(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 737 827**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **26.03.2013 PCT/CN2013/073197**

(87) Fecha y número de publicación internacional: **02.10.2014 WO14153718**

(96) Fecha de presentación y número de la solicitud europea: **26.03.2013 E 13880191 (5)**

(97) Fecha y número de publicación de la concesión europea: **01.05.2019 EP 2985946**

(54) Título: **Procedimiento y aparato para comando de protección de protección de retransmisión de transmisión**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.01.2020

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Werner-von-Siemens-Straße 1
80333 München, DE

(72) Inventor/es:

SHU, ZHONGHUA

(74) Agente/Representante:

LOZANO GANDIA, José

DESCRIPCIÓN

Procedimiento y aparato para comando de protección de protección de retransmisión de transmisión

CAMPO TÉCNICO

La presente invención se refiere al campo de Ethernet, y particularmente a un procedimiento y aparato para transmitir un comando de protección para una protección de retransmisión.

ANTECEDENTES

El sistema de protección de retransmisión convencional en general comprende un dispositivo de transmisión, que se utiliza para transmitir un comando de protección de protección de retransmisión. Este dispositivo de transmisión del comando de protección existente (como el SWT3000 de Siemens Ltd.) en general transmite un comando de protección de protección de retransmisión entre dos subestaciones a través de una jerarquía digital síncrona (SDH) o una red de jerarquía digital plesiócrona (PDH), como se muestra en la Fig. 1. Aquí, el comando de protección de protección de retransmisión, por ejemplo, puede ser un comando de activación de una retransmisión.

Con la amplia aplicación de la tecnología de Ethernet y para reducir el costo, la transmisión del comando de protección de la protección de retransmisión se ha transformado de la transmisión a través de la red SDH/PDH a la transmisión a través de Ethernet, como se muestra en la Fig. 2.

Sin embargo, cuando el comando de protección de la protección de retransmisión se transmite a través de Ethernet, un atacante captura y manipula fácilmente el comando de protección transmitido, de modo que el SWT3000 recibirá un comando de protección dañino y se producirá una acción incorrecta en el dispositivo de la subestación.

UGWON HONG ET AL, "Evaluación de algoritmos de seguridad en la arquitectura de comunicación de la subestación", CÁLCULO Y COMUNICACIONES ESCALABLES; OCTAVA CONFERENCIA INTERNACIONAL SOBRE CÁLCULO INTEGRADO, 2009. SCALCOM-EMBEDDEDCOM'09. CONFERENCIA INTERNACIONAL SOBRE IEEE, PISCATAWAY, NJ, EE. UU., (20090925), ISBN 978-0-7695-3825-9, páginas 314 - 318 divulga las características de las primeras partes de las reivindicaciones 1, 2, 4 y 5.

"IEC TS 62351-6. Gestión de sistemas de energía e intercambio de información asociado - Seguridad de datos y comunicaciones - Parte 6: Seguridad para IEC 61850 ", TÉCNICA DE ESPECIFICACIONES CEI - ESPECIFICACIÓN TÉCNICA IEC, (20070622), vol. 62351-6, n.º 1ª edición, páginas 1 a 16, enseña el uso de una firma digital para proporcionar autentificación de mensajes, en el que los mensajes IEC 62351 contienen un número de estado y un número de secuencia para proporcionar protección de reproducción.

CN 102 280 929 enseña el uso de una función hash con clave para proporcionar autentificación de mensajes a los mensajes intercambiados en un sistema SCADA.

SUMARIO DE LA INVENCIÓN

El objeto de la presente invención es proporcionar un procedimiento y un aparato para transmitir o recibir un comando de protección para una protección de retransmisión, que pueda mejorar la seguridad de transmitir un comando de protección de protección de retransmisión a través de Ethernet.

La presente invención está definida por los procedimientos de las reivindicaciones independientes 1 y 2 y el aparato de las reivindicaciones independientes 4 y 5. Se divulgan modos de realización preferentes en las subreivindicaciones.

Un procedimiento para transmitir un comando de protección para una protección de retransmisión de acuerdo con los modos de realización de la presente invención comprende: calcular un resumen de mensajes de datos designados, en el que los datos designados comprenden un comando de protección que debe enviarse y la información de contraseña establecida con una parte receptora por adelantado; y enviar un paquete de datos que incluya el comando de protección y el resumen del mensaje calculado a la parte receptora a través de Ethernet.

En una implementación particular, el procedimiento comprende además: generar información del orden de envío sobre el comando de protección de acuerdo con un orden de prioridad de envío del comando de protección, en el que los datos designados y el paquete de datos comprenden además la información del orden de envío generada.

En una implementación particular, la información del orden de envío comprende un número de estado y un número de secuencia, en el que el número de estado representa una ronda de envío de comandos a la que se envía el comando de protección, y el número de secuencia representa un lote de envío de comandos donde se envía el comando de protección en la ronda de envío de comandos donde se envía el comando de protección.

En una implementación particular, la información del orden de envío comprende además una marca de tiempo, en la que la marca de tiempo representa una hora de inicio de la ronda de envío de comandos donde se envía el comando de protección, y los datos designados y el paquete de datos comprenden además un tiempo permitido activo, en el que el tiempo permitido activo se utiliza para notificar a la parte receptora el tiempo más largo de espera del siguiente paquete de datos.

Un procedimiento para transmitir un comando de protección para una protección de retransmisión de acuerdo con los modos de realización de la presente invención comprende: cuando se recibe un paquete de datos que comprende un comando de protección y un resumen de mensajes, calcular un resumen de mensajes de datos designados, en el que los datos designados comprenden una información de contraseña establecida con una parte remitente por adelantado y el comando de protección; comparar si el resumen del mensaje calculado es el mismo que el resumen del mensaje comprendido en el paquete de datos recibido; y si el resultado de la comparación es no, descartar el paquete de datos recibido.

En una implementación particular, el paquete de datos recibidos comprende además enviar información del orden sobre el comando de protección, en el que el procedimiento comprende además: comprobar si la información del orden de envío sobre el comando de protección es más reciente que la última información del orden de envío almacenada; y si el resultado de la comprobación es no, descartar el paquete de datos.

En una implementación particular, el procedimiento comprende además: si el resultado de la comprobación y el resultado comparativo son ambos sí, aceptar el paquete de datos recibido; y almacenar la información del orden de envío sobre el comando de protección como la información del orden de envío más reciente.

