(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 687 275**

(51) Int. CI.:

G01S 19/21 (2010.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **23.03.2015 PCT/EP2015/056120**

(87) Fecha y número de publicación internacional: **15.10.2015 WO15154981**

(96) Fecha de presentación y número de la solicitud europea: **23.03.2015 E 15712859 (6)**

(97) Fecha y número de publicación de la concesión europea: **01.08.2018 EP 3129806**

(54) Título: **Método y sistema para optimizar la autenticación de señales de radionavegación**

(30) Prioridad:

08.04.2014 EP 14163902

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.10.2018

(73) Titular/es:

THE EUROPEAN UNION, REPRESENTED BY THE EUROPEAN COMMISSION (100.0%)
1049 Brussels, BE

(72) Inventor/es:

FERNANDEZ HERNANDEZ, IGNACIO

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método y sistema para optimizar la autenticación de señales de radionavegación

Campo técnico

La presente invención se refiere a la autenticación de señales de radionavegación por satélite, y más particularmente a un método y un sistema para autenticar datos y señales de navegación por satélite, optimizados para entornos con condiciones de recepción difíciles.

Antecedentes de la técnica

Mediante el uso de sistemas tales como GPS, la navegación por satélite se ha convertido en un elemento crítico de la sociedad y la economía. Sin embargo, a pesar de su alta importancia, las señales civiles de los Sistemas de satélites de navegación global (GNSS) son muy fáciles de falsear. Se transmiten y reciben a potencia muy baja (alrededor de -160 dBW, o 10^{-16} vatios), lo que significa que un dispositivo que transmita señales falsas a baja potencia puede hacerse con el control de un receptor GNSS. En la actualidad, las señales GNSS civiles no proporcionan ningún medio para determinar su autenticidad a fin de impedir tales ataques, aunque se considera que tal característica se puede implementar en algún GNSS en el futuro. Sin embargo, se han propuesto algunas medidas de autenticación de señales y datos GNSS, como se describirá en lo que sigue.

El término “autenticación”, en el dominio de la navegación por satélite, hace referencia, en general, a la autenticidad de una posición calculada a partir de señales de satélite para navegación. A fin de autenticar una posición, tiene que asegurarse la autenticidad de las señales utilizadas en el cálculo de posiciones y, además de esto, el receptor debe asegurar que no se ha falseado el proceso interno para calcular esta posición. Como se usa en la presente memoria, “autenticación” significa principalmente autenticación de señales. Los dos elementos de información principales que un receptor extrae de las señales GNSS son la información de posición y tiempo del satélite (contenidas en el mensaje de navegación) y la señal tiempo de llegada (que se obtiene, en la mayoría de receptores, por mediciones de fase de códigos). Por lo tanto, la autenticación de señales de radionavegación hace referencia a la confirmación de la autenticidad y la integridad de los datos transmitidos desde el satélite, y la autenticación de la señal tiempo de llegada (TOA) medida por el receptor.

Del mismo modo que las señales de Acceso múltiple por división de código (CDMA) de Espectro ensanchado de secuencia directa (DSSS), las señales GNSS contienen un flujo de bits de datos modulado sobre un código de ensanchamiento que dispersa la potencia de señal a través de un cierto ancho de banda, y que se usa también para el cálculo del tiempo de llegada. Las medidas de autenticación se dividen en las relacionadas con códigos de ensanchamiento y las relacionadas con datos de navegación, denominadas también autenticación de mensajes de navegación (NMA).

Los elementos de la presente invención están basados en aspectos del protocolo TESLA (Autenticación tolerante a pérdidas de flujos eficientes temporizados) para la autenticación de mensajes de radionavegación.

A. Perrig et al.: "Timed Efficient Stream LossTolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction”, (2005, Universidad de Carnegie Mellon, Network Working Group), presenta el concepto de TESLA como un método para permitir que un receptor de información de multidifusión o emisión desde un remitente verifique la integridad y autentique la información. TESLA usa criptografía simétrica, y descripción de claves de retardo temporal para conseguir la propiedad de asimetría y minimizar por lo tanto las tareas de gestión de claves. La publicación hace referencia específicamente al uso de TESLA en la autenticación de paquetes de datos en el contexto de las comunicaciones de red. No hace referencia a su aplicación en radiolocalización o radionavegación, o a comunicaciones vía satélite. Los autores no proponen el uso del protocolo TESLA en radionavegación y no analizan su disponibilidad bajo canales de transmisión con desvanecimiento y sombreado.

Sherman C. Lo, et al.: "Assessing the Security of a Navigation System: A Case Study using Enhanced Loran", Universidad de Stanford, describe una versión adaptada de TESLA para canales de navegación en Loran mejorada, por ejemplo en los que se usa una clave dada para varios MAC. La autenticación se describe con relación a la criptografía de claves, así como otras técnicas para mejorar la seguridad de Loran. La técnica de autenticación de datos TESLA se describe en una sección, y es la técnica conocida que se ha descrito con anterioridad. Los autores establecen una adaptación de TESLA para canales de navegación, a fin de hacerla más adecuada para Loran. Se indica que para una modificación ser más tolerante a la pérdida de mensajes de una manera eficiente a los datos es usar una clave dada para varios MAC.

C Wullems et al.: "Signal Authentication and Integrity Schemes for Next Generation Global Navigation Satellite Systems", Proceedings of the European Navigation Conference GNSS, 22 de julio de 2005 (22-07-2005), páginas 1-11, XP055141309, Múnich, describe técnicas para la autenticación con base NMA de señales GNSS basándose en TESLA. Un transmisor genera una cadena de claves mediante una función *hash* F. Se realiza la autenticación, para el intervalo temporal actual, determinando si existe una coincidencia entre (i) un MAC (MAC'_{n+2}) derivado de los MAC obtenidos de un primer tipo (datos) de mensaje durante un intervalo temporal previo y una clave (K'_{n+2}) obtenida aplicando una función de generación F’ de claves seguras a una clave (K_{n+2}) obtenida de un segundo tipo de

mensaje durante el intervalo temporal actual, y (ii) un MAC (MAC'_{n+2}) obtenido del segundo tipo de mensaje durante el intervalo temporal previo.

Los sistemas conocidos que hacen uso de TESLA para la autenticación de señales de radionavegación están basados en las siguientes etapas:

- la generación para cada transmisor i, a partir de una semilla aleatoria inicial $K_{i,n}$, de una cadena de claves $K_{i,n}$ a $K_{i,0}$ generadas de modo recursivo a través de una función unidireccional, y el uso de dicha cadena unidireccional en orden inverso ($K_{i,0}$ a $K_{i,n}$), por el que, en un cierto intervalo temporal j, un transmisor i del sistema de radionavegación autentica sus datos emitidos con un código de autenticación de mensajes ($MAC_{i,j}$) que usa dicha clave $K_{i,j}$ a partir de dicha cadena unidireccional;
- la transmisión, por cada transmisor i, de los datos para autenticar, junto con dicho MAC y, después de un cierto período de tiempo, dicha clave $K_{i,j}$;
- la recepción, por el receptor desde cada transmisor, de los datos de transmisor, el $MAC_{i,j}$ y la clave $K_{i,j}$;
- la verificación, por el receptor, de la autenticidad de los datos de satélite por la generación del $MAC_{i,j}$, con los propios datos y $K_{i,j}$, y la comparación con el $MAC_{i,j}$ recibido desde el satélite i;
- la verificación por el receptor, para cada una de las señales desde cada transmisor i citado, de la autenticidad de $K_{i,j}$ al realizar la función unidireccional de modo recursivo para generar una clave previa de la cadena, por ejemplo $K_{i,0}$, que se certifica como auténtica a partir de un certificado recibido previamente.

Por lo tanto, los usos conocidos de los protocolos TESLA para radionavegación siguen un planteamiento por el que cada señal desde cada transmisor se autentica independientemente, y un problema es que todos los datos requeridos para el proceso de autenticación tienen que recibirse desde el transmisor cuyos datos se han de autenticar.

Un problema adicional con los sistemas usuales es que no proporcionan la posibilidad de usar óptimamente los datos desde un satélite para autenticar otros satélites y minimizar el número total de bits requeridos para la autenticación de varios satélites. Tampoco proporcionan la posibilidad de usar los datos desde satélites con condiciones de recepción potencialmente mejores para autenticar otros satélites.

Estos factores representan un problema principal para algunos sistemas de radionavegación, tales como los basados en navegación por satélite, donde las condiciones de recepción pueden degradarse, en general, y pueden variar significativamente para satélites diferentes debido a las obstrucciones locales en ciertos entornos terrestres, por ejemplo áreas urbanas o suburbanas.

