(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 645 812**

(51) Int. CI.:

H04L 9/12 (2006.01)
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **19.09.2011 PCT/IT2011/000326**

(87) Fecha y número de publicación internacional: **28.03.2013 WO13042143**

(96) Fecha de presentación y número de la solicitud europea: **19.09.2011 E 11785138 (6)**

(97) Fecha y número de publicación de la concesión europea: **09.08.2017 EP 2748966**

(54) Título: **Gestión de claves simétricas sincronizadas para asegurar datos intercambiados por nodos de comunicaciones**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.12.2017

(73) Titular/es:

TELESPAZIO S.P.A. (100.0%)
Via Tiburtina 965
00156 Roma, IT

(72) Inventor/es:

VALLETTA, DAMIANO;
SAITTO, ANTONIO y
BELLOFIORE, PAOLO

(74) Agente/Representante:

PONS ARIÑO, Ángel

DESCRIPCIÓN

Gestión de claves simétricas sincronizadas para asegurar datos intercambiados por nodos de comunicaciones

Campo técnico de la invención

La presente invención se refiere a la gestión de claves simétricas sincronizadas y al uso de las mismas para asegurar datos intercambiados por nodos de comunicaciones. En particular, un aspecto específico de la presente invención se refiere a la gestión de claves sincronizadas de cifrado / descifrado simétrico y al cifrado / descifrado simétrico basado en las mismas.

Antecedentes de la técnica

En la actualidad, se usan de forma generalizada las claves simétricas para asegurar datos intercambiados por nodos de comunicaciones.

Por ejemplo, en criptografía, los algoritmos de clave simétrica usan una y la misma clave criptográfica, que se denomina clave simétrica, tanto para el cifrado como para el descifrado, es decir, para transformar el texto plano en texto cifrado y viceversa. La clave simétrica debe ser conocida por los nodos de comunicaciones que intercambian los datos cifrados sobre la base de dicha clave simétrica con el fin de admitir un cifrado correcto.

En muchos sistemas de comunicaciones actuales que usan un cifrado / descifrado simétrico para asegurar las comunicaciones, las claves simétricas se distribuyen a priori a los nodos de comunicaciones con el fin de minimizar el riesgo de que las claves distribuidas sean captadas de manera furtiva. De todas maneras, dicho riesgo nunca se elimina por completo y, por lo tanto, si las claves distribuidas son captadas de manera furtiva por una persona no autorizada, tal persona puede descifrar los datos intercambiados por los nodos de comunicaciones autorizados.

Por lo tanto, los actuales sistemas de comunicaciones que distribuyen a priori las claves simétricas a los nodos de comunicaciones nunca son completamente seguros.

En los documentos WO 01/63832 A1 y WO 01/91366 A2 se divulgan sistemas y métodos conocidos para comunicaciones criptográficas.

En particular, el documento WO 01/63832 A1 divulga un aparato y método para asegurar las comunicaciones criptográficas entre un emisor y un receptor o múltiples receptores, que incluye un primer y un segundo elementos de temporización, y una primera y una segunda unidades de almacenamiento de clave que contienen múltiples claves en un orden previamente determinado para su selección dependiendo de los respectivos tiempos de clave, en el que los tiempos de clave aparecen de forma periódica de acuerdo con el primer y el segundo elementos de temporización, de forma respectiva. Una unidad de cifrado de datos obtiene una nueva clave a partir de la primera unidad de almacenamiento de clave en cada aparición del tiempo de clave de la primera unidad de almacenamiento de clave, y usa la clave para cifrar los datos de entrada. Y al menos una unidad de descifrado de datos obtiene una nueva clave a partir de la segunda unidad de almacenamiento de clave en cada aparición del tiempo de clave de la segunda unidad de almacenamiento de clave. La sincronización de tiempos del equipo de los participantes proporciona el método de seleccionar unas claves compatibles para el proceso de cifrado y de descifrado.

Además, el documento WO 01/91366 A2 divulga un aparato y método para generar unas claves criptográficas pseudo aleatorias en un sistema de comunicaciones criptográficas, con lo que, dado un conjunto común de datos de configuración de inicialización, las claves criptográficas pseudo aleatorias se pueden generar de manera duplicativa por medio de diversos generadores de claves pseudo aleatorias independientes del sistema de comunicaciones criptográficas.

Objeto y sumario de la invención

El objetivo de la presente invención es proporcionar una metodología para gestionar claves simétricas que pueda subsanar al menos en parte los inconvenientes que se han mencionado en lo que antecede.

Este objetivo se logra mediante la presente invención en el sentido de que la misma se refiere a un método para asegurar / desasegurar datos intercambiados por los nodos de comunicaciones, un aparato de comunicaciones configurado para poner en práctica dicho método y un producto de programa de soporte lógico para poner en práctica dicho método, tal como se define en las reivindicaciones adjuntas.

Breve descripción de los dibujos

Para una mejor comprensión de la presente invención, las formas de realización preferidas, que se han de entender meramente a modo de ejemplo y no se han de interpretar como limitantes, se describirán a continuación con referencia a los dibujos que se adjuntan (no todos ellos dibujados a escala), en los que:

- la figura 1 ilustra de forma esquemática un primer proceso de generación de claves de acuerdo con una primera forma de realización preferida de la presente invención;
- la figura 2 ilustra de forma esquemática un segundo proceso de generación de claves de acuerdo con una segunda forma de realización preferida de la presente invención;
- la figura 3 muestra los saltos de clave de acuerdo con una forma de realización a modo de ejemplo de la presente invención;
- la figura 4 muestra una relación entre un tiempo de tic tac de un reloj interno de un aparato de comunicaciones y un tiempo de permanencia de clave de acuerdo con una forma de realización a modo de ejemplo de la presente invención;
- la figura 5 ilustra de forma esquemática un ejemplo de una arquitectura funcional de un nodo de emisión de acuerdo con una forma de realización preferida específica de la presente invención;
- la figura 6 muestra una generación de tiempo de sincronización a modo de ejemplo realizada por el nodo de emisión de la figura 5;
- la figura 7 muestra un ejemplo de una ventana de clave usada en la recepción de acuerdo con dicha forma de realización preferida específica de la presente invención; y
- la figura 8 ilustra de forma esquemática un ejemplo de una arquitectura funcional de un nodo de recepción de acuerdo con dicha forma de realización preferida específica de la presente invención.

Descripción detallada de formas de realización preferidas de la invención

El siguiente análisis se presenta para posibilitar que un experto en la materia realice y use la invención. Diversas modificaciones de las formas de realización les resultarán evidentes a los expertos en la materia, sin apartarse del alcance de la presente invención, tal como se reivindica. Por lo tanto, se entiende que la presente invención no está limitada a las formas de realización mostradas, sino que se le ha de conceder el alcance más extenso que resulte coherente con los principios y las características que se divulgan en el presente documento y que se define en las reivindicaciones adjuntas.

La presente invención se refiere a la generación local de claves simétricas sincronizadas y al uso de las mismas para asegurar los datos intercambiados por los nodos de comunicaciones.

Algunos conceptos básicos de la presente invención son independientes de los diferentes escenarios de aplicación, en tanto que algunas características están adaptadas a escenarios de aplicación específicos. Por lo tanto, en lo que sigue se describirán en primer lugar los conceptos generales de la presente invención y entonces las características específicas de los diferentes escenarios.

Algunos conceptos de la presente invención son aplicables a todos los nodos de comunicaciones implicados en una comunicación segura, es decir, al emisor o emisores y al receptor o receptores y, por lo tanto, en la siguiente descripción, no se repetirán dichos conceptos, en tanto que sí se resaltarán las funcionalidades específicas puestas en práctica solo por el emisor o emisores y el receptor o receptores.

Un aspecto específico de la presente invención se refiere a la generación local de claves de cifrado simétrico sincronizadas, a ambos lados de un canal de comunicaciones, en concreto de un canal de comunicaciones público, es decir, que se pueda captar de manera furtiva.

En particular, de acuerdo con dicho aspecto específico de la presente invención, los nodos de comunicaciones cifran y descifran los datos mutuamente intercambiados por un canal de comunicaciones usando claves de cifrado / descifrado sincronizadas extraídas de una y la misma secuencia de claves, y cambiando la clave de cifrado / descifrado usada durante la transmisión / recepción. El cambio de clave se puede planificar según un criterio temporal o de eventos y se sincroniza entre los nodos de comunicaciones con el fin de garantizar un cifrado correcto. Este concepto presenta una analogía con las técnicas de comunicación por saltos de frecuencia de acuerdo con las cuales el transmisor o transmisores y el receptor o receptores cambian de frecuencia según un criterio temporal, siguiendo una secuencia compartida de frecuencias. En particular, en las técnicas de comunicación por saltos de frecuencia, el cambio entre dos frecuencias consecutivas de una determinada secuencia de frecuencias se denomina “salto de frecuencia” y, de manera análoga, en lo que sigue se adoptará un nombre similar, en concreto “salto de clave”, para identificar el cambio entre dos claves consecutivas de una determinada secuencia de claves.

En una perspectiva más general, la presente invención permite que los nodos de comunicaciones generen las mismas secuencias de claves y extraigan las claves sincronizadas de dichas secuencias. Las claves extraídas se pueden aprovechar de forma ventajosa para proporcionar diferentes servicios de seguridad como el cifrado / descifrado, la comprobación de integridad y la comprobación de autenticación o, se pueden usar como un índice para encontrar una única clave en una determinada secuencia de claves. En particular, las claves extraídas de cada secuencia se pueden usar para proporcionar un respectivo servicio de seguridad.

De acuerdo con la presente invención, la generación de claves es realizada de manera independiente por cada nodo de comunicaciones. Los nodos de comunicaciones no intercambian ningún mensaje para llegar a un acuerdo acerca

de la clave a emplear. El único requisito para la generación de claves es que las funciones utilizadas de generación de claves creen las mismas claves para ambos nodos de comunicaciones con el fin de permitir que el nodo o nodos de recepción recuperen de manera correcta la información.

Preferiblemente, la generación de claves local se realiza en dos etapas:

1. una generación o recuperación de una o más secuencias ordenadas de números (OSN, *Ordered Sequence of Numbers*); y
2. una generación de claves sobre la base de la o las OSN generadas / recuperadas.

Dicho proceso de generación de claves en dos etapas permite generar de manera independiente diferentes claves para los diferentes servicios de seguridad sobre la base de una y la misma OSN. En particular, dicho proceso de generación de claves en dos etapas permite generar diferentes secuencias ordenadas de claves (OSK, *Ordered Sequence of Keys*) sobre la base de una y la misma OSN.

En conexión con lo anterior, la figura 1 ilustra de forma esquemática un primer proceso de generación de claves para generar las diferentes OSK sobre la base de una única OSN de acuerdo con una primera forma de realización preferida de la presente invención.