En una implementación particular, la información del orden de envío comprende un número de estado y un número de secuencia, en el que el número de estado representa una ronda de envío de comandos a la que se envía el comando de protección, y el número de secuencia representa un lote de envío de comandos donde se envía el comando de protección en la ronda de envío de comandos donde se envía el comando de protección.

Un aparato para transmitir un comando de protección para una protección de retransmisión de acuerdo con los modos de realización de la presente invención comprende: un módulo de cálculo para calcular un resumen de mensajes de datos designados, en el que los datos designados comprenden un comando de protección que debe enviarse y la información de la contraseña se establece con una parte de recepción con antelación y un módulo de envío para enviar un paquete de datos que comprende el comando de protección y el resumen del mensaje calculado a la parte receptora a través de Ethernet.

En una implementación particular, el aparato comprende además: un módulo de generación para generar información del orden de envío sobre el comando de protección de acuerdo con un orden de prioridad de envío del comando de protección, en el que los datos designados y el paquete de datos comprenden además la información del orden de envío generada.

En una implementación particular, la información del orden de envío comprende un número de estado y un número de secuencia, en el que el número de estado representa una ronda de envío de comandos a la que se envía el comando de protección, y el número de secuencia representa un lote de envío de comandos donde se envía el comando de protección en la ronda de envío de comandos donde se envía el comando de protección.

En una implementación particular, la información del orden de envío comprende además una marca de tiempo, en la que la marca de tiempo representa una hora de inicio de la ronda de envío de comandos donde se envía el comando de protección, y los datos designados y el paquete de datos comprenden además un tiempo permitido activo, en el que el tiempo permitido activo se utiliza para notificar a la parte receptora el tiempo más largo de espera del siguiente paquete de datos.

Un aparato para recibir un comando de protección para una protección de retransmisión de acuerdo con los modos de realización de la presente invención comprende: un módulo de cálculo para calcular, cuando se recibe un paquete de datos que comprende un comando de protección y un resumen de mensajes, una síntesis de mensaje de datos designados, en el que los datos designados comprenden información de contraseña establecida con una parte remitente por adelantado y el comando de protección; un módulo de comparación para comparar si el resumen del mensaje calculado es el mismo que el resumen del mensaje comprendido en el paquete de datos recibido; y un módulo de descarte para descartar el paquete de datos recibido si el resultado de comparación es no.

En una implementación particular, el paquete de datos recibidos comprende además enviar información del orden sobre el comando de protección, en el que el aparato comprende además un módulo de comprobación para comprobar si la información del orden de envío sobre el comando de protección es más nueva que la última información del orden de envío almacenada, y en el que el módulo de descarte se usa para descartar el paquete de datos si el resultado de la comprobación es no.

En una implementación particular, el aparato comprende además: un módulo de aceptación para aceptar el paquete de datos recibido si el resultado de la comprobación y el resultado de comparación son ambos sí; y un módulo de almacenamiento para almacenar la información del orden de envío sobre el comando de protección como la información del orden de envío más reciente.

En una implementación particular, la información del orden de envío comprende un número de estado y un número de secuencia, en el que el número de estado representa una ronda de envío de comandos a la que se envía el comando de protección, y el número de secuencia representa un lote de envío de comandos donde se envía el comando de protección en la ronda de envío de comandos donde se envía el comando de protección.

A partir de la descripción anterior, se puede ver que la solución de los modos de realización de la presente invención transmite un paquete de datos que comprende un comando de protección de protección de retransmisión y un resumen de mensajes que se obtiene a través del cálculo combinando el comando de protección y la información de contraseña entre una parte remitente y una parte receptora juntas de antemano y se utiliza para identificar la integridad del comando de protección a través de Ethernet; sin embargo, el paquete de datos no incluye la información de la contraseña. Por lo tanto, si un atacante captura y manipula el comando de protección en el paquete de datos, dado que el atacante no conoce la información de la contraseña, tanto si todavía utiliza el resumen del mensaje original en el paquete de datos como si recalcula un resumen del mensaje, un resumen de la información en el paquete es incorrecto con respecto al comando de protección que ha sido manipulado, y la parte receptora puede detectar fácilmente que el comando de protección ha sido manipulado basándose en el resumen de información en el paquete de datos, de modo que la solución de los modos de realización del presente la invención puede mejorar la seguridad de transmitir un comando de protección a través de Ethernet.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Estas y otras características y ventajas de la presente invención resultarán más evidentes a partir de la siguiente descripción detallada cuando se tome conjuntamente con los dibujos adjuntos.

La Fig. 1 muestra un diagrama esquemático de transmisión de un comando de protección de protección de retransmisión de la técnica anterior.

La Fig. 2 muestra un diagrama esquemático de transmisión de un comando de protección de protección de retransmisión de la técnica anterior.

La Fig. 3 muestra un diagrama de flujo de un procedimiento para transmitir un comando de protección de protección de relé de acuerdo con un modo de realización de la presente invención.

La Fig. 4 muestra un diagrama esquemático del cambio de información del orden de envío de acuerdo con un modo de realización de la presente invención.

La Fig. 5 es un diagrama esquemático de un aparato para transmitir un comando de protección de protección de relé de acuerdo con un modo de realización de la presente invención.

La Fig. 6 muestra un diagrama esquemático de un aparato para transmitir un comando de protección de protección de retransmisión de acuerdo con otro modo de realización de la presente invención.

La Fig. 7 muestra un diagrama esquemático de un dispositivo de transmisión del comando de protección de acuerdo con un modo de realización de la presente invención.

DESCRIPCIÓN DETALLADA

Varios modos de realización de la presente invención se describirán en más detalle a continuación conjuntamente con los dibujos adjuntos.

Ahora, consulte la Fig. 3 que muestra un diagrama de flujo de un procedimiento para transmitir un comando de protección para una protección de retransmisión de acuerdo con un modo de realización de la presente invención. Aquí, el procedimiento de este modo de realización se describe en detalle al tomar que un dispositivo de transmisión del comando de protección A transmite un comando de protección de protección de retransmisión a un dispositivo de transmisión del comando de protección B a través de Ethernet como ejemplo.

