(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 644 799**

(51) Int. CI.:

***G01S 19/21*** (2010.01)
***G01S 19/09*** (2010.01)
***H04W 12/08*** (2009.01)
***H04W 12/12*** (2009.01)
*H04W 12/10* (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **05.09.2012 PCT/US2012/053810**

(87) Fecha y número de publicación internacional: **14.03.2013 WO13036541**

(96) Fecha de presentación y número de la solicitud europea: **05.09.2012 E 12772568 (7)**

(97) Fecha y número de publicación de la concesión europea: **26.07.2017 EP 2753955**

(54) Título: **Autenticación basada en bits aleatorios de mensajes de navegación satelital**

(30) Prioridad:

**05.09.2011 US 201161531046 P**
**04.09.2012 US 201213603316**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**30.11.2017**

(73) Titular/es:

**THE BOEING COMPANY (100.0%)**
**100 North Riverside Plaza**
**Chicago, IL 60606-1596, US**

(72) Inventor/es:

**TROY, JAMES J. y**
**LEA, SCOTT W.**

(74) Agente/Representante:

**CARVAJAL Y URQUIJO, Isabel**

## DESCRIPCIÓN

Autenticación basada en bits aleatorios de mensajes de navegación satelital

Campo

Las formas de realización de la presente divulgación se refieren en general a la comunicación radioeléctrica y los sistemas de navegación. Más particularmente, se refieren a sistemas satelitales que validan ubicaciones o posiciones globales.

Antecedentes

Puede perderse una fracción significativa de la potencia de un componente secreto en una señal satelital de navegación, tal como una señal del sistema satelital de navegación global (GNSS, por su sigla inglesa), cuando dicha señal pasa a través de los filtros pasa banda que utiliza un dispositivo de cliente GNSS (receptor). La pérdida de potencia degrada el desempeño en los entornos de baja proporción de señal a ruido (SNR, por su sigla inglesa). El desempeño degradado puede impedir o minimizar la capacidad del sistema de autenticación de validar como de buena fe un cálculo o una declaración basados en una posición global.

La Patente de Estados Unidos No. US 2010/0134352 divulga un sistema y método para protegerse contra datos de medición a-GNSS falsificados. La información puede transmitirse a un dispositivo inalámbrico, e incluye una solicitud de que éste proporcione a un sistema verificador de ubicación una porción de un mensaje de datos de navegación proveniente de uno o más satélites. Pueden recibirse del dispositivo inalámbrico una o más mediciones satelitales y la porción del mensaje de datos de navegación. Puede establecerse que el mensaje de datos de navegación sea una función de información de una red de referencia. El mensaje de datos de navegación determinado se compara después con la porción recibida del mensaje de datos de navegación para verificar así si se ha falsificado cualquiera de una o más mediciones satelitales transmitidas por el dispositivo.

Síntesis

Se presentan un sistema y métodos para la autenticación de ubicaciones. Se sincroniza un subconjunto de señales de navegación entrantes demoduladas por servidor con las tramas de bits de cliente para proporcionar las tramas de bits de servidor sincronizadas. Se calcula una función de las tramas de bits de cliente para proporcionar un conjunto de signaturas de cliente. Se calcula una función de las tramas de bits de servidor sincronizadas para proporcionar un conjunto de signaturas de servidor. Se comparan el conjunto de signaturas de cliente y el conjunto de signaturas de servidor, se calcula un resultado y, en base a él, se autentica la ubicación del dispositivo de cliente.

De esa manera, las formas de realización de la divulgación proporcionan un sistema que posibilita la autenticación de ubicaciones de los dispositivos de cliente situados en entornos de baja proporción de señal a ruido (SNR), tales como el interior de edificios y el centro de una ciudad.

