(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 667 865**

(51) Int. CI.:

H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **24.07.2012 PCT/EP2012/064527**

(87) Fecha y número de publicación internacional: **21.02.2013 WO13023885**

(96) Fecha de presentación y número de la solicitud europea: **24.07.2012 E 12743425 (6)**

(97) Fecha y número de publicación de la concesión europea: **28.03.2018 EP 2695324**

(54) Título: **Procedimiento para enviar mensajes con protección de integridad**

(30) Prioridad:

16.08.2011 DE 102011081036

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.05.2018

(73) Titular/es:

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

(72) Inventor/es:

FALK, RAINER y
FRIES, STEFFEN

(74) Agente/Representante:

LOZANO GANDIA, José

PROCEDIMIENTO PARA ENVIAR MENSAJES CON PROTECCIÓN DE INTEGRIDAD

DESCRIPCIÓN

La invención se refiere a un procedimiento para enviar mensajes con protección de integridad, así como a un emisor correspondiente. Además se refiere la invención a un procedimiento para procesar mensajes con protección de integridad, así como a un receptor correspondiente para recibir y procesar tales mensajes.

En una pluralidad de campos de aplicación técnicos es necesario proteger la integridad de datos transmitidos entre emisores y receptores. Entonces protección de integridad significa que pueden detectarse manipulaciones que se han realizado en un mensaje mediante una suma de prueba criptográfica correspondiente. Por ejemplo se transmiten en sistemas de automatización o redes de sensores mensajes que implican a continuación la correspondiente acción, como por ejemplo la apertura de una válvula en una instalación de automatización. La comunicación entre emisores y receptores se realiza entonces a menudo mediante una comunicación broadcast (de difusión general) o multicast (multidifusión). En muchos escenarios no es suficiente entonces comprobar en un instante determinado si una información previamente transmitida en un determinado período de tiempo era íntegra. Si se descubren entonces faltas, pueden retrotraerse por lo general las acciones o bien puede originarse un cambio a un estado seguro para el funcionamiento mediante el correspondiente receptor.

Para una protección de integridad de mensajes mediante sumas de prueba criptográficas es necesario gestionar las correspondientes claves para generar las sumas de prueba. Por el estado de la técnica se conoce la generación de las llamadas cadenas Hash. Entonces, partiendo de un valor generado inicialmente mediante aplicación consecutiva de una función hash criptográfica, comenzando con el valor inicial, se genera una cadena de valores que representan claves previamente calculadas, que son válidas durante un determinado periodo de tiempo en una transmisión de mensajes entre emisor y receptor. Las funciones hash criptográficas se conocen de por sí por el estado de la técnica. Las mismas se caracterizan por la ausencia de colisiones, es decir, a partir de dos valores diferentes se generan mediante la función hash siempre dos valores funcionales diferentes. Además tales funciones son funciones unidireccionales, es decir, a partir del valor funcional no puede calcularse hacia atrás el valor de la variable que mediante aplicación de la función hash ha conducido a dicho valor funcional. Por el estado de la técnica se conoce por ejemplo el protocolo TESLA o bien µTESLA, con los que se generan cadenas hash y se transmiten los correspondientes valores hash de la cadena.

Cuando se utilizan cadenas hash para la protección de integridad, se utilizan los valores correspondientes de la cadena durante un espacio de tiempo predeterminado para formar la suma de prueba criptográfica de mensajes. Una vez transcurrido el espacio de tiempo, se transmiten los valores al receptor de los mensajes protegidos en integridad, el cual puede a continuación comprobar la integridad de los mensajes. La utilización de cadenas hash presenta el inconveniente de que en el caso de que un emisor tenga que enviar a través de aplicaciones separadas mensajes con protección de integridad, ha de generarse para cada aplicación separadamente una cadena hash con una función hash.

El documento de Stefan Lucks y colab.: "Concrete Security for Entity Recognition: The Jane Doe Protocol (Full Paper)" (Seguridad concreta para el reconocimiento de entidades: El protocolo de Jane Doe (documento completo), International Association for Cryptologic Research, vol. 20090423: 130758, 20 abril 2009, páginas 1 a 20, describe un procedimiento para la protección de integridad de mensajes basándose en la generación de sumas de comprobación mediante valores hash de cadenas hash.

En el documento de T. Aura: "Strategies against replay attacks" (Estrategias frente a ataques de reproducción), Computer Security Foundations Workshop, 1997, actas, 10º Rockport, MA, USA, 10 - 12. Junio 1997, páginas 59 a 68, se da a conocer la generación de un código MAC para un mensaje utilizando el tipo de mensaje y una clave maestra.

Es objetivo de la invención lograr un procedimiento sencillo y eficiente en cálculo para proteger la integridad de mensajes.

Este objetivo se logra mediante el procedimiento de acuerdo con la reivindicación 1 y con el emisor de acuerdo con la reivindicación 10 y/o el procedimiento de acuerdo con la reivindicación 12 y el receptor de acuerdo con la reivindicación 16. En las reivindicaciones dependientes se definen perfeccionamientos de las invenciones.

En el procedimiento de acuerdo con la invención para enviar mensajes, se dotan en el correspondiente emisor previsto para enviar los mensajes dichos mensajes antes de enviarlos de una protección de integridad. Al respecto se genera de manera de por sí conocida una cadena hash de valores consecutivos, generándose los valores partiendo de un valor generado inicialmente, que por ejemplo puede ser un número aleatorio, mediante la aplicación consecutiva de una función hash criptográfica sobre el valor inicialmente generado (es decir, comenzando con el valor inicialmente generado). Si la

cadena hash sólo incluye el valor generado inicialmente y otro valor hash, se aplica la función hash sólo una vez sobre el valor generado inicialmente. El último valor generado de la cadena hash representa entonces un valor de anclaje, que se proporciona a uno o varios receptores predeterminados de los mensajes y los valores restantes son válidos en secuencia inversa a su generación en períodos de validez consecutivos. El concepto del período de validez ha de entenderse entonces en sentido amplio. El mismo puede referirse aquí a un intervalo de tiempo fijo. Pero también puede especificarse de otra manera, por ejemplo mediante una cantidad fijada de mensajes enviados para los cuales es válido el correspondiente valor.