Un objeto de la presente invención es permitir la autenticación de señales de radionavegación con un nivel óptimo de robustez y disponibilidad, incluyendo entornos donde la recepción de señales y las condiciones de desmodulación de datos impiden la desmodulación exitosa de todos los datos desde todos los transmisores de radionavegación.

Descripción de la invención

En un aspecto de la invención, se proporciona un sistema de radionavegación, que comprende una pluralidad de transmisores portados por satélite y al menos un receptor situado en tierra, estando el receptor adaptado para recibir señales de radionavegación desde cada uno de una pluralidad de los transmisores, estando cada uno de los transmisores y el receptor adaptados para acceder a una primera cadena de claves predeterminada, comprendiendo la primera cadena de claves una primera clave de encriptación y una o más claves de encriptación adicionales, comprendiendo el sistema: un primer grupo de transmisores de dicha pluralidad de transmisores, pudiendo hacer que cada transmisor en el primer grupo de transmisores funcione para transmitir una primera señal de radionavegación, incluyendo las primeras señales de radionavegación, en un instante dado o para una subtrama dada, datos de radionavegación, un código de autenticación de mensajes (MAC) y una de dichas una o más claves de encriptación adicionales; en donde el MAC es exclusivo para cada transmisor y se genera usando la primera clave de encriptación; en donde dicha una de dichas una o más claves de encriptación adicionales se transmite un tiempo predeterminado después de la transmisión del MAC; y en donde el receptor se puede hacer funcionar, tras recibir toda o parte de la primera señal de radionavegación desde uno o más del primer grupo de transmisores, para autenticar una primera señal de radionavegación recibida desde uno del primer grupo de transmisores basándose en el MAC recibido desde dicho un transmisor y en una de dichas una o más claves de encriptación adicionales recibidas desde ese transmisor o desde cualquier otro transmisor en dicho primer grupo de transmisores.

El receptor se puede hacer funcionar para autenticar la primera señal de radionavegación usando la recibida de dichas una o más claves de encriptación adicionales o usando otra de dichas una o más claves de encriptación adicionales derivables de la misma.

Preferiblemente, el receptor se puede hacer funcionar para autenticar la primera señal de radionavegación recibida basándose en la recibida de dichas una o más claves de encriptación adicionales tras recibir al menos los datos de radionavegación y el MAC de esa primera señal de radionavegación.

La o cada primera señal de radionavegación puede estar en múltiples partes, de manera que la clave de encriptación se transmite un retardo predeterminado después de los datos de radionavegación y/o el MAC.

En una realización, la clave de encriptación transmitida es la misma para todos los transmisores dentro del primer grupo. En otra realización, la clave de encriptación transmitida comprende, para cada transmisor del primer grupo, una diferente de dicha primera cadena de claves.

Para cada subtrama de la primera señal de radionavegación, cada clave de encriptación de dicha primera cadena de claves puede comprender una de n claves de encriptación derivadas de modo recursivo de una función unidireccional. De manera preferible, n es aproximadamente igual y, en todo caso, mayor que el número total de transmisores portados por satélite en dicho sistema de radionavegación.

Para cada transmisor del primer grupo, un MAC respectivo se puede derivar de una clave raíz de la primera cadena de claves.

El receptor puede estar adaptado para autenticar la señal de radionavegación recibida al generar un MAC derivado basándose en los datos de radionavegación recibidos y la recibida de dichas una o más claves de encriptación adicionales y al comparar el MAC derivado con el MAC recibido.

En una realización, el primer grupo de transmisores comprende todos de dicha pluralidad de transmisores en el sistema de radionavegación.

En otra realización, el primer grupo de transmisores comprende un subconjunto estricto de dicha pluralidad de transmisores en el sistema de radionavegación. Los transmisores restantes pueden comprender un segundo grupo de transmisores, en donde una segunda cadena de claves predeterminada es accesible por el segundo grupo de transmisores y el receptor, comprendiendo la segunda cadena de claves una primera clave de encriptación y una o más claves de encriptación adicionales. Preferiblemente, cada transmisor en el segundo grupo se puede hacer funcionar para transmitir una segunda señal de radionavegación, incluyendo las segundas señales de radionavegación, en un instante dado o para una subtrama dada, datos de radionavegación, un MAC y una de dichas una o más claves de encriptación adicionales; en donde el código MAC es exclusivo para cada transmisor y se genera usando la primera clave de encriptación; en donde dicha una de dichas una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales se transmite un tiempo predeterminado después de la transmisión del MAC; y en donde el receptor se puede hacer funcionar, tras recibir toda o parte de la segunda señal de radionavegación desde uno o más del segundo grupo de transmisores, para autenticar una segunda señal de radionavegación recibida desde uno del segundo grupo de transmisores basándose en el MAC recibido desde dicho un transmisor y en una de dichas una o más claves de encriptación adicionales recibidas desde ese transmisor o desde cualquier otro transmisor de dicho segundo grupo de transmisores.

El receptor se puede hacer funcionar para autenticar la primera señal de radionavegación usando la recibida de dichas una o más claves de encriptación adicionales o usando otra de dichas una o más claves de encriptación adicionales derivables de la misma.

El receptor se puede hacer funcionar para autenticar la segunda señal de radionavegación recibida basándose en la clave de encriptación recibida tras recibir al menos los datos de radionavegación y el MAC de esa segunda señal de radionavegación.

La o cada segunda señal de radionavegación puede estar en múltiples partes, de manera que la clave de encriptación se transmite un retardo predeterminado después de los datos de radionavegación y/o el MAC.

En una realización, la clave de encriptación transmitida es la misma para todos los transmisores dentro del segundo grupo. En otra realización, la clave de encriptación transmitida comprende, para cada transmisor del segundo grupo, una diferente de dicha segunda cadena de claves.

Las primeras señales de radionavegación y/o las segundas señales de radionavegación se pueden transmitir de manera que partes de la señal que comprenden bits impredecibles están intercaladas con partes que comprenden bits predecibles.

Según otro aspecto de la invención, se proporciona un transmisor para un sistema de radionavegación, comprendiendo el sistema de radionavegación una pluralidad de transmisores portados por satélite y al menos un receptor situado en tierra, estando el receptor adaptado para recibir señales de radionavegación desde cada uno de una pluralidad de los transmisores, estando cada uno de los transmisores y el receptor adaptados para acceder a una primera cadena de claves predeterminada, comprendiendo la primera cadena de claves una primera clave de encriptación y una o más claves de encriptación adicionales, pudiendo hacer que el receptor funcione, tras recibir toda o parte de la primera señal de radionavegación desde uno o más del primer grupo de transmisores, para

autenticar una primera señal de radionavegación recibida desde uno de los transmisores basándose en el MAC recibido desde dicho un transmisor y en una de dichas una o más claves de encriptación adicionales recibidas desde ese transmisor o desde cualquier otro de dicha pluralidad de los transmisores, en donde: el transmisor se puede hacer funcionar para transmitir una primera señal de radionavegación, incluyendo las primeras señales de radionavegación, en un instante dado o para una subtrama dada, datos de radionavegación, un MAC y una de dichas una o más claves de encriptación adicionales; el MAC es exclusivo para cada transmisor y se genera usando la primera clave de encriptación, y en donde dicha una de dichas una o más claves de encriptación adicionales se transmite un tiempo predeterminado después de la transmisión del MAC.

Según otro aspecto de la invención, se proporciona un receptor para un sistema de radionavegación, comprendiendo el sistema de radionavegación una pluralidad de transmisores portados por satélite y al menos el receptor, estando cada uno de los transmisores y el receptor adaptados para acceder a una primera cadena de claves predeterminada, comprendiendo la primera cadena de claves una primera clave de encriptación y una de dichas una o más claves de encriptación adicionales, pudiendo hacer que cada transmisor funcione para transmitir una primera señal de radionavegación, incluyendo las primeras señales de radionavegación, en un instante dado o para una subtrama dada, datos de radionavegación, un MAC y una de dichas una o más claves de encriptación adicionales; en donde el MAC es exclusivo para cada transmisor y se genera usando la primera clave de encriptación; en donde dicha una de dichas una o más claves de encriptación adicionales se transmite un tiempo predeterminado después de la transmisión del MAC; en donde el receptor está adaptado para recibir señales de radionavegación desde cada uno de la pluralidad de los transmisores, y en donde el receptor se puede hacer funcionar, tras recibir toda o parte de la primera señal de radionavegación desde uno o más de los transmisores, para autenticar la primera señal de radionavegación recibida desde uno de los transmisores basándose en el MAC recibido desde dicho un transmisor y en una de dichas una o más claves de encriptación adicionales recibida desde ese transmisor o desde cualquier otro de dicha pluralidad de los transmisores.

