(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 386 040**

(51) Int. CI.:
H04W 12/04 (2009.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07704444 .4**
(96) Fecha de presentación: **08.02.2007**
(97) Número de publicación de la solicitud: **2011302**
(97) Fecha de publicación de la solicitud: **07.01.2009**

(54) Título: **Procedimiento y sistema para la creación, protegida frente a manipulación, de una clave criptográfica**

(30) Prioridad:
26.04.2006 DE 102006019466

(45) Fecha de publicación de la mención BOPI:
07.08.2012

(45) Fecha de la publicación del folleto de la patente:
07.08.2012

(73) Titular/es:
SIEMENS AKTIENGESELLSCHAFT
WITTELSBACHERPLATZ 2
80333 MÜNCHEN, DE

(72) Inventor/es:
FALK, Rainer y
KOHLMAYER, Florian

(74) Agente/Representante:
Zuazo Araluze, Alexander

DESCRIPCIÓN

Procedimiento y sistema para la creación, protegida frente a manipulación, de una clave criptográfica

La invención se refiere a un procedimiento y a un sistema para la creación, protegida frente a manipulación, de una clave criptográfica común entre dos nodos a través de una interfaz de radio.

En los sistemas de radio de corto alcance, tales como Bluetooth, WLAN, ZigBee o WiMax, los terminales se comunican entre sí a través de una interfaz de radio. Para proteger la información transmitida a través de la interfaz de radio frente a manipulación o escuchas por terceros, la información entre los nodos o terminales del sistema de radio de corto alcance se transmite de manera cifrada. Para ello es necesario que los terminales o nodos creen una clave criptográfica común.

En los sistemas de radio de corto alcance, el usuario final debe crear la clave criptográfica por sí mismo y no recibe apoyo a este respecto de ningún operador de red. La configuración o la creación de una clave criptográfica es complicada y susceptible a errores para usuarios finales privados. Muchos usuarios finales tienden a crear claves o contraseñas sencillas, fácilmente reconocibles, por ejemplo “1234”, que son relativamente fáciles de averiguar por terceros.

En la creación de una clave criptográfica común se conocen protocolos de seguridad convencionales, que crean una clave secreta, que sólo conocen los participantes implicados activamente en el desarrollo del protocolo, pero no un atacante pasivo externo, es decir que sólo está a la escucha. Dos protocolos de seguridad conocidos son el protocolo de seguridad según Diffie Hellman para el acuerdo de clave y una variante anónima, no autentificable, del protocolo de seguridad SSL/TLS (*Secure Source Layer/Transport Layer Security*).

El acuerdo de clave según Diffie Hellman permite acordar una clave secreta a través de un canal no seguro. Dos participantes A, B conocen a este respecto dos valores públicos, un valor de módulo m, es decir un número primo alto, y un número entero g.

En el acuerdo de clave, A calcula en primer lugar un número aleatorio alto a y calcula a continuación $X = g^a \bmod m$. El otro participante B calcula un número aleatorio alto b y calcula $Y = g^b \bmod m$.

Después de que el participante A haya enviado el valor X calculado al otro participante B, este participante B calcula un valor $W1 = X^b \bmod m$.

El participante B envía el valor Y calculado al participante A. A continuación el participante A calcula el valor $W2 = Y^a \cdot \bmod m$. Los dos valores W1, W2 calculados por los participantes A, B son $g^{db} \bmod m$. Los valores W1, W2 calculados representan la clave secreta común de ambos participantes A, B. Esta clave acordada S no puede generarse sin el conocimiento de A, B por un tercero. La inversión de la exponenciación realizada por A, B requiere muchísimas etapas de cálculo y dura por consiguiente mucho tiempo. Esta propiedad garantiza el mantenimiento del secreto de la clave común acordada W1 = W2 = S.

Una clave criptográfica común acordada de este modo S es segura con respecto a atacantes terceros pasivos, es decir segura frente a una intercepción por terceros. No obstante, una creación de este tipo de la clave común S no es segura frente a un atacante activo (*man in the middle*), que manipula la comunicación entre los dos participantes, si el acuerdo de clave no se desarrolla de manera autenticada. Entonces es posible, concretamente, que un mensaje “construido” no proceda del supuesto emisor, sino de un tercero no autorizado. El receptor del mensaje no puede darse cuenta de esta diferencia.

La figura 1 muestra esquemáticamente un ataque activo por un tercer nodo al crear una clave criptográfica común S entre dos nodos K1, K2 en el caso de un protocolo de acuerdo de clave convencional. El atacante A trata de influir por ejemplo en el desarrollo o evolución de los mensajes intercambiados según el protocolo de seguridad de tal manera que, tras el desarrollo del protocolo de seguridad, se ha creado una relación de seguridad entre el primer nodo K1 y el atacante A y una relación de seguridad adicional entre el segundo nodo K2 y el atacante A, de modo que el atacante A, sin que se dé cuenta ninguno de los dos nodos K1, K2, está integrado en la comunicación entre los dos nodos K1, K2 (*man in the middle*).

El documento US 2005/0010680 A1 da a conocer un procedimiento para acordar una clave secreta entre dos aparatos según un protocolo denominado ESSPP (*Enhanced Shared Secret Provisioning Protocol*). Durante este proceso, un sistema de monitorización monitoriza el canal de radio en busca de mensajes ESSPP adicionales de un tercer aparato. De este modo, puede reconocerse de manera fiable un ataque *man-in-the-middle*, en el que un atacante finge ser ante un participante de la comunicación el respectivo contrario.

Es por tanto el objetivo de la presente invención crear un procedimiento y un sistema para la creación, protegida frente a manipulación, de una clave criptográfica común entre dos nodos a través de una interfaz de radio, que ofrezcan también en caso de emplear un protocolo de acuerdo de clave sin autenticación una protección eficaz con

respecto a ataques activos.

Este objetivo se soluciona según la invención mediante un procedimiento con las características indicadas en la reivindicación 1, mediante un sistema con las características indicadas en la reivindicación 9 y mediante un aparato de radio de corto alcance con las características indicadas en la reivindicación 10.