En particular, la figura 1 muestra un diagrama de bloques funcionales de una unidad de generación de claves 1 configurada para:

- proporcionar una OSN (el bloque 11) mediante la generación de la misma sobre la base de una semilla de grupo de servicios que preferiblemente funciona como un generador de números pseudo aleatorios (PRNG, *Pseudo Random Number Generator*) (el sub-bloque 111) o, como alternativa, mediante la recuperación de la misma de las OSN almacenadas (el sub-bloque 112); y
- aplicar, a cada uno de los N servicios de seguridad (en donde N es un número entero igual a o mayor que uno, es decir, $N \geq 1$) a proporcionar sobre la base de una respectiva OSK, una respectiva transformación de seguridad sobre la base de una respectiva Palabra del Día (WOD, *Word Of Day*) de servicio para la OSN generada / recuperada con el fin de generar un respectivo servicio de OSK (los bloques 12).

En detalle, tal como se muestra en la figura 1, se genera una OSK diferente para cada servicio de seguridad, aplicando una respectiva transformación de seguridad en la única OSN generada / recuperada. Cada transformación de seguridad utiliza, como entradas, la única OSN generada / recuperada y una WOD específica del respectivo servicio.

La generación de claves que se ha mencionado en lo que antecede permite la generación de las OSK que son idénticas al emisor o emisores y el receptor o receptores, si dichos nodos de comunicaciones se alimentan con una o más OSN idénticas y una o más WOD de servicio.

De manera conveniente, las transformaciones de seguridad usadas son de tal modo que aseguran unas buenas propiedades estadísticas del texto cifrado, incluso con patrones de texto plano aplicados como entrada, y garantizan que no sea posible hacer una predicción acerca de la OSN de entrada observando las OSK de salida.

En su lugar, la figura 2 ilustra de forma esquemática un segundo proceso de generación de claves sobre la base de unas OSN diferentes, de acuerdo con una segunda forma de realización preferida de la presente invención.

En particular, la figura 2 ilustra de forma esquemática un segundo proceso de generación de claves para generar diferentes OSK, cada una sobre la base de una respectiva OSN.

En detalle, la figura 2 muestra un diagrama de bloques funcionales de una unidad de generación de claves 2 configurada, en cada uno de los N servicios de seguridad (con $N \geq 1$) con el fin de proporcionarse sobre la base de una respectiva OSK, para:

- proporcionar una respectiva OSN (los bloques 21) mediante la generación de la misma sobre la base de una semilla de servicio respectiva que funciona preferiblemente como un PRNG (los sub-bloques 211) o, como alternativa, mediante la recuperación de la misma de las respectivas OSN almacenadas (los sub-bloques 212); y
- aplicar una respectiva transformación de seguridad sobre la base de un respectivo servicio de WOD a la respectiva OSN generada / recuperada con el fin de generar un respectivo servicio de OSK (los bloques 22).

Esta segunda solución para generar las OSK de servicio es más complejo desde el punto de vista computacional que la primera descrita en lo que antecede en conexión con la figura 1, pero resulta preferida en algunos escenarios de aplicación, por ejemplo cuando algunas de las OSK de servicio se han de enviar en texto plano por un canal público con el fin de usar las mismas como índices que identifican las claves de otras OSK de servicio.

Se puede obtener una solución intermedia dividiendo los servicios de seguridad en grupos y usando una semilla de grupo de servicios diferente para cada grupo de servicios de seguridad.

Tal como se ha descrito en lo que antecede, hay disponibles dos opciones principales para la generación local de una OSN, en concreto:

1. se genera una OSN usando un PRNG; o
2. se recupera una OSN de un almacenamiento de las OSN que contiene secuencias de números previamente generadas y es idéntica para el emisor o emisores y el receptor o receptores.

Usando la primera opción para la generación local de una OSN, se crean de forma dinámica todos los elementos de la OSN con una función de PRNG que se inicia a partir de una semilla, que se denomina semilla de grupo de servicios o semilla de servicio.

Una función de PRNG se puede definir como una función de generación de números aleatorios que produce una secuencia de valores sobre la base de una semilla y un estado actual. Dada la misma semilla, una función de PRNG siempre producirá la misma secuencia de valores. Esta propiedad asegura que se generará la misma OSN en ambos extremos de un canal de comunicaciones al iniciar una y la misma semilla. Un generador de números no pseudo aleatorios, tal como un generador de números aleatorios de soporte físico, no es adecuado para la presente invención, debido a que generaría OSN diferentes en los dos lados de un canal de comunicaciones.

Cuando ningún algoritmo de tiempo polinómico puede distinguir la salida de un PRNG y una secuencia aleatoria real, se dice que el PNRG es “criptográficamente fuerte”. Preferiblemente, de acuerdo con la presente invención, se usa un PRNG criptográficamente fuerte debido a que no posibilita predecir la secuencia generada. Además, tener un gran fragmento de conocimiento de la salida del PRNG no ayuda a predecir los valores pasados o futuros.

Además, con el fin de garantizar el carácter impredecible de la salida del PRNG criptográficamente fuerte utilizado, dicho PRNG se inicia, de manera conveniente, a partir de una semilla impredecible, por ejemplo una semilla que se genera usando una función no lineal.

En su lugar, usando la segunda opción para la generación local de una OSN, la OSN empleada para generar las claves de servicio se recupera de un almacenamiento de las OSN; resulta obvio que el almacenamiento o almacenamientos de las OSN son idénticos para todos los nodos de comunicaciones.

La primera opción tiene la ventaja de permitir una comunicación de duración potencialmente ilimitada debido a que los elementos de OSN se generan de forma dinámica, en tanto que la segunda opción está limitada a la dimensión del almacenamiento de las OSN. Esta ventaja está limitada de algún modo por la periodicidad del PRNG. De hecho, después de una cantidad fija de operaciones de generación (por lo general, muy alta), el PRNG produce de nuevo la misma secuencia de salida.

Los patrones en un PRNG pueden introducir riesgos de seguridad. Esos riesgos se pueden evitar de manera conveniente usando la transformación o transformaciones de seguridad que aseguran buenas propiedades estadísticas de texto cifrado incluso con patrones de texto plano, aplicados como entrada.

Además, preferiblemente, el ciclo de PRNG es más largo que la duración necesaria de la OSK. Por cierto, si se usa una transformación de seguridad de cifrado por bloques que funciona en un modo de libro de códigos electrónico (ECB, *Electronic Code Book*) para generar una OSK a partir de una OSN, la OSK generada tiene la misma duración de ciclo del PRNG. Este problema se puede evitar de manera conveniente usando, tal como se ha indicado en lo que antecede, la transformación o transformaciones de seguridad que aseguran buenas propiedades estadísticas de texto cifrado, incluso con patrones de texto plano aplicados como entrada. Por ejemplo, la transformación o transformaciones de seguridad de cifrado por bloques que funcionan en un modo de encadenamiento de bloques de cifrado (CBC, *Cipher Block Chaining*) se pueden usar de forma ventajosa, debido a que tienen la propiedad de ocultar los patrones de datos.

En lo que sigue, por razones de simplicidad de la descripción, se describirá el funcionamiento de los nodos de comunicaciones, cuando actúan como nodos de envío y de recepción, en conexión con un solo servicio de seguridad aplicado a los datos intercambiados por dichos nodos de comunicaciones, si bien se entiende que los conceptos de la presente invención descrita en lo que sigue con respecto a un solo servicio de seguridad son claramente aplicables también con el fin de proporcionar una pluralidad de servicios de seguridad.

En lo que respecta al funcionamiento de los emisores, un nodo de emisión selecciona una clave de servicio de una OSK de servicio generada usando su tiempo local sincronizado con un tiempo común de referencia global por medio de una referencia externa de tiempo local exacto y estable (LASTER, *Local Accurate and Stable Time External Reference*). La LASTER se puede adquirir de manera conveniente de una fuente externa o de una fuente interna usada por el nodo de emisión para marcar los paquetes de datos transmitidos.

Cada clave de servicio en una OSK de servicio tiene un tiempo de validez limitado, que en lo que sigue se denomina tiempo de permanencia de clave T.

En particular, el tiempo de permanencia de clave T es el tiempo que transcurre usando cada clave de servicio extraída de una OSK de servicio entre dos saltos de clave consecutivos.

En detalle, el tiempo de permanencia de clave T se relaciona con las unidades de tiempo interno que caracterizan, por lo general, una fuente de tiempo interno, tal como un reloj interno, de los nodos de comunicaciones, reloj interno que normalmente limita la resolución del tiempo por medio de su frecuencia. Por lo tanto, el tiempo de permanencia de clave T se puede calcular de manera conveniente como un múltiplo de un tiempo de tic tac del reloj interno, en el que el tiempo de tic tac es el inverso de la frecuencia del reloj interno.

Dicho de otra forma, usando un formalismo matemático, resulta que:

$$T = m \times tiempo\_tictac,$$

en el que m es un número entero igual a o mayor que uno (es decir, $m \geq 1$), y el tiempo de tic tac, tal como se ha explicado en lo que antecede, es el inverso de la frecuencia del reloj interno, en concreto:

$$tiempo\_tictac = \frac{1}{frecuencia\_reloj}$$

Se puede usar un índice n = 0, 1, 2, ... para identificar los intervalos consecutivos de validez de clave. En particular, el intervalo genérico de validez de clave n se corresponde con el tiempo de permanencia de clave que se inicia en t_0 + nT y finaliza en t_0 + (n + 1) T.

El tiempo inicial t_0 se puede elegir de manera conveniente como el tiempo inicial del servicio de seguridad, que se denomina tiempo de referencia global y que se expresa en el tiempo universal coordinado (UTC, *Coordinated Universal Time*).

Todas las tramas de datos a transmitir en el intervalo de validez de clave n se aseguran con una clave de servicio K [n] que se extrae de una OSK de servicio generada para el servicio de seguridad considerado, y que se puede expresar matemáticamente como:

$$K[n] = GenK(n, WOD, semilla),$$

en la que GenK denota una función de generación de claves para dicho servicio de seguridad considerado, función de generación de claves GenK que

- genera una OSK de servicio para el servicio de seguridad considerado sobre la base de una WOD de servicio asociada con dicho servicio de seguridad considerado y de una semilla de grupo de servicios o una semilla de servicio asociadas con dicho servicio de seguridad considerado, por ejemplo de acuerdo con el primer proceso de generación de claves descrito en lo que antecede en conexión con la figura 1 o, de acuerdo con el segundo proceso de generación de claves descrito en lo que antecede en conexión con la figura 2 o, de acuerdo con un proceso de generación de claves intermedio entre el primer y el segundo procesos de generación de claves; y
- extrae una clave de servicio K [n] de la OSK de servicio generada sobre la base del índice de intervalo de validez de clave n (que se puede ver también como un índice de etapa de generación de claves).

La figura 3 muestra cómo se relacionan el tiempo inicial (de servicio de seguridad) t_0, el tiempo de permanencia de clave T y el índice de intervalo de validez de clave n, y los diferentes intervalos de validez para las diferentes claves de servicio K [n], en la que n = 0, 1, 2, 3, 4, 5, 6.

La figura 4 muestra un ejemplo de relaciones entre el tiempo de tic tac, el tiempo de permanencia de clave T y el índice de intervalo de validez de clave n, según la hipótesis de que $T = 5 \times tiempo\_tictac$.

