anillo ethernet redundante que comprende un controlador de redundancia (15) y una pluralidad de elementos de autenticación (13) conectados a una pluralidad de puertos (11) de un nodo (10) del anillo, caracterizado por que la pluralidad de elementos de autenticación (13) están configurados para:
- recibir una trama que comprende un destinatario (1) y una cabecera de un protocolo de seguridad (3) encapsulada dentro de una cabecera de un protocolo de redundancia (4);
- comprobar si el nodo (10) es o no un destinatario (1) de la trama recibida y, si el nodo (10) es destinatario, autenticar la cabecera del protocolo de redundancia (4).

9. Sistema de acuerdo con la reivindicación 8 caracterizado por que la pluralidad de elementos de autenticación (14) están configurados para, si el nodo (10) no es el destinatario (1) de la trama, no autenticar la cabecera de redundancia (4) mediante el protocolo de seguridad.

10. Sistema de acuerdo con la reivindicación 8 caracterizado por que la pluralidad de elementos de autenticación (13) están configurados para, si el nodo (10) no es el destinatario (1) de la trama, autenticar la cabecera del protocolo de redundancia (4) si el retardo ocasionado por la autenticación es menor que un umbral.

11. Sistema de acuerdo con la reivindicación 10 caracterizado por que la pluralidad de elementos de autenticación (13) están configurados para, si el nodo (10) no es el destinatario (1) de la trama:
- iniciar la autenticación de la cabecera del protocolo de redundancia (4) al recibir la trama;
- detener la autenticación de la cabecera del protocolo de redundancia (4) si la trama puede ser retransmitida antes de haber finalizado la autenticación.

12. Sistema de acuerdo con cualquiera de las reivindicaciones 8 a 11, caracterizado por que la pluralidad de elementos de autenticación (13) implementan un estándar de seguridad de control de acceso al medio.

13. Sistema de acuerdo con cualquiera de las reivindicaciones 8 a 12, caracterizado por que el controlador de redundancia (15) implementa un protocolo de anillo homogéneo de alta disponibilidad.

14. Sistema de acuerdo con cualquiera de las reivindicaciones 8 a 13 caracterizado por que la pluralidad de elementos de autenticación (13) están además configurados para desencriptar la trama recibida.

15. Programa de ordenador que comprende medios de código de programa de ordenador adaptados para

realizar las etapas del método de cualquiera de las reivindicaciones 1 a 7, cuando el mencionado programa se ejecuta en un procesador digital de la señal, un circuito integrado específico de la aplicación, un microprocesador, un microcontrolador o cualquier otra forma de hardware programable.