La invención crea un procedimiento para la creación, protegida frente a manipulación, de una clave criptográfica común entre dos nodos a través de una interfaz de radio, en el que al menos uno de los dos nodos monitoriza durante la creación de la clave criptográfica común durante un periodo de creación si un tercer nodo se comunica con uno de los dos nodos a través de la interfaz de radio. Los dos nodos crean la clave criptográfica común según un protocolo de acuerdo de clave mediante el intercambio de mensajes de acuerdo de clave predeterminados a través de al menos un primer canal de radio de la interfaz de radio. El nodo de monitorización monitoriza varios canales de radio de la interfaz de radio en el sentido de si se envían mensajes de acuerdo de clave por un tercer nodo a uno de los dos nodos a través de la interfaz de radio.

En el procedimiento según la invención está prevista una función de monitorización de radio para detectar a un atacante activo eventualmente presente (*man in the middle*). Puesto que el atacante activo debe comunicarse con ambos nodos, la distancia espacial entre los dos nodos que deben configurarse es reducida y la comunicación del atacante con los dos nodos tiene lugar a través de un canal de radio, un atacante activo no puede manipular la comunicación entre los dos nodos sin que la función de monitorización de radio prevista según la invención se dé cuenta de que el atacante activo participa como tercer nodo.

El procedimiento según la invención combina por tanto un procedimiento de seguridad criptográfico con un procedimiento de monitorización de radio no criptográfico durante la creación de una clave criptográfica común, que es segura con respecto a atacantes activos.

En una primera forma de realización del procedimiento según la invención, el nodo de monitorización interrumpe la creación de la clave criptográfica común con el otro nodo, si el nodo de monitorización observa que un tercer nodo se comunica a través de la interfaz de radio con uno de los dos nodos.

En una forma de realización alternativa del procedimiento según la invención, el nodo de monitorización no interrumpe la creación de la clave criptográfica común con el otro nodo, si un tercer nodo se comunica a través de la interfaz de radio con uno de los dos nodos, pero la clave criptográfica creada se almacena como una clave criptográfica no segura.

En una forma de realización preferida del procedimiento según la invención, el nodo de monitorización monitoriza si se envía un mensaje de aviso de error desde otro nodo.

En una forma de realización preferida del procedimiento según la invención, el nodo de monitorización monitoriza si durante la creación de la clave criptográfica en el periodo de creación disminuye una calidad de canal de radio.

En una forma de realización preferida del procedimiento según la invención, el nodo de monitorización monitoriza adicionalmente si un tercer nodo durante periodos de protección antes y después del periodo de creación se comunica con uno de los dos nodos a través de la interfaz de radio.

En una forma de realización preferida del procedimiento según la invención, los nodos se forman por aparatos de radio de corto alcance.

La invención crea además un sistema de radio de corto alcance con varios aparatos de radio de corto alcance, que se comunican entre sí a través de una interfaz de radio, en el que, al crear una clave criptográfica común entre dos aparatos de radio de corto alcance del sistema de radio de corto alcance, al menos uno de los dos aparatos de radio de corto alcance monitoriza, durante la creación de la clave criptográfica a través de la interfaz de radio durante un periodo de creación, si un aparato de radio de corto alcance adicional se comunica con uno de los dos aparatos de radio de corto alcance a través de la interfaz de radio. Los dos aparatos de radio de corto alcance crean la clave criptográfica común según un protocolo de acuerdo de clave mediante el intercambio de mensajes de acuerdo de clave predeterminados a través de al menos un primer canal de radio de la interfaz de radio. El aparato de radio de corto alcance de monitorización monitoriza varios canales de radio de la interfaz de radio en el sentido de si se envían mensajes de acuerdo de clave por el aparato de radio de corto alcance adicional a uno de los dos aparatos de radio de corto alcance a través de la interfaz de radio.

La invención crea además un aparato de radio de corto alcance que, al crear una clave criptográfica común con otro aparato de radio de corto alcance a través de una interfaz de radio, monitoriza esta interfaz de radio para observar una manipulación en el sentido de si durante la creación de la clave criptográfica común un tercer aparato de radio de corto alcance se comunica con uno de los dos aparatos de radio de corto alcance a través de una interfaz de radio. Los dos aparatos de radio de corto alcance crean la clave criptográfica común según un protocolo de acuerdo de clave mediante el intercambio de mensajes de acuerdo de clave predeterminados a través de al menos un primer

canal de radio de la interfaz de radio. El aparato de radio de corto alcance de monitorización monitoriza varios canales de radio de la interfaz de radio en el sentido de si se envían mensajes de acuerdo de clave por un tercer aparato de radio de corto alcance a uno de los dos aparatos de radio de corto alcance a través de la interfaz de radio.

A continuación se describirán formas de realización preferidas del procedimiento según la invención y del sistema de radio de corto alcance según la invención haciendo referencia a las figuras adjuntas para explicar las características esenciales de la invención.

Muestran:

la figura 1: un diagrama para explicar la problemática base de la invención;

la figura 2: un diagrama de bloques de un sistema de radio de corto alcance según la invención con dos aparatos de radio de corto alcance con función de monitorización de radio;

la figura 3: un diagrama de bloques de una forma de realización preferida de un aparato de radio de corto alcance utilizado en el sistema de radio de corto alcance según la invención con función de monitorización de radio;

la figura 4: un diagrama de señales para explicar el procedimiento según la invención para la creación de una clave criptográfica común sin un ataque activo por parte de un tercero;

la figura 5: un diagrama de señales del procedimiento según la invención para la creación de una clave criptográfica común en caso de un ataque activo por parte de un tercero.

Tal como puede observarse en la figura 2, un sistema 1 de radio de corto alcance según la invención presenta al menos dos aparatos 2-1, 2-2 de radio de corto alcance o nodos. Los aparatos 2-1, 2-2 de radio de corto alcance se comunican entre sí por medio de antenas 5-1, 5-2 de emisión/recepción a través de una interfaz 3 de radio. Al menos uno de los dos aparatos de radio de corto alcance o nodos presenta una función de monitorización de radio o *watch-dog-funktion* (WD). Al crear una clave criptográfica común entre los dos aparatos 2-1, 2-2 de radio de corto alcance del sistema 1 de radio de corto alcance, el aparato 2-2 de radio de corto alcance, que contiene una unidad 4 de monitorización de radio, monitoriza la creación de la clave criptográfica a través de la interfaz 3 de radio durante un periodo de creación predeterminado en el sentido de si un aparato de radio de corto alcance adicional se comunica con uno de los dos aparatos 2-1, 2-2 de radio de corto alcance a través de la interfaz 3 de radio.