Según otro aspecto de la invención, se proporciona un método de radionavegación para un sistema de radionavegación, comprendiendo el sistema de radionavegación una pluralidad de transmisores portados por satélite y al menos un receptor situado en tierra, estando el receptor adaptado para recibir señales de radionavegación desde cada uno de una pluralidad de los transmisores, comprendiendo el método: proporcionar a cada uno de los transmisores y al receptor acceso a una primera cadena de claves predeterminada, comprendiendo la primera cadena de claves una primera clave de encriptación y una o más claves de encriptación adicionales, transmitir, desde cada uno de dicha pluralidad de transmisores, una primera señal de radionavegación, incluyendo las primeras señales de radionavegación, en un instante dado o para una subtrama dada, datos de radionavegación, un MAC y una de dichas una o más claves de encriptación adicionales, siendo el MAC exclusivo para cada transmisor y generándose usando la primera clave de encriptación, en donde dicha una de dichas una o más claves de encriptación adicionales se transmite un tiempo predeterminado después de la transmisión del MAC; recibir, en el receptor, toda o parte de la primera señal de radionavegación desde uno o más de dicha pluralidad de transmisores, y autenticar, en el receptor, una primera señal de radionavegación recibida desde uno de dicha pluralidad de transmisores basándose en el MAC recibido desde dicho un transmisor y en una de dichas una o más claves de encriptación adicionales recibidas desde ese transmisor o desde cualquier otro transmisor en dicha pluralidad de transmisores.

Según otro aspecto de la invención, se proporciona un soporte que se puede grabar, reescribir o almacenar, que tiene grabados o almacenados en el mismo datos que definen o son transformables en instrucciones para la ejecución por circuitería de procesamiento y que corresponde al menos a las etapas de la reivindicación 21 de las reivindicaciones adjuntas.

Según otro aspecto de la invención, se proporciona un ordenador servidor, que incorpora un dispositivo de comunicaciones y un dispositivo de memoria y que está adaptado para la transmisión, bajo demanda o de otro modo, de datos que definen o son transformables en instrucciones para la ejecución por circuitería de procesamiento y que corresponde al menos a las etapas de la reivindicación 21 de las reivindicaciones adjuntas.

Las realizaciones de la invención proporcionan una implementación optimizada del protocolo TESLA para la autenticación de radionavegación. Las realizaciones de la presente invención usan una única cadena unidireccional para todos o una pluralidad de transmisores de señales de radionavegación, en oposición al uso de una única cadena unidireccional para cada transmisor de señales de radionavegación. Las realizaciones de la invención se pueden resumir como sigue. (En este documento, “transmisor” y “remitente” se usan de modo intercambiable).

1) Un sistema de radionavegación realiza las siguientes etapas (lado del remitente):

- A partir de una semilla inicial K_n, una única cadena de claves K_n a K_0 generadas de modo recursivo a través de una función unidireccional H se calcula por ordenador mediante el sistema, según el protocolo TESLA;

- Las claves que componen dicha cadena unidireccional se usan en orden inverso (K_0 a K_n) para autenticar los datos de remitente desde la pluralidad de remitentes del siguiente modo:

  - en un cierto período de tiempo j, el sistema usa una única clave K_j de dicha cadena;

• dicha única clave K_j se usa para autenticar los datos D_i actuales o recientes transmitidos por cada remitente i de una pluralidad de remitentes, generando un código de autenticación de mensajes $MAC_{(j,i)}$ que es a priori diferente para cada remitente i;

• los remitentes transmiten, además de sus propios datos de navegación D_i, dicho código de autenticación de mensajes $MAC_{(j,i)}$ generado con la misma única clave K_j para todos los remitentes, y algún momento más adelante, dicha única clave K_j desde todos los remitentes.

2) Un receptor de radionavegación realiza las siguientes etapas:

• se reciben y se almacenan los datos de navegación D_i desde cada remitente visible;

• se reciben y se almacenan dichos códigos de autenticación de mensajes $MAC_{(j,i)}$ desde dichos remitentes del sistema;

• una vez que dicha única clave K_j se recibe con éxito desde todos los remitentes, alguno de ellos, o cualquiera de ellos, se usa para verificar la autenticidad de los datos de navegación D_i desde cada remitente al generar los códigos de autenticación de mensajes $MAC_{(j,i)}$ recibidos previamente;

• el receptor es capaz de verificar la autenticidad de dicha única clave K_j aplicable en dicho intervalo al ejecutar la función unidireccional que lo relaciona a una clave previa en la cadena entre K_{j-1} y K_0, cuya autenticidad se certifica a partir de un certificado recibido previamente desde cualquiera, algunos o la totalidad de dichos remitentes, o cualquier otro medio.

Una ventaja de la invención es la mejora del comportamiento en los servicios de radionavegación por el uso de una única clave o claves de la misma cadena, desde varios transmisores de señales de radionavegación.

Una ventaja adicional es que el sistema puede autenticar los datos y las señales de radionavegación de un cierto remitente usando los datos y el MAC desde tal remitente, mientras usa la clave desde dicho remitente o cualquier otro remitente, si la clave desde dicho remitente no está desmodulada apropiadamente respecto a la señal de radionavegación. Una ventaja consiguiente es reducir drásticamente la tasa de errores de autenticación (AER) en condiciones de recepción degradadas: permitiendo que todos los satélites sean autenticados mediante la misma clave o la misma cadena, un usuario tiene que recibir solamente una clave correcta desde un satélite cada subtrama para autenticar todos los satélites. Esto reduce espectacularmente la cantidad de bits requeridos para una posición y un tiempo fijos calculados por ordenador usando remitentes autenticados.

En las realizaciones, el uso de una única cadena no solamente es beneficioso para reducir la tasa de errores de autenticación en condiciones estacionarias (es decir, después de que se certifica como correcta una clave previa de la cadena), sino también ayuda en la inicialización, dado que solamente se requiere una clave certificada recibida desde cualquier remitente o cualquier otra fuente.

Además de lo anterior, son especialmente ventajosas las realizaciones de la invención donde se observan uno o pocos satélites en buenas condiciones de recepción con una baja tasa de errores de bits, rodeados por otros satélites de altura inferior o peor visibilidad con una tasa de errores de bits mucho más alta, dado que el receptor puede usar la clave desde los satélites de buena visibilidad para autenticar los satélites de mala visibilidad, en tanto que los pocos bits de MAC se reciben desde los satélites de mala visibilidad, en oposición a la necesidad de recibir la clave desde cada satélite de mala visibilidad a autenticar.

Breve descripción de los dibujos

Las realizaciones de la invención se describirán a continuación a modo de ejemplo de referencia para los dibujos que se acompañan, en los que:

la figura 1 es una ilustración esquemática de un sistema de radionavegación según una realización de la invención;

la figura 2 muestra trazados gráficos del comportamiento de la Tasa de errores de autenticación (AER) para una Tasa de errores de bits (BER) dada, para la realización de la figura 1 y otras implementaciones conocidas;

la figura 3 es una ilustración esquemática de las técnicas que subyacen en un sistema de radionavegación según otra realización de la invención que ilustra el uso de claves de una única cadena para transmitir claves diferentes desde satélites diferentes;

la figura 4 es una ilustración esquemática de un sistema de radionavegación según otra realización de la invención, por el que cada satélite está transmitiendo una clave ($K_{j,1}$, $K_{j,2}$, etc.) diferente desde la misma cadena, siendo las claves de cadena utilizadas, como se muestra en la figura 3;

la figura 5 ilustra una implementación clásica de la transmisión de la autenticación de datos de navegación; y

la figura 6 es una ilustración esquemática del concepto que subyace en otra realización de la invención, por el que se intercalan bits impredecibles y predecibles a fin de minimizar el tiempo predecible máximo.

Modo o modos de llevar a cabo la invención

En lo que sigue, se usarán números semejantes para indicar elementos semejantes.

La figura 1 es una ilustración esquemática de un sistema de radionavegación 100 según una realización de la invención, por el que cada satélite está transmitiendo, primero, su propio MAC y, a continuación, la misma clave K. Un objeto de esta realización es optimizar la disponibilidad de autenticación minimizando la AER, reduciendo el número de bits requeridos a desmodular desde todos los satélites para calcular una posición y un tiempo fijos usando al menos cuatro satélites.