Como se muestra en la Fig. 3, en el paso S300, cuando un comando de protección M de protección de retransmisión se transmite al dispositivo de transmisión del comando de protección B, el dispositivo de transmisión del comando de protección A genera información del orden de envío CX sobre el comando de protección M de acuerdo con un orden de prioridad de envío del comando de protección M. Aquí, el comando de protección M puede ser uno o más comandos, y la información del orden de envío CX sobre el comando de protección M comprende un número de estado stNum, un número de secuencia sqNum y una marca de tiempo t, donde el estado el número stNum representa

una ronda de envío de comandos donde se envía el comando de protección M. En general, en un sistema de energía eléctrica, existe la necesidad de transmitir un comando de protección para una protección de retransmisión solo cuando se produce un problema a un dispositivo protegido; y dado que el dispositivo protegido no siempre presenta el problema, la transmisión del comando de protección para una protección de retransmisión es intermitente, es decir, puede ser necesario transmitir el comando de protección en un período de tiempo determinado, y a continuación puede ser necesario para transmitir el comando de protección en un período de tiempo determinado después de un intervalo regular. Por lo tanto, la ronda de envío de comandos aquí representa el período de tiempo en el que se envía el comando de protección M. El número de secuencia sqNum representa un lote de envío de comandos donde se envía el comando de protección M en la ronda de envío de comandos donde se envía el comando de protección M. En general, se pueden enviar uno o más comandos de protección en cada ronda de envío de comandos, y el comando que envía el lote aquí representa el comando de protección M que se envía, en qué lote de la ronda de envío de comandos a la que se envía el comando de protección M. La marca de tiempo t representa una hora de inicio de la ronda de envío de comandos a la que se envía el comando de protección M.

En el paso S304, el dispositivo de transmisión del comando de protección A combina el comando de protección M, la información del orden de envío CX sobre el comando de protección M, el tiempo permitido para timeToAlive activo y la información de contraseña PW preestablecida por el dispositivo de transmisión del comando de protección A y la transmisión del comando de protección dispositivo B en los datos SJ1. Aquí, el comando de protección M, la información del orden de envío CX, el tiempo permitido para el timeToAlive activo y la información de contraseña PW pueden organizarse sucesivamente juntos para formar los datos SJ1 de acuerdo con un orden negociado por los dispositivos de transmisión del comando de protección A y B de antemano. El tiempo permitido para timeToAlive activo se usa para notificar que el dispositivo de transmisión B del comando de protección sirve como parte receptora del tiempo más largo de espera para el próximo paquete de datos.

En el paso S308, el dispositivo de transmisión del comando de protección A utiliza el algoritmo de resumen de mensajes MD5 para calcular un resumen de mensajes XZ1 de los datos SJ1. El resumen del mensaje también se denomina resumen digital, y es un valor que corresponde únicamente a una longitud fija de datos (como un mensaje o texto), que se genera al operar los datos mediante una función de cifrado hash de una sola vía. Si los datos cambian en el recorrido, un receptor puede saber si los datos se cambian comparando el resumen recién generado de los datos recibidos con el resumen original. Por lo tanto, el resumen del mensaje garantiza la integridad de los datos. El algoritmo de resumen de mensajes MD5 es una función hash ampliamente utilizada en el campo de la seguridad informática, y se utiliza para proporcionar protección de integridad de datos. Los estándares del algoritmo de resumen de mensajes MD5 se indican en RFC1321.

En el paso S312, el dispositivo de transmisión del comando de protección A envía un paquete de datos SB al dispositivo de transmisión del comando de protección B a través de Ethernet, en el que el paquete de datos SB comprende el comando de protección M, la información del orden de envío CX sobre el comando de protección M, el tiempo permitido para timeToAlive activo y el resumen del mensaje XZ1.

En el paso S316, después de recibir el paquete de datos SB del dispositivo de transmisión del comando de protección A, el dispositivo de transmisión del comando de protección B combina el comando de protección M, la información del orden de envío CX sobre el comando de protección M, el tiempo permitido para el timeToAlive activo y la información de contraseña PW preestablecida por el dispositivo de transmisión del comando de protección A y el dispositivo de transmisión del comando de protección B que están comprendidos en el paquete de datos SB en datos SJ2. Aquí, el comando de protección M, la información del orden de envío CX, el tiempo permitido para el timeToAlive activo y la información de contraseña PW que se incluyen en el paquete de datos SB se pueden organizar de manera sucesiva para formar los datos SJ2 de acuerdo con un orden negociado mediante los dispositivos de transmisión del comando de protección A y B por adelantado.

En el paso S320, el dispositivo de transmisión del comando de protección B usa el algoritmo de resumen de mensajes MD5 para calcular un resumen de mensajes XZ2 de los datos SJ2.

En el paso S324, el dispositivo de transmisión del comando de protección B comprueba si el resumen XZ2 de mensaje calculado es el mismo que el resumen XZ1 del mensaje comprendido en el paquete de datos SB.

En el paso S328, si el resultado de la comprobación del paso S324 es no, es decir, el resumen del mensaje XZ2 es diferente del resumen del mensaje XZ1, el comando de protección M en el paquete de datos SB puede manipularse en el proceso de transmisión, el dispositivo de transmisión del comando de protección B descarta el paquete de datos SB y el proceso finaliza.

En el paso S332, si el resultado de la comprobación del paso S324 es sí, es decir, el resumen de mensajes XZ2 es el mismo que el resumen de mensajes XZ1, el dispositivo de transmisión del comando de protección B detecta si la información del orden de envío CX sobre el comando de protección M comprendida en el paquete de datos SB es más nueva que la última información del orden de envío CXnew almacenada en el dispositivo de transmisión del comando de protección B.

Si el resultado de la comprobación del paso S332 es no, es decir, la información del orden de envío CX sobre el comando de protección M incluida en el paquete de datos SB no es más reciente que la información del orden de envío más reciente CXnew almacenada en el dispositivo de transmisión del comando de protección B, el paquete de datos SB puede ser un paquete de datos reproducido por un atacante para lanzar un ataque de reproducción, y el proceso pasa al paso S328.

En el paso S336, si el resultado de la comprobación del paso S332 es sí, es decir, la información del orden de envío CX sobre el comando de protección M que se incluye en el paquete de datos SB es más reciente que la información del orden de envío más reciente CXnew almacenada en el dispositivo de transmisión del comando de protección B, se puede considerar que el paquete de datos SB no fue atacado por la reproducción en el proceso de transmisión, y el dispositivo de transmisión del comando de protección B acepta el paquete de datos SB.

En el paso S340, el dispositivo de transmisión del comando de protección B almacena la información del orden de envío CX sobre el comando de protección M incluida en el paquete de datos SB como la última información del orden de envío CXnew.