En el emisor se genera en el período de validez del correspondiente valor de la cadena hash una suma de prueba criptográfica para un mensaje a enviar (siempre que exista) utilizando el correspondiente valor. Esta suma de prueba se envía junto con el mensaje. Entonces pueden verificar el receptor o los receptores predeterminados del mensaje y de la suma de prueba, conociendo el correspondiente valor, la suma de prueba y comprobar de esta manera la integridad del mensaje. Para que los receptores reciban el correspondiente valor, el emisor envía este valor una vez transcurrido su periodo de validez. Entonces pueden verificar el o los receptores predeterminados el correspondiente valor basándose en el valor de anclaje proporcionado.

El procedimiento de acuerdo con la invención se caracteriza porque la generación de la suma de prueba se realiza tal que para el mensaje a enviar se determina una categoría que caracteriza el mensaje, a partir de la cual, junto con el valor válido en ese momento, se deduce a partir de la cadena hash, mediante una función de deducción de claves, una clave con la que se genera la suma de prueba para el mensaje.

La invención se basa en la experiencia de que para generar la suma de prueba, además del correspondiente valor de una cadena hash, puede incluirse también una categoría específica de los mensajes. Se logra así una posibilidad de generar, mediante una única cadena hash, separadamente sumas de prueba para mensajes de distinta categoría, sin que para ello se necesiten varias cadenas hash diferentes. El concepto de la categoría ha de entenderse aquí y en lo que sigue en un sentido amplio, e incluye cualquier característica relacionada con un mensaje con la que un mensaje o bien un grupo de mensajes puede diferenciarse de otros mensajes u otros grupos de mensajes, respectivamente.

En una forma de realización especialmente preferida, procede la categoría determinada de una o varias de las siguientes categorías:

- una o varias categorías que especifican en cada caso un tipo de un mensaje, pudiendo diferenciarse los tipos por ejemplo según la finalidad o el contenido del mensaje (por ejemplo mensajes específicos de la seguridad, mensajes de control, mensajes de vigilancia);
- una o varias categorías que especifican en cada caso uno o varios protocolos y/o números de puerto a través de los que se envía un mensaje;
- una o varias categorías que especifican en cada caso al menos un receptor predeterminado o un grupo de receptores para el o los que está previsto el mensaje;
- una o varias categorías que especifican en cada caso un intervalo de tiempo en el que se envía un mensaje, siendo el intervalo de tiempo con preferencia más corto que los correspondientes periodos de validez y pudiendo determinarse dado el caso también implícitamente mediante un número de mensajes.

En función del caso de aplicación, pueden determinarse como distintas las categorías de los mensajes individuales. En una variante preferida están contenidas las categorías explícitamente en los mensajes a enviar y son leídas por el emisor. Alternativa o adicionalmente existe también la posibilidad de que las categorías no estén incluidas explícitamente en los mensajes, sino que puedan deducirse de los mensajes basándose en sus características.

De acuerdo con la invención puede utilizarse como función de deducción de claves cualquier función unidireccional. En una forma de realización especialmente preferente se utiliza entonces una función hash criptográfica. Como función de deducción de claves o bien para generar la cadena hash puede utilizarse cualquier función hash conocida por el estado de la técnica. Ejemplos de tales funciones hash son MD5, SHA1, SHA256, HMAC - MD5, HMAC - SHA1, HMAC - SHA256 y AES – CBC - MAC.

Para generar las sumas de prueba criptográficas pueden utilizarse procedimientos de por sí conocidos, siendo no obstante esencial para la invención que al generarse la suma de prueba se considere una clave que depende de la categoría del mensaje. En una variante preferida se utilizan como sumas de prueba los llamados códigos MAC (MAC = Message Authentication Code, código de autentificación de mensajes) o bien códigos MIC (MIC = Message Integrity Code, mensaje de integridad de código).

Los mensajes enviados en el marco del procedimiento de acuerdo con la invención no están destinados en una variante preferida a un único receptor, sino a un grupo de receptores más amplio. Es decir, los mensajes se envían en este caso como mensajes de broadcast (difusión general) y/o multicast (multidifusión).

Los mensajes enviados según el procedimiento de la invención pueden tener cualquier configuración. En una variante de la invención son los mensajes paquetes de datos y/o estructuras de datos de un protocolo predeterminado, como por ejemplo estructuras de datos de la capa L2 del modelo de referencia OSI o paquetes de datos de la familia de protocolos WLAN.

El valor de anclaje, que se proporciona al o a los receptor/es predeterminados en el marco de la protección de la integridad, sirve para que el receptor pueda verificar mediante el mismo un valor correspondiente de la cadena hash. El valor de anclaje puede proporcionarse entonces a los receptores de distintas formas. En una forma de realización preferida, se proporciona el valor de anclaje al o a los receptor/es predeterminados firmado digitalmente, pudiendo verificarse la firma mediante el o los receptor/es predeterminados, por ejemplo mediante acceso a un servidor, en el que están archivados los correspondientes certificados para comprobar la firma. Entonces está firmado y enviado con preferencia el valor de anclaje por el emisor.

El procedimiento de acuerdo con la invención puede utilizarse para transmitir mensajes en cualesquiera redes de datos. Un caso de aplicación especialmente preferido es la transmisión de mensajes en una red de datos para la automatización industrial y/o para la automatización de la energía. El procedimiento puede utilizarse entonces para proteger la integridad de mensajes del protocolo Profinet y/o protocolo Profibus. Otro caso de aplicación es la protección de la identidad de mensajes que se transmiten con el protocolo GOOSE a los correspondientes aparatos en el campo de la automatización de la energía. Igualmente puede utilizarse el procedimiento para transmitir mensajes en una red de sensores y en particular en una red de sensores inalámbrica.