Los transmisores (no mostrados) en múltiples satélites transmiten señales de radionavegación respectivas, que se reciben en un receptor 104 situado en tierra 106, a través de una antena 108. (En esta realización, se muestran 4 satélites; sin embargo, los expertos en la técnica apreciarán que se pueden usar en la práctica más satélites, o menos. En este documento, con fines explicativos, “satélite” y “transmisor” se pueden usar de modo intercambiable).

Un primer satélite 110 transmite una primera señal de radionavegación 112 que incluye un código MAC, MAC1, que corresponde exclusivamente al primer satélite 110, seguido por la clave K. Un segundo satélite 114 transmite una segunda señal de radionavegación 116 que incluye un código MAC, MAC2, que corresponde exclusivamente al segundo satélite 114, seguido por la clave K. Un tercer satélite 118 transmite una tercera señal de radionavegación 120 que incluye un código MAC, MAC3, que corresponde exclusivamente al tercer satélite 114, seguido por la clave K. Un cuarto satélite 122 transmite una cuarta señal de radionavegación 124 que incluye un código MAC, MAC4, que corresponde exclusivamente al cuarto satélite 122, seguido por la clave K.

El resultado deseado de esta realización -minimización de la AER- implica que, dado que la NMA debe funcionar para toda clase de usuarios y entornos de recepción, la solución NMA debe estar optimizada para funcionar en condiciones de recepción difíciles. Se debe señalar que los receptores de gran consumo estándares son capaces de combinar bloques de mensajes a partir de subtramas diferentes para componer una estructura de datos de navegación completa. Esto no es posible para la NMA, donde la totalidad de los bits de autenticación se deben recibir correctamente en una única subtrama, dado que serán diferentes en subtramas diferentes para mejorar la robustez.

Se usa la siguiente notación y terminología:

- K_n: semilla de cadena unidireccional, es decir, el primer valor de la cadena unidireccional;
- K_0: raíz de cadena unidireccional, es decir, el último valor de la cadena unidireccional (o el valor más reciente que se certifica como correcto por el certificado K_0);
- K_j: clave asociada a todos los MAC transmitidos en una cierta subtrama j;
- MAC_i: Código de autenticación de mensajes generado autenticando los datos desde el satélite i, transmitido en la señal de navegación del satélite i;
- H: función unidireccional utilizada para calcular por ordenador la cadena, de manera que K_0 = H^n(K_n), donde H^n significa realizar la función H de modo recursivo n veces; y
- $K_{j,i}$: clave transmitida por el satélite i en la subtrama j.

Con estas suposiciones, se hace referencia de nuevo a la figura 1, y el procedimiento para esta realización se puede describir como sigue.

- En un cierto período de 30 segundos asociado con una cierta clave K, cada satélite i transmite un MAC_i usando K_j y los datos de satélite, o un subconjunto de ellos D_i. Los datos D_i a autenticar pueden incluir al menos el tiempo, las órbitas y los relojes del satélite y pueden llevar adjunta también otra información como el ID del satélite, como la información de contexto, las correcciones ionosféricas, las desviaciones temporales para otras constelaciones de satélites o las referencias temporales como la UTC, o los retardos de grupo de emisión de señales.
- Después de la transmisión del MAC_i, los satélites transmiten, todos, la misma clave K utilizada para generar cada uno del MAC_i. Es decir, la clave K se transmite un tiempo predeterminado después de la transmisión del MAC_i. En la práctica, esto puede significar que la transmisión de la clave K comienza un tiempo predeterminado después de la finalización de la transmisión del MAC_i. El tiempo predeterminado puede ser del orden de uno o pocos milisegundos a varios minutos, y más preferiblemente del orden de uno a menos de 30 segundos, a fin de ajustar en el período de 30 segundos.

• El receptor 104 se requiere para desmodular con éxito solamente una clave K a fin de calcular por ordenador una Posición, velocidad y temporización (PVT) autenticadas en datos. Como se muestra en la figura 1, recibiendo K desde el satélite 2 (marcado con 114) -el de la elevación más alta y, por lo tanto, con mejores condiciones de visibilidad a priori-, los datos desde todos los otros satélites 110, 118 y 122 se pueden autenticar si solamente se reciben sus MAC (MAC1, MAC3, MAC4, respectivamente).

En las realizaciones, el sistema adopta uno, algunos o la totalidad de los siguientes parámetros de diseño.

• La cadena unidireccional usa una función de la familia SHA-2, por ejemplo SHA-256, o SHA-224, que es esencialmente una SHA-256 por la que se dejan caer los últimos bits, para componer una cadena de claves (K) de longitud de 224 bits. Esto permite un nivel suficiente de seguridad (112 bits simétricos) según los estándares de seguridad. Se pueden usar claves más largas o más cortas, dependiendo de los requisitos de seguridad en el sistema.

• La primitiva del MAC puede ser HMAC-256.

• El MAC transmitido por los satélites se puede truncar a los últimos 15 bits. La probabilidad de adivinar correctamente un MAC de 15 bits sin tener la clave es alrededor de $3*10^{-5}$, que se considera suficientemente baja para disuadir de tales ataques.

• El período de clave puede ser 30 segundos.

• La longitud de cadena es 1 semana, lo que conduce a un número de 20.160 claves.

Sin embargo, los expertos en la técnica apreciarán que se pueden adoptar otros valores, según otras realizaciones y dependiendo de la implementación.

La figura 2 muestra el comportamiento de la AER para una Tasa de errores de bits (BER) dada, para la realización de la figura 1 y otras implementaciones conocidas. Con fines comparativos, la figura 2 presenta el comportamiento de la AER, para tres implementaciones NMA:

• NMA a través de una firma digital de 466 bits estándar, una por satélite;

• NMA a través de un planteamiento de protocolo TESLA estándar, con una clave de 224 bits diferente y un MAC truncado a 15 bits por satélite; y

• NMA a través del único planteamiento de TESLA de cadena según la presente realización, con la misma clave de 224 bits desde todos los satélites y los MAC truncados a 15 bits.

En la figura 2, se calcula AER a partir de BER y NA a través de la siguiente fórmula:

$$AER = 1 - (1-BER)^{NA},$$

donde BER es la tasa de errores de bits y NA es el número de bits requerido para la autenticación. La figura 2 se debería interpretar del siguiente modo: suponiendo que hay 4 satélites (110, 114, 118, 122) en vista del receptor 104 con una BER dada, el valor “4-sat AER” es la probabilidad de que 4 satélites estén autenticados en mensajes de navegación, permitiendo calcular un valor autenticado en NM de la posición y el tiempo (haciendo referencia a este último ocasionalmente como PVT). Se supone en todos los casos que el receptor 104 ya ha recibido los datos de navegación para autenticar. Los resultados muestran una mejora significativa mediante el uso de la realización de la presente invención (trazo continuo "224/15-1C-TESLA") en comparación con los otros métodos existentes. Por ejemplo, usando 4 satélites para calcular por ordenador una posición y un tiempo fijos:

• Bits de autenticación requeridos a través de firmas digitales estándares usando una firma curva elíptica de 466 bits: 446 * 4 = 1.864 bits.

• Bits de autenticación requeridos a través del caso TESLA estándar usando un MAC truncado a 15 bits y una clave de 224 bits: (15+224)*4 = 956 bits.

• Bits de autenticación requeridos a través de la realización actual de la invención (MAC truncado a 15 bits + clave de 224 bits): 15 * 4 + 224 = 284 bits.

Esta diferencia de bits es incluso más alta si se usan más de 4 satélites para el cálculo de la posición y el tiempo, que es el caso estándar. Por ejemplo, si se usan 7 satélites, la diferencia sería 1.673 bits en el caso TESLA estándar frente a 329 bits para una realización de la presente invención, es decir, cinco veces menos.

La figura 3 es una ilustración esquemática de un sistema de radionavegación según otra realización de la invención que ilustra el uso de claves desde una única cadena para transmitir claves diferentes desde satélites diferentes, a fin de aumentar las características de impredecibilidad de la señal. Esto es lo mismo que la realización de la figura 1, excepto en lo que se describe como sigue.

Un objeto de esta realización es la maximización de la robustez contra los ataques de reproducción al aumentar las características que hacen la señal impredecible, al tiempo que se mantienen las mismas ventajas de usar una única cadena unidireccional, como en la realización previa. La maximización de la impredecibilidad de los símbolos o bits de navegación proporciona robustez contra los ataques de reproducción de señales; siempre que los símbolos impredecibles tengan que ser verificados más adelante como correctos por el proceso de autenticación.