Con referencia ahora a la Fig. 4, muestra un diagrama esquemático del cambio de información del orden de envío de acuerdo con un modo de realización de la presente invención. Como se muestra en la Fig. 4, al principio, el dispositivo de transmisión del comando de protección A no tiene un comando de protección para una protección de transmisión que sea necesario enviar al dispositivo de transmisión del comando de protección B, y por lo tanto, en un momento T1, el dispositivo de transmisión del comando de protección A envía un paquete de datos que comprende una protección de comando de discriminación de frecuencia y envía información del orden sobre la protección del comando de discriminación de frecuencia al dispositivo de comando de transmisión B, y en la información del orden de envío, la marca de tiempo t es una hora t1 en el momento T1, el número de estado stNum es uno, y el número de secuencia es uno.

Después del momento T1 pero antes de un momento T2, el dispositivo de transmisión A de comando de protección recibe un comando de protección que se envía al dispositivo de transmisión B de comando de protección y, por lo tanto, en el momento T2, el dispositivo de transmisión A de comando de protección envía un paquete de datos que comprende el comando de protección, información del orden de envío sobre el comando de protección, un tiempo permitido de activación y un resumen del mensaje al dispositivo de transmisión del comando de protección B, en el que en la información del orden de envío, la marca de tiempo t es un tiempo t2 en el momento T2, el número de estado stNum es dos y el número de secuencia es uno.

En un momento T3, todavía existe un comando de protección que se envía al dispositivo de transmisión B del comando de protección y, por lo tanto, en el momento T3, el dispositivo de transmisión A del comando de protección envía un paquete de datos que comprende el comando de protección, información del orden de envío sobre el comando de protección, un tiempo permitido activo y un resumen del mensaje al dispositivo de transmisión del comando de protección B, en el que en la información del orden de envío, la marca de tiempo t sigue siendo el tiempo t2 en el momento T2 y el número de estado stNum sigue siendo dos, pero el número de secuencia es dos.

En un momento T4, todavía existe un comando de protección que debe enviarse al dispositivo de transmisión B del comando de protección y, por lo tanto, en el momento T4, el dispositivo de transmisión A del comando de protección envía un paquete de datos que comprende el comando de protección, información del orden de envío sobre el comando de protección, un tiempo permitido activo y un resumen del mensaje al dispositivo de transmisión del comando de protección B, en el que en la información del orden de envío, la marca de tiempo t sigue siendo el tiempo t2 en el momento T2 y el número de estado stNum sigue siendo dos, pero el número de secuencia es tres.

En un momento T5, todavía existe un comando de protección que se envía al dispositivo de transmisión B del comando de protección y, por lo tanto, en el momento T5, el dispositivo de transmisión A del comando de protección envía un paquete de datos que comprende el comando de protección, información del orden de envío sobre el comando de protección, un tiempo permitido activo y un resumen del mensaje al dispositivo de transmisión del comando de protección B, en el que en la información del orden de envío, la marca de tiempo t sigue siendo el tiempo t2 en el momento T2 y el número de estado stNum sigue siendo dos, pero el número de secuencia es cuatro.

En un momento T6, ya no hay un comando de protección que se envíe al dispositivo de transmisión B del comando de protección y, por lo tanto, en el momento T6, el dispositivo de transmisión A del comando de protección envía un paquete de datos que incluye una protección de comando de discriminación de frecuencia e información del orden de envío sobre la protección de comando de discriminación de frecuencia al dispositivo de transmisión del comando de protección B, en el que en la información del orden de envío, la marca de tiempo t es un tiempo t6 en el momento T6, el número de estado stNum es tres y el número de secuencia es uno.

En un momento T7, todavía no hay un comando de protección que se envíe al dispositivo de transmisión B del comando de protección y, por lo tanto, en el momento T7, el dispositivo de transmisión A del comando de protección envía un paquete de datos que incluye una protección de comando de discriminación de frecuencia e información del orden de envío sobre la protección de comando de discriminación de frecuencia al dispositivo de transmisión del

comando de protección B, en el que en la información del orden de envío, la marca de tiempo t sigue siendo el tiempo t6 en el momento T6 y el número de estado stNum sigue siendo tres, pero el número de secuencia es dos.

De la descripción anterior, se puede ver que un paquete de datos que comprende un comando de protección para una protección de retransmisión y un resumen del mensaje que se obtiene a través del cálculo combinando el comando de protección y la información de la contraseña establecida entre una parte remitente y una parte receptora juntos de antemano y se utiliza para identificar la integridad del comando de protección en Ethernet se transmite a través de Ethernet; sin embargo, el paquete de datos no incluye la información de la contraseña, si un atacante captura y manipula el comando de protección en el paquete de datos, ya que el atacante no conoce la información de la contraseña, tanto si está utilizando el resumen del mensaje original en el paquete de datos como recalculando un resumen de mensajes, un resumen de información en el paquete de datos es incorrecto con respecto al comando de protección que ha sido manipulado, y la parte receptora puede detectar fácilmente que el comando de protección ha sido manipulado basándose en el resumen de información en el paquete de datos, para que la solución de los modos de realización pueda reconocer si el comando de protección ha sido manipulado, mejorando así la seguridad de transmitir un comando de protección para una protección de retransmisión a través de Ethernet.

Además, dado que un paquete de datos transmitido a través de Ethernet comprende enviar información del orden sobre un comando de protección para una protección de retransmisión y una parte receptora almacena la última información del orden de envío, la parte receptora puede detectar si el paquete de datos recibido es un paquete de datos reproducido por un atacante comparando la información del orden de envío comprendida en el paquete de datos recibido con la información del orden de envío almacenada, de modo que la solución de este modo de realización pueda evitar un ataque de reproducción, mejorando así la seguridad de transmitir un comando de protección para una retransmisión a través de Ethernet. Otras variaciones

Un experto en la materia debería entender que, aunque en los modos de realización anteriores, las operaciones (es decir, los pasos S332-S344) para comprobar si un paquete de datos es un paquete de ataque de reproducción se ejecutan después de ejecutar las operaciones (es decir, los pasos S316-S328) para comprobar si se manipula un comando de protección, la presente invención no se limita a esto. En algunos otros modos de realización de la presente invención, las operaciones de ejecución (es decir, los pasos S316-S328) para comprobar si un comando de protección está manipulado pueden realizarse después de las operaciones de ejecución (es decir, los pasos S332-S344) para comprobar si un paquete de datos es un ataque de ataque de reproducción, o las operaciones de ejecución (es decir, los pasos S316-S328) para comprobar si un comando de protección está manipulado y las operaciones (es decir, los pasos S332-S344) para comprobar si un paquete de datos es un paquete de ataque de repetición se pueden realizar simultáneamente.