En una forma de realización, un método de autenticación de ubicaciones demodula una pluralidad de señales de navegación satelital que se reciben en una antena de servidor provenientes de los satélites de navegación, respectivamente, para proporcionar una pluralidad de señales de navegación entrantes demoduladas por servidor y selecciona un subconjunto de ellas sincronizadas con una pluralidad de tramas de bits de cliente para proporcionar una pluralidad de tramas de bits de servidor sincronizadas. Asimismo, el método calcula una función de las tramas de bits de servidor sincronizadas para reducir el tamaño de una combinación de la pluralidad de tales tramas y proveer un conjunto de signaturas de servidor. El método además demodula una pluralidad de señales de navegación que se reciben en el dispositivo de cliente provenientes de una pluralidad de satélites de navegación, respectivamente, para proveer las señales de navegación entrantes demoduladas por cliente, y selecciona un subconjunto de ellas con el objeto de proporcionar la pluralidad de tramas de bits de cliente. Asimismo, el método calcula la función de la pluralidad de tramas de bits de cliente para reducir el tamaño de una combinación de las mismas y proporcionar el conjunto de signaturas de cliente. El método además recibe de parte del servidor el conjunto de signaturas de cliente y lo compara con el conjunto de signaturas de servidor para obtener un resultado en base al cual autentica la ubicación del dispositivo de cliente.

En otra forma de realización, un sistema de autenticación de ubicaciones comprende un módulo selector de tramas de datos de servidor, un módulo de operación de datos de servidor, un módulo de correlación de servidor y un módulo de autenticación. El módulo selector de tramas de datos de servidor elige un subconjunto de señales de navegación entrantes demoduladas por servidor, que se sincronizan con una pluralidad de tramas de bits de cliente a fin de brindar una pluralidad de tramas de bits de servidor sincronizadas. El módulo de operación de datos de servidor calcula una función de las tramas de bits de servidor sincronizadas para reducir el tamaño de una combinación de la pluralidad de ellas y proporcionar un conjunto de signaturas de servidor. El módulo de correlación de servidor recibe el conjunto de signaturas de cliente y lo compara con el conjunto de signaturas de servidor para obtener un resultado de esa

comparación. El módulo de autenticación verifica una ubicación de un dispositivo de cliente en base a dicho resultado. El sistema además comprende un módulo selector de tramas de datos de cliente, que es operable para seleccionar un subconjunto de una pluralidad de señales de navegación entrantes demoduladas por cliente a fin de proveer las tramas de bits de cliente. El sistema además comprende un módulo de operación de datos de cliente, que es operable para calcular la función de la pluralidad de tramas de bits de cliente y reducir el tamaño de una combinación de la pluralidad de tales tramas con el objeto de proporcionar el conjunto de signaturas de cliente. El sistema además comprende un módulo de demodulación de cliente, que es operable para recibir una pluralidad de señales de navegación satelital que se reciben en el dispositivo de cliente, provenientes de una pluralidad de satélites de navegación, respectivamente; y demodula la pluralidad de las mencionadas señales para proporcionar una pluralidad de señales de navegación entrantes demoduladas por cliente. El sistema además comprende un módulo de demodulación de servidor, que es operable para recibir una pluralidad de señales de navegación satelital que llegan al receptor del servidor provenientes de los satélites de navegación, respectivamente; y las demodula para proporcionar señales de navegación entrantes demoduladas por servidor.

En un ejemplo, un medio de almacenamiento legible por computadora no transitorio comprende instrucciones ejecutables por computadora para la autenticación de ubicaciones. Las instrucciones ejecutables por computadora seleccionan un subconjunto de señales de navegación entrantes demoduladas por cliente para proveer las tramas de bits de cliente. Las instrucciones ejecutables por computadora además calculan una función de las tramas de bits de cliente para proporcionar un conjunto de signaturas de cliente. Las instrucciones ejecutables por computadora además transmiten el conjunto de signaturas de cliente a un servidor de autenticación a los efectos de autenticar la ubicación de un dispositivo de cliente.

Esta síntesis se brinda para presentar de forma simplificada una selección de conceptos, que se exponen más adelante pormenorizados en la descripción detallada. Esta síntesis no pretende identificar características clave o esenciales del asunto reivindicado ni ser usada como ayuda para determinar el alcance de dicho asunto.

Breve descripción de las figuras

Puede derivarse una comprensión más cabal de las formas de realización de la presente divulgación haciendo referencia a la descripción detallada y las reivindicaciones, si se las considera conjuntamente con las figuras siguientes donde, en todas ellas, los números iguales señalan elementos similares. Las figuras se proporcionan para facilitar la comprensión de la divulgación sin limitar su amplitud, alcance, escala o aplicabilidad. Las figuras no están trazadas necesariamente a escala.