Un fenómeno que surge cuando se usa una única cadena unidireccional para todos los satélites (110, 114, 118, 122; figura 1) es que, si la misma clave se usa y se transmite al mismo tiempo desde todos los satélites, se recibirán en momentos diferentes por los usuarios (en el receptor 104), debido a las desviaciones de reloj de los satélites y, principalmente, debido al tiempo de llegada relacionado con la distancia desde los satélites hasta el receptor 104. Por ejemplo, la señal desde un satélite en el cénit, a una altura de 23.200 km, tardará en llegar a la superficie de la Tierra aproximadamente 77,3 ms. Sin embargo, una señal desde un satélite en la misma órbita circular o una similar, pero a una altura inferior, tardará algunos milisegundos más en llegar a la superficie de la Tierra (siempre menos de 21 ms para los usuarios terrestres, equivalente aproximadamente al radio de la Tierra a la velocidad de la luz). Un atacante podría usar estos milisegundos para estimar los bits impredecibles que componen la clave TESLA desde el satélite más alto y reproducirlos con un retardo entre sí, facilitando el falseamiento de la posición, incluso si los datos utilizados son auténticos, mediante la modificación de la señal tiempo de llegada.

Por lo tanto, si todos los satélites están transmitiendo la misma clave al mismo tiempo, solamente serán impredecibles los símbolos desde el satélite más próximo al cénit, dado que un atacante podría estimarlos y reproducirlos en la señal desde satélites a alturas inferiores.

Este problema puede superarse aumentando la longitud de la cadena de claves y transmitiendo claves diferentes, pero todavía desde la misma cadena, desde satélites diferentes. Las claves permitirían la determinación de la clave K_j utilizada para el cálculo por ordenador de todos los MAC en una cierta subtrama al realizar la función unidireccional.

En la realización de la figura 3, se usa la siguiente relación de MAC frente a CLAVE.

- Para cada subtrama j, se usa una única clave para calcular por ordenador todos los MAC transmitidos por todos los satélites. Esta clave es una función unidireccional de 40 veces de la clave utilizada sobre la subtrama j-1 previa:

$$K_j=H^{40}(K_j\text{-}1).$$

Señalar que se ha usado 40 para alojar 40 claves por subtrama: una que se usará para los MAC (k, k+1, etc.) y otras 39 que se pueden usar por 39 satélites. Esto proporciona suficiente margen para alojar todos los satélites desde una constelación GNSS.

- Para cada subtrama j, cada satélite i transmite un MAC basándose en la clave K_j, de manera que

$$MAC_{(j,i)}=M(d_{j,i}||m_i, K_j),$$

donde M es la función MAC, HMAC-SHA-224, truncada a 15 bits, $d_{j,i}$ es la información adicional (al menos el tiempo de los SVID y del sistema) que hace único el resultado HMAC y m_i son los datos de navegación a firmar.

- Para cada subtrama j, cada satélite i transmite una clave $K_{j,i}$ de manera que

$$K_{j,i}=H^i(K_j).$$

Así, por ejemplo, el satélite SVID5 transmitirá una clave ($K_{j,5}$) a la que se tiene que aplicar la función *hash* 5 veces para obtener K_j. De este modo, el MAC desde cualquier satélite se puede verificar frente a cualquier clave recibida desde cualquier otro satélite. Por otro lado, seguirán siendo impredecibles todos los bits desde todas las K_j que se transmiten en cada subtrama. Se debe señalar que la carga adicional de tener 40 funciones unidireccionales por subtrama para mantener esta característica de impredecibilidad de bits parece asequible para los receptores estándares y futuros.

Como se ve en la figura 3, usando las claves desde una única cadena, se transmiten claves diferentes desde satélites diferentes. La primera cadena muestra que, para cada subtrama, las claves entre K_m y K_m+41 se atribuyen a una única subtrama y a toda una constelación de satélites. La segunda cadena muestra que la primera clave K_j, equivalente a K_m en la cadena previa, se usa para calcular por ordenador los MAC desde todos los satélites, mientras que $K_{j,i}$ es la clave transmitida por el satélite i, estando i entre 1 y 40 en esta realización.

Usando este planteamiento, un receptor 104 puede recibir una única clave $K_{j,i}$ y realizar la función unidireccional i veces para determinar la clave K_j utilizada para calcular por ordenador los MAC. Al mismo tiempo, no se pueden predecir las claves $K_{j,i}$ transmitidas por cada satélite i, maximizando la robustez frente a la reproducción de señales.

La figura 4 es una ilustración esquemática de un sistema de radionavegación 400 según otra realización de la invención, por el que cada satélite está transmitiendo una clave ($K_{j,1}$, $K_{j,2}$, etc.) diferente desde la misma cadena en

una cierta subtrama. Esto es lo mismo que la realización de la figura 1, excepto en lo que se describe como sigue. De manera adecuada, esta realización usa las claves de cadena como se presentan en la figura 3.

Un primer satélite 110 transmite una primera señal de radionavegación 412 que incluye un código MAC, MAC1, que corresponde exclusivamente al primer satélite 110, seguido por la clave $K_{j,1}$. Un segundo satélite 114 transmite una segunda señal de radionavegación 416 que incluye un código MAC, MAC2, que corresponde exclusivamente al segundo satélite 114, seguido por la clave $K_{j,2}$. Un tercer satélite 118 transmite una tercera señal de radionavegación 420 que incluye un código MAC, MAC3, que corresponde exclusivamente al tercer satélite 114, seguido por la clave $K_{j,3}$. Un cuarto satélite 122 transmite una cuarta señal de radionavegación 424 que incluye un código MAC, MAC4, que corresponde exclusivamente al cuarto satélite 122, seguido por la clave $K_{j,4}$.

Como se ha descrito, si el receptor 104 recibe los MAC (MAC1, MAC2, MAC3, MAC4) desde los 4 satélites 110, 114, 118, 122 y solamente la clave desde los satélites más altos ($K_{j,2}$), puede calcular K_j ($K_j = H^2(K_{j,2})$) y verificar por lo tanto los datos desde los satélites frente a los MAC, así como verificar la robustez contra la reproducción de señales a partir de cada una de las señales.

Esas claves, que se transmiten en una cierta subtrama pero que no se pueden calcular por ordenador a partir de las claves correctamente desmoduladas en esta subtrama (p. ej., $K_{j,3}$ y $K_{j,4}$ en la figura 4), se pueden calcular por ordenador a partir de cualquier clave desde cualquier satélite recibido en cualquiera de las siguientes subtramas. Por ejemplo: $K_{j,3}=H^{41}(K_{j+1,4})$.

En otra realización, en vez de la totalidad de los remitentes (satélites 110, 114, 118, 122) enviando la misma clave K_j (véase la realización de la figura 1), pueden existir dos o más grupos de remitentes, usando cada remitente dentro de un grupo claves diferentes desde cadenas unidireccionales diferentes para cada grupo. Esta realización puede mejorar la seguridad dado que, para la gestión de claves o por otras razones, puede considerarse más seguro evitar el uso de una única clave desde todos los remitentes.

En otra realización, la misma clave K_j está codificada de modo distinto desde cada remitente (satélites 110, 114, 118, 122) y de modo que es impredecible para el receptor 104 hasta que se recibe la totalidad de la información clave codificada. Esto se puede conseguir, por ejemplo, mediante la codificación de K_j y un *nonce* a través de una red de sustitución y permutación, y la transmisión del *nonce*, que debería ser diferente e impredecible para cada satélite, junto con la clave K_j.

En otra realización, el funcionamiento implica dispersar la impredecibilidad de bits y símbolos en el flujo de datos transmitido. Esto tiene la ventaja de aumentar la robustez contra los ataques de reproducción.

La figura 5 ilustra una implementación clásica de la transmisión de la autenticación de datos de navegación. Más particularmente, la figura 5 muestra la implementación por la que se transmiten por completo los bits de información impredecibles, como la firma digital. La autenticación 50 ocurre un tiempo 52 después de la transmisión 54. Esto conduce a un tiempo predecible máximo 56 que constituye la mayor parte del tiempo 52 entre autenticaciones. El tiempo predecible máximo 56 es el tiempo durante el que un atacante podría tomar el control de los bucles de seguimiento antes de un ataque de reproducción de señales. Por lo tanto, cuanto más corto sea el tiempo predecible máximo 56, más robusto puede ser el receptor 104 contra este tipo de ataques.