Una persona experta en la técnica debería entender que, aunque en los modos de realización anteriores, un paquete de datos comprende además un tiempo permitido para timeToAlive activo, la presente invención no se limita a esto. En algunos otros modos de realización de la presente invención, un paquete de datos también puede no incluir un tiempo permitido para timeToAlive activo.

Una persona experta en la técnica debe entender que, aunque en los modos de realización anteriores, la información del orden de envío comprende un número de estado stNum, un número de secuencia sqNum y una marca de tiempo t, la presente invención no se limita a esto. En algunos otros modos de realización de la presente invención, la información del orden de envío también puede no incluir una marca de tiempo t.

Una persona experta en la técnica debe entender que, aunque en los modos de realización anteriores, se incluyen las operaciones (es decir, los pasos S332-S344) para comprobar si un paquete de datos es un paquete de ataque de reproducción, la presente invención no se limita a esto. En algunos otros modos de realización de la presente invención, por ejemplo, bajo la condición de que el ataque de repetición no ocurra, las operaciones (es decir, los pasos S332-S344) para comprobar si un paquete de datos es un paquete de ataque de repetición tal vez tampoco se incluyan.

Una persona experta en la técnica debería entender que, aunque en los modos de realización anteriores, MD5 se utiliza para calcular un resumen de mensajes, la presente invención no se limita a esto. En algunos otros modos de realización de la presente invención, se puede usar cualquier algoritmo apropiado de resumen de mensajes para calcular un resumen de mensajes.

Haciendo ahora referencia a la Fig. 5, muestra un diagrama esquemático de un aparato para transmitir un comando de protección para una protección de retransmisión de acuerdo con un modo de realización de la presente invención. El aparato que se muestra en la Fig. 5 puede instalarse en un dispositivo de transmisión del comando de protección que actúa como una parte emisora, y puede realizarse utilizando software, hardware (por ejemplo, un circuito integrado, un FPGA, etc.) o una combinación de software y hardware.

Como se muestra en la Fig. 5, un aparato 500 para transmitir un comando de protección puede comprender un módulo de cálculo 510 y un módulo de envío 520, en el que el módulo de cálculo 510 se usa para calcular un resumen de mensajes de datos designados, en el que los datos designados comprenden un comando de protección para que se

envíe una protección de retransmisión y se establezca información de contraseña con una parte receptora por adelantado; y un módulo de envío 520 se utiliza para enviar un paquete de datos que comprende el comando de protección y el resumen del mensaje calculado a la parte receptora a través de Ethernet.

Además, el aparato 500 puede comprender además un módulo de generación 530 para generar información del orden de envío sobre el comando de protección de acuerdo con un orden de prioridad de envío del comando de protección, en el que los datos designados y el paquete de datos comprenden además la información del orden de envío generada.

Además, la información del orden de envío comprende un número de estado y un número de secuencia, en el que el número de estado representa una ronda de envío de comandos donde se envía el comando de protección, y el número de secuencia representa un lote de envío de comandos donde el comando de protección se envía en la ronda de envío de comandos donde se envía el comando de protección.

Además, la información del orden de envío puede comprender además una marca de tiempo, en la que la marca de tiempo representa una hora de inicio de la ronda de envío de comandos donde se envía el comando de protección, y los datos designados y el paquete de datos pueden comprender además un tiempo permitido activo, en el que el tiempo permitido activo se utiliza para notificar a la parte receptora el tiempo más largo de espera del siguiente paquete de datos.

Con referencia ahora a la Fig. 6, muestra un diagrama esquemático de un aparato para recibir un comando de protección para una protección de retransmisión de acuerdo con otro modo de realización de la presente invención. El aparato que se muestra en la Fig. 6 puede instalarse en un dispositivo de transmisión del comando de protección que actúa como parte receptora, y puede realizarse utilizando software, hardware (por ejemplo, un circuito integrado, un FPGA, etc.) o una combinación de software y hardware.

Como se muestra en la Fig. 6, un aparato 600 para recibir un comando de protección puede comprender un módulo de cálculo 610, un módulo de comparación 620 y un módulo de descarte 630. El módulo de cálculo 610 se utiliza para calcular, cuando se recibe un paquete de datos que comprende un comando de protección para una protección de retransmisión y un resumen de mensajes, un resumen de mensajes de datos designados, en el que los datos designados comprenden información de contraseña establecida con una parte de envío por adelantado y el comando de protección. El módulo de comparación 620 se utiliza para comparar si el resumen del mensaje calculado es el mismo que el resumen del mensaje comprendido en el paquete de datos recibido. El módulo de descarte 630 se utiliza para descartar el paquete de datos recibido si el resultado de comparación es no.

Además, el paquete de datos recibido comprende además la información del orden de envío del comando de protección, en el que el aparato 600 puede comprender además un módulo de comprobación 640 para comprobar si la información del orden de envío sobre el comando de protección es más reciente que la última información del orden de envío almacenada, y en el que el módulo de descarte 630 también se puede usar para descartar el paquete de datos si el resultado de la comprobación es no.

Además, el aparato 600 puede comprender además un módulo de aceptación 650 y un módulo de almacenamiento 660, en el que el módulo de aceptación 650 se usa para aceptar el paquete de datos recibido si el resultado de la comprobación y el resultado de comparación son ambos sí; y el módulo de almacenamiento 660 se utiliza para almacenar la información del orden de envío sobre el comando de protección como la información del orden de envío más reciente.

Además, la información del orden de envío comprende un número de estado y un número de secuencia, en el que el número de estado representa una ronda de envío de comandos donde se envía el comando de protección, y el número de secuencia representa un lote de envío de comandos donde el comando de protección se envía en la ronda de envío de comandos donde se envía el comando de protección.

Haciendo referencia ahora a la Fig. 7, muestra un diagrama esquemático de un dispositivo de transmisión de comando de protección de acuerdo con un modo de realización de la presente invención. Como se muestra en la Fig. 7, un dispositivo de transmisión del comando de protección 700 puede comprender una memoria 710 y un procesador 720, en el que la memoria 710 se usa para almacenar una instrucción ejecutable, y el procesador 720 se usa para ejecutar operaciones ejecutadas por varios módulos en el aparato 500 o 600 de acuerdo con la instrucción ejecutable almacenada en la memoria 710.

Además, el modo de realización de la presente invención también proporciona un medio legible por máquina en el que se almacena una instrucción ejecutable, en el que cuando se ejecuta, la instrucción ejecutable hace que una máquina realice las operaciones del procesador 720.