Además de al procedimiento antes descrito, se refiere la invención a un emisor para enviar mensajes con protección de la integridad, estando configurado el emisor tal que con el emisor puede realizarse durante el funcionamiento el procedimiento antes descrito o bien una o varias variantes de este procedimiento.

La invención se refiere además a un procedimiento para procesar mensajes con protección de la integridad, habiéndose enviado los mensajes mediante un emisor con el procedimiento antes descrito. Entonces se realizan en un receptor predeterminado, al que se ha proporcionado el valor de anclaje de la cadena hash generada en el emisor, los pasos que se describen a continuación. Primeramente se reciben los mensajes junto con las sumas de prueba, así como el correspondiente valor una vez transcurrido su período de validez. Al recibirse el correspondiente valor se realiza una verificación del valor basándose en el valor de anclaje. Si la verificación del correspondiente valor tiene éxito, se determina la categoría de mensajes recibidos durante el período de validez del correspondiente valor. A continuación, mediante la misma función de deducción de claves que utiliza el emisor, se genera a partir de la categoría de un mensaje y del valor correspondiente una clave con la que se verifica la suma de prueba del mensaje. De esta manera se logra comprobar una suma de prueba que se ha encriptado con una clave específica del mensaje.

En una variante preferida del procedimiento que acabamos de describir, se siguen procesando los mensajes inmediatamente tras la recepción, aún cuando la comprobación de la integridad de los mensajes sólo se realiza en un instante posterior tras recibirse el correspondiente valor de la cadena hash. Si no tiene éxito entonces la verificación del valor recibido, pueden iniciar los receptores medidas adecuadas. Con preferencia finaliza y/o se retrotrae entonces la realización de una o varias acciones que se iniciaron mediante los mensajes que se recibieron durante el período de validez del correspondiente valor junto con el valor de prueba. Alternativa o adicionalmente existe la posibilidad de que un receptor pase a un estado de servicio seguro cuando la verificación no tiene éxito.

También puede implicar una verificación sin éxito de la suma de prueba de un mensaje determinadas medidas. Con preferencia, análogamente a la variante que acabamos de describir, finaliza y/o se retrotrae la realización de una o varias acciones que se han iniciado mediante el mensaje cuando no tiene éxito la verificación de la suma de prueba de un mensaje. Alternativa o adicionalmente existe la posibilidad de que un receptor pase a un estado de servicio seguro cuando la verificación no tiene éxito.

En otra variante se proporciona al receptor predeterminado el valor de anclaje de la cadena hash firmado digitalmente, verificándose en el receptor la firma digital del valor de anclaje. Con preferencia finaliza el procedimiento cuando la verificación de la firma digital no tiene éxito.

La invención se refiere además a un receptor para recibir y procesar mensajes con protección de integridad, habiendo sido enviados los mensajes con el procedimiento antes descrito y habiéndose proporcionado al receptor el valor de anclaje. El receptor está configurado entonces tal que el procedimiento que acabamos de describir para procesar mensajes y/o una o varias variantes preferidas de este procedimiento pueden realizarse con los receptores.

La invención se refiere además a un procedimiento para transmitir mensajes con protección de integridad, enviándose los mensajes con el procedimiento que acabamos de describir para enviar mensajes

mediante un emisor y recibiéndose y procesándose con el procedimiento que acabamos de describir para procesar mensajes mediante un receptor.

La invención se refiere además a un sistema para transmitir mensajes con protección de integridad, incluyendo al menos un emisor de acuerdo con la invención y al menos un receptor de acuerdo con la invención.

Una forma de realización de la invención se describirá detalladamente a continuación en base a la adjunta figura 1. Esta figura muestra un diagrama secuencial que reproduce las etapas de una variante del procedimiento de acuerdo con la invención.

El procedimiento de la invención parte de la utilización de por sí conocida de una llamada cadena hash, que usualmente se denomina también hash-chain y de un emisor de los correspondientes mensajes. Entonces se parte de un valor inicial h0, que es por ejemplo un valor aleatorio generado en el emisor. Con una función hash H criptográfica cualquiera, de por sí conocida, se generan entonces para una cadena hash de la longitud n los correspondientes valores hash h1, h2, ..., hn mediante aplicación repetida de la función hash como sigue:

Valor inicial h0, h1 = H(h0), h2 = H(h1), ..., h(n-1) = H(h(n-2)), hn = H(h(n-1)).

Los elementos h0, h1, …, hn de la cadena hash se utilizan como claves para la protección de integridad del mensaje enviado por un emisor. Una clave es válida entonces para un periodo de validez predeterminado. Este periodo de validez puede especificarse explícitamente mediante un intervalo de tiempo o bien también implícitamente mediante un número de mensajes para los cuales ha de utilizarse la clave. En procedimientos tradicionales se utiliza el correspondiente valor de la cadena hash dentro de su período de validez directamente para generar una suma de prueba criptográfica para un mensaje a utilizar, transmitiéndose la suma de prueba junto con el mensaje. Una vez transcurrido el período de validez, se envía finalmente mediante el emisor el correspondiente valor de la cadena hash para el período de validez que acaba de transcurrir. Un receptor puede a continuación verificar mediante este valor la suma de prueba y con ello la integridad de los mensajes previamente transmitidos. A diferencia de este procedimiento tradicional, no se utilizan de acuerdo con la invención directamente los valores de la cadena hash para generar la suma de prueba, sino que se determina con una función de deducción de claves adecuada otra clave, que está acoplada a las categorías, tal como se describirá posteriormente.

En el procedimiento de la figura 1 se envían desde un emisor SE mensajes de broadcast (de difusión general) y/o multicast (multidifusión) a una pluralidad de receptores, que continúan procesando los mensajes, describiéndose a continuación la comunicación entre el emisor SE y uno de los receptores RE. En el procedimiento se genera de manera de por sí conocida en la etapa S1 la cadena hash basándose en un valor inicial h0 mediante aplicación repetida de la función hash criptográfica H a h0. En el ejemplo de la figura 1 se generan tres valores hash h1, h2 y h3, es decir, la cadena hash presenta la longitud n = 3.