La figura 6 es una ilustración esquemática del concepto que subyace en otra realización de la invención, con relación a la transmisión de la autenticación de datos de navegación, por lo que los bits impredecibles y predecibles se intercalan para minimizar el tiempo predecible máximo 66. Esto es lo mismo que la realización de la figura 1, excepto en lo que se describe como sigue.

La autenticación 60 ocurre un tiempo 62 después de la transmisión 64. Un objeto de la realización de la figura 6 es aumentar la robustez contra la reproducción de señales. Para proporcionar tal protección, se tienen que verificar los bits impredecibles 68 en la verificación de autenticaciones realizada una vez que se han recibido completamente los datos a autenticar y los datos utilizados para la autenticación. Esto se puede hacer para los datos, el MAC y la clave de un cierto satélite, así como con el certificado K_0, si se transmite en la señal. Por lo tanto, en la presente realización, los bits de datos que se pueden considerar impredecibles son:

- la clave K_j;
- los MAC: MAC1, MAC2, etc.; y
- la firma digital de un certificado, $DS(K_0)$, transmitida en la señal para certificar la autenticidad de K_0 (la clave raíz de la cadena) por un esquema de encriptación asimétrico.

El fin de la verificación del certificado K_0 puede ser doble: en primer lugar, para asegurar que el MAC y la clave son K_j correctos y, en segundo lugar, para aumentar la protección contra las reproducciones de señales. Si se transmiten continuamente certificados K_0 que incluyen una firma digital impredecible, esto permite el comportamiento de más verificaciones de antirreproducciones, de modo que el satélite puede transmitir continuamente bits impredecibles que se verifican más adelante.

Aunque se han descrito realizaciones con referencia a realizaciones que tienen diversos componentes en sus implementaciones respectivas, se apreciará que otras realizaciones hacen uso de otras combinaciones y permutaciones de estos y otros componentes.

Además, algunas de las realizaciones se describen en la presente memoria como un método o una combinación de elementos de un método que se puede implementar por un procesador de un sistema informático o por otros medios para llevar a cabo la función. Así, un procesador con las instrucciones necesarias para llevar a cabo tal método o tal elemento de un método forma unos medios para llevar a cabo el método o el elemento de un método. Además, un elemento descrito en la presente memoria de una realización de aparato es un ejemplo de unos medios para llevar a cabo la función realizada por el elemento con el fin de llevar a cabo la invención.

En la descripción proporcionada en la presente memoria, se exponen numerosos detalles específicos. Sin embargo, se entiende que las realizaciones de la invención se pueden poner en práctica sin estos detalles específicos. En otros casos, no se han mostrado con detalle métodos, estructuras y técnicas bien conocidos a fin de no hacer confusa la comprensión de esta descripción.

Así, aunque se ha descrito lo que se considera que son las realizaciones preferidas de la invención, los expertos en la técnica reconocerán que se pueden realizar en las mismas otras modificaciones, y adicionales, sin salirse del alcance de la invención. Por ejemplo, cualquier fórmula dada anteriormente es simplemente representativa de los procedimientos que se pueden usar. Se pueden añadir o suprimir funcionalidades de los diagramas de bloques y se pueden intercambiar operaciones entre bloques funcionales. Se pueden añadir o suprimir etapas a los métodos descritos dentro del alcance de la presente invención.

REIVINDICACIONES

1. Un sistema de radionavegación (100; 400), que comprende una pluralidad de transmisores (110, 114, 118, 122) portados por satélite y al menos un receptor (104) situado en tierra, estando el receptor (104) adaptados para recibir señales de radionavegación (112, 116, 120, 124; 412, 416, 420, 424) desde cada uno de una pluralidad de los transmisores (110, 114, 118, 122), estando cada uno de los transmisores (110, 114, 118, 122) y el receptor (104) adaptados para acceder a una primera cadena de claves predeterminada, comprendiendo la primera cadena de claves una primera clave de encriptación (K; K_j) y una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales, comprendiendo el sistema:

un primer grupo de transmisores de dicha pluralidad de transmisores (110, 114, 118, 122), pudiendo hacer que cada transmisor en el primer grupo de transmisores funcione para transmitir una primera señal de radionavegación (112, 116, 120, 124; 412, 416, 420, 424), incluyendo las primeras señales de radionavegación, en un instante dado o para una subtrama (k, k+1) dada, datos de radionavegación, un código de autenticación de mensajes (MAC) (MAC1, MAC2, MAC3, MAC4) y una de dichas una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales;

en donde el MAC (MAC1, MAC2, MAC3, MAC4) es exclusivo para cada transmisor (110, 114, 118, 122) y se genera usando dicha primera clave de encriptación (K; K_j);

en donde dicha una de dichas una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales se transmite un tiempo predeterminado después de la transmisión del MAC, y

en donde el receptor (104) se puede hacer funcionar, tras recibir toda o parte de la primera señal de radionavegación (112, 116, 120, 124; 412, 416, 420, 424) desde uno o más del primer grupo de transmisores (110, 114, 118, 122), para autenticar una primera señal de radionavegación recibida desde uno del primer grupo de transmisores basándose en el MAC recibido desde dicho un transmisor y en una de dichas una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales recibidas desde ese transmisor o desde cualquier otro transmisor en dicho primer grupo de transmisores.

2. El sistema de radionavegación según la reivindicación 1, en donde el receptor (104) se puede hacer funcionar para autenticar la primera señal de radionavegación usando la recibida de dichas una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales o usando otra de dichas una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales derivables de la misma.

3. El sistema de radionavegación según la reivindicación 1 o 2, en donde el receptor (104) se puede hacer funcionar para autenticar la primera señal de radionavegación (112, 116, 120, 124; 412, 416, 420, 424) recibida basándose en la recibida de dichas una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales tras recibir al menos los datos de radionavegación y el MAC (MAC1, MAC2, MAC3, MAC4) de esa primera señal de radionavegación.

4. El sistema de radionavegación según la reivindicación 1, 2 o 3, en donde la clave de encriptación (K) transmitida es la misma para todos los transmisores dentro del primer grupo.

5. El sistema de radionavegación según la reivindicación 1, 2 o 3, en donde la clave de encriptación ($K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) transmitida comprende, para cada transmisor del primer grupo, una diferente de dicha primera cadena de claves.

6. El sistema de radionavegación según la reivindicación 5, en donde, para cada subtrama (k, k+1) de la primera señal de radionavegación (112, 116, 120, 124; 412, 416, 420, 424), cada clave de encriptación de dicha primera cadena de claves comprende una de n claves de encriptación (K_m ... K_{m+40}) derivadas de modo recursivo de una función unidireccional.

7. El sistema de radionavegación según la reivindicación 6, en donde n es aproximadamente igual y, en todo caso, mayor que el número total de transmisores (110, 114, 118, 122) portados por satélite en dicho sistema de radionavegación (100; 400).

8. El sistema de radionavegación según cualquiera de las reivindicaciones precedentes, en donde, para cada transmisor (110, 114, 118, 122) del primer grupo, una respectiva de dichas una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales se deriva de una clave raíz (K_0) de la primera cadena de claves.

9. El sistema de radionavegación según cualquiera de las reivindicaciones precedentes, en donde el receptor (104) está adaptado para autenticar la señal de radionavegación (112, 116, 120, 124; 412, 416, 420, 424) recibida al generar un código MAC derivado basándose en los datos de radionavegación recibidos y la recibida de dichas una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales y al comparar el MAC derivado con el MAC (MAC1, MAC2, MAC3, MAC4) recibido.

10. El sistema de radionavegación según cualquiera de las reivindicaciones precedentes, en donde el primer grupo de transmisores comprende todos de dicha pluralidad de transmisores (110, 114, 118, 122) en el sistema de radionavegación (100; 400).

11. El sistema de radionavegación según cualquiera de las reivindicaciones 1 a 9, en donde el primer grupo de transmisores comprende un subconjunto estricto de dicha pluralidad de transmisores (110, 114, 118, 122) en el sistema de radionavegación (100; 400).

12. El sistema de radionavegación según la reivindicación 11, en donde los transmisores (110, 114, 118, 122) restantes comprenden un segundo grupo de transmisores, y en donde una segunda cadena de claves predeterminada es accesible por el segundo grupo de transmisores y el receptor, comprendiendo la segunda cadena de claves una primera clave de encriptación (K; K_j) y una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales.