REIVINDICACIONES

1. Un procedimiento para transmitir un comando de protección para una protección de retransmisión, que comprende:

calcular un resumen de mensajes de datos designados, en el que los datos designados comprenden un comando de protección que debe enviarse y la información de contraseña establecida con una parte receptora por adelantado; y

enviar un paquete de datos que comprende el comando de protección y el resumen del mensaje calculado a la parte receptora a través de Ethernet;

caracterizado por

generar una información del orden de envío sobre el comando de protección de acuerdo con un orden de prioridad de envío del comando de protección, en el que los datos designados y el paquete de datos comprenden la información del orden de envío generada, y en el que la información del orden de envío comprende un número de estado, un número de secuencia y una marca de tiempo, con el número de estado que representa una ronda de envío de comandos a la que se envía el comando de protección, el número de secuencia que representa un lote de envío de comandos donde se envía el comando de protección en la ronda de envío de comandos donde se envía el comando de protección y la marca de tiempo que representa una hora de inicio de la ronda de envío de comandos donde se envía el comando de protección.

2. Un procedimiento para recibir un comando de protección para una protección de retransmisión, que comprende:

cuando un paquete de datos que comprende un comando de protección y un resumen de mensajes se recibe a través de Ethernet, calcular un resumen de mensajes de datos designados, en el que los datos designados comprenden información de contraseña establecida con una parte de envío por adelantado y el comando de protección;

comparar si el resumen del mensaje calculado es el mismo que el resumen del mensaje comprendido en el paquete de datos recibido; y

si el resultado de comparación es no, descartar el paquete de datos recibido.

caracterizados por que

el paquete de datos recibido además comprende una información del orden de envío sobre el comando de protección, en el que la información del orden de envío comprende un número de estado, un número de secuencia y una marca de tiempo, con el número de estado que representa una ronda de envío de comandos donde se envía el comando de protección, el número de secuencia que representa un lote de envío de comandos donde se envía el comando de protección en la ronda de envío de comandos donde se envía el comando de protección, y la marca de tiempo que representa la hora de inicio de la ronda de envío de comandos donde se envía el comando de protección,

el procedimiento comprende además:

comprobar si la información del orden de envío sobre el comando de protección es más reciente que la información del orden de envío más reciente almacenada; y

si el resultado de la comprobación es no, descartar el paquete de datos.

3. El procedimiento según la reivindicación 2, **caracterizado por que** comprende además:

si el resultado de la comprobación y el resultado de comparación son ambos sí, aceptar el paquete de datos recibido; y

almacenar la información del orden de envío sobre el comando de protección como la información del orden de envío más reciente.

4. Un aparato para transmitir un comando de protección para una protección de retransmisión, que comprende:

un módulo de cálculo (510) para calcular un resumen de mensajes de datos designados, en el que los datos designados comprenden un comando de protección que debe enviarse y la información de contraseña establecida con una parte receptora de antemano; y

un módulo de envío (520) para enviar un paquete de datos que comprende el comando de protección y el resumen del mensaje calculado a la parte receptora a través de Ethernet,

caracterizado por

un módulo de generación (530) para generar información del orden de envío sobre el comando de protección de acuerdo con un orden de prioridad de envío del comando de protección, en el que los datos designados y el paquete de datos comprenden además la información del orden de envío generada, y en el que la información del orden de envío comprende una número de estado, un número de secuencia y una marca de tiempo, con el número de estado que representa una ronda de envío de comandos donde se envía el comando de protección, el número de secuencia que representa un lote de envío de comandos donde se envía el comando de protección en la ronda de envío de comandos donde se envía el comando de protección, y la marca de tiempo que representa una hora de inicio de la ronda de envío de comandos donde se envía el comando de protección.

5. Un aparato para recibir un comando de protección para una protección de retransmisión, que comprende:

un módulo de cálculo (610) para calcular, cuando un paquete de datos que comprende un comando de protección y un resumen de mensajes se recibe a través de Ethernet, un resumen de mensajes de datos designados, en el que los datos designados incluyen información de contraseña establecida con una parte de envío por adelantado y el comando de protección;

un módulo de comparación (620) para comparar si el resumen del mensaje calculado es el mismo que el resumen del mensaje comprendido en el paquete de datos recibido; y

un módulo de descarte (630) para descartar el paquete de datos recibido si el resultado de comparación es no.

caracterizados por que

el paquete de datos recibidos comprende además la información del orden de envío sobre el comando de protección, en el que la información del orden de envío comprende un número de estado, un número de secuencia y una marca de tiempo, con el número de estado que representa una ronda de envío de comandos donde se envía el comando de protección, el número de secuencia representa un lote de envío de comandos donde se envía el comando de protección en la ronda de envío de comandos donde se envía el comando de protección, y la marca de tiempo representa una hora de inicio de la ronda de envío de comandos donde se envía el comando de protección,

en el que el aparato comprende además un módulo de comprobación (640) para comprobar si la información del orden de envío sobre el comando de protección es más reciente que la última información del orden de envío almacenada,

y en el que el módulo de descarte se usa además para descartar el paquete de datos si el resultado de la comprobación es no.

6. El aparato de acuerdo con la reivindicación 5, **caracterizado por que** comprende además:

un módulo de aceptación (650) para aceptar el paquete de datos recibido si el resultado de la comprobación y el resultado de comparación son ambos sí; y

un módulo de almacenamiento (660) para almacenar la información del orden de envío sobre el comando de protección como la información del orden de envío más reciente.

7. Un dispositivo para transmitir un comando de protección para una protección de retransmisión, que comprende:

una memoria (710) para almacenar una instrucción ejecutable; y

un procesador (720) para ejecutar las operaciones ejecutadas en cualquiera de las reivindicaciones 1 a 4 de acuerdo con la instrucción ejecutable almacenada en la memoria.