Al comienzo de la comunicación se envía en la etapa S2 el último valor hash generado h3 juntamente con una firma Sig desde el emisor SE. Esta etapa es de por sí conocida por el estado de la técnica en el marco de la utilización de cadenas hash. Mediante la etapa S2 se comunica el valor h3 como valor de anclaje al receptor RE. El receptor puede entonces verificar de manera adecuada la firma Sig mediante un certificado, que él mismo puede descargarse por ejemplo de un servidor de certificados. Es decir, mediante una clave que se le da a conocer puede él comprobar la firma generada con la correspondiente clave privada del emisor. En el marco de la etapa S2 puede transmitirse al receptor dado el caso también una información sobre el periodo de validez de los correspondientes valores de la cadena hash, por ejemplo en forma de una variable. No obstante, el periodo de validez puede ser conocido dado el caso también implícitamente (por ejemplo fijamente prescrito) por los receptores.

En la etapa S3 de la figura 1 se realiza la ya antes mencionada verificación de la firma Sig, prosiguiendo el procedimiento sólo cuando puede verificarse la firma. De esta manera queda asegurado que no se continúa procesando ninguna cadena hash de terceros no autorizados. Además se memoriza en la etapa S3 el valor de anclaje h3 de la cadena hash en el receptor RE.

Tras el envío del valor de anclaje h3 y de la firma Sig se genera en el emisor SE para el primer mensaje a enviar M1 una suma de prueba criptográfica adecuada. En la forma de realización aquí descrita se genera el Message Integrity Code (código de integridad del mensaje) de por sí conocido, pudiendo generarse también otras clases de sumas de prueba criptográficas y en particular el Message Authentication Code (código de autentificación de mensajes). Según el estado de la técnica se utiliza para ello directamente el valor hash h2 generado antes del valor de anclaje h3. No obstante, de acuerdo con la invención se genera en la etapa S4 primeramente con una función de deducción de claves KDF adecuada una clave que depende de una categoría que se asocia al correspondiente mensaje M1. Como función de deducción de claves KDF puede utilizarse a su vez una función hash criptográfica cualquiera, pero pueden utilizarse también cualesquiera otras clases de funciones de deducción de claves conocidas. Las categorías

pueden referirse a cualesquiera características relacionadas con el correspondiente mensaje. Las categorías pueden entonces estar contenidas como etiquetas en el propio mensaje, pero existe dado el caso también la posibilidad de que las categorías se deduzcan del mensaje.

En la variante aquí descrita de la invención se utilizan etiquetas para determinar la categoría en los mensajes. Entonces puede determinar la etiqueta por ejemplo a qué servicio o a qué aplicación o a qué grupo de servicios o aplicaciones pertenece el mensaje. En particular pueden especificarse en los mensajes servicios de seguridad sobre etiquetas. Para un servicio de autentificación puede utilizarse por ejemplo la etiqueta SID_Authenticity y para un servicio de integridad de mensajes la etiqueta SID_Integrity. Además pueden diferenciarse alternativa o adicionalmente tipos de mensajes mediante etiquetas, pudiendo designarse el tipo X (X=1, 2, …) mediante la correspondiente etiqueta MID_TYP_X.

En la forma de realización de la figura 1 se denominan las categorías de mensajes consideradas k1, k2 y k3. La categoría k1 significa entonces "Safety", es decir, el mensaje se refiere a paquetes de seguridad. Por el contrario designa k2 la categoría "Control", es decir, el mensaje es un mensaje de control. La categoría k3 significa "Monitoring", es decir, el mensaje correspondiente es un mensaje de vigilancia.

En la etapa S4 determina el emisor SE para el mensaje M1 la categoría k1. Basándose en ello, genera el mismo a continuación, mediante la función de deducción de claves KDF con el valor hash h2 en combinación con la categoría k1, la clave h21, es decir, el mismo determina h21 = KDF(h2, k1). En la generación de claves con la función de deducción de claves KDF se aplica esta función con preferencia a una concatenación del correspondiente valor hash con la categoría. Tal como ya se ha mencionado, pueden utilizarse cualesquiera funciones de deducción de claves, como por ejemplo la función hash criptográfica SHA1 o bien HMAC-SHA1. Con la clave h21 determinada, se genera a continuación la suma de prueba utilizando el Message Integrity Codes MIC, es decir, para el mensaje M1 resulta la suma de prueba MIC1 = MIC(h21, M1). Se genera así en la etapa S4 una clave específica del mensaje h21 y con ello una suma de prueba específica del mensaje MIC1.

En la etapa S5 envía el emisor SE el mensaje M1 y la suma de prueba MIC1. El receptor RE memoriza a continuación en la etapa S6 el mensaje M1, así como la suma de prueba MIC1 y ejecuta las acciones que implica el mensaje M1. El procedimiento puede entonces utilizarse para la comunicación en una red de datos de una instalación industrial, en la que un emisor en forma de un sensor envía un mensaje con valores correspondientemente captados a receptores en forma de actuadores, que basándose en los valores ejecutan otras acciones.

En el procedimiento de la figura 1 envía el emisor SE en una etapa S7 otro mensaje M2, determinándose ahora a su vez la categoría de este mensaje. Se trata al respecto de un mensaje de la categoría k2. Análogamente a en la etapa S4, se genera entonces una clave h22 basándose en la función de deducción de claves KDF a partir del valor hash h2 y de la categoría k2. Es decir, es h22 = KDF(h2, k2). Con esta clave específica del mensaje se genera a su vez la suma de prueba MIC2 = MIC(h22, M2) para el mensaje M2. El emisor SE envía entonces el mensaje M2 junto con la suma de prueba MIC2 en la etapa S8. El mensaje y la suma de prueba se memorizan a continuación en el receptor RE en la etapa S9. Análogamente pueden generarse otros mensajes con las sumas de prueba correspondientes y transmitirse desde el emisor SE al receptor RE.