La función de generación de claves GenK puede generar de manera conveniente la OSK de servicio sobre la base de valores fijos de la WOD de servicio y de la semilla (de grupo) de servicios, y extraer de la OSK de servicio generada, a medida que transcurre el tiempo interno, una clave de servicio actual K [n] sobre la base del índice actual de intervalo de validez de clave n.

De manera conveniente, la semilla (de grupo) de servicios, el tiempo de permanencia de clave T y el tiempo inicial (de servicio de seguridad) t_0 pueden ser intercambiados en texto plano por los nodos de comunicaciones antes de iniciarse el intercambio de datos asegurados, pueden ser valores fijos o se pueden mantener secretos pero conocidos por los dos nodos de comunicaciones, por ejemplo pueden ser valores secretos pre-compartidos o ser

intercambiados por los nodos de comunicaciones por un canal de comunicaciones de una manera segura. Manteniendo secretos la semilla (de grupo) de servicios, el tiempo de permanencia de clave T y el tiempo inicial (de servicio de seguridad) t_0, se potencia la seguridad de la comunicación.

La figura 5 ilustra de forma esquemática un ejemplo de una arquitectura funcional de un nodo de transmisión diseñado para proporcionar un servicio de seguridad específico, por ejemplo el cifrado, de acuerdo con una forma de realización preferida específica de la presente invención.

En particular, la figura 5 muestra un diagrama de bloques funcionales de un nodo de emisión 5 que comprende:

- una fuente de LASTER 51 configurada para proporcionar una LASTER actual;
- una fuente de tiempo local 52 configurada para proporcionar un tiempo local actual;
- una unidad de sincronización 53 que está acoplada con la fuente de LASTER 51 y la fuente de tiempo local 52 para adquirir de las mismas, de forma respectiva, la LASTER actual y el tiempo local actual, y que está configurada para sincronizar el tiempo local actual con la LASTER actual con el fin de proporcionar un tiempo de sincronización actual;
- una unidad de cola de cabida útil 54 configurada para recibir los datos de cabida útil a asegurar de acuerdo con el servicio de seguridad específico (por ejemplo, a cifrar), y para proporcionar una señal de activación en relación con dichos datos de cabida útil;
- una unidad de cálculo de índices 55 que está acoplada con la fuente de tiempo local 52, la unidad de sincronización 53 y la unidad de cola de cabida útil 54 para adquirir de las mismas, de forma respectiva, el tiempo local actual, el tiempo de sincronización actual y la señal de activación, y que está configurada para calcular un índice actual de intervalo de validez de clave n sobre la base del tiempo local actual, del tiempo de sincronización actual, de la señal de activación, de un tiempo de permanencia de clave previamente definido T y de un tiempo inicial t_0 que está asociado con el servicio de seguridad específico;
- una unidad de generación de claves 56 que está acoplada con la unidad de cálculo de índices 55 para adquirir de las mismas el índice actual de intervalo de validez de clave n, y que está configurada para generar una OSK de servicio sobre la base de una WOD de servicio y una semilla (de grupo) de servicios asociada con el servicio de seguridad específico, y para extraer una clave de servicio actual K [n] de la OSK de servicio generada sobre la base del índice actual de intervalo de validez de clave n; y
- una unidad de transformación de seguridad de cabida útil 57 que está acoplada con la unidad de cola de cabida útil 54 y la unidad de generación de claves 56 para adquirir de las mismas, de forma respectiva, los actuales datos de cabida útil a asegurar de acuerdo con el servicio de seguridad específico y la clave de servicio actual K [n], y que está configurada para aplicar a dichos actuales datos de cabida útil una transformación de seguridad de cabida útil sobre la base de la clave de servicio actual K [n] y en relación con el servicio de seguridad específico con el fin de producir unos datos de cabida útil asegurados (por ejemplo, datos de cabida útil cifrados).

En detalle, la fuente de LASTER 51 puede ser, de manera conveniente:

- un terminal de Sistema Global de Navegación por Satélite (GNSS, *Global Navigation Satellite System*), tal como un terminal de Sistema de Posicionamiento Global (GPS, *Global Positioning System*) o Galileo o GLONASS, que está acoplado con el nodo de emisión 5 y del cual dicho nodo de emisión 5 adquiere un tiempo de GNSS actual; o
- un receptor configurado para recibir señales de radio relacionadas con el tiempo de una estación de radio basada en reloj atómico, y para extraer de las señales de radio relacionadas con el tiempo un tiempo exacto actual, tal como un receptor de DCF77, o un receptor de HBG o un receptor de WWVB; o
- un cliente de Protocolo de Tiempo de Red (NTP, *Network Time Protocol*); u
- otra fuente de tiempo global de la cual el nodo de emisión 5 puede adquirir una LASTER actual, por ejemplo el nodo de emisión 5 podría usar como una LASTER una referencia temporal que el mismo utiliza para sincronizar las tramas.

Por lo general, una fuente de LASTER, tal como un receptor de GPS, tiene dos salidas, en concreto:

- una salida de datos que transporta valores de tiempo global en términos de valores de fecha y hora de UTC (es decir, AAAA / MM / DD HH / mm / ss); y
- una señal de activación que señaliza el tiempo en el que se vuelve válido el último valor de tiempo global escrito en la salida de datos.

Durante el uso, una fuente de LASTER normalmente escribe los valores de tiempo global en la salida de datos antes de señalizar su tiempo inicial de validez por medio de la señal de activación.

Preferiblemente, la fuente de tiempo local 52 es un reloj interno del nodo de emisión 5, reloj interno que está configurado para proporcionar un contador de tiempo de tic tac local.

Tal como se ha descrito en lo que antecede, la unidad de sincronización 53 sincroniza el tiempo local actual con la LASTER actual con el fin de garantizar un impacto mínimo de las desviaciones del tiempo local.

El tiempo de sincronización al que da salida la unidad de sincronización 53 es un tiempo de referencia que se expresa en unidades de tiempo interno sincronizadas / relacionadas con / con respecto al tiempo global y exacto que es suministrado por la fuente de LASTER 51.

Preferiblemente, el tiempo de sincronización comprende dos campos:

- el contador de tiempo de tic tac local enclavado en el activador de LASTER (que se denota en lo que sigue como TiempoSinc.c); y
- un valor de tiempo local de LASTER en el activador de LASTER (que se denota en lo que sigue como TiempoSinc.TiempoGlobal).

La figura 6 muestra una generación de tiempo de sincronización a modo de ejemplo que es efectuada por la unidad de sincronización 53.

La unidad de cálculo de índices 55 calcula el índice actual de intervalo de validez de clave n sobre la base de:

- el último tiempo de sincronización;
- el contador de tic tac local actual;
- el tiempo inicial t_0;
- el tiempo de permanencia de clave previamente definido T; y
- la señal de activación a partir de la unidad de cola de cabida útil 54.

En un escenario asíncrono, la unidad de cola de cabida útil 54 preferiblemente proporciona la señal de activación cuando una nueva cabida útil está lista para ser transmitida.

Preferiblemente, la unidad de cálculo de índices 55 enclava el contador de tic tac actual en un tiempo de recepción de la señal de activación que señaliza que están disponibles los actuales datos de cabida útil a asegurar (que se denotan en lo que sigue como c_actual), y calcula el índice actual de intervalo de validez de clave n de acuerdo con la siguiente expresión matemática:

$$n = \frac{\frac{t\_0 - TiempoSinc.TiempoGlobal}{contador\_tiempo\_tictac\_local} + c\_actual - TiempoSinc.c}{T}$$

De manera conveniente, la unidad de generación de claves 56 está configurada para generar una OSK de servicio de acuerdo con el primer proceso de generación de claves descrito en lo que antecede en conexión con la figura 1 o de acuerdo con el segundo proceso de generación de claves descrito en lo que antecede en conexión con la figura 2 o de acuerdo con un proceso de generación de claves intermedio entre el primer y el segundo procesos de generación de claves.

Es importante resaltar el hecho de que la forma de realización preferida específica anteriormente descrita de la presente invención se puede poner en práctica mediante una arquitectura diferente de la del nodo de emisión 5 descrito en lo que antecede y que se muestra en la figura 5, siempre que dicha arquitectura diferente esté configurada para llevar a cabo la sincronización anteriormente descrita de un tiempo local actual con una LASTER actual, el cálculo anteriormente descrito de un índice actual de intervalo de validez de clave, y la extracción anteriormente descrita de una clave de servicio actual procedente de una OSK de servicio.

Dicho de otra forma, el nodo de emisión 5 puede ser cualquier dispositivo / aparato de comunicaciones configurado para llevar a cabo la sincronización anteriormente descrita de un tiempo local actual con una LASTER actual, el cálculo anteriormente descrito de un índice actual de intervalo de validez de clave y la extracción anteriormente descrita de una clave de servicio actual procedente de una OSK de servicio.

En particular, el nodo de emisión 5 puede ser, de manera conveniente, un ordenador, un portátil, una tableta, una estación de trabajo, un teléfono inteligente, un dispositivo de comunicaciones de satélite o un aparato de red, tal como un encaminador o una estación transceptora de base (BTS, *Base Transceiver Station*), correctamente configurados para llevar a cabo la sincronización anteriormente descrita de un tiempo local actual con una LASTER actual, el cálculo anteriormente descrito de un índice actual de intervalo de validez de clave y la extracción anteriormente descrita de una clave de servicio actual procedente de una OSK de servicio.

Además, las funciones puestas en práctica por el nodo de emisión 5 se pueden usar de forma ventajosa para asegurar los datos en relación con cualquier capa del modelo de interconexión de sistemas abiertos (OSI, *Open Systems Interconnection*).

Por último, las funciones puestas en práctica por el nodo de emisión 5 se pueden usar de forma ventajosa para proporcionar uno o más servicios de seguridad, tales como servicios de cifrado y / o de autenticación y / o de

integridad.

En lo que respecta al funcionamiento de los receptores, también los nodos de recepción usan su tiempo local sincronizado con una LASTER.

A diferencia de los emisores que usan una única clave para la transformación de seguridad de cabida útil en cada salto de clave, los receptores usan preferiblemente una ventana de clave con el fin de compensar las desviaciones de reloj y las demoras de propagación.

La ventana de clave, preferiblemente, comprende al menos tres claves extraídas de una OSK de servicio generada. En particular, la ventana de clave se desliza una posición en la OSK de servicio cada tiempo de permanencia de clave T.

En algunos escenarios, cuando la información de tiempo se entrega directamente en el flujo de datos, el receptor puede recuperar de los datos el tiempo del emisor eliminando de este modo la necesidad de una ventana de clave.

Resulta obvio que los emisores y receptores deberían usar la misma OSK de servicio con el fin de permitir que los receptores recuperen los datos de cabida útil de los datos de cabida útil asegurados recibidos.

Esto se obtiene mediante el uso de la misma función o funciones de generación de claves GenK y los mismos valores para la o las WOD de servicio y la semilla o semillas (de grupo) de servicios en la transmisión y en la recepción. Además el tiempo de permanencia de clave T y el tiempo inicial (de servicio de seguridad) t_0 son compartidos de manera conveniente por los nodos de comunicaciones para una correcta sincronización.