FIG 1

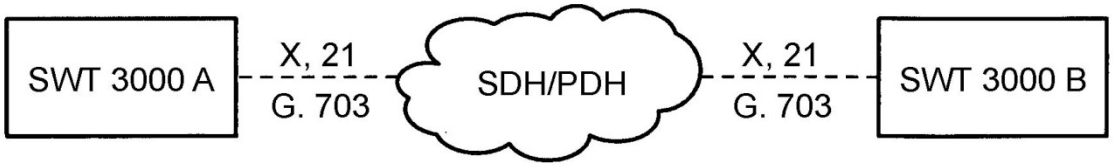
SWT 3000 A
X, 21
G. 703
SDH/PDH
X, 21
G. 703
SWT 3000 B

FIG 2

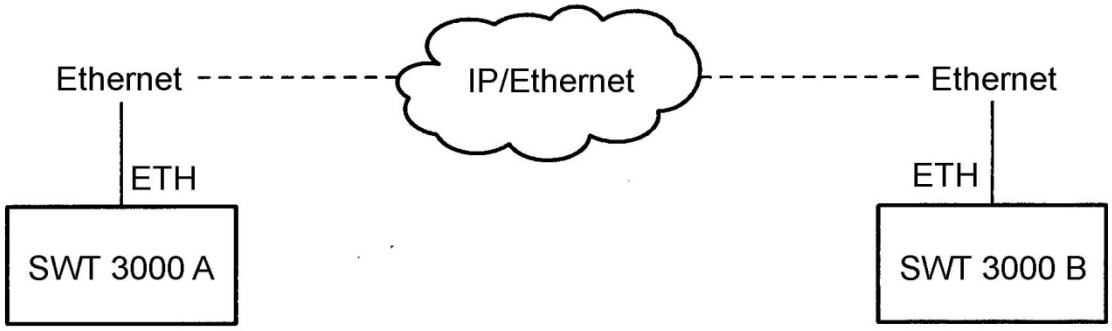
Ethernet
IP/Ethernet
Ethernet
ETH
ETH
SWT 3000 A
SWT 3000 B

FIG 3

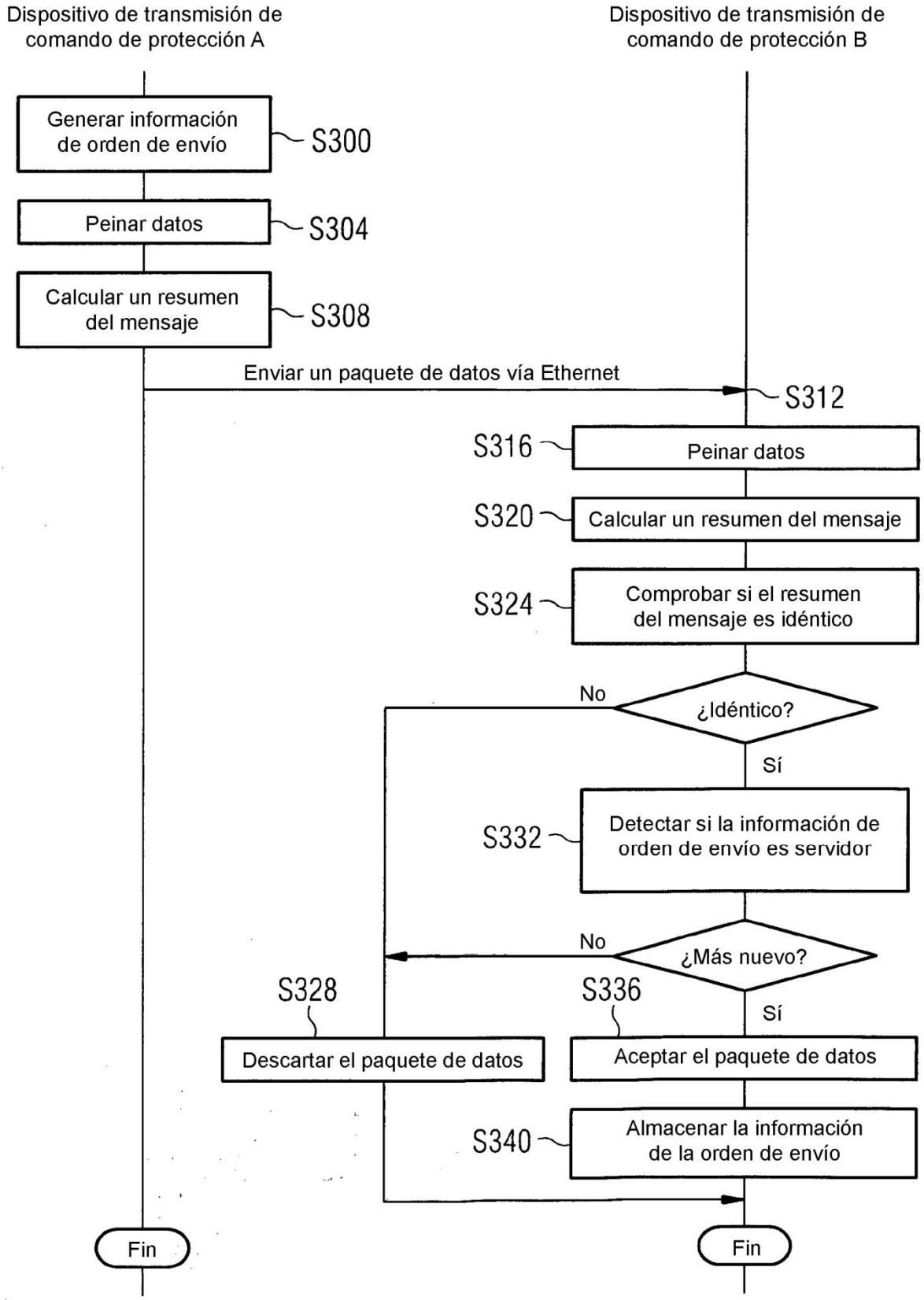
Dispositivo de transmisión de comando de protección A
Dispositivo de transmisión de comando de protección B
Generar información de orden de envío
S300
Peinar datos
S304
Calcular un resumen del mensaje
S308
Enviar un paquete de datos vía Ethernet
S312
S316
Peinar datos
S320
Calcular un resumen del mensaje
S324
Comprobar si el resumen del mensaje es idéntico
No
¿Idéntico?
Sí
S332
Detectar si la información de orden de envío es servidor
No
¿Más nuevo?
S328
S336
Sí
Descartar el paquete de datos
Aceptar el paquete de datos
S340
Almacenar la información de la orden de envío
Fin
Fin