La figura 3 muestra esquemáticamente un diagrama de bloques de una forma de realización preferida de un aparato 2 de radio de corto alcance o nodo, tal como se utiliza en el sistema 1 de radio de corto alcance según la invención. El nodo 2 presenta una unidad 4 de monitorización de radio, que monitoriza señales de radio, que se transmiten a través de la interfaz 3 de radio. El nodo 2 presenta una antena 5 de emisión/recepción para emitir y recibir señales de radio. La antena 5 de emisión/recepción está unida por un lado con la unidad 4 de monitorización de radio y por otro lado con una unidad 6 de comunicación de radio del nodo 2. La unidad 6 de comunicación de radio contiene un dispositivo de emisión y uno de recepción para emitir y recibir señales de radio. La unidad 4 de monitorización de radio puede implementarse, en una forma de realización, también como parte de la unidad 6 de comunicación de radio. En una forma de realización alternativa, la unidad 4 de monitorización de radio presenta una antena de emisión/recepción separada propia. El aparato 2 de radio de corto alcance presenta preferiblemente además una unidad 7 de control, en la que se ejecuta un programa correspondiente al procedimiento según la invención. El aparato 2 de radio de corto alcance contiene una memoria 8 para almacenar una clave criptográfica creada, que se utiliza para cifrar mensajes.

Tal como puede observarse en la figura 2, no todos los aparatos 2 de radio de corto alcance o nodos 2 del sistema 1 de radio de corto alcance según la invención deben contener una unidad 4 de monitorización de radio, sino sólo al menos uno de los dos nodos, que desean acordar una clave criptográfica común. Si la unidad 4 de monitorización de radio del nodo 2-2 de monitorización para la creación de la clave criptográfica común observa que un tercer nodo se comunica a través de la interfaz 3 de radio con uno de los dos nodos 2-1, 2-2, en una primera forma de realización del procedimiento según la invención, la unidad 7 de control del nodo 2-2 de monitorización interrumpe la operación de creación. En una forma de realización alternativa, ante la detección de un tercer nodo el nodo 2-2 de monitorización no interrumpe la creación de la clave criptográfica común, pero la clave criptográfica creada se almacena en las dos memorias 8 de claves de ambos nodos 2-1, 2-2 en cada caso identificada como “no segura”. Si la unidad 4 de monitorización de radio del nodo 2-2 de monitorización observa la comunicación de un tercer nodo a través de la interfaz 3 de radio con uno de los dos nodos 2-1, 2-2, el nodo 2-2 de monitorización genera en una forma de realización preferida un mensaje de error y lo emite a través de la interfaz 3 de radio. En el procedimiento según la invención, la creación de la clave criptográfica común entre los dos nodos 2-1, 2-2 tiene lugar a través de la interfaz 3 de radio según un protocolo de acuerdo de clave predeterminado, en el que se intercambian mensajes de acuerdo de clave predeterminados a través de al menos un canal de radio de la interfaz 3 de radio entre los nodos 2-1, 2-2. Este protocolo de acuerdo de clave es, por ejemplo, un protocolo de acuerdo de clave de Diffie-Hellman o un protocolo de acuerdo de clave SSL/DLS. Ambos protocolos de acuerdo de clave son protocolos de acuerdo de clave

sin autenticación, es decir un nodo, que recibe mensajes, no tiene la posibilidad de determinar con seguridad de qué emisor proviene el mensaje.

Para aumentar la protección en el procedimiento según la invención puede tener lugar, a continuación de un protocolo de acuerdo de clave sin autenticación, una autenticación por medio de un número PIN. En una forma de realización alternativa, tras acordar la clave criptográfica común el usuario compara, para aumentar la protección, la clave criptográfica creada en los dos aparatos de radio de corto alcance o su valor *Hash*, o la clave criptográfica indicada por un aparato de radio de corto alcance se introduce en el otro nodo o aparato de radio de corto alcance. El procedimiento según la invención mejora mediante la función de monitorización de radio la seguridad de la creación de la clave criptográfica común entre dos aparatos de radio de corto alcance. Si se emplea un protocolo de acuerdo de clave sin autenticación, en el procedimiento según la invención el usuario puede prescindir totalmente de la introducción de un número PIN o de una contraseña o de una comprobación de la clave común creada. Sin embargo, de manera alternativa, es posible realizar además de la función de monitorización de radio también una autenticación durante el acuerdo de clave, para aumentar la seguridad del trayecto de comunicación entre los aparatos de radio de corto alcance frente a ataques.

En una primera forma de realización del procedimiento según la invención, el nodo 2-2 de monitorización sólo monitoriza un canal de radio de la interfaz de radio. En este caso, la creación de la clave criptográfica común tiene lugar entre los nodos en un canal de radio previamente establecido. Esto tiene la ventaja de que el esfuerzo técnico de conmutación para la realización de la monitorización de radio es reducido, ya que sólo se monitorizan envíos de radio en el canal de radio predeterminado.

En una forma de realización alternativa, la unidad de monitorización de radio monitoriza varios canales de radio de la interfaz 3 de radio.

El canal de radio es un canal de radio cualquiera, por ejemplo un canal de radio FDM (*Frequency Division Multiplexing*), un canal de radio TDM (*Time Division Multiplexing*) o un canal de radio CDM (*Code Division Multiplexing*). La unidad 4 de monitorización de radio monitoriza si tiene lugar alguna comunicación sospechosa entre uno de los dos nodos 2-1, 2-2 y un tercer nodo. Para ello, la unidad 4 de monitorización de radio del nodo 2-2 de monitorización monitoriza si se envían mensajes de acuerdo de clave por un tercer nodo a uno de los dos nodos a través de la interfaz 3 de radio.

Adicionalmente, la unidad 4 de monitorización de radio monitoriza si se ha enviado un mensaje de aviso de error generado.

Además, la unidad 4 de monitorización de radio puede monitorizar si durante la creación de la clave criptográfica durante un periodo de creación predeterminado disminuye una calidad de canal de radio. La disminución significativa de la calidad de canal durante el procedimiento de creación en comparación con una calidad de canal observada previamente es un indicio de que, a través de la interfaz de radio, tiene lugar una comunicación adicional. Una disminución de la calidad de canal se manifiesta en particular en una mayor probabilidad de pérdida de paquetes. En una posible forma de realización del procedimiento según la invención, la creación de la clave criptográfica común entre los dos nodos se interrumpe, si el nodo 2-2 de monitorización observa una perturbación en el canal de transmisión, por ejemplo la aparición de una pérdida de paquetes de datos.