En la figura 1 se indican para los distintos valores h0, h1 y h2 sus periodos de validez con I0, I1 e I2. En el periodo de validez I2 se utiliza siempre el valor hash h2 en combinación con la correspondiente categoría de mensajes para generar la suma de prueba. Por el contrario, en el intervalo de validez I1 se utiliza el valor hash h1 y en el periodo de validez 10 el valor inicial h0 para generar las correspondientes sumas de prueba.

Una vez transcurrido el periodo de validez 12, envía el emisor SE en la etapa S10 el valor hash h2. Queda asegurado así que la transmisión de este valor hash sólo se realiza cuando el mismo ya no es válido, con lo que aumenta la seguridad del procedimiento. A continuación comienza el periodo de validez I1 para el valor hash h1. En este periodo de tiempo pueden de nuevo enviarse los correspondientes mensajes, que análogamente a en las etapas S4 y S7, basándose en la misma función de deducción de claves KDF, se dotan directamente, pero utilizando el valor hash h1, de una suma de prueba. Pero en el escenario de la figura 1 no se transmite ningún mensaje en el intervalo de tiempo I1. Con independencia de ello, realiza el receptor RE en el intervalo de tiempo I1 la comprobación de las sumas de prueba de los mensajes transmitidos en el período de tiempo de validez 12. Para ello se verifica primeramente en la etapa S11 con la misma función hash H, mediante la cual el emisor ha generado la cadena hash, el valor hash h2. Esto se realiza aplicando la función hash al valor h2 y comprobando si el valor que de ello resulta coincide con el valor de anclaje h3. Si no es éste el caso, inicia el receptor las correspondientes medidas. En particular se retrotraen acciones realizadas por el receptor en base a los mensajes recibidos en el período de validez 12.Pero si hay coincidencia, es que se ha verificado con éxito el valor hash h2 correspondiente y se memoriza a continuación.

Si la verificación se realiza con éxito, determina el receptor en la etapa S12 la categoría del mensaje M1 recibido. Con la misma función de deducción de claves KDF utilizada también por parte del receptor, se deduce entonces la clave h21 basándose en la categoría k1 y el valor hash h2, es decir, se determina h21 = KDF(h2, k1). A continuación se realiza la verificación de la suma de prueba, determinándose el Message Integrity Code MIC(h21, M1) para la concatenación de h21 y M1 y se compara con la suma de prueba MIC1 recibida. Si hay coincidencia, se determina la integridad del mensaje M1 mediante el receptor RE. Si no hay coincidencia, el mensaje se ha manipulado sin autorización y puede iniciar de nuevo el receptor contramedidas adecuadas. En particular se retrotraen acciones que se activaron en base a la recepción del mensaje M1.

Con el mensaje M2 se procede en la etapa S13 con el mensaje M2 análogamente a con el mensaje M1. Es decir, se determina la categoría k2 del mensaje M2 y basándose en ello, se determina la clave h22=KDF(h2, k2). Con h22 se calcula entonces el Message Integrity Code MIC(h22, M2), que se compara con el código MIC2 recibido. Si no existe integridad, existe de nuevo la posibilidad de retrotraer las acciones ligadas al mensaje M2, que previamente habían sido ejecutadas por el receptor RE.

Una vez transcurrido el periodo de validez I1 del valor hash h1 envía el emisor SE este valor en la etapa S14., realizando el receptor RE a continuación en la etapa S15, análogamente a en la etapa S11, una verificación del valor hash h1, al comprobar el mismo si la aplicación de la función hash H al valor h1 conduce al valor h2, memorizado en la etapa S11. Entonces se memoriza en la etapa S15 el valor h1. Si la verificación no tiene éxito, pueden retrotraerse dado el caso las acciones correspondientes que se activaron en el periodo de validez I1 mediante el mensaje transmitido. En el escenario de la figura 1 no se recibió en el periodo de validez I1 ningún mensaje, con lo que sobran etapas adicionales para comprobar sumas de prueba.

En la etapa S16 se prepara en el periodo de validez 10 del valor h0 el envío de otro mensaje M3 por parte del emisor SE. En analogía a las etapas S4 y S7, se determina primeramente la categoría k3 para el mensaje M3. A partir de ello, se determina la clave h03 = KDF(h0, k3), que a continuación se utiliza para generar la suma de prueba MIC3 = MIC(h03, M3). El emisor SE envía en la etapa S17 el mensaje M3 y la suma de prueba MIC3. El receptor RE, que recibe M3 y MIC3, memoriza los mismos en la etapa S18. Una vez transcurrido el periodo de validez 10, envía el emisor SE 4 el valor h0 en la etapa S19. El receptor RE verifica entonces en la etapa S20 este valor, comprobando si H(h0) coincide con el valor h1 memorizado en la etapa S15. Si la verificación tiene éxito, se memoriza h0. A continuación se determina a su vez la categoría del mensaje M3, mediante la que a continuación se determina en la etapa S21 la clave h03 = KDF(h0, k3) con la función de deducción de claves KDF. A continuación se realiza la verificación del valor de prueba MIC3 previamente recibido, comprobándose si es MIC3 = MIC(h03, M3). Si no tienen éxito las correspondientes verificaciones en la etapa S20 y/o en la etapa S21, pueden por ejemplo retrotraerse las acciones que implica el mensaje.

Tal como resulta de las explicaciones anteriores, puede deducirse una clave especifica del mensaje, de manera adecuada, mediante la determinación de las correspondientes categorías para mensajes a enviar, la cual se utiliza en combinación con una cadena hash para generar una suma de prueba. Las categorías se designan entonces con preferencia mediante etiquetas, que caracterizan por ejemplo tipos de mensajes y/o aplicaciones o servicios. No obstante, las categorías pueden caracterizar un mensaje de otra manera. En particular puede fijar la categoría un subintervalo de tiempo del periodo de validez del valor correspondiente de la cadena hash, perteneciendo un mensaje a una categoría del correspondiente subintervalo de tiempo cuando el mismo se ha enviado en este subintervalo de tiempo. De esta manera pueden afinarse más aún los periodos de validez de los valores hash.