Suponiendo que k es un valor relacionado con el tamaño de ventana de clave, para el índice de intervalo de validez de clave n, la ventana de clave KW [n] preferiblemente comprende:

- algunas claves de servicio anteriores

$$K [n - i] = GenK ((n - i), WOD, semilla),$$

en la que i está comprendido en el rango [1, k];

- la clave de servicio actual

$$K [n] = GenK (n, WOD, semilla);$$

y

- algunas claves de servicio futuras

$$K [n + i] = GenK ((n + i), WOD, semilla)$$

en la que i está siempre comprendido en el rango [1, k].

Por lo tanto, la ventana de clave global para el intervalo de validez de clave n, KW [n], comprende 2k + 1 claves de servicio. Cada clave de servicio de una KW genérica se puede identificar de manera conveniente usando la siguiente notación: kw [n ; i], con i en el rango [- k, k].

Además, por razones de simplicidad de la descripción, la ventana de clave KW [n] se puede expresar de manera conveniente por medio de la fórmula siguiente:

$$kw [n ; i] = GenK ((n + i), WOD, semilla),$$

en la que i está comprendido en el rango [- k, k].

La figura 7 muestra un ejemplo de una ventana de clave que se está deslizando en una OSK de servicio. En particular, en el ejemplo que se muestra en la figura 7, la ventana de clave KW incluye tres claves de servicio, en concreto una clave de servicio anterior, una clave de servicio actual y una clave de servicio siguiente, de manera que el resultado es que el valor relacionado con el tamaño de ventana de clave k es uno, es decir, k = 1, y el índice i está comprendido en el rango [- 1, 1].

En detalle, tal como se muestra en la figura 7, en el intervalo de validez de clave n = 1, la ventana de clave incluye:

- la clave de servicio kw [1, -1] = K [0],
- la clave de servicio kw [1, 0] = K [1], y
- la clave de servicio kw [1, 1] = K [2];

en el intervalo de validez de clave n = 2, la ventana de clave incluye:

- la clave de servicio kw [2, -1] = K [1],
- la clave de servicio kw [2, 0] = K [2], y
- la clave de servicio kw [2, 1] = K [3];

en el intervalo de validez de clave n = 3, la ventana de clave incluye:

- la clave de servicio kw [3, -1] = K [2],
- la clave de servicio kw [3, 0] = K [3], y
- la clave de servicio kw [3, 1] = K [4];

y así sucesivamente.

La ventana de clave de recepción se actualiza sobre la base del tiempo local del nodo de recepción sincronizado con una LASTER. Este tiempo sincronizado se usa para recuperar el índice de intervalo de validez de clave n tal como se ha descrito en lo que antecede para el emisor.

La figura 8 ilustra de forma esquemática un ejemplo de una arquitectura funcional de un nodo de recepción diseñado para aplicar una correspondiente transformación inversa de seguridad de cabida útil a los datos de cabida útil asegurados recibidos del nodo de emisión 5 descrito en lo que antecede y que se muestra en la figura 5, por ejemplo para descifrar los datos de cabida útil cifrados y transmitidos por el nodo de emisión 5.

En particular, la figura 8 muestra un diagrama de bloques funcionales de un nodo de recepción 8 de acuerdo con la forma de realización preferida específica de la presente invención, nodo de recepción 8 que comprende:

- una fuente de LASTER 81 configurada para proporcionar una LASTER actual;
- una fuente de tiempo local 82 configurada para proporcionar un tiempo local actual;
- una unidad de sincronización 83 que está acoplada con la fuente de LASTER 81 y la fuente de tiempo local 82 para adquirir de las mismas, de forma respectiva, la LASTER actual y el tiempo local actual, y que está configurada para sincronizar el tiempo local actual con la LASTER actual con el fin de proporcionar un tiempo de sincronización actual;
- una unidad de cola de cabida útil 84 que está acoplada con la fuente de tiempo local 82 para adquirir de ella el tiempo local actual, y que está configurada para recibir datos asegurados (por ejemplo, cifrados) de cabida útil, llegados del nodo de emisión 5, y para proporcionar una referencia de tiempo de llegada sobre la base del tiempo local actual y de un tiempo en el cual se reciben del nodo de emisión 5 los datos de cabida útil asegurados;
- una unidad de cálculo de índices 85 que está acoplada con la unidad de sincronización 83 y la unidad de cola de cabida útil 84 para adquirir de las mismas, de forma respectiva, el tiempo de sincronización actual y la referencia de tiempo de llegada, y que está configurada para calcular un índice actual de intervalo de validez de clave n sobre la base del tiempo de sincronización actual, de la referencia de tiempo de llegada, del tiempo de permanencia de clave previamente definido T (compartido por el receptor 8 y el emisor 5) y del tiempo inicial t_0 (compartido por el receptor 8 y el emisor 5);
- una unidad de generación de ventana de clave 86 que está acoplada con la unidad de cálculo de índices 85 para adquirir de ella el índice actual de intervalo de validez de clave n, y que está configurada para generar una OSK de servicio sobre la base de la WOD de servicio y la semilla (de grupo) de servicios (compartida por el receptor 8 y el emisor 5) y para proporcionar una ventana de clave actual KW [n] sobre la base de la OSK de servicio generada, del índice actual de intervalo de validez de clave n y de un valor previamente definido relacionado con el tamaño de ventana k; y
- una unidad de transformación inversa de seguridad de cabida útil 87 que está acoplada con la unidad de cola de cabida útil 84 y la unidad de generación de ventana de clave 86 para adquirir de las mismas, de forma respectiva, los datos de cabida útil asegurados y la ventana de clave actual KW [n], y que está configurada para aplicar a dichos datos de cabida útil asegurados una transformación inversa de seguridad de cabida útil sobre la base de la ventana de clave actual KW [n] y del valor previamente definido relacionado con el tamaño de ventana k con el fin de recuperar y dar salida a los datos originales de cabida útil (por ejemplo, con el fin de descifrar los datos de cabida útil cifrados recibidos del emisor 5).

En detalle, algunos de los bloques funcionales del receptor 8 son iguales a los del emisor 5.

En concreto, la unidad de sincronización 83 funciona como la unidad de sincronización 53 del nodo de emisión 5.

La fuente de LASTER 81 del nodo de recepción 8, como la fuente de LASTER 51 del nodo de emisión 5, puede ser, de manera conveniente:

- un terminal de GNSS; o
- un receptor configurado para recibir las señales de radio relacionadas con el tiempo procedentes de una estación

de radio basada en reloj atómico; o
- un cliente del Protocolo de tiempo de red (NTP, *Network Time Protocol*); u
- otra fuente de tiempo global de la cual el nodo de recepción 8 puede adquirir una LASTER actual, por ejemplo el nodo de recepción 8 podría usar como una LASTER una referencia de tiempo que el mismo utilice para sincronizar las tramas.

De manera conveniente, las fuentes de LASTER 51 y 81 pueden ser un mismo tipo de fuente de LASTER, o la fuente de LASTER 81 puede ser diferente de la fuente de LASTER 51.

Preferiblemente, la fuente de tiempo local 82 es un reloj interno del nodo de recepción 8, reloj interno que está configurado para proporcionar un contador de tiempo de tic tac local.

Una de las diferencias entre el emisor 5 y el receptor 8 radica en la unidad de cola de cabida útil 84 que está configurada para mantener una referencia de tiempo interna del tiempo en el que se reciben los paquetes asegurados de cabida útil. Esta referencia de tiempo interna, que se denomina tal como se ha indicado en lo que antecede, referencia de tiempo de llegada, se proporciona a la unidad de cálculo de índices 85 con el fin de permitir que dicha unidad de cálculo de índices 85 calcule el correspondiente índice de intervalo de validez de clave n para los paquetes asegurados de cabida útil recibidos. La referencia de tiempo de llegada es obtenida por la unidad de cola de cabida útil 84 enclavando el contador de tiempo de tic tac local en el tiempo en el que se reciben los paquetes asegurados de cabida útil.

Además, otra diferencia entre el emisor 5 y el receptor 8 radica en la generación de claves. De hecho, la unidad de generación de ventana de clave 86 no genera una única clave para un índice de intervalo de validez de clave n como la unidad de generación de claves 56 sino que, en su lugar, genera, para cada índice de intervalo de validez de clave n, una respectiva ventana de clave total que comprende 2k + 1 respectivas claves de servicio.

Tal como se ha descrito en lo que antecede, la unidad de transformación inversa de seguridad de cabida útil 87 aplica a las tramas de datos que llegan la transformación inversa de seguridad de cabida útil sobre la base de las claves de servicio comprendidas en la ventana de clave actual KW [n] con el fin de obtener las tramas de datos originales de cabida útil y, de forma opcional, validar la integridad de los datos. Se descartan las tramas de datos de llegada que no se pueden descifrar de manera correcta.

En particular, la unidad de transformación inversa de seguridad de cabida útil 87 está preferiblemente configurada para llevar a cabo la transformación inversa de seguridad de cabida útil en una cantidad variable de etapas, en la que la máxima cantidad de etapas es igual a la cantidad de claves de servicio de la ventana de clave KW, es decir, es igual a 2k + 1.

A la llegada de una trama de datos, se calcula el valor del índice de intervalo de validez de clave n sobre la base del tiempo de sincronización actual, de la referencia de tiempo de llegada, del tiempo de permanencia de clave previamente definido T y del tiempo inicial t_0. Entonces se crea la ventana de clave actual KW [n] de dicha trama de datos, seleccionando las claves de servicio de la OSK.

En detalle, la ventana de clave actual KW [n] incluye 2k + 1 claves de servicio K [n + i], en la que i está comprendido en el rango [- k, k].

En cada etapa j de la transformación inversa de seguridad de cabida útil de una cabida útil asegurada actual proporcionada por la unidad de cola de cabida útil 84, la unidad de transformación inversa de seguridad de cabida útil 87 aplica una respectiva clave de servicio kw [n ; j] = K [n + j] de la ventana de clave actual KW [n] a dicha cabida útil asegurada actual de la siguiente manera:

- la cabida útil asegurada actual se transforma usando el algoritmo inverso del emisor 5 y la respectiva clave de servicio kw [n ; j] generando de este modo un respectivo candidato para la cabida útil válida; y
- dicha respectiva candidata se comprueba usando uno de los criterios descritos en detalle en lo que sigue y, si el proceso de comprobación tiene éxito, dicha respectiva candidata se elige como una cabida útil válida y se le da salida junto con el índice de etapa con éxito j (en la figura 8, dicho índice de etapa con éxito se representa mediante una salida m de la unidad de transformación inversa de seguridad de cabida útil 87).

Durante el uso, la unidad de transformación inversa de seguridad de cabida útil 87 aplica a la cabida útil asegurada actual las diferentes claves de servicio comprendidas en la ventana de clave actual KW [n] hasta que la cabida útil asegurada actual se transforma inversamente de manera correcta o se han aplicado todas las claves de servicio de la ventana de clave actual KW [n].