FIG 4

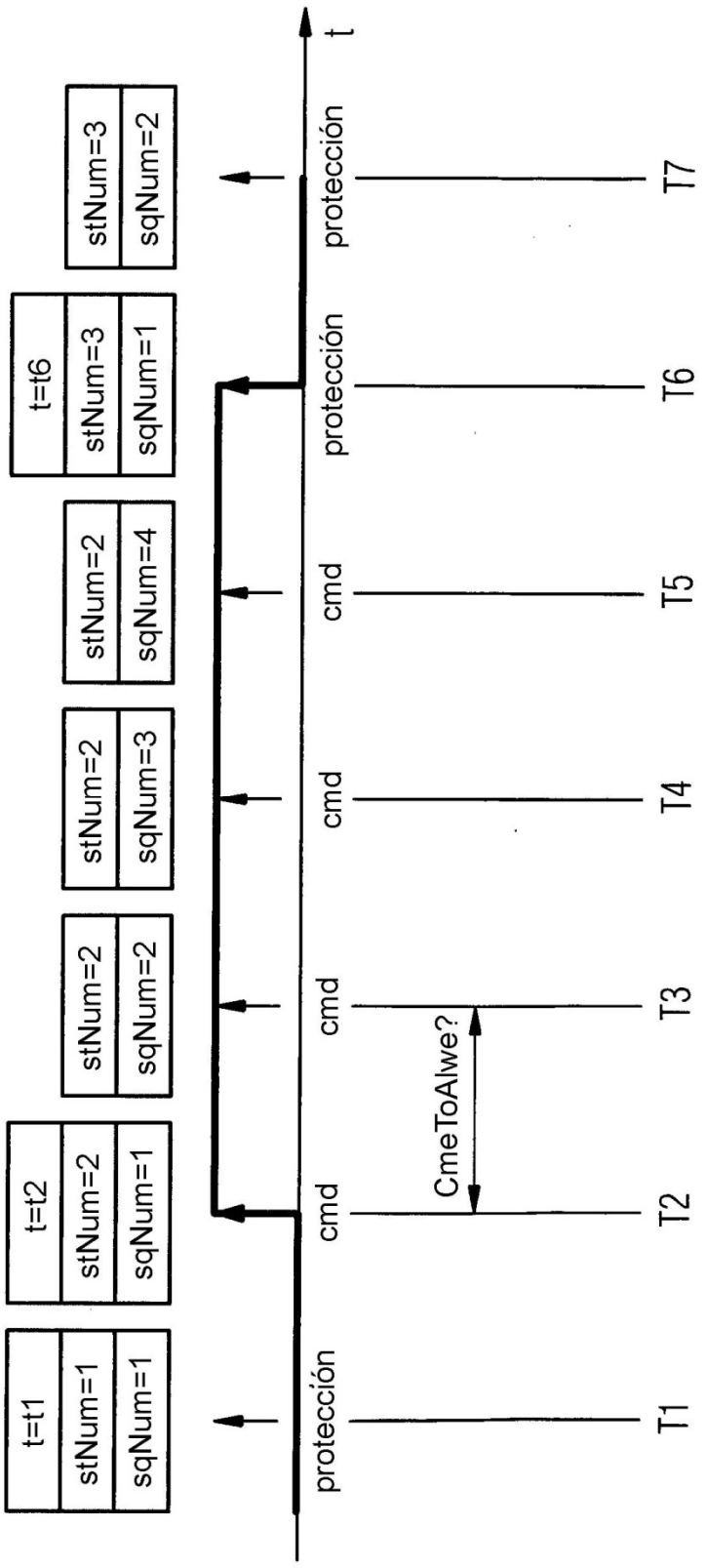
t=t1
stNum=1
sqNum=1
t=t2
stNum=2
sqNum=1
stNum=2
sqNum=2
stNum=2
sqNum=3
stNum=2
sqNum=4
t=t6
stNum=3
sqNum=1
stNum=3
sqNum=2
protección
cmd
cmd
cmd
cmd
cmd
protección
protección
t
T1
T2
T3
T4
T5
T6
T7
CmeToAlwe?

FIG 5

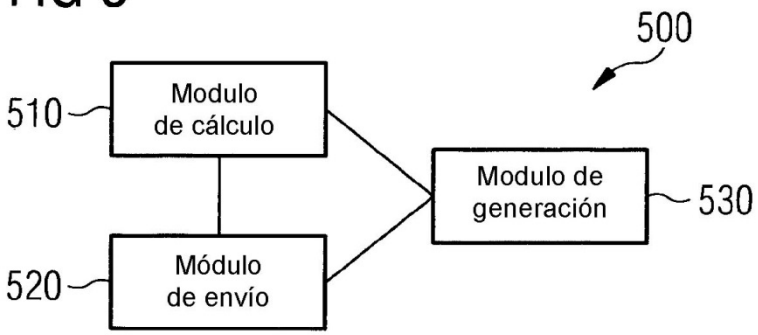

FIG 6

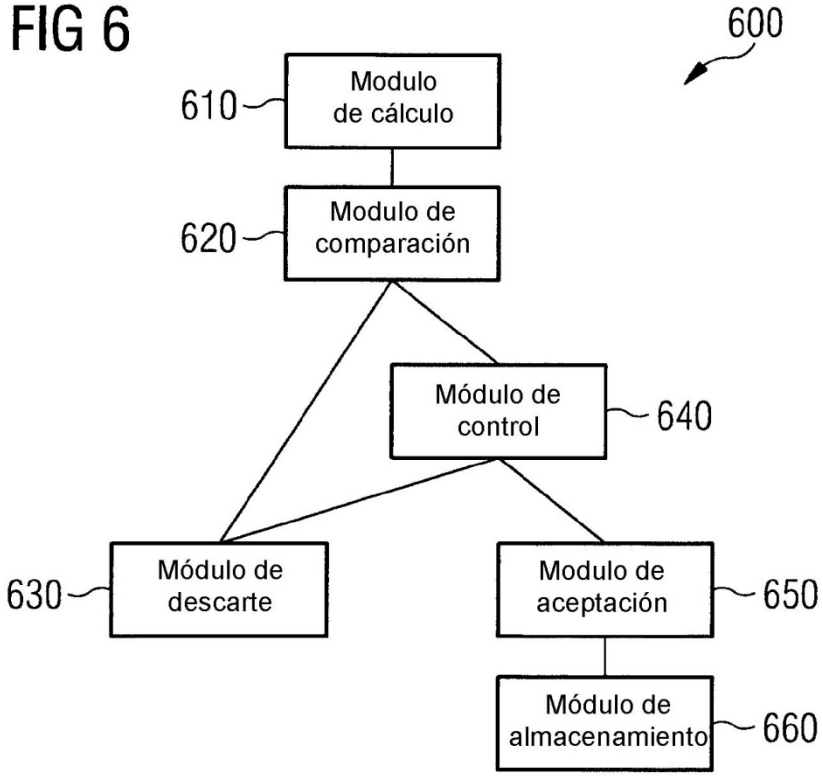

FIG 7