El procedimiento de acuerdo con la invención puede utilizarse para proteger cualquier mensaje. En particular pueden protegerse mensajes en forma de paquetes de datos individuales o bien estructuras de datos, como por ejemplo estructuras de datos de la capa 2 según MACsec o bien paquetes de datos en el formato WLAN-CCMP o en el formato 802.15.4 AES-CCM. La cadena hash utilizada en el procedimiento de acuerdo con la invención puede determinarse mediante procedimientos de por sí conocidos y transmitirse sus valores con un retardo a nodos de recepción. Para ello pueden utilizarse los protocolos TESLA o µTESLA ya citados al principio. También para generar la suma de prueba para los mensajes transmitidos pueden utilizarse procedimientos de por sí conocidos, pudiendo generarse en particular una suma de prueba criptográfica en forma de un Message Authentication Code o bien Message Integrity Code.

Las formas de realización del procedimiento de acuerdo con la invención que se han descrito presentan una serie de ventajas. En particular puede realizarse el procedimiento mediante un único componente de gestión de claves del emisor y/o receptor para distintas aplicaciones y/o servicios. Un componente de software del emisor y/o receptor que procesa mensajes de una categoría específica (por ejemplo mensajes críticos para la seguridad o mensajes Real-Time-Control, de control en tiempo real) recibe entonces de un componente de gestión de claves del emisor y/o receptor sólo aquellas claves que son necesarias para esta tarea, determinándose estas claves teniendo en cuenta la categoría. De esta manera puede enviar en particular un componente del emisor sólo aquellos mensajes que pertenecen a

aquella categoría para la que este componente ha recibido material de claves válido. Tampoco en una implementación incorrecta del componente de software queda por ello amenazada la seguridad de aquellos componentes de software con una mayor necesidad de protección.

En el procedimiento de acuerdo con la invención se necesita además sólo una cadena hash entre un emisor y uno o varios receptores para proteger varios servicios o tipos de mensajes mediante material de claves separado. De esta manera se reducen las necesidades de memoria para la gestión de cadenas hash por parte del emisor y del receptor, ya que sólo tiene que gestionarse una cadena hash por cada emisor. Las claves específicas, utilizadas para la `protección de la integridad, pueden deducirse en cada momento según se necesite a partir del valor válido en ese momento de la cadena hash.

REIVINDICACIONES

1. Procedimiento para enviar mensajes (M1, M2, M3) con protección de integridad, en el que en un emisor (SE) previsto para enviar los mensajes (M1, M2, M3):
   - se genera una cadena hash de valores consecutivos (h1, h2, h3), generándose los valores (h1, h2, h3) partiendo de un valor generado inicialmente (h0), mediante la aplicación consecutiva de una función hash criptográfica (H) sobre el valor inicialmente generado (h0), representando el último valor generado (h3) un valor de anclaje, que se proporciona a uno o varios receptores predeterminados (RE) de los mensajes (M1, M2, M3) y los valores restantes (h0, h1, h2) son válidos en secuencia inversa a su generación en períodos de validez consecutivos (I0, I1, I2);
   - en el período de validez (I0, I1, I2) del correspondiente valor (h1, h2, h3) se genera una suma de prueba criptográfica (MIC1, MIC2, MIC3) para un mensaje (M1, M2, M3) a enviar utilizando el correspondiente valor (h0, h1, h2) y se envía la suma de prueba junto con el mensaje (M1, M2, M3);
   - el correspondiente valor (h0, h1, h2) se envía una vez transcurrido su periodo de validez (I0, I1, I2),

   caracterizado porque la generación de la suma de prueba (MIC1, MIC2, MIC3) se realiza tal que para el mensaje (M1, M2, M3) a enviar se determina una categoría (k1, k2, k3) que caracteriza el mensaje (M1, M2, M3), a partir de la cual, junto con el valor (h0, h1, h2) válido en ese momento, se deduce mediante una función de deducción de claves (KDF), una clave (h21, h22, h03) con la que se genera la suma de prueba (MIC1, MIC2, MIC3) para el mensaje (M1, M2, M3).

2. Procedimiento de acuerdo con la reivindicación 1,
   en el que la categoría determinada procede de una o varias de las siguientes categorías (k1, k2, k3):
   - una o varias categorías (k1, k2, k3) que especifican en cada caso un tipo de un mensaje (M1, M2, M3);
   - una o varias categorías (k1, k2, k3) que especifican en cada caso al menos un servicio o al menos una aplicación, mediante el que o mediante la que se envía un mensaje (M1, M2, M3);
   - una o varias categorías (k1, k2, k3) que especifican en cada caso uno o varios protocolos y/o números de puerto a través de los que se envía un mensaje (M1, M2, M3);
   - una o varias categorías (k1, k2, k3) que especifican en cada caso al menos un receptor predeterminado (RE) para el que está previsto el mensaje (M1, M2, M3);
   - una o varias categorías (k1, k2, k3) que especifican en cada caso un intervalo de tiempo en el que se envía un mensaje, siendo el intervalo de tiempo con preferencia más corto que los correspondientes periodos de validez (I0, I1, I2).

3. Procedimiento de acuerdo con la reivindicación 1 ó 2,
   en el que las categorías (k1, k2, k3) están contenidas en los mensajes (M1, M2, M3) a enviar y/o se deducen de los mensajes (M1, M2, M3) a enviar.

4. Procedimiento de acuerdo con una de las reivindicaciones precedentes,
   en el que la función de deducción de claves (KDF) es una función hash criptográfica.