Cuando la ventana de clave KW está terminada, se descarta la cabida útil asegurada actual; de lo contrario se identifica un índice de etapa con éxito m.

Es importante resaltar el hecho de que la unidad de transformación de seguridad de cabida útil 57 del emisor 5 y la unidad de transformación inversa de seguridad de cabida útil 87 del receptor 8 manejan, de forma respectiva, la transformación de seguridad de cabida útil y la transformación inversa de seguridad de cabida útil en relación con el servicio de seguridad específico a proporcionar, por ejemplo, el cifrado / descifrado de datos de cabida útil. En conexión con lo anterior, es importante hacer notar que la unidad de transformación de seguridad de cabida útil 57 del emisor 5 y la unidad de transformación inversa de seguridad de cabida útil 87 del receptor 8 pueden funcionar de modo diferente en los diferentes escenarios de aplicación, es decir, la transformación de seguridad de cabida útil y la transformación inversa de seguridad de cabida útil pueden diferir según el servicio de seguridad específico a proporcionar.

En lo que respecta a la comprobación de candidatas de cabida útil válidas, con el fin de aplicar de manera correcta una transformación de seguridad de cabida útil del lado del emisor y la correspondiente transformación inversa de seguridad de cabida útil del lado del receptor, se puede introducir de manera conveniente alguna información en las cabidas útiles intercambiadas con el fin de permitir que el receptor 8 comprenda si la transformación inversa de seguridad de cabida útil aplicada sobre la base de una de las claves de servicio de la ventana de clave actual KW [n] da el resultado correcto, es decir, si la cabida útil asegurada actual se transforma inversamente de modo correcto sobre la base de una de las claves de servicio de la ventana de clave actual KW [n].

En particular, la información introducida en las cabidas útiles intercambiadas permite que la unidad de transformación inversa de seguridad de cabida útil 87 comprenda de manera correcta cuál de las claves de servicio de la ventana de clave actual KW [n] posibilita una correcta recuperación de la cabida útil original después de aplicar la transformación inversa de seguridad de cabida útil, es decir, permite que la unidad de transformación inversa de seguridad de cabida útil 87 compruebe y detecte cuál de las candidatas de cabida útil válidas (cada una de las cuales, tal como se ha descrito en lo que antecede, se obtiene aplicando a la cabida útil asegurada actual la transformación inversa de seguridad de cabida útil sobre la base de una respectiva clave de servicio de la ventana de clave actual KW [n]) es la cabida útil válida real.

El uso de la información introducida en las cabidas útiles intercambiadas se debe, de forma inherente, al hecho de que no hay intercambio alguno de claves entre el emisor 5 y el receptor 8.

La decisión acerca de la clave correcta, es decir, acerca de la cabida útil válida real que no es segura, en el lado del receptor, se toma solo cuando se reciben los datos del emisor 5. De hecho, el receptor 8 no puede comprender qué clave de servicio de la OSK de servicio es utilizada por el emisor 5 cuando no se recibe dato alguno procedente del emisor 5 por parte del receptor 8.

En detalle, la información para permitir que la unidad de transformación inversa de seguridad de cabida útil 87 detecte la real cabida útil válida se puede transmitir en las cabidas útiles intercambiadas usando diferentes enfoques:

- cuando las cabidas útiles ya tienen un encabezado conocido, ese encabezado se puede comprobar del lado del receptor como una información conocida;
- cuando las cabidas útiles ya tienen un patrón de secuenciación, ese patrón se podría usar para recuperar de inmediato la clave de servicio que es usada por el emisor 5; y
- la nueva información se puede añadir en el lado del emisor, estando dividida dicha nueva información en dos subclases, en concreto:

    - la nueva información se usa para suministrar algunos otros servicios de seguridad, tales como los servicios de autenticación; o
    - la nueva información contiene un patrón variable que ayuda al receptor 8 a recuperar de inmediato la clave de servicio que es usada por el emisor 5.

Preferiblemente, la ventana de clave KW se explora de manera secuencial. En particular, la ventana de clave actual KW [n] se explora preferiblemente aplicando en cada etapa j de la transformación inversa de seguridad de cabida útil la respectiva clave de servicio kw [n ; j] = K [n + j] de dicha ventana de clave actual KW [n] y cambiando el valor del índice j del siguiente modo:

$$j = 0, +1, -1, +2, -2, \ldots, +(k - 1), -(k - 1), +k, -k.$$

Cuando la transformación inversa de seguridad de cabida útil tiene éxito, el valor inicial del índice j usado para las transformaciones inversas de seguridad de cabida útil de los paquetes de cabida útil subsiguientes, recibidos de la misma fuente, se pueden modificar de manera conveniente con el fin de compensar la desviación de las demoras de propagación. Por ejemplo, el valor inicial del índice j usado para las transformaciones inversas de seguridad de cabida útil de paquetes de cabida útil subsiguientes, recibidos de la misma fuente, se puede modificar de manera conveniente sobre la base el valor del índice j que se corresponde con la última etapa con éxito de transformación inversa de seguridad de cabida útil. Esta potenciación se puede aplicar de manera conveniente con el fin de reducir las etapas necesarias de transformación inversa de seguridad de cabida útil para los datos recibidos de la misma

fuente de emisión.

Además, el receptor puede crear de manera conveniente un contexto de recepción para cada emisor que contenga la respectiva información en relación con una respectiva demora estimada entre los nodos de comunicaciones, un respectivo tamaño de la ventana de clave KW y, por ejemplo, también un respectivo estado del contexto. El contexto se puede usar para acelerar el proceso de transformación inversa de seguridad de cabida útil.

En particular, se pueden prever de manera conveniente dos diferentes estados para el contexto de recepción, en concreto:

- un estado de búsqueda; y
- un estado de seguimiento.

En el estado de búsqueda, el receptor utiliza una extensa ventana de clave (seleccionando un valor grande para k) con el fin de compensar y evaluar las grandes demoras de propagación. Cuando se halla una coincidencia, es decir, cuando tiene éxito la transformación inversa de seguridad de cabida útil de un paquete de cabida útil recibido, el sistema pasa al estado de seguimiento, en el que se reduce a tres elementos el tamaño de ventana de clave (es decir, k = 1) con el fin de compensar solo las desviaciones de reloj de transmisor / receptor.

El contexto de recepción puede volver de manera segura al estado de búsqueda cuando no se recibe dato alguno del emisor durante un tiempo prolongado o puede usar estados intermedios entre los estados de búsqueda y de seguimiento, reduciendo el tamaño de la ventana de clave cuando se obtiene una correcta estimación de la demora y la fluctuación.

Además, los nodos de recepción que no tienen una LASTER pueden usar el índice de etapa con éxito m para compensar sus desviaciones de reloj suponiendo que el emisor tiene una buena referencia de tiempo y se conoce la demora de propagación entre el emisor y el receptor.

Es importante resaltar el hecho de que la forma de realización preferida específica anteriormente descrita de la presente invención se puede poner en práctica mediante una arquitectura diferente de la del nodo de recepción 8 descrito en lo que antecede y que se muestra en la figura 8, siempre que dicha arquitectura diferente esté configurada para llevar a cabo la sincronización anteriormente descrita de un tiempo local actual con una LASTER actual, el cálculo anteriormente descrito de un índice actual de intervalo de validez de clave y la generación anteriormente descrita de una ventana de clave actual y su uso para transformar inversamente los datos asegurados.

Dicho de otra forma, el nodo de recepción 8 puede ser cualquier dispositivo / aparato de comunicaciones configurado para llevar a cabo la sincronización anteriormente descrita de un tiempo local actual con una LASTER actual, el cálculo anteriormente descrito de un índice actual de intervalo de validez de clave y la generación anteriormente descrita de una ventana de clave actual y su uso para transformar inversamente los datos asegurados.

En particular, el nodo de recepción 8 puede ser, de manera conveniente, un ordenador, un portátil, una tableta, una estación de trabajo, un teléfono inteligente, un dispositivo de comunicaciones de satélite o un aparato de red, tal como un encaminador o una estación transceptora de base (BTS, *Base Transceiver Station*), correctamente configurados para llevar a cabo la sincronización anteriormente descrita de un tiempo local actual con una LASTER actual, el cálculo anteriormente descrito de un índice actual de intervalo de validez de clave, y la generación anteriormente descrita de una ventana de clave actual y su uso para transformar inversamente los datos asegurados.

Además, las funciones puestas en práctica por el nodo de recepción 8 se pueden usar de manera ventajosa en cualquier capa del modelo de OSI.

Por último, las funciones puestas en práctica por el nodo de recepción 8 se pueden usar de forma ventajosa para proporcionar uno o más servicios de seguridad, tales como el servicio o servicios de cifrado y / o de autenticación y / o de integridad.

A partir de lo anterior, se puede apreciar de inmediato que la presente invención permite evitar el riesgo de que las claves simétricas sean captadas de manera furtiva; de acuerdo con la presente invención, ningún mensaje es intercambiado por los nodos de comunicaciones con el fin de llegar a un acuerdo acerca de la clave a usar.

Además, la presente invención puede ser usada de manera conveniente por uno o más emisores y uno o más receptores y, por lo tanto, aprovecharse de forma ventajosa, en escenarios tanto de unidifusión como de multidifusión, y usarse de forma ventajosa, tal como se ha explicado en lo que antecede, en cualquier capa del modelo de OSI y / o para diferentes servicios de seguridad.

Además, la presente invención, mediante el uso de la ventana de clave en la recepción, permite compensar la demora o demoras de propagación y la fluctuación o fluctuaciones de red que, en ciertos escenarios, tales como las comunicaciones de satélite, pueden ser muy grandes.

Por último, resulta evidente que en la presente invención se pueden realizar numerosas modificaciones y variantes, todas las cuales caen dentro del alcance de la invención, tal como se define en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Método para asegurar / desasegurar datos intercambiados por nodos de comunicaciones, comprendiendo el método:

- generar, por un primer nodo de comunicaciones (5) y por uno o más segundo(s) nodo(s) de comunicaciones (8), una y la misma secuencia ordenada de claves de seguridad, cada una de las cuales se va a usar en un intervalo de tiempo de validez respectivo;
- sincronizar, por cada uno del primer y el segundo nodos de comunicaciones (5, 8), una referencia de tiempo interna respectiva con una referencia de tiempo global, obteniendo de ese modo una referencia de tiempo de sincronización respectiva;
- extraer, por el primer nodo de comunicaciones (5), una clave de seguridad de dicha una y la misma secuencia ordenada de claves de seguridad sobre la base de la referencia de tiempo de sincronización respectiva;
- asegurar, por el primer nodo de comunicaciones (5), datos a enviar al / los segundo(s) nodo(s) de comunicaciones (8) sobre la base de la clave de seguridad extraída;
- extraer, por cada segundo nodo de comunicaciones (8), un grupo ordenado respectivo de claves de seguridad de dicha una y la misma secuencia ordenada de claves de seguridad sobre la base de la referencia de tiempo de sincronización respectiva; y
- desasegurar, por cada segundo nodo de comunicaciones (8), los datos asegurados recibidos del primer nodo de comunicaciones (5) sobre la base del grupo ordenado respectivo de claves de seguridad extraídas;

estando el método **caracterizado por que** cada segundo nodo de comunicaciones (8):

- intenta desasegurar los datos asegurados recibidos del primer nodo de comunicaciones (5) al
  - seguir una secuencia dada respectiva de intentos de desasegurar, cada uno de los cuales está basado en una correspondiente clave de seguridad que está incluida en el grupo ordenado respectivo de claves de seguridad extraídas, y
  - comenzar con un intento de desasegurar sobre la base de una clave de seguridad que se encuentra en una posición inicial respectiva en el grupo ordenado respectivo de claves de seguridad extraídas;
- modifica la posición inicial respectiva con el fin de compensar una demora de propagación respectiva estimada para datos asegurados previos que son enviados por el primer nodo de comunicaciones (5) y que son recibidos por dicho segundo nodo de comunicaciones (8); y
- determina, sobre la base de dicha demora de propagación respectiva, un número respectivo de claves de seguridad a incluir en el grupo ordenado respectivo de claves de seguridad a extraer.