13. El sistema de radionavegación según la reivindicación 12, en donde:

cada transmisor (110, 114, 118, 122) en el segundo grupo se puede hacer funcionar para transmitir una segunda señal de radionavegación (112, 116, 120, 124; 412, 416, 420, 424), incluyendo las segundas señales de radionavegación, en un instante dado o para una subtrama dada, datos de radionavegación, un MAC (MAC1, MAC2, MAC3, MAC4) y una de dichas una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales;

en donde el MAC (MAC1, MAC2, MAC3, MAC4) es exclusivo para cada transmisor (110, 114, 118, 122) y se genera usando la primera clave de encriptación (K; K_j),

en donde dicha una de dichas una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales se transmite un tiempo predeterminado después de la transmisión del MAC, y

en donde el receptor (104) se puede hacer funcionar, tras recibir toda o parte de la segunda señal de radionavegación (112, 116, 120, 124; 412, 416, 420, 424) desde uno o más del segundo grupo de transmisores, para autenticar una segunda señal de radionavegación recibida desde uno del segundo grupo de transmisores basándose en el MAC recibido desde dicho un transmisor y en una de dichas una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales recibidas desde ese transmisor o desde cualquier otro transmisor de dicho segundo grupo de transmisores.

14. El sistema de radionavegación según la reivindicación 13, en donde el receptor (104) se puede hacer funcionar para autenticar la primera señal de radionavegación usando la recibida de dichas una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales o usando otra de dichas una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales derivables de la misma.

15. El sistema de radionavegación según la reivindicación 14, en donde el receptor se puede hacer funcionar para autenticar la segunda señal de radionavegación (112, 116, 120, 124; 412, 416, 420, 424) recibida basándose en la clave de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) recibida tras recibir al menos los datos de radionavegación y el MAC (MAC1, MAC2, MAC3, MAC4) de esa segunda señal de radionavegación.

16. El sistema de radionavegación según la reivindicación 13, 14 o 15, en donde la clave de encriptación (K) transmitida es la misma para todos los transmisores dentro del segundo grupo.

17. El sistema de radionavegación según la reivindicación 13, 14 o 15, en donde la clave de encriptación ($K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) transmitida comprende, para cada transmisor del segundo grupo, una diferente de dicha segunda cadena de claves.

18. El sistema de radionavegación según cualquiera de las reivindicaciones precedentes, en donde las primeras señales de radionavegación (112, 116, 120, 124; 412, 416, 420, 424) y/o las segundas señales de radionavegación se transmiten de manera que partes (68) de la señal que comprenden bits impredecibles están intercaladas con partes que comprenden bits predecibles.

19. Un transmisor para un sistema de radionavegación (100; 400), comprendiendo el sistema de radionavegación (100; 400) una pluralidad de transmisores (110, 114, 118, 122) portados por satélite y al menos un receptor (104) situado en tierra, estando el receptor (104) adaptado para recibir señales de radionavegación (112, 116, 120, 124; 412, 416, 420, 424) desde cada uno de una pluralidad de los transmisores (110, 114, 118, 122), estando cada uno de los transmisores (110, 114, 118, 122) y el receptor (104) adaptados para acceder a una primera cadena de claves predeterminada, comprendiendo la primera cadena de claves una primera clave de encriptación (K; K_j) y una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales, pudiendo hacer que el receptor (104) funcione, tras recibir toda o parte de la primera señal de radionavegación (112, 116, 120, 124; 412, 416, 420, 424) desde uno o más del primer grupo de transmisores (110, 114, 118, 122), para autenticar una primera señal de radionavegación recibida desde uno de los transmisores basándose en el MAC recibido desde dicho un transmisor y en una de dichas una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales recibidas desde ese transmisor o desde cualquier otro de dicha pluralidad de los transmisores, en donde:

el transmisor se puede hacer funcionar para transmitir una primera señal de radionavegación (112, 116, 120, 124; 412, 416, 420, 424), incluyendo las primeras señales de radionavegación, en un instante dado o

para una subtrama (k, k+1) dada, datos de radionavegación, un MAC (MAC1, MAC2, MAC3, MAC4) y una de dichas una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales;

en donde el MAC (MAC1, MAC2, MAC3, MAC4) es exclusivo para cada transmisor (110, 114, 118, 122) y se genera usando la primera clave de encriptación (K; K_j); y

en donde dicha una de dichas una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales se transmite un tiempo predeterminado después de la transmisión del MAC.

20. Un receptor (104) para un sistema de radionavegación (100; 400), comprendiendo el sistema de radionavegación (100; 400) una pluralidad de transmisores (110, 114, 118, 122) portados por satélite y al menos el receptor (104), estando cada uno de los transmisores (110, 114, 118, 122) y el receptor (104) adaptados para acceder a una primera cadena de claves predeterminada, comprendiendo la primera cadena de claves una primera clave de encriptación (K; K_j) y una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales, pudiendo hacer que cada transmisor (110, 114, 118, 122) funcione para transmitir una primera señal de radionavegación (112, 116, 120, 124; 412, 416, 420, 424), incluyendo las primeras señales de radionavegación, en un instante dado o para una subtrama (k, k+1) dada, datos de radionavegación, un MAC (MAC1, MAC2, MAC3, MAC4) y una de dichas una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales;

en donde el MAC (MAC1, MAC2, MAC3, MAC4) es exclusivo para cada transmisor (110, 114, 118, 122) y se genera usando la primera clave de encriptación (K; K_j);

en donde dicha una de dichas una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales se transmite un tiempo predeterminado después de la transmisión del MAC,

en donde el receptor (104) está adaptado para recibir señales de radionavegación (112, 116, 120, 124; 412, 416, 420, 424) desde cada uno de la pluralidad de los transmisores (110, 114, 118, 122); y

en donde el receptor (104) se puede hacer funcionar, tras recibir toda o parte de la primera señal de radionavegación (112, 116, 120, 124; 412, 416, 420, 424) desde uno o más de los transmisores (110, 114, 118, 122), para autenticar la primera señal de radionavegación recibida desde uno de los transmisores basándose en el MAC recibido desde dicho un transmisor y en una de dichas una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales recibida desde ese transmisor o desde cualquier otro de dicha pluralidad de los transmisores (110, 114, 118, 122).

21. Un método de radionavegación para un sistema de radionavegación (100; 400), comprendiendo el sistema de radionavegación (100; 400) una pluralidad de transmisores (110, 114, 118, 122) portados por satélite y al menos un receptor (104) situado en tierra, estando el receptor (104) adaptado para recibir señales de radionavegación (112, 116, 120, 124; 412, 416, 420, 424) desde cada uno de una pluralidad de los transmisores (110, 114, 118, 122), comprendiendo el método:

proporcionar a cada uno de los transmisores (110, 114, 118, 122) y al receptor (104) acceso a una primera cadena de claves predeterminada, comprendiendo la primera cadena de claves una primera clave de encriptación (K; K_j) y una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales,

transmitir, desde cada uno de dicha pluralidad de transmisores (110, 114, 118, 122), una primera señal de radionavegación (112, 116, 120, 124; 412, 416, 420, 424), incluyendo las primeras señales de radionavegación, en un instante dado o para una subtrama (k, k+1) dada, datos de radionavegación, un MAC (MAC1, MAC2, MAC3, MAC4) y una de dichas una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales, siendo el MAC (MAC1, MAC2, MAC3, MAC4) exclusivo para cada transmisor (110, 114, 118, 122) y generándose usando la primera clave de encriptación (K; K_j), siendo dicha una de dichas una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales transmitida un tiempo predeterminado después de la transmisión del MAC;

recibir, en el receptor (104), toda o parte de la primera señal de radionavegación (112, 116, 120, 124; 412, 416, 420, 424) desde uno o más de dicha pluralidad de transmisores (110, 114, 118, 122), y

autenticar, en el receptor (104), una primera señal de radionavegación recibida desde uno de dicha pluralidad de transmisores basándose en el MAC recibido desde dicho un transmisor y en una de dichas una o más claves de encriptación (K; $K_{j,1}$, $K_{j,2}$, $K_{j,3}$, $K_{j,4}$) adicionales recibidas desde ese transmisor o desde cualquier otro transmisor en dicha pluralidad de transmisores.

22. Un soporte que se puede grabar, reescribir o almacenar, que tiene grabados o almacenados en el mismo datos que definen o son transformables en instrucciones para la ejecución por circuitería de procesamiento de las etapas de la reivindicación 21.

23. Un ordenador servidor, que incorpora un dispositivo de comunicaciones y un dispositivo de memoria y que está adaptado para la transmisión, bajo demanda o de otro modo, de datos que definen o son transformables en instrucciones para la ejecución por circuitería de procesamiento de las etapas de la reivindicación 21.