La unidad 4 de monitorización de radio puede monitorizar además si un nodo adicional está activo en el mismo canal de radio, pudiendo observarse esto mediante su dirección, por ejemplo una dirección MAC. Además, la unidad 4 de monitorización de radio puede monitorizar si el propio nombre de red (WLAN-SSID) se indica en varios puntos de acceso, es decir en el mismo o en otro canal de radio. Existe concretamente la posibilidad de que un atacante haya establecido un nodo con el mismo nombre de red.

Si la unidad 4 de monitorización de radio determina uno de los tipos de comunicación sospechosa anteriormente mencionados, existe la posibilidad de que se produzca un ataque activo por parte de un tercero. Los tipos de comunicación sospechosa anteriormente mencionados se observan preferiblemente por separado y, en caso de que aparezca al menos un tipo de comunicación sospechosa, en una posible forma de realización del procedimiento según la invención se interrumpe la creación de la clave criptográfica común. En una forma de realización alternativa, los diferentes tipos de comunicación sospechosa se monitorizan por separado y a continuación se suman de manera ponderada en caso de que aparezcan. Si el valor de suma ponderada así calculado sobrepasa un valor umbral determinado, en una forma de realización del procedimiento según la invención se produce la interrupción de la creación de la clave criptográfica común.

En una forma de realización adicional del procedimiento según la invención, el nodo de monitorización monitoriza adicionalmente si un tercer nodo, durante periodos de protección antes y después del periodo de creación, se comunica con uno de los dos nodos a través de la interfaz 3 de radio. Debido a que también antes y después del verdadero periodo de creación tiene lugar una monitorización, está protegido el periodo percibido por un usuario como fase de creación, es decir desde el inicio de la creación hasta su finalización. De este modo se evita que tengan lugar dos o incluso más operaciones de creación separadas de manera muy seguida, es decir de manera no

perceptible o apenas perceptible para el usuario. De este modo se evita que un atacante interconecte un nodo de atacante en primer lugar con uno de los nodos 2-1 y más tarde, de manera independiente, con el otro nodo 2-1. Los periodos de protección antes y después del periodo de creación se eligen por tanto preferiblemente con un tamaño tal que los ataques se observen fácilmente, por ejemplo en el intervalo de desde 1 hasta 5 segundos.

Para la realización de los periodos de protección, en una forma de realización preferida del procedimiento según la invención se prevén temporizadores o contadores, para monitorizar si en un periodo de protección previo o en un periodo de protección subsiguiente ha aparecido una comunicación sospechosa. Los temporizadores o contadores están previstos preferiblemente en la unidad 7 de control del nodo.

Si la unidad 4 de monitorización de radio observa una comunicación sospechosa, entonces se inicia un temporizador. Esto tiene lugar independientemente de si el aparato de radio de corto alcance o el nodo 2 ya se encuentra o no en un modo operativo de enlace. De este modo se consigue una monitorización del canal de radio antes del propio procedimiento de enlace, en el que se crea la clave criptográfica común. Cuando se inicia un procedimiento de enlace, puede consultarse por tanto si en un intervalo de tiempo previo, predeterminado por el temporizador, se ha observado un tipo de comunicación sospechosa de este tipo. En una forma de realización preferida la unidad 4 de monitorización de radio monitoriza el canal de radio o los canales de radio también una vez finalizada la operación de creación para la creación de la clave criptográfica común. La función de monitorización de radio está activa en este caso tras la creación de la clave todavía durante un lapso de tiempo predeterminado y comunica tipos de comunicación sospechosa. De este modo se consigue una monitorización del canal de radio a lo largo de un periodo completo, que abarca un lapso de tiempo definido antes y después del periodo de creación para la creación de la clave criptográfica.

En una forma de realización alternativa esto se consigue mediante retardos durante el procedimiento de enlace. Al inicio del procedimiento de enlace se monitoriza durante un cierto lapso de tiempo el canal de radio en el sentido de si aparece un tipo de comunicación sospechosa. De este modo, aunque se prolonga la duración de tiempo necesaria para el enlace, la función de monitorización no debe estar activa sin embargo fuera de la fase de enlace.

En caso de que aparezca un tipo de comunicación sospechosa, en una primera forma de realización se interrumpe la creación de clave totalmente, es decir no se crea ninguna clave criptográfica común. En una forma de realización alternativa, en caso de sospecha la clave criptográfica se crea, pero se almacena como poco fiable en la memoria 8 de claves. Una configuración explícita tiene lugar por el usuario a continuación mediante comparación o mediante autenticación adicional por medio de un número PIN.

Los nodos 2-1, 2-2 se forman por aparatos de radio de corto alcance con un alcance relativamente reducido. En una forma de realización preferida los aparatos de radio de corto alcance son terminales de radio WLAN, Bluetooth, ZigBee o WiMax. Los nodos 2-1, 2-2 o los aparatos de radio pueden ser terminales móviles o estaciones fijas.

La figura 4 muestra un diagrama de señales, que representa la creación de una clave común S entre dos nodos 2-1, 2-2 sin un ataque activo por parte de un tercer nodo.

El aparato 2-1 de radio de corto alcance o el nodo K1 envía un mensaje Setup-Start al segundo aparato 2-1 de radio de corto alcance o al nodo K2. Esto se confirma a continuación en un mensaje Setup-Start-Okay por el segundo nodo. A continuación, el primer aparato 2-1 de radio de corto alcance envía al segundo nodo 2-2 un valor g^x, siendo g un número entero y representando x un número aleatorio calculado por el primer nodo 2-1. El segundo nodo 2-2 transmite de vuelta al primer nodo 2-1 un valor g^Y, representando g un número entero conocido por los dos nodos y siendo y un valor aleatorio calculado por el segundo nodo 2-2. Ambos nodos 2-1, 2-2 calculan a continuación la clave común $S = \mathbf{Y^X \bmod m}$ así como $S = \mathbf{X^y \bmod m}$. La clave criptográfica común S se almacena a continuación en cada caso en la memoria 8 de claves del nodo respectivo. En una posible forma de realización se almacena una clave pseudoaleatoria derivada de la clave criptográfica, que presenta por ejemplo una menor longitud de bits, en la memoria 8 de claves.