2. El método de la reivindicación 1, en el que:

- el primer nodo de comunicaciones (5) extrae la clave de seguridad de dicha una y la misma secuencia ordenada de claves de seguridad también sobre la base de un tiempo inicial dado y una duración dada de los intervalos de tiempo de validez; y
- cada segundo nodo de comunicaciones (8) extrae el grupo ordenado respectivo de claves de seguridad de dicha una y la misma secuencia ordenada de claves de seguridad también sobre la base de dicho tiempo inicial dado y dicha duración dada de los intervalos de tiempo de validez.

3. El método de la reivindicación 2, que comprende adicionalmente intercambiar, entre el primer nodo de comunicaciones (5) y cada segundo nodo de comunicaciones (8), dicho tiempo inicial dado y dicha duración dada de los intervalos de tiempo de validez.

4. El método de acuerdo con cualquier reivindicación precedente, en el que el primer nodo de comunicaciones (5) extrae la clave de seguridad de dicha una y la misma secuencia ordenada de claves de seguridad sobre la base de la referencia de tiempo interna respectiva enclavada en un instante en el que se encuentran disponibles los datos a enviar al / los segundo(s) nodo(s) de comunicaciones (8).

5. El método de acuerdo con cualquier reivindicación precedente, en el que cada segundo nodo de comunicaciones (8) extrae el grupo ordenado respectivo de claves de seguridad de dicha una y la misma secuencia ordenada de claves de seguridad sobre la base de la referencia de tiempo interna respectiva enclavada en un instante respectivo en el que los datos asegurados se reciben del primer nodo de comunicaciones (5).

6. El método de acuerdo con cualquier reivindicación precedente, en el que cada segundo nodo de comunicaciones (8) determina la posición inicial respectiva sobre la base de una posición de una clave de seguridad que:

- se incluyó en un grupo ordenado respectivo de claves de seguridad previamente extraídas de dicha una y la misma secuencia ordenada de claves de seguridad; y
- dio lugar a que datos asegurados previamente recibidos del primer nodo de comunicaciones (5) se

desaseguraran con éxito.

7. El método de acuerdo con cualquier reivindicación precedente, que comprende adicionalmente adquirir, por cada uno del primer y el segundo nodos de comunicaciones (5, 8), la referencia de tiempo global de una fuente de tiempo global respectiva que está comprendida en el conjunto que consiste en: un terminal de Sistema Global de Navegación por Satélite, un receptor configurado para recibir señales de radio relacionadas con el tiempo de una estación de radio basada en reloj atómico, y un cliente de Protocolo de Tiempo de Red (NTP).

8. El método de acuerdo con cualquier reivindicación precedente, en el que dicha una y la misma secuencia ordenada de claves de seguridad es generada por el primer y el segundo nodos de comunicaciones (5, 8) sobre la base de una y la misma palabra del día dada y una y la misma semilla dada.

9. El método de la reivindicación 8, que comprende adicionalmente intercambiar, entre el primer nodo de comunicaciones (5) y cada segundo nodo de comunicaciones (8), dicha una y la misma palabra del día dada y / o dicha una y la misma semilla dada.

10. El método de acuerdo con cualquier reivindicación precedente, en el que dicha una y la misma secuencia ordenada de claves de seguridad es generada por el primer y el segundo nodos de comunicaciones (5, 8) al aplicar, a una y la misma secuencia ordenada de números aleatorios, una y la misma transformación de seguridad sobre la base de una y la misma palabra del día dada.

11. El método de la reivindicación 10, en el que dicha una y la misma transformación de seguridad es puesta en práctica por el primer y el segundo nodos de comunicaciones (5, 8) en un modo de encadenamiento de bloques de cifrado.

12. El método de acuerdo con la reivindicación 10 u 11, en el que el primer y el segundo nodos de comunicaciones (5, 8) o bien generan dicha una y la misma secuencia ordenada de números aleatorios al funcionar como generadores de números pseudo aleatorios sobre la base de una y la misma semilla dada, o bien recuperan dicha una y la misma secuencia ordenada de números aleatorios de secuencias ordenadas almacenadas de números aleatorios.

13. Aparato de comunicaciones (5, 8) configurado para llevar a cabo el método que se reivindica en cualquier reivindicación precedente.

14. Producto de programa de soporte lógico que comprende porciones de código de soporte lógico que son:

- almacenables en, y ejecutables por, un aparato de comunicaciones; y
- tales que dan lugar, cuando están almacenadas, a que dicho aparato de comunicaciones quede configurado para llevar a cabo el método que se reivindica en cualquiera de las reivindicaciones 1 - 12.

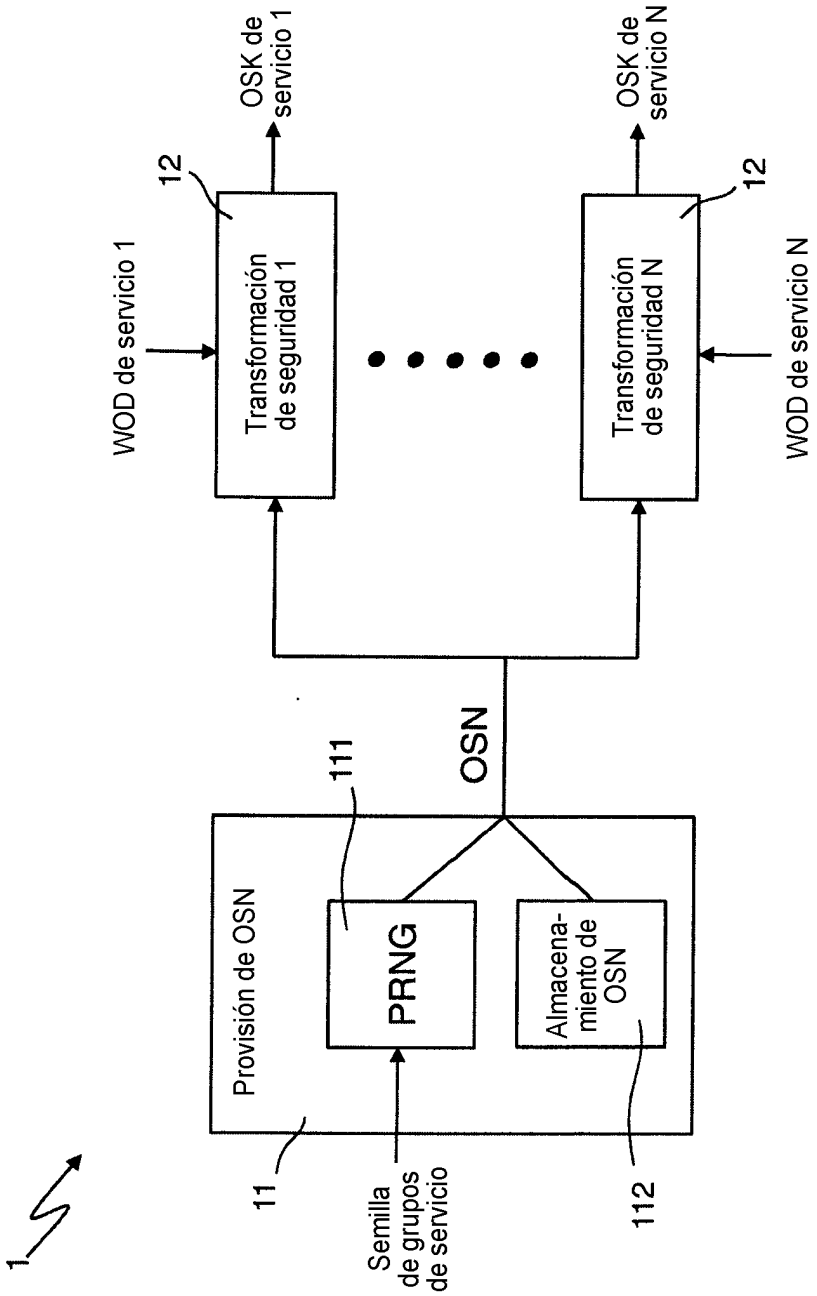
1
11
Provisión de OSN
111
PRNG
Semilla de grupos de servicio
Almacena-miento de OSN
112
OSN
12
Transformación de seguridad 1
WOD de servicio 1
OSK de servicio 1
12
Transformación de seguridad N
WOD de servicio N
OSK de servicio N