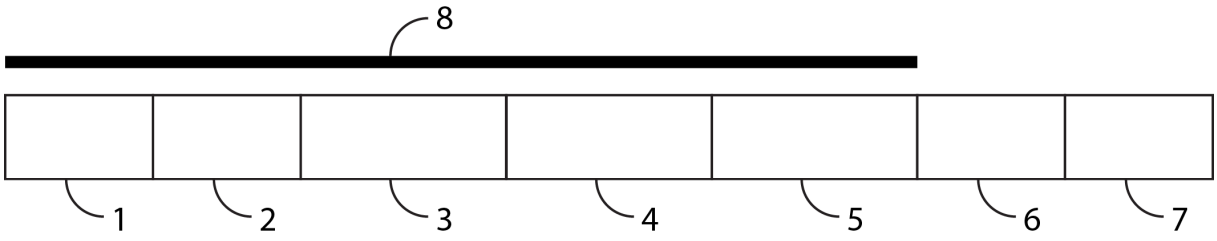

Fig. 1

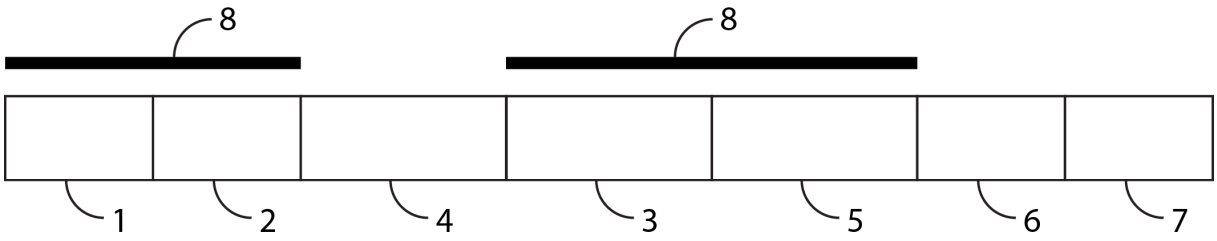

Fig. 2

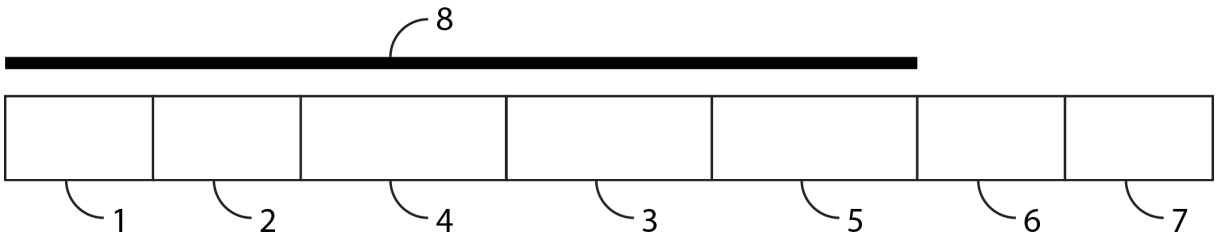

Fig. 3

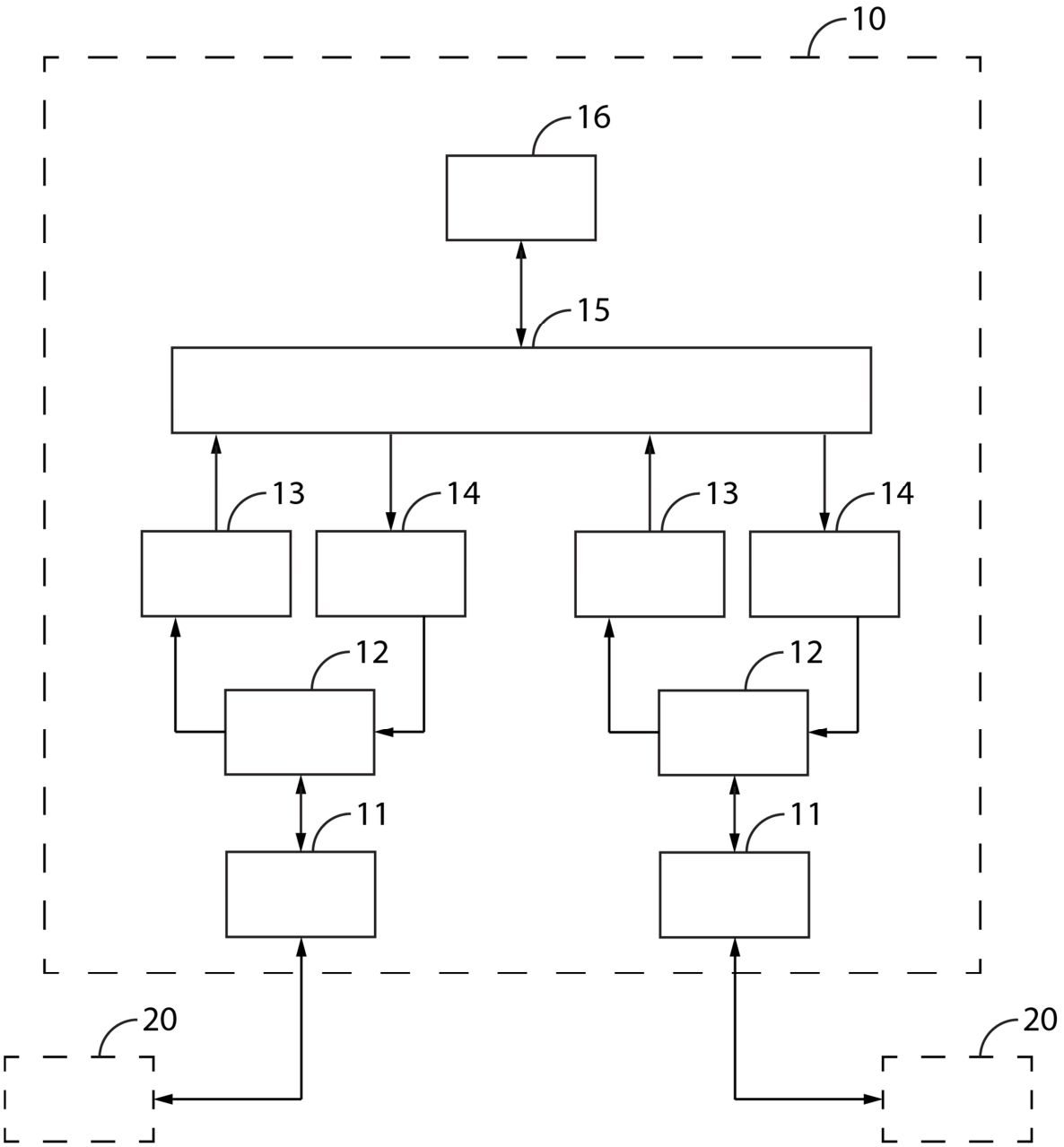

Fig. 4

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201530970

(22) Fecha de presentación de la solicitud: 06.07.2015

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***H04L1/22*** (2006.01)
H04L12/00 (2006.01)