Preferiblemente tiene lugar a continuación una comprobación o verificación en el sentido de si ambos nodos 2-1, 2-2 han determinado la misma clave común. A este respecto se espera preferiblemente un lapso de tiempo establecido, durante el que no debe aparecer ninguna comunicación sospechosa. Para ello se emplea un temporizador dentro de la unidad 4 de monitorización de radio del nodo 2-2 de monitorización. Una vez transcurrido el tiempo de espera se concluye la comprobación o verificación.

Son posibles numerosas desviaciones de la operación representada en la figura 4. Por ejemplo en una forma de realización la creación de la clave criptográfica común puede realizarse directamente sin mensaje de inicio. Además es posible que el tiempo de espera empiece ya después del mensaje “Setup 2” o tras el cálculo y almacenamiento de la clave K. En una forma de realización adicional se monitoriza como tiempo de espera de monitorización adicional un periodo que no empieza hasta el mensaje “Setup_Ver OK ·2”. En una forma de realización alternativa se prescinde totalmente de una verificación de la clave común creada.

Los lapsos de tiempo para la monitorización de comunicaciones aleatorias pueden variar dentro de un intervalo

amplio. El periodo se elige de tal manera que, durante el periodo que el usuario percibe para la creación de la clave, sólo estén activos dos aparatos. Preferiblemente, el valor del temporizador se establece en un intervalo de aproximadamente 1 a 5 segundos.

La figura 5 muestra un diagrama de señales en el caso de un ataque activo por parte de un tercer nodo 9. El nodo 2-2 no puede distinguir a este respecto por sí mismo si el nodo 2-1 o el tercer nodo 9 representado en la figura 5 es un nodo atacante. Sin embargo, la unidad 4 de monitorización de radio del nodo 2-2 de monitorización observa que a través de la interfaz 3 de radio se comunica o está activo más de un nodo. El intercambio de mensajes de protocolo de acuerdo de clave empieza tal como se representa en la figura 4, sólo que la creación no tiene lugar entre los nodos 2-1, 2-2, sino entre el nodo 2-1 y el nodo 9 atacante. No obstante, en cuanto el nodo 9 atacante se activa, es decir envía también un mensaje Setup-Start al nodo 2-2, la unidad 4 de monitorización de radio del nodo de monitorización observa esto y señala una comunicación sospechosa. La creación de la clave criptográfica se interrumpe entonces por la unidad 7 de control del nodo 2-2 de monitorización. El nodo 2-2 de monitorización identifica la comunicación sospechosa entre el nodo 2-1 y el nodo 9 atacante como un error, sólo cuando él mismo pasa también a un modo para la creación de una clave criptográfica común. De lo contrario, la comunicación entre el nodos 2-1 y el nodo 9 podría ser una creación deseada de una clave o una relación de seguridad entre los dos nodos 2-1, 9. En el ejemplo dado, el nodo 2-2 de monitorización pasa al modo para la creación de clave al recibir un mensaje “Setup_Start” (A, K2). Alternativamente, el nodo 2-2 también podría pasar al modo Setup o al modo para la creación de la clave mediante una interacción de usuario.

En cuanto la unidad 7 de control del nodo 2-2 de monitorización interrumpe la creación de la clave común, el nodo 2-2 de monitorización envía a través de su antena 5-2 un mensaje Setup-Failure a los otros nodos o a todos los nodos observados presentes en un envío de multidifusión o en un envío de difusión. En cuanto el nodo 2-1 obtiene el mensaje Setup-Failure del nodo 2-2 de monitorización, también interrumpe la operación para la creación de la clave común. En una posible forma de realización se indica al usuario la interrupción de la operación de creación, por ejemplo, mediante un LED de error parpadeante.

El diagrama representado en la figura 5 ilustra también un valor de temporizador, que mide cuánto tiempo dura ya una comunicación sospechosa observada. Con la observación de la comunicación sospechosa “Setup” (K1, A), en el ejemplo representado en la figura 5 se inicia el contador o temporizador y, en el plazo de por ejemplo de 1 a 5 segundos, realiza una cuenta atrás. El intento de creación de una clave con el nodo 2-2 de monitorización antes de que haya transcurrido el temporizador, lleva al mensaje de error “Setup_Failure”. Una comunicación sospechosa previa adicional, por ejemplo 5 minutos antes, no lleva a una interrupción.

En una forma de realización preferida, la función de monitorización de radio de la unidad 4 de monitorización de radio está activa también antes y después de la propia creación. Si dentro de este lapso de tiempo se observa una señal de radio sospechosa, se anula posteriormente la creación del nodo o se rechaza ya desde el principio con un mensaje de error “Setup_Failure”. En una forma de realización alternativa, la función de monitorización de radio se activa sólo con el comienzo de la creación y/o se desactiva de nuevo con la finalización de la creación. En esta forma de realización no está previsto entonces ningún almacenamiento intermedio de seguridad temporal, ni está previsto después de la propia creación. Alternativamente sin embargo puede preverse un tiempo de espera o retardo correspondiente durante la operación de creación.

Una cierta protección adicional puede conseguirse previendo un breve almacenamiento intermedio de seguridad temporal. En este caso, la monitorización de radio sólo está activa durante la propia creación y tampoco están previstos tiempos de espera durante la operación de creación para la monitorización de radio. En este caso se observan ataques activos cuando tienen lugar dentro del periodo de creación, que normalmente sólo es corto, que dura por ejemplo sólo fracciones de segundo.

Mediante el procedimiento según la invención se mejora considerablemente la seguridad frente a un ataque activo también en el caso de un procedimiento de creación criptográfico no seguro o sin autenticación.

REIVINDICACIONES

1. Procedimiento para la creación, protegida frente a manipulación, de una clave criptográfica común entre dos nodos (2-1, 2-2) a través de una interfaz (3) de radio,

en el que al menos uno de los dos nodos (2-1, 2-2) monitoriza, durante la creación de la clave criptográfica común (S) durante un periodo de creación, si un tercer nodo (9) se comunica con uno de los dos nodos (2-1, 2-2) a través de la interfaz (3) de radio,

creando ambos nodos (2-1, 2-2) la clave criptográfica común según un protocolo de acuerdo de clave mediante el intercambio de mensajes de acuerdo de clave predeterminados a través de un canal de radio de la interfaz (3) de radio,

caracterizado porque el nodo (2-2) de monitorización monitoriza varios canales de radio de la interfaz (3) de radio en el sentido de si se envían mensajes de acuerdo de clave por el tercer nodo (9) a uno de los dos nodos (2-1, 2-2) a través de la interfaz (3) de radio.