La FIGURA 1 es una ilustración de un entorno de comunicaciones inalámbricas ejemplificativo para autenticar una ubicación declarada en base a señales satelitales de navegación, de acuerdo con una forma de realización de la divulgación.

La FIGURA 2 es una ilustración de un diagrama de bloques funcionales simplificado ejemplificativo de un receptor satelital de navegación.

La FIGURA 3 es una ilustración de un entorno de comunicaciones inalámbricas ejemplificativo que muestra modos en que los entornos de interiores de edificios y centros de ciudad pueden atenuar las señales satelitales de navegación.

La FIGURA 4 es una ilustración de un diagrama ejemplificativo que muestra un mensaje de navegación de un satélite de navegación.

La FIGURA 5 es una ilustración de un diagrama ejemplificativo que muestra la superposición de mensajes de navegación provenientes de tres satélites de navegación.

La FIGURA 6 es una ilustración de un diagrama ejemplificativo que muestra que, de acuerdo con una forma de realización de la divulgación, los mensajes de navegación provenientes de los tres satélites de navegación expuestos en la FIGURA 5 se muestrean durante un período apenas mayor que un bit.

La FIGURA 7 es una ilustración de un diagrama ejemplificativo que muestra que, de acuerdo con una forma de realización de la divulgación, los mensajes de navegación provenientes de los tres satélites expuestos en la FIGURA 5 se muestrean durante un período de varios bits.

La FIGURA 8 es una ilustración de un diagrama ejemplificativo que muestra una cantidad de signaturas de ubicación que pueden proporcionarse, de acuerdo con dos formas de realización de la divulgación.

La FIGURA 9 es una ilustración de un diagrama de bloques funcionales ejemplificativo de un sistema de autenticación, de acuerdo con una forma de realización de la divulgación.

La FIGURA 10 es una ilustración de un diagrama de bloques funcionales ejemplificativo de un sistema de autenticación, de acuerdo con una forma de realización de la divulgación.

La FIGURA 11 es una ilustración de un diagrama de bloques funcionales ejemplificativo de un sistema de autenticación, de acuerdo con una forma de realización de la divulgación.

La FIGURA 12 es una ilustración de un diagrama de bloques funcionales ejemplificativo de un sistema de autenticación, de acuerdo con una forma de realización de la divulgación.

La FIGURA 13 es una ilustración de un diagrama de flujo ejemplificativo que muestra un proceso de autenticación, de acuerdo con una forma de realización de la divulgación.

La FIGURA 14 es una ilustración de un diagrama de flujo ejemplificativo que muestra un proceso de autenticación, de acuerdo con una forma de realización de la divulgación.

Descripción detallada

La siguiente descripción detallada es de carácter ejemplificativo y no pretende limitar la divulgación o la aplicación y usos de sus formas de realización. Las descripciones de dispositivos, técnicas y aplicaciones que son específicos sólo se dan como ejemplos. Por otra parte, no hay ninguna intención de ceñirse a ninguna teoría expresada o implícita ya expuesta o que se exponga en el campo, los antecedentes y la síntesis anteriores o bien, en la siguiente descripción detallada. A la presente divulgación debe otorgársele el alcance coherente con las reivindicaciones y no limitarla a los ejemplos aquí descritos y mostrados. Las formas de realización de la divulgación pueden describirse en la presente en términos de componentes de bloques funcionales y/o diversos pasos de procesamiento. Debe apreciarse que tales componentes de bloques pueden plasmarse mediante una variada cantidad de componentes de hardware, software y/o firmware configurados para ejecutar las funciones especificadas. En aras de la brevedad, en la presente pueden no describirse en detalle técnicas y componentes convencionales relacionados con sistemas de comunicaciones, protocolos de red, sistemas de posicionamiento global y otros aspectos funcionales de los sistemas (y los componentes operativos individuales de los mismos).

Las formas de realización de la divulgación se describen aquí en el contexto de una aplicación no limitativa, a saber, un sistema de autenticación para una aplicación telefónica móvil. No obstante, las formas de realización de la divulgación, no están limitadas a tales aplicaciones telefónicas móviles, y las técnicas que se describen en la presente también pueden utilizarse en otras aplicaciones. Por ejemplo, las formas de realización pueden ser aplicables en una computadora de escritorio, una computadora laptop o notebook, un iPad™, un iPod™, un procesador central, un servidor, un cliente o cualquier otro tipo de dispositivo de computación de uso especial o general, según convenga o sea apropiado para una determinada aplicación o entorno.