5. Procedimiento de acuerdo con una de las reivindicaciones precedentes,
   en el que las sumas de prueba (MIC1, MIC2, MIC3) son códigos MAC o códigos MIC.

6. Procedimiento de acuerdo con una de las reivindicaciones precedentes,
   en el que los mensajes (M1, M2, M3) son mensajes de broadcast y/o multicast.

7. Procedimiento de acuerdo con una de las reivindicaciones precedentes,
   en el que los mensajes (M1, M2, M3) son paquetes de datos y/o estructuras de datos de un protocolo predeterminado.

8. Procedimiento de acuerdo con una de las reivindicaciones precedentes,
   en el que el valor de anclaje (h3) se proporciona al o a los receptor/es predeterminados (RE) firmado digitalmente, pudiendo verificarse la firma mediante el o los receptor/es predeterminados (RE).

9. Procedimiento de acuerdo con una de las reivindicaciones precedentes,
   en el que los mensajes (M1, M2, M3) se transmiten en una red de datos para la automatización industrial y/o para la automatización de la energía y/o en una red de sensores.

10. Emisor para enviar mensajes con protección de integridad, estando configurado el emisor tal que con el emisor (RE), durante el funcionamiento:
    - se genera una cadena hash de valores consecutivos (h1, h2, h3), generándose los valores (h1, h2, h3) partiendo de un valor generado inicialmente (h0), mediante la aplicación consecutiva de una función hash criptográfica (H) sobre el valor inicialmente generado (h0), representando el último valor generado (h3) un valor de anclaje, que se proporciona a uno o varios receptores

predeterminados (RE) de los mensajes (M1, M2, M3) y los valores restantes (h0, h1, h2) son válidos en secuencia inversa a su generación en períodos de validez consecutivos (I0, I1, I2);

- en el período de validez (I0, I1, I2) del correspondiente valor (h1, h2, h3) se genera una suma de prueba criptográfica (MIC1, MIC2, MIC3) para un mensaje (M1, M2, M3) a enviar utilizando el correspondiente valor (h0, h1, h2) y se envía la suma de prueba junto con el mensaje (M1, M2, M3);
- el correspondiente valor (h0, h1, h2) se envía una vez transcurrido su periodo de validez (I0, I1, I2),

caracterizado porque la generación de la suma de prueba (MIC1, MIC2, MIC3) se realiza tal que para el mensaje (M1, M2, M3) a enviar se determina una categoría (k1, k2, k3) que caracteriza el mensaje (M1, M2, M3), a partir de la cual, junto con el valor (h0, h1, h2) válido en ese momento, se deduce mediante una función de deducción de claves (KDF), una clave (h21, h22, h03) con la que se genera la suma de prueba (MIC1, MIC2, MIC3) para el mensaje (M1, M2, M3).

11. Emisor de acuerdo con la reivindicación 10,
en el que el emisor está configurado para realizar un procedimiento de acuerdo con una de las reivindicaciones 2 a 9.

12. Procedimiento para procesar mensajes con protección de integridad, habiéndose enviado los mensajes mediante un emisor con un procedimiento de acuerdo con una de las reivindicaciones 1 a 9, en el que en un receptor predeterminado (RE), al que se ha proporcionado el valor de anclaje (h3):

- se reciben los mensajes (M1, M2, M3) junto con las sumas de prueba (MIC1, MIC2, MIC3), así como el correspondiente valor (h0, h1, h2) una vez transcurrido su período de validez (I0, I1, I2),
- al recibirse el correspondiente valor (h0, h1, h2) se realiza una verificación del valor (h0, h1, h2) basándose en el valor de anclaje (h3),
- si la verificación del correspondiente valor (h0, h1, h2) tiene éxito, se determina la categoría (k1, k2, k3) de mensajes (M1, M2, M3) recibidos durante el período de validez del correspondiente valor (h0, h1, h2) y mediante la misma función de deducción de claves (KDF) que utiliza el emisor (SE), se genera, a partir de la categoría (k1, k2, k3) de un mensaje y del valor correspondiente (h0, h1, h2), una clave (h21, h22, h03) con la que se verifica la suma de prueba (MIC1, MIC2, MIC3) del mensaje (M1, M2, M3).

13. Procedimiento de acuerdo con la reivindicación 12,
en el que si no tiene éxito la verificación del correspondiente valor (h0, h1, h2), finaliza y/o se retrotrae la realización de una o varias acciones que se iniciaron mediante mensajes que se recibieron durante el período de validez (I0, I1, I2) del correspondiente valor (h0, h1, h2) junto con un valor de prueba (h0, h1, h2).

14. Procedimiento de acuerdo con la reivindicación 12 ó 13,
en el que cuando se verifica sin éxito la suma de prueba (MIC1, MIC2, MIC3) de un mensaje (M1, M2, M3), finaliza y/o se retrotrae la realización de una o varias acciones que se han iniciado mediante el mensaje.

15. Procedimiento de acuerdo con una de las reivindicaciones 12 a 14,
en el que al receptor predeterminado (RE) se le proporciona el valor de anclaje (h3) firmado digitalmente, verificándose en el receptor (RE) la firma digital del valor de anclaje (h3).