2. Procedimiento según la reivindicación 1, en el que el nodo (2-2) de monitorización interrumpe la creación de la clave criptográfica común (S) con el otro nodo (2-1), si el nodo (2-2) de monitorización observa que el tercer nodo (9) se comunica a través de la interfaz (3) de radio con uno de los dos nodos (2-1, 2-2).

3. Procedimiento según la reivindicación 1, en el que el nodo (2-2) de monitorización no interrumpe la creación de la clave criptográfica común con el otro nodo (2-1), si el tercer nodo (9) se comunica a través de la interfaz (3) de radio con uno de los dos nodos (2-1, 2-2) y almacena la clave criptográfica creada (S) como una clave criptográfica no segura.

4. Procedimiento según la reivindicación 2 ó 3, en el que el nodo (2-2) de monitorización envía además un mensaje de aviso de error, si el tercer nodo (9) se comunica a través de la interfaz (3) de radio con uno de los dos nodos (2-1, 2-2) en el periodo de creación.

5. Procedimiento según la reivindicación 1, en el que el nodo (2-2) de monitorización monitoriza si se envía un mensaje de aviso de error por el tercer nodo (9).

6. Procedimiento según la reivindicación 1, en el que el nodo (2-2) de monitorización monitoriza si durante la creación de la clave criptográfica en el periodo de creación disminuye una calidad de canal de radio.

7. Procedimiento según la reivindicación 1, en el que el nodo (2-2) de monitorización monitoriza además si el tercer nodo (9) se comunica durante periodos de protección antes y después del periodo de creación con uno de los dos nodos (2-1, 2-2) a través de la interfaz (3) de radio.

8. Procedimiento según la reivindicación 1, en el que los nodos (2-1, 2-2) se forman por aparatos (2) de radio de corto alcance.

9. Sistema (1) de radio de corto alcance con varios aparatos (2) de radio de corto alcance, que se comunican entre sí a través de una interfaz (3) de radio,

en el que, al crear una clave criptográfica común (S) entre dos aparatos (2-1, 2-2) de radio de corto alcance del sistema (1) de radio de corto alcance, al menos uno de los dos aparatos (2-1, 2-2) de radio de corto alcance monitoriza, durante la creación de la clave criptográfica (S) a través de la interfaz (3) de radio durante un periodo de creación, si un aparato (9) de radio de corto alcance adicional se comunica con uno de los dos aparatos (2-1, 2-2) de radio de corto alcance a través de la interfaz (3) de radio,

creando los dos aparatos (2-1, 2-2) de radio de corto alcance la clave criptográfica común según un protocolo de acuerdo de clave mediante el intercambio de mensajes de acuerdo de clave predeterminados a través de un canal de radio de la interfaz (3) de radio,

caracterizado porque el aparato (2-2) de radio de corto alcance de monitorización monitoriza varios canales de radio de la interfaz (3) de radio en el sentido de si se envían mensajes de acuerdo de clave por el aparato (9) de radio de corto alcance adicional a uno de los dos aparatos (2-1, 2-2) de radio de corto alcance a través de la interfaz (3) de radio.

10. Aparato (2) de radio de corto alcance que, al crear una clave criptográfica común (S) con otro aparato (2) de radio de corto alcance a través de una interfaz (3) de radio, monitoriza esta interfaz (3) de radio para observar una manipulación en el sentido de si durante la creación de la clave criptográfica común (S) un tercer aparato (9) de radio de corto alcance se comunica con uno de los dos aparatos (2-1, 2-2) de radio de corto alcance a través de la interfaz (3) de radio, creando los dos aparatos (2) de radio de corto alcance la

clave criptográfica común según un protocolo de acuerdo de clave mediante el intercambio de mensajes de acuerdo de clave predeterminados a través de un canal de radio de la interfaz (3) de radio,

caracterizado porque el aparato (2) de radio de corto alcance de monitorización monitoriza varios canales de radio adicionales de la interfaz (3) de radio en el sentido de si se envían mensajes de acuerdo de clave por el tercer aparato (9) de radio de corto alcance a uno de los dos aparatos (2-1, 2-2) de radio de corto alcance a través de la interfaz (3) de radio.