Como le resultará evidente a un conocedor común de la técnica tras leer esta descripción, los siguientes son ejemplos y formas de realización de la divulgación, las cuales no están limitadas a operar de acuerdo con esos ejemplos. Pueden utilizarse otras formas de realización e introducirse cambios sin apartarse del alcance de las formas de realización ejemplificativas de la presente divulgación. Las formas de realización de la divulgación proporcionan un sistema de autenticación con adecuada potencia de la señal recibida en el caso de una señal satelital de navegación que llega a un dispositivo de cliente (cliente) situado en un entorno de baja proporción de señal a ruido (SNR), tal como el interior de un edificio de ciudad.

La FIGURA 1 es una ilustración de un entorno de comunicaciones inalámbricas ejemplificativo 100 (entorno 100) para autenticar una ubicación declarada en base a señales satelitales de navegación, de acuerdo con una forma de realización de la divulgación. El entorno 100 puede comprender los satélites de navegación 102, 104 y 106, un cliente 108 que incluye un receptor satelital 200 (receptor satelital de navegación 200) y un servidor de autenticación 112 con un receptor satelital 200 (receptor satelital de navegación 200).

Cada uno de los satélites de navegación 102-106 puede comprender un satélite del sistema satelital de navegación global (GNSS), un satélite del sistema de posicionamiento global (GPS™), un satélite del sistema Globalnaya Navigatsionnaya Sputnikovaya (GLONASS™), un satélite del sistema de navegación BeiDou (COMPASS™), un satélite Galileo™ u otro satélite de navegación.

Las señales satelitales de navegación 116, 118 y 120 transmitidas desde los satélites de navegación 102, 104 y 106, respectivamente, pueden procesarse en el cliente 108 para establecer de él una velocidad, una hora y una ubicación 122. Sin embargo, en los sistemas existentes, las señales satelitales de navegación pueden falsificarse de tal manera que el cliente existente tal vez y/o informe acerca de una posición fraudulenta 124. La falsificación se está volviendo una preocupación general porque los satélites de navegación se usan cada vez más para sustentar transacciones de ubicación que tienen valor financiero o implicaciones para la seguridad de la vida.

Cada una de las señales satelitales de navegación 116-120 comprende una señal 130 a una frecuencia (frecuencia portadora), tal como una frecuencia GPS L1, que se usa como portadora (portadora en fase 130) para modular una señal de datos con un código de propagación, tal como un código de acceso múltiple por división de código (CDMA, por su sigla inglesa), comúnmente denominado código de grosor/captación (C/A, "Coarse/Acquisition") (el código de propagación de espectro 132). En el caso de un sistema GPS, el código C/A puede identificarse con diversos nombres, a saber, de grosor/captación ("Coarse/Acquisition"), de acceso transparente ("Clear/Access") y de acceso civil ("Civil/Access"). Cada uno de los satélites de navegación 102-106 transmite al menos otra señal que emplea la frecuencia portadora y se desplaza 90 grados (señal en cuadratura, que no se muestra). La al menos otra señal (segunda señal) es modulada por otro código, conocido como código cifrado "P(Y)" (que no se muestra). El código P(Y) es o bien un código de "precisión" (P), públicamente conocido, o un código cifrado “Y”. Muchos satélites GNSS usan el código Y, y por consiguiente, la señal transmitida resultante codificada con el código Y no puede ser usada por otra señal más que la que tenga un algoritmo de cifrado y una clave para el código Y.

Además, un mensaje de navegación 134 modula la difusión tanto del código (conocido) P como del código (desconocido) Y por parte de los satélites de navegación 102, 104, 106.

Por ejemplo, en las aplicaciones comerciales, se conoce públicamente el código C/A y, por consiguiente, un receptor satelital de navegación existente puede ser vulnerable al fraude. En los sistemas existentes, una parte hostil puede generar un facsímil de una o más señales satelitales que transmiten información incorrecta. Un receptor satelital de navegación existente en un dispositivo de cliente que acepta las señales fraudulentas puede ser burlado y calcular una posición incorrecta, tal como la parte hostil desea que lo haga. El fraude es infructuoso en los casos en que se usa el código Y, porque el mismo no se conoce públicamente, de manera que una parte hostil no puede crear una señal que parezca de buena fe.