Fig. 1

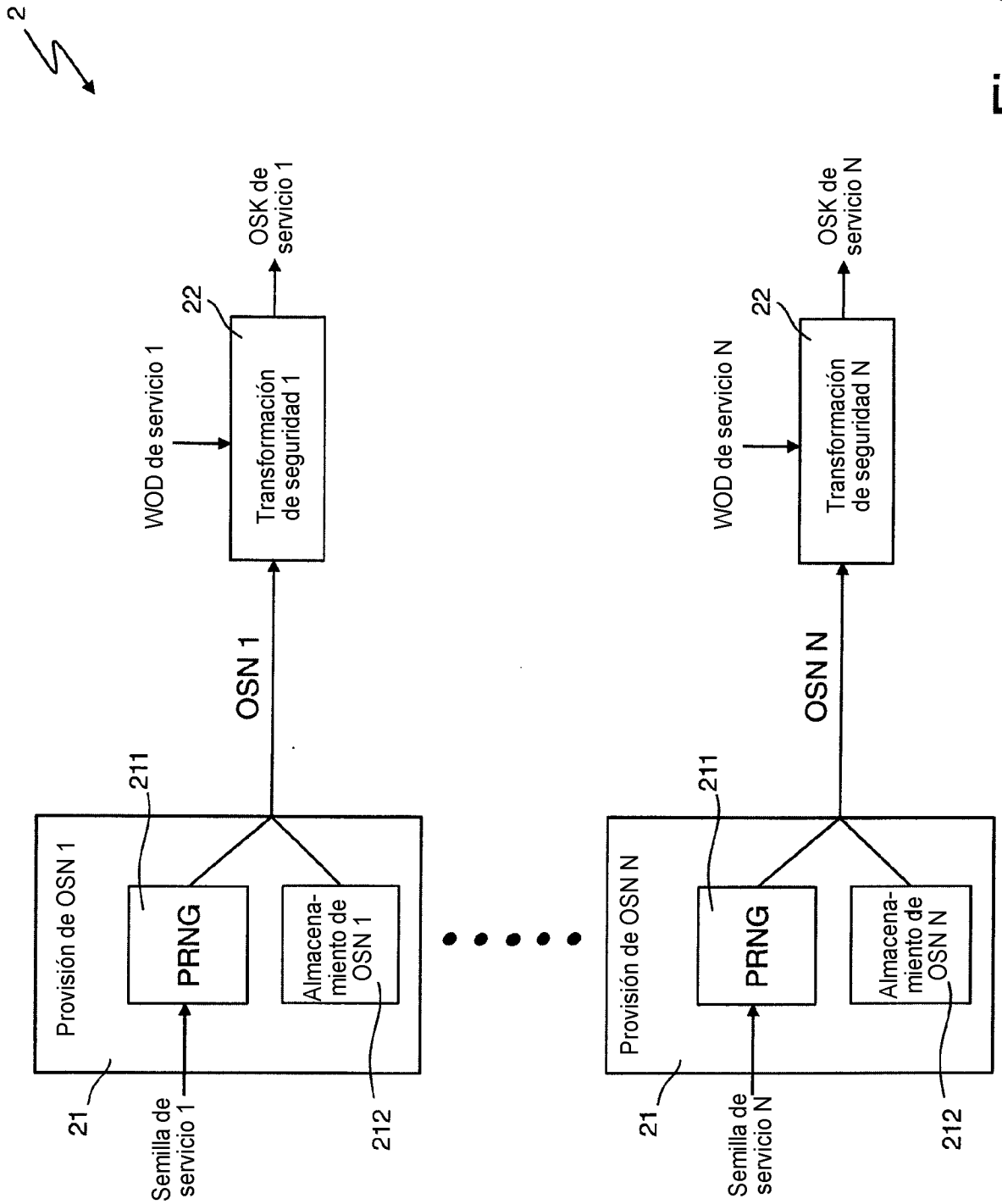
2
Provisión de OSN 1
211
PRNG
Almacena-miento de OSN 1
OSN 1
Transformación de seguridad 1
22
WOD de servicio 1
OSK de servicio 1
21
Semilla de servicio 1
212
Provisión de OSN N
211
PRNG
Almacena-miento de OSN N
OSN N
Transformación de seguridad N
22
WOD de servicio N
OSK de servicio N
21
Semilla de servicio N
212

Fig. 2

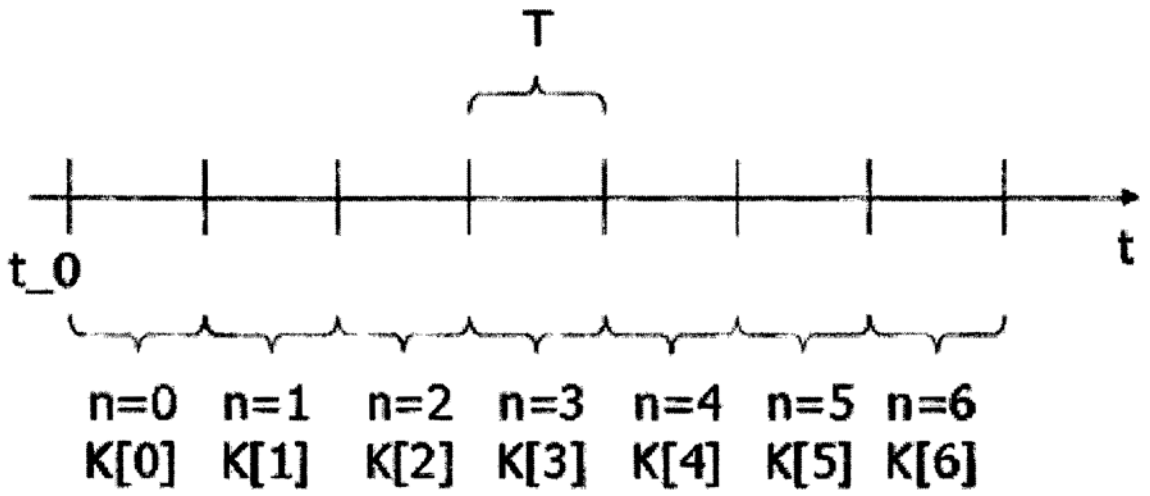
T
t_0
t
n=0 n=1 n=2 n=3 n=4 n=5 n=6
K[0] K[1] K[2] K[3] K[4] K[5] K[6]

Fig. 3

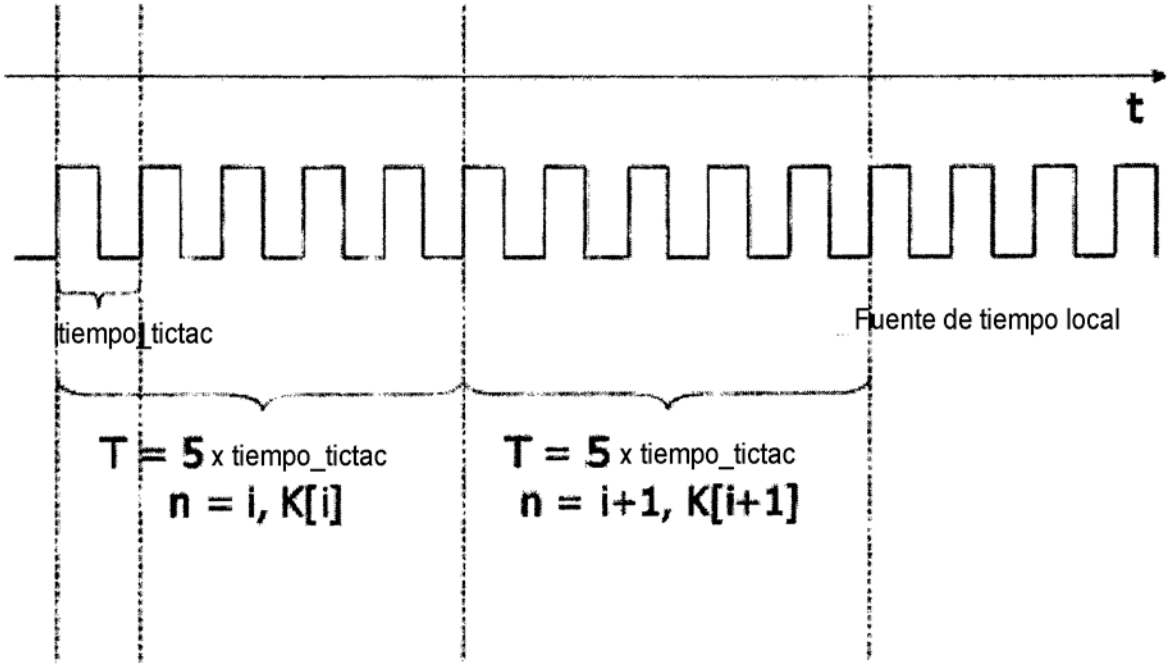
t
tiempo_tictac
Fuente de tiempo local
T = 5 x tiempo_tictac
n = i, K[i]
T = 5 x tiempo_tictac
n = i+1, K[i+1]

Fig. 4

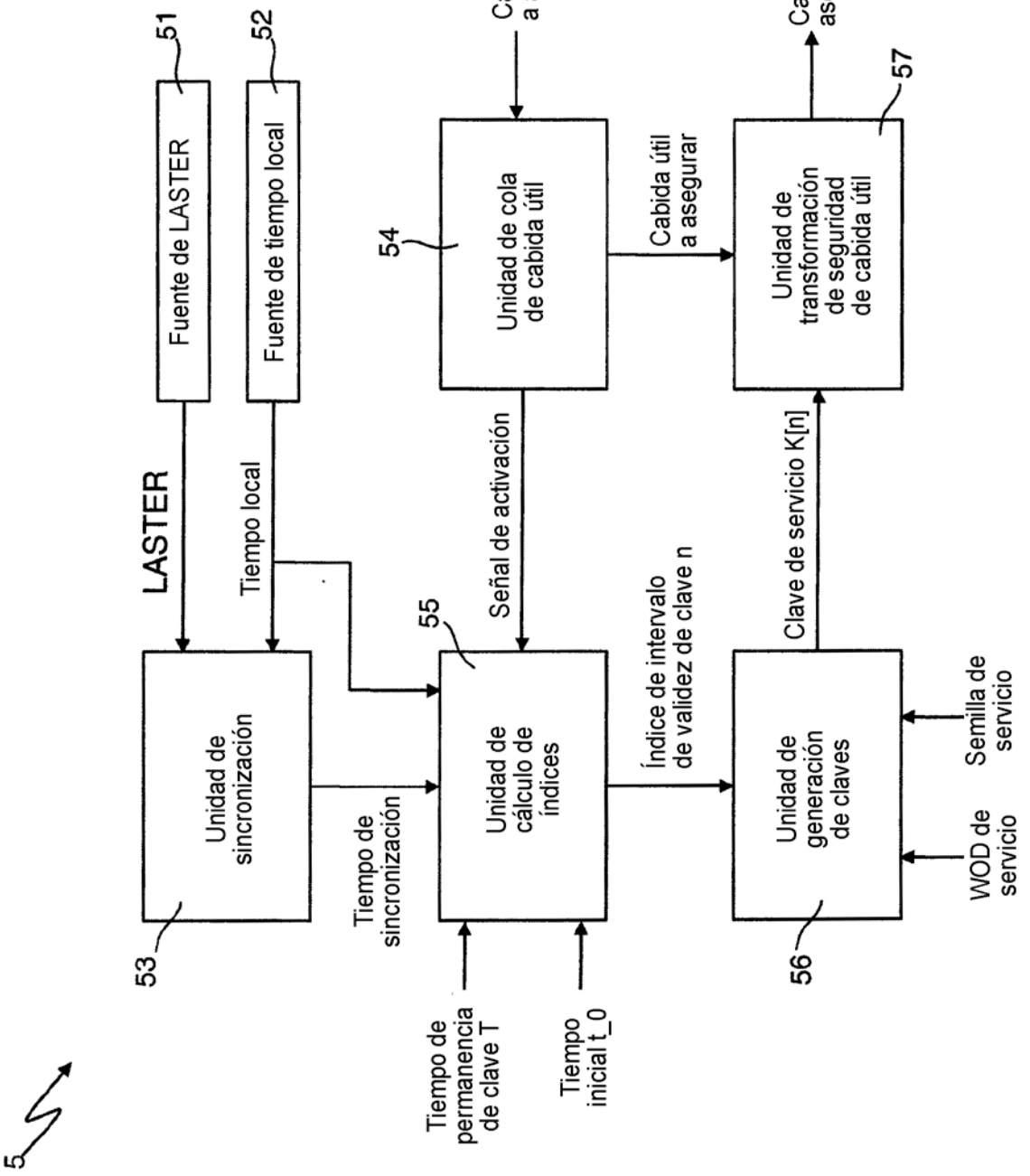
5
LASTER
Fuente de LASTER
51
Fuente de tiempo local
52
Unidad de sincronización
53
Unidad de cola de cabida útil
54
Unidad de cálculo de índices
55
Unidad de generación de claves
56
Unidad de transformación de seguridad de cabida útil
57
Cabida útil a asegurar
Cabida útil asegurada
Tiempo local
Señal de activación
Tiempo de sincronización
Índice de intervalo de validez de clave n
Clave de servicio K[n]
Tiempo de permanencia de clave T
Tiempo inicial t_0
Semilla de servicio
WOD de servicio