FIG 1
Estado de la técnica

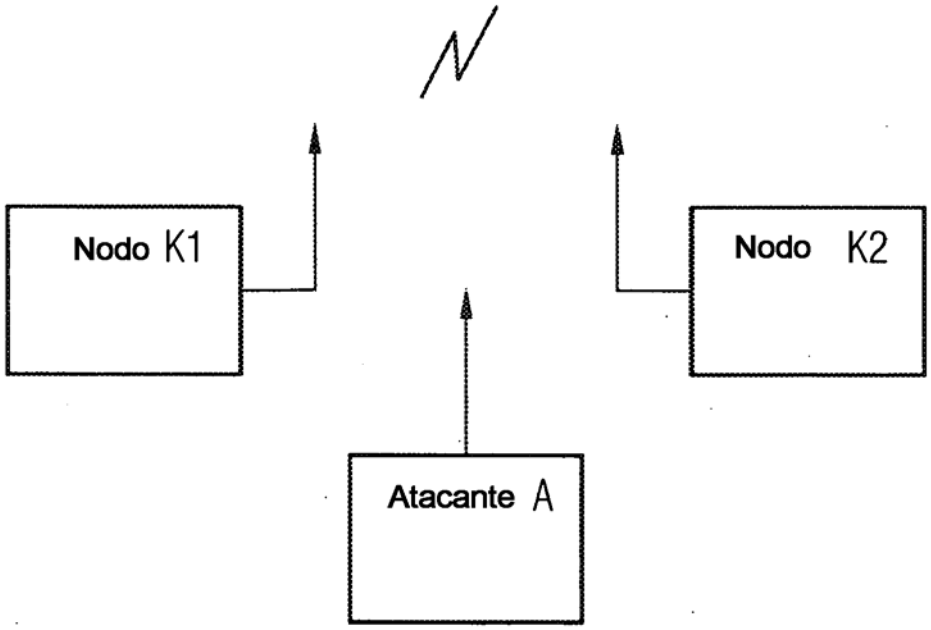


FIG 2

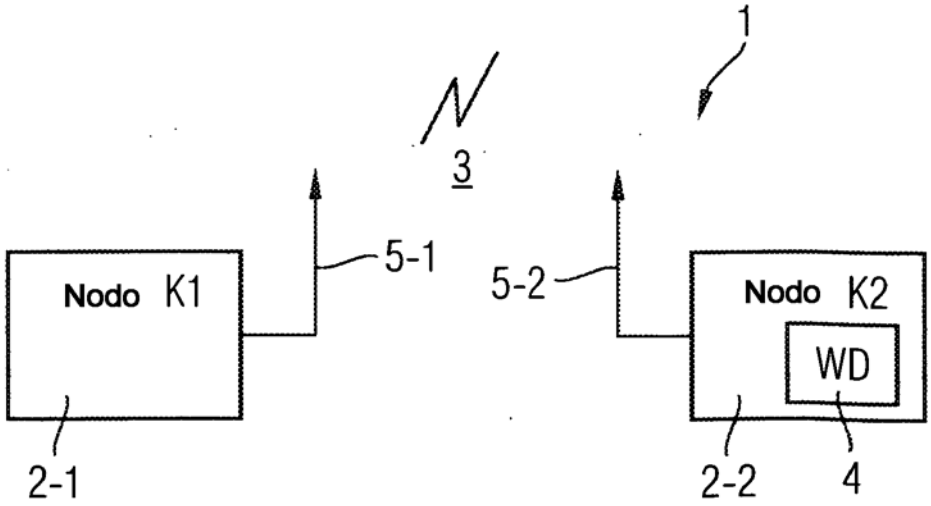


FIG 3

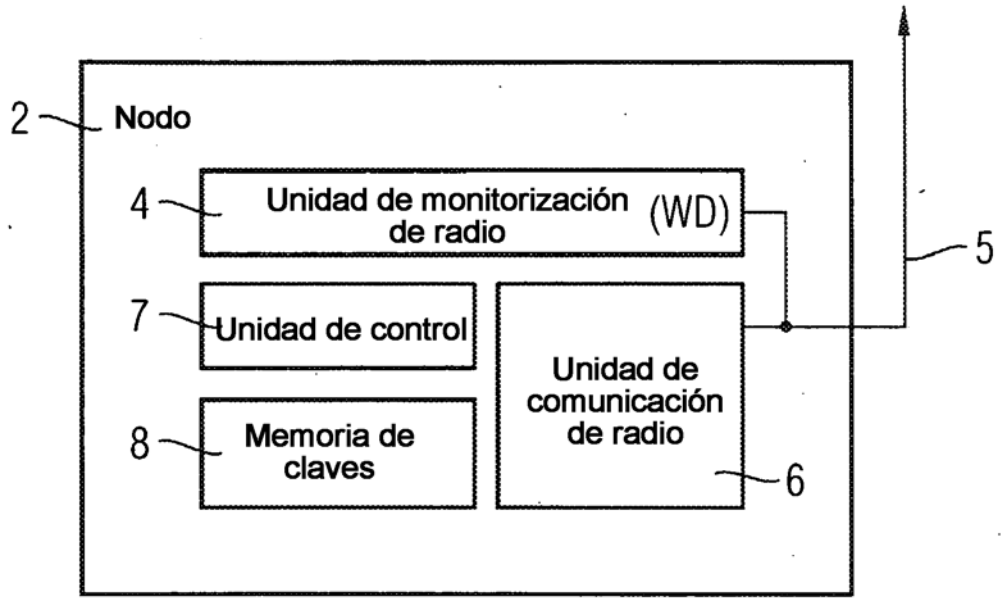

2
Nodo
4
Unidad de monitorización de radio
(WD)
5
7
Unidad de control
Unidad de comunicación de radio
8
Memoria de claves
6