DOCUMENTOS RELEVANTES

Categoría	(56) Documentos citados	Reivindicaciones afectadas
A	CLEMENS HOGA Seamless communication redundancy of IEC 62439.Advanced Power System Automation and Protection (APAP), 2011 International Conference on, 20111016 IEEE 16/10/2011 VOL: Pags: 489 – 494 ISBN 978-1-4244-9622-8 ; ISBN 1-4244-9622-5 Doi: 10.1109/APAP.2011.6180451. Todo el documento.	1-15
A	TAL MIZRAHI Time synchronization security using IPsec and MACsec.Precision Clock Synchronization for Measurement Control and Communication (ISPCS), 2011 International IEEE Symposium on, 20110912 IEEE 12/09/2011 VOL: Pags: 38 - 43 ISBN 978-1-61284-893-8 ; ISBN 1-61284-893-1 doi:10.1109/ISPCS.2011.6070153. Todo el documento.	1-15
A	US 5400334 A (HAYSSEN CARL G) 21/03/1995, todo el documento.	1-15
A	EP 1657888 A1 (ABB RESEARCH LTD) 17/05/2006, todo el documento.	1-15

Categoría de los documentos citados
X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	Examinador	Página
30.11.2016	M. Muñoz Sanchez	1/4

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

H04L

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, WPI, NPL, XPIEE, XPI3E

Fecha de Realización de la Opinión Escrita: 30.11.2016

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	1-15	**SI**
	Reivindicaciones		**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones	1-15	**SI**
	Reivindicaciones		**NO**

Se considera que la solicitud cumple con el requisito de aplicación industrial. Este requisito fue evaluado durante la fase de examen formal y técnico de la solicitud (Artículo 31.2 Ley 11/1986).

Base de la Opinión.-

La presente opinión se ha realizado sobre la base de la solicitud de patente tal y como se publica.

1. Documentos considerados.-

A continuación se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	CLEMENS HOGA Seamless communication redundancy of IEC 62439.Advanced Power System Automation and Protection (APAP), 2011 International Conference on, 20111016 IEEE 16/10/2011 VOL: Pags: 489 - 494 ISBN 978-1-4244-9622-8 ; ISBN 1-4244-9622-5 Doi: 10.1109/APAP.2011.6180451. Todo el documento.	16.10.2011
D02	TAL MIZRAHI Time synchronization security using IPsec and MACsec.Precision Clock Synchronization for Measurement Control and Communication (ISPCS), 2011 International IEEE Symposium on, 20110912 IEEE 12/09/2011 VOL: Pags: 38 - 43 ISBN 978-1-61284-893-8 ; ISBN 1-61284-893-1 doi:10.1109/ISPCS.2011.6070153. Todo el documento.	12.09.2011
D03	US 5400334 A (HAYSSEN CARL G)	21.03.1995
D04	EP 1657888 A1 (ABB RESEARCH LTD)	17.05.2006

2. Declaración motivada según los artículos 29.6 y 29.7 del Reglamento de ejecución de la Ley 11/1986, de 20 de marzo, de Patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración

Se considera D01 el documento más próximo del estado de la técnica al objeto de la solicitud.

Reivindicaciones independientes

Reivindicación 1: El documento D01, divulga un sistema de anillo Ethernet cuyo protocolo de funcionamiento de capa 2 del modelo OSI utiliza una cabecera de redundancia HSR para controlar el flujo del par de tramas idénticas del protocolo HSR. El documento no menciona cabeceras de autenticación/ seguridad y, por tanto, tampoco los nodos autentican la cabecera de redundancia, en particular el nodo destinatario de una trama no lo hace. El problema técnico así consistiría en cómo añadir un protocolo de seguridad con autenticación del contenido de tramas pero sin introducir retardos excesivos en el tráfico de la red.
El documento D02 por su parte presenta varios escenarios relativos a la seguridad de tratamiento de tramas describiendo el protocolo de seguridad de capa 2 del modelo OSI MACSEC en el que se introduce una cabecera de autenticación de trama. En este documento no se menciona la existencia de una cabecera de redundancia y, por tanto, tampoco la estructura de la trama completa que incluiría ambas cabeceras.
Los documentos D03 y D04 por su parte tratan la seguridad de mensajes en redes de anillo con paso de testigo, *token ring*, y tratamiento de tramas redundantes y no redundantes pero sin incluir ambas funcionalidades a la vez ni tampoco, por tanto, la estructura de trama que permite no acumular retardos en el procesamiento del tráfico de red.
En consecuencia, a la luz de los documentos más relevantes del estado de la técnica anterior: D01, D02, D03 y D04, la reivindicación 1 presenta actividad inventiva según el art. 8.1 de la Ley de Patentes.

Reivindicación 8: el sistema reivindicado es el necesario para la implementación del método de la reivindicación 1, consiguiendo por tanto las funcionalidades que implican actividad inventiva de dicho método. En consecuencia, la reivindicación 8 también presenta actividad inventiva según el art. 8.1 de la Ley de Patentes.

Reivindicación 15: el programa de ordenador reivindicado es el necesario para la implementación del método de la reivindicación 1, utilizando el sistema de la reivindicación 8, consiguiendo por tanto las funcionalidades que implican actividad inventiva de dicho método y dicho sistema. En consecuencia, la reivindicación 15 también presenta actividad inventiva según el art. 8.1 de la Ley de Patentes.

Reivindicaciones dependientes

Reivindicaciones 2-7, 9-14: estas reivindicaciones también poseen actividad inventiva según el art. 8.1 de la Ley de Patentes, por depender de las reivindicaciones 1 y 8 respectivamente que también la presentan.