Fig. 5

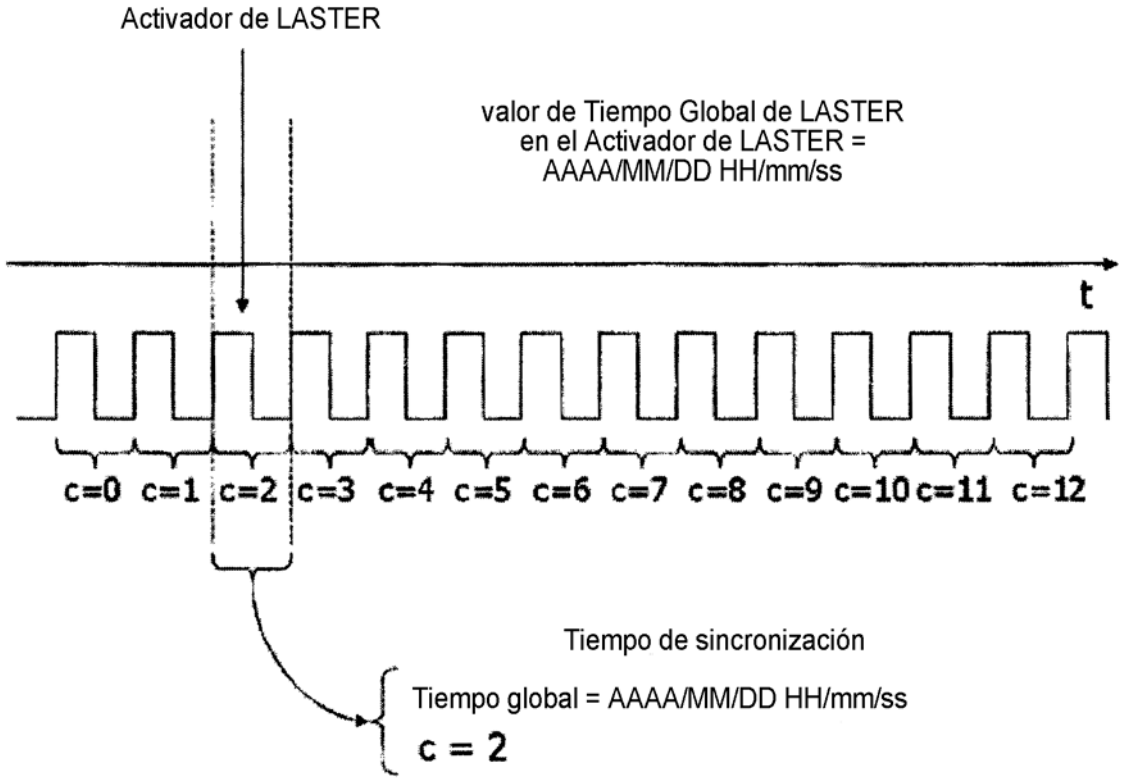
Activador de LASTER
valor de Tiempo Global de LASTER
en el Activador de LASTER =
AAAA/MM/DD HH/mm/ss
t
c=0 c=1 c=2 c=3 c=4 c=5 c=6 c=7 c=8 c=9 c=10 c=11 c=12
Tiempo de sincronización
Tiempo global = AAAA/MM/DD HH/mm/ss
c = 2

Fig. 6

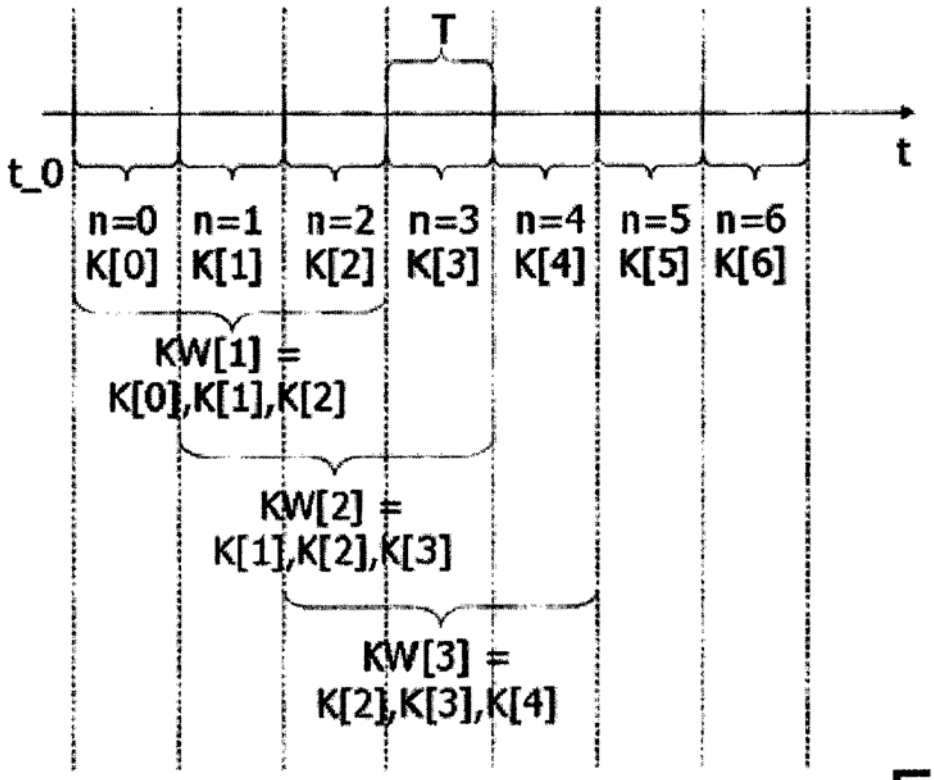
T
t
t_0
n=0 K[0]
n=1 K[1]
n=2 K[2]
n=3 K[3]
n=4 K[4]
n=5 K[5]
n=6 K[6]
KW[1] = K[0],K[1],K[2]
KW[2] = K[1],K[2],K[3]
KW[3] = K[2],K[3],K[4]

Fig. 7

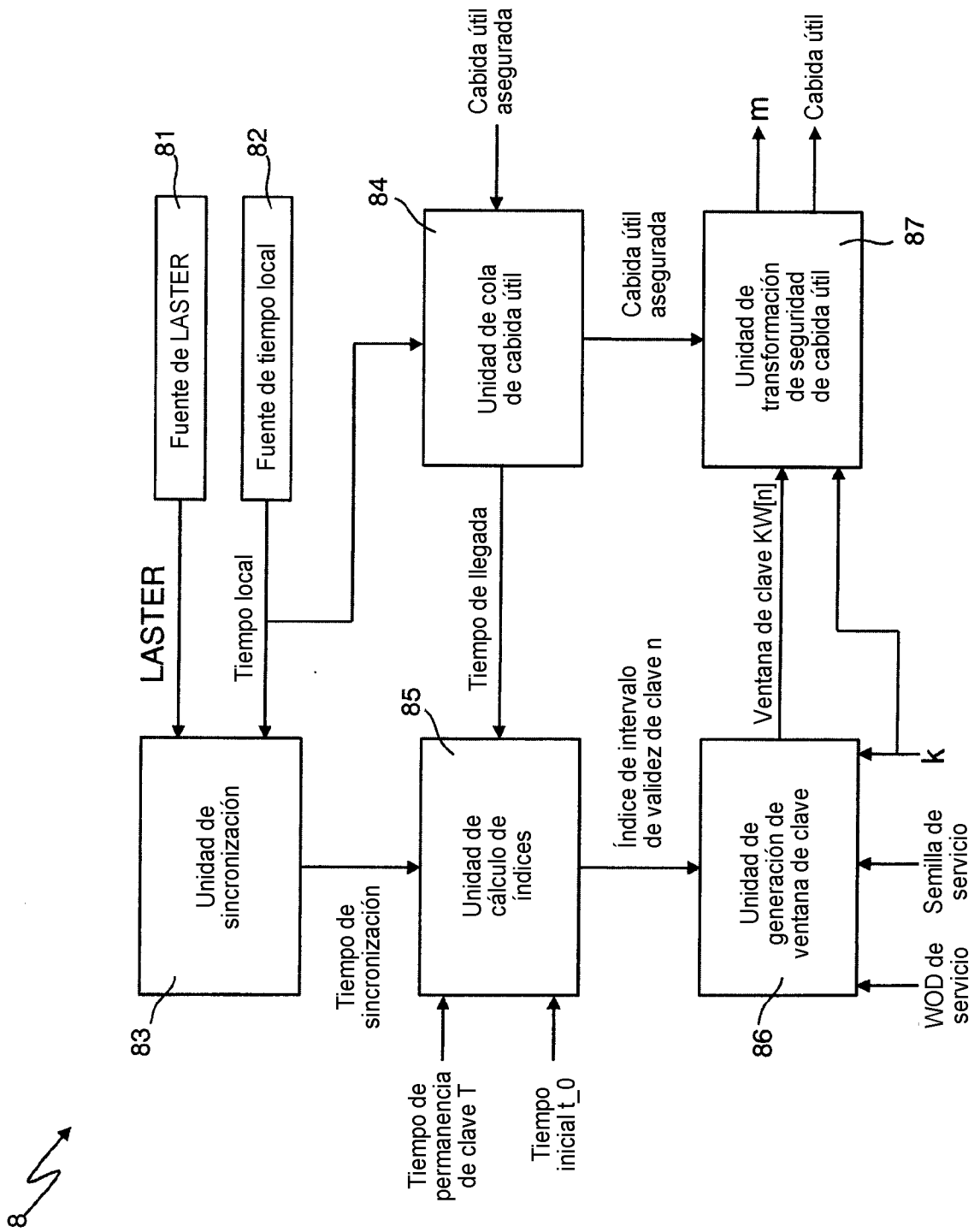
8
81
Fuente de LASTER
82
Fuente de tiempo local
LASTER
Tiempo local
83
Unidad de sincronización
Tiempo de sincronización
84
Cabida útil asegurada
Unidad de cola de cabida útil
Tiempo de llegada
85
Unidad de cálculo de índices
Tiempo de permanencia de clave T
Tiempo inicial t_0
Índice de intervalo de validez de clave n
Cabida útil asegurada
Unidad de transformación de seguridad de cabida útil
m
Cabida útil
87
Ventana de clave KW[n]
Unidad de generación de ventana de clave
86
k
Semilla de servicio
WOD de servicio

Fig. 8