FIG 4

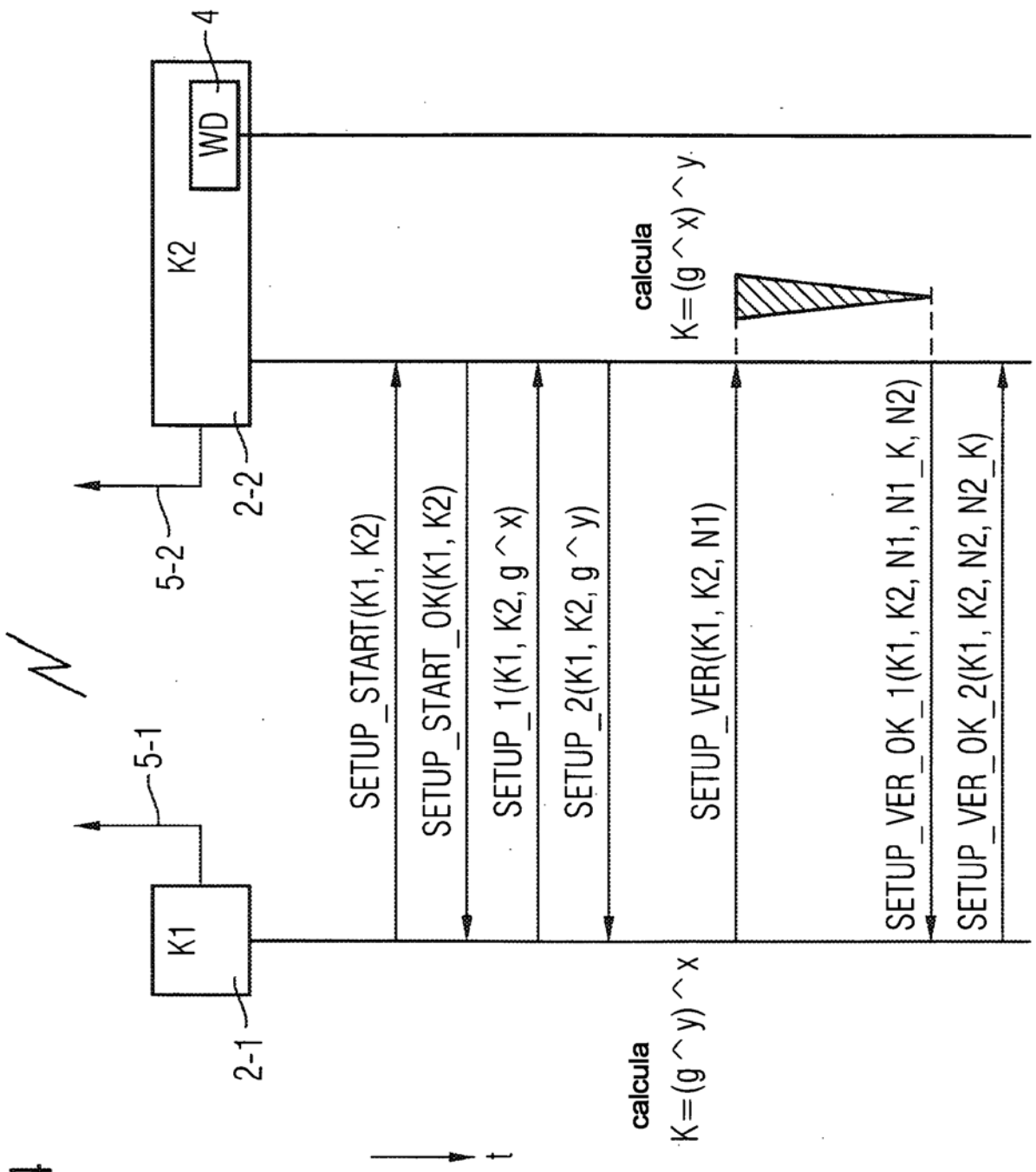
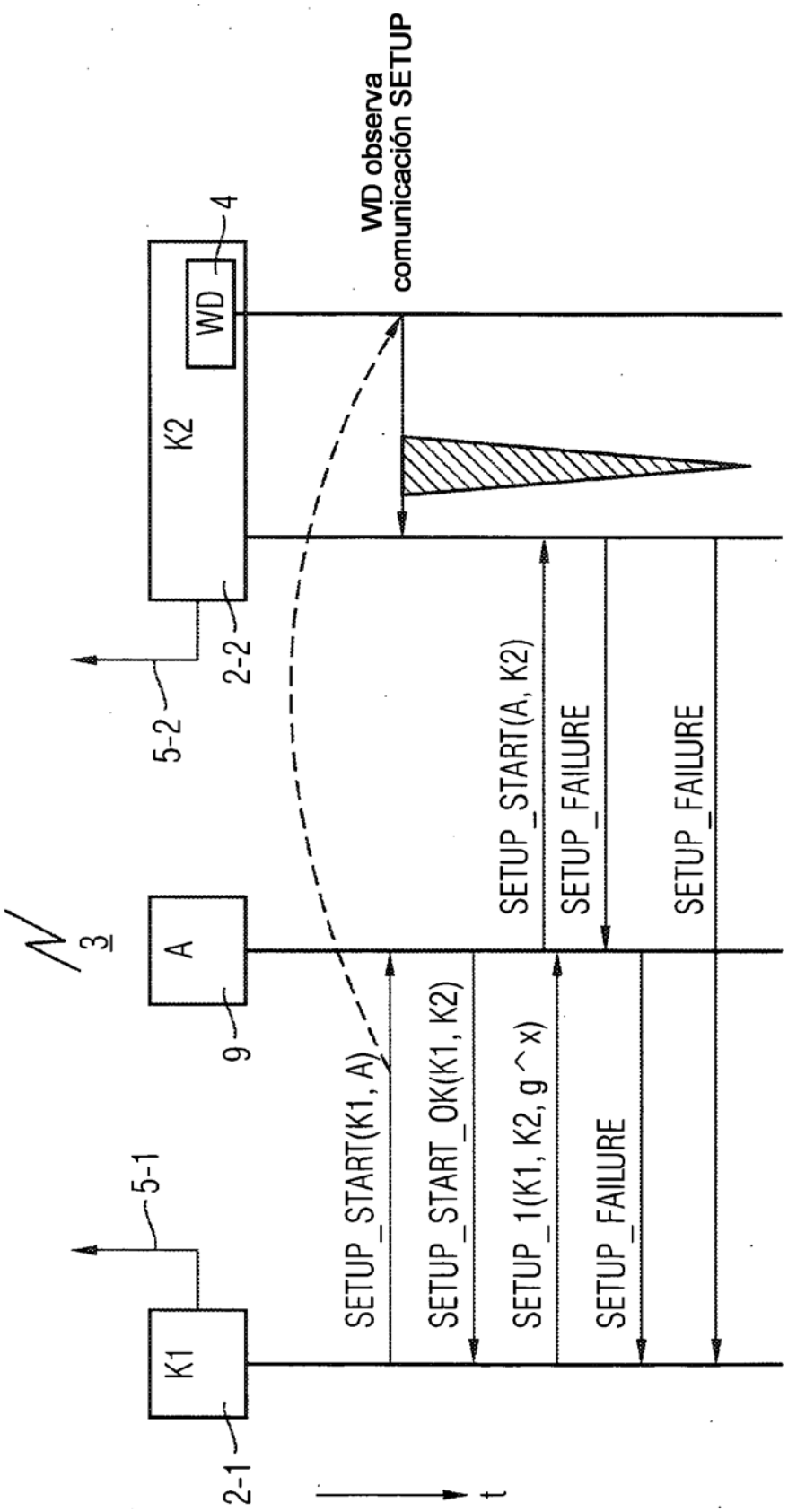

K1
K2
WD
4
2-1
2-2
5-1
5-2
SETUP_START(K1, K2)
SETUP_START_OK(K1, K2)
SETUP_1(K1, K2, g ^ x)
SETUP_2(K1, K2, g ^ y)
SETUP_VER(K1, K2, N1)
SETUP_VER_OK_1(K1, K2, N1, N1_K, N2)
SETUP_VER_OK_2(K1, K2, N2, N2_K)
calcula
K=(g ^ y) ^ x
calcula
K=(g ^ x) ^ y
t

FIG 5


WD observa comunicación SETUP
4
WD
K2
2-2
5-2
3
A
9
5-1
K1
2-1
SETUP_START(K1, A)
SETUP_START_OK(K1, K2)
SETUP_1(K1, K2, g^x)
SETUP_FAILURE
SETUP_START(A, K2)
SETUP_FAILURE
SETUP_FAILURE
t