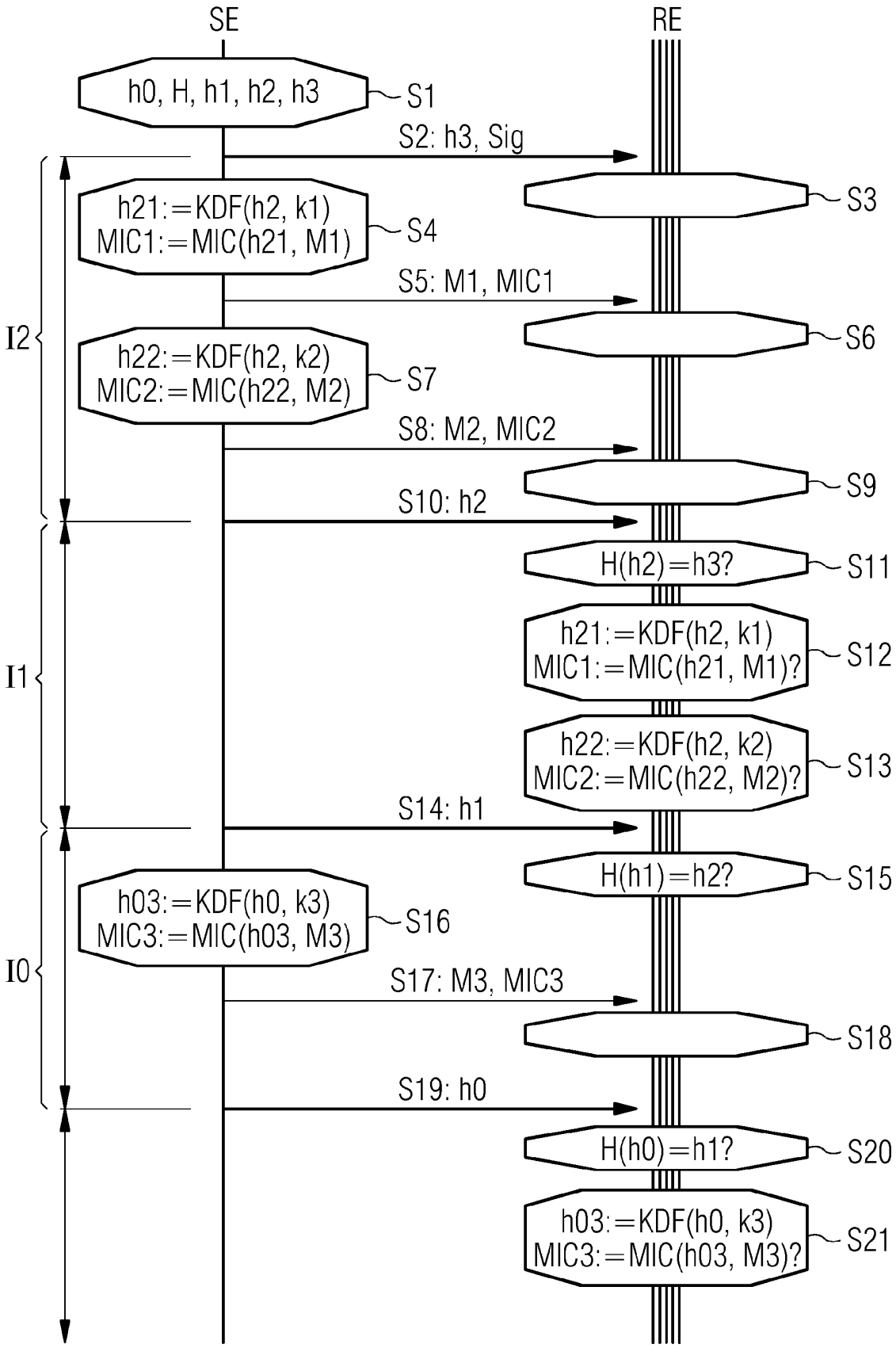
16. Receptor para recibir y para procesar mensajes con protección de integridad, habiéndose enviado los mensajes con un procedimiento de acuerdo con una de las reivindicaciones 1 a 9,
en el que al receptor se le ha proporcionado el valor de anclaje (h3) y el receptor está configurado tal que durante su funcionamiento::

- se reciben los mensajes (M1, M2, M3) junto con las sumas de prueba (MIC1, MIC2, MIC3), así como el correspondiente valor (h0, h1, h2) una vez transcurrido su período de validez (I0, I1, I2),
- al recibirse el correspondiente valor (h0, h1, h2) se realiza una verificación del valor (h0, h1, h2) basándose en el valor de anclaje (h3),
- si la verificación del correspondiente valor (h0, h1, h2) tiene éxito, se determina la categoría (k1, k2, k3) de mensajes (M1, M2, M3) recibidos durante el período de validez del correspondiente valor (h0, h1, h2) y mediante la misma función de deducción de claves (KDF) que utiliza el emisor (SE), se genera a partir de la categoría (k1, k2, k3) de un mensaje y del valor correspondiente (h0, h1, h2) una clave (h21, h22, h03) con la que se verifica la suma de prueba (MIC1, MIC2, MIC3) del mensaje (M1, M2, M3).

17. Receptor de acuerdo con la reivindicación 16,
en el que el receptor (RE) está configurado para realizar un procedimiento de acuerdo con una de las reivindicaciones 13 a 15.

18. Procedimiento para transmitir mensajes con protección de integridad, enviándose los mensajes con un procedimiento de acuerdo con una de las reivindicaciones 1 a 9 mediante un emisor (SE) y recibiéndose y procesándose con un procedimiento de acuerdo con una de las reivindicaciones 12 a 15 mediante un receptor (RE).

19. Sistema para transmitir mensajes con protección de integridad, que incluye al menos un emisor (SE) de acuerdo con la reivindicación 10 u 11 y al menos un receptor (RE) de acuerdo con la reivindicación 16 ó 17.


SE
RE
h0, H, h1, h2, h3
S1
S2: h3, Sig
S3
h21:=KDF(h2, k1)
MIC1:=MIC(h21, M1)
S4
S5: M1, MIC1
S6
h22:=KDF(h2, k2)
MIC2:=MIC(h22, M2)
S7
S8: M2, MIC2
S9
S10: h2
H(h2)=h3?
S11
h21:=KDF(h2, k1)
MIC1:=MIC(h21, M1)?
S12
h22:=KDF(h2, k2)
MIC2:=MIC(h22, M2)?
S13
S14: h1
H(h1)=h2?
S15
h03:=KDF(h0, k3)
MIC3:=MIC(h03, M3)
S16
S17: M3, MIC3
S18
S19: h0
H(h0)=h1?
S20
h03:=KDF(h0, k3)
MIC3:=MIC(h03, M3)?
S21
I2
I1
I0