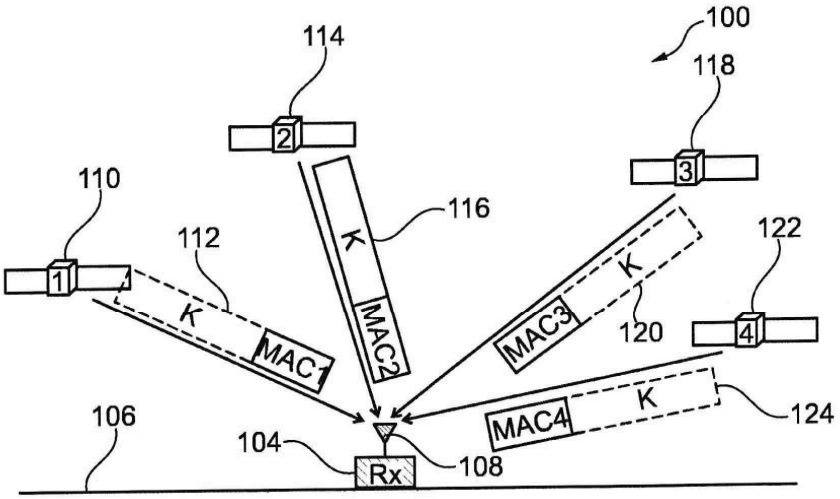
100
114
118
110
116
112
122
K
MAC1
MAC2
MAC3
MAC4
120
124
106
104
108
Rx
1
2
3
4

Fig. 1

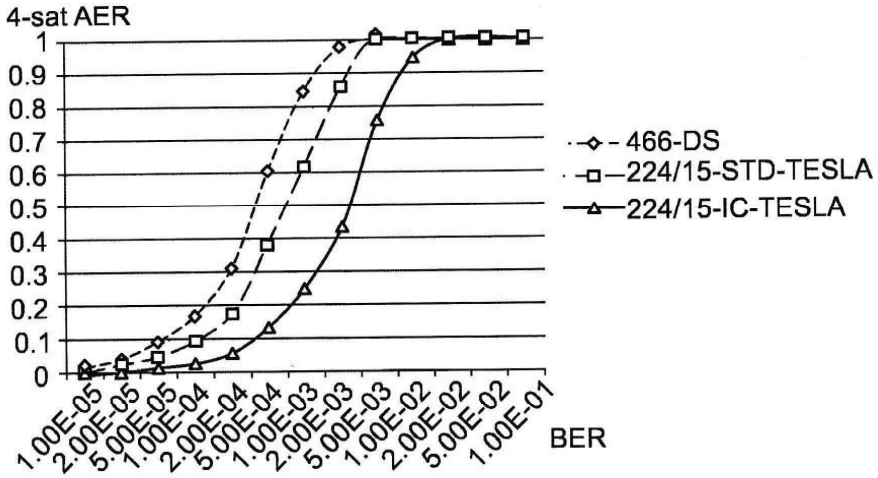
4-sat AER
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
1.00E-05
2.00E-05
5.00E-05
1.00E-04
2.00E-04
5.00E-04
1.00E-03
2.00E-03
5.00E-03
1.00E-02
2.00E-02
5.00E-02
1.00E-01
BER
466-DS
224/15-STD-TESLA
224/15-IC-TESLA

Fig. 2

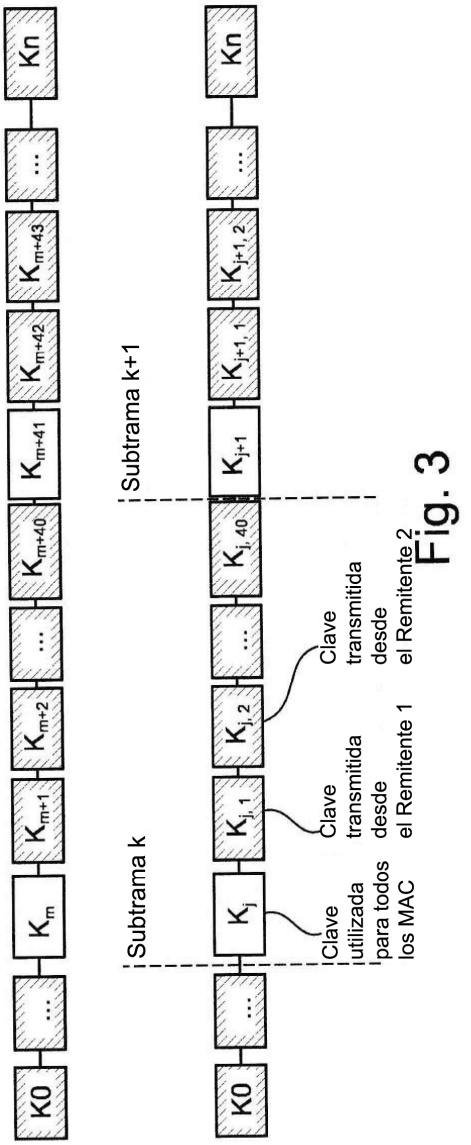
K0
...
Km
Km+1
Km+2
...
Km+40
Km+41
Km+42
Km+43
...
Kn
Subtrama k
Subtrama k+1
Kj
Kj, 1
Kj, 2
...
Kj, 40
Kj+1
Kj+1, 1
Kj+1, 2
...
Kn
Clave utilizada para todos los MAC
Clave transmitida desde el Remitente 1
Clave transmitida desde el Remitente 2

Fig. 3

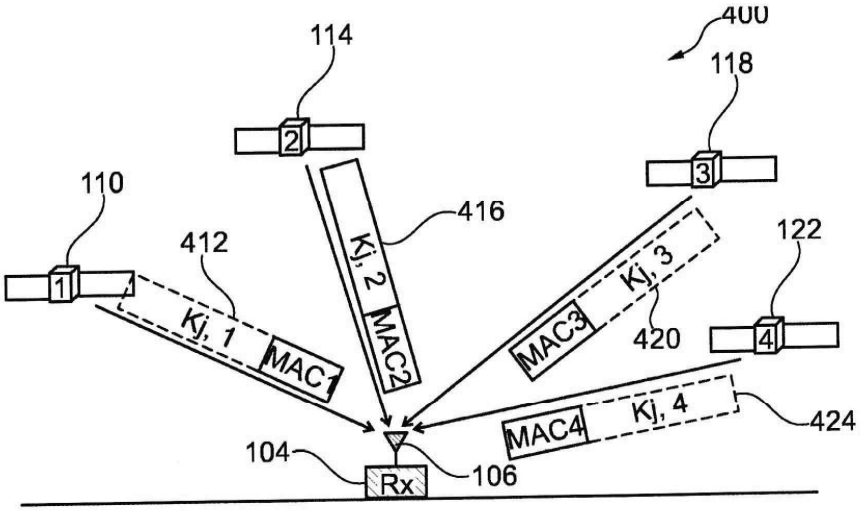

Fig. 4

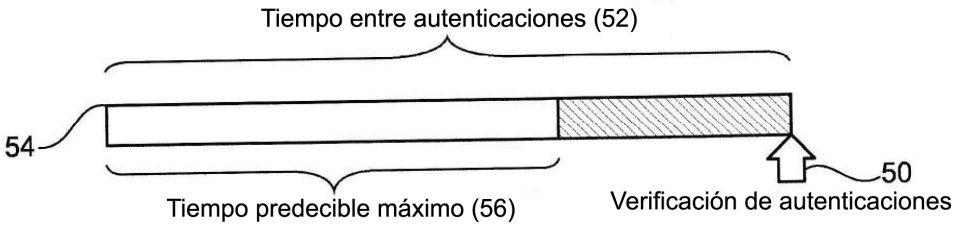

Fig. 5

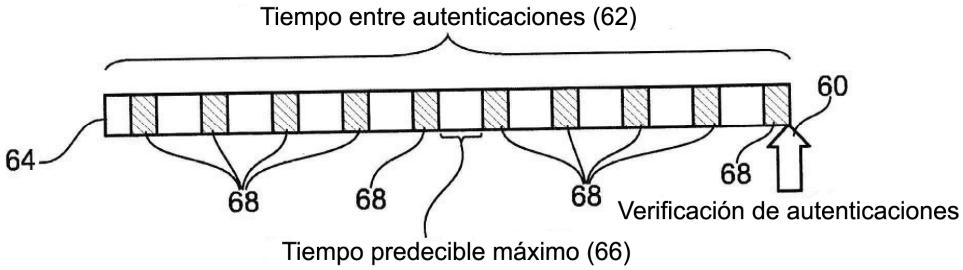

Fig. 6