Sin embargo, puede perderse una fracción significativa de potencia del componente de señal del código Y (secreto) cuando cada una de las señales satelitales de navegación 116-120 pasa a través de un filtro pasa banda que usa el receptor satelital de navegación 200 del cliente 108. La pérdida de potencia de señal puede degradar el desempeño del cliente 108 en los entornos de baja proporción de señal a ruido (SNR). La degradación puede reducir una capacidad del servidor de autenticación 112 en cuanto a brindar confianza de que son de buena fe un cálculo o declaración basados en una posición global. Las formas de realización de la divulgación proporcionan un medio para autenticar la ubicación 122 en base a la información aleatoria o pseudo aleatoria contenida en la difusión del mensaje de navegación 134 efectuada por los satélites de navegación 102, 104, 106 u otros transmisores de navegación. De ese modo se brinda una cobertura mejorada, donde pueden obstruirse las señales satelitales de navegación 116-120, en comparación con los métodos existentes.

El cliente 108 integra el receptor satelital de navegación 200 que está configurado para indicar su ubicación mediante rastreo, en base a la recepción del mensaje de navegación 134 de cada una de las señales satelitales de navegación 116-120, a través de las señales de navegación satelital de cliente recibidas del servidor 146 (señales de navegación recibidas por el cliente 146) por una antena de cliente 110. El cliente 108 está configurado para estimar los bits de datos de navegación 136 contenidos en el mensaje de navegación 134 de una multiplicidad de las señales de navegación recibidas por el cliente 146 para proveer tramas de bits de cliente 1030 (que comprenden los mensajes de navegación 502/504/506 demodulados a partir de las señales de navegación recibidas por el cliente 146, FIGURA 10). En una forma de realización, el cliente 108 calcula una función tal como un ”O” excluyente (XOR) 1008 (FIGURA 10) en todas las tramas de bits de cliente 1030 (es decir, provenientes de los satélites de navegación 102, 104, 106) para proporcionar un conjunto de signaturas de cliente 138 de una ubicación de cliente declarada respecto de la ubicación 122, como se explica más adelante con mayor detalle.

El cliente 108 puede admitir muchas aplicaciones de consumidor. Por ejemplo, muchas transacciones financieras utilizan teléfonos celulares como el cliente 108 situado en el interior de un edificio de ciudad. El cliente 108 puede comprender dispositivos de comunicaciones cableados o inalámbricos tales como, pero sin limitarse a ello, una computadora de escritorio, una laptop o computadora notebook, un iPod™, una central de procesamiento, un servidor u otro tipo de dispositivo de computación de uso especial o general que comprende un receptor, tal como el receptor satelital de navegación 200, apto para recibir las señales de navegación que se comunican al cliente 146 y puede convenir o ser apropiado para una determinada aplicación o entorno.

El servidor de autenticación 112 está configurado para recibir o estimar (calcular) el conjunto de signaturas de cliente 138 de la ubicación 122. El servidor de autenticación 112 puede recibir el conjunto de signaturas de cliente 138 por medio de un enlace de comunicación cableado 126, un canal de comunicaciones inalámbrico 128, una combinación y ambos o bien, estimar (calcular) localmente el conjunto de signaturas de cliente 138 en el servidor de autenticación 112. El servidor de autenticación 112 comprende el receptor satelital de navegación 200 y también está configurado para recibir el mensaje de navegación 134 (los mensajes de navegación) de las señales satelitales de navegación 116-120 a través de las señales de navegación recibidas por el servidor 148 por una antena de servidor 114. El servidor de autenticación 112 también estima los bits de datos de navegación 136 contenidos en el mensaje de navegación 134 de las señales de navegación recibidas por el servidor 148, que se sincronizan con las tramas de bits de cliente 1030 para proporcionar las tramas de bits de servidor sincronizadas 1032 (FIGURA 10). El servidor de autenticación

112 calcula una función de las tramas de bits de servidor sincronizadas 1032 para dar un conjunto de signaturas de servidor 140, tal como se explica más adelante con mayor detalle. En una forma de realización, un módulo de correlación de servidor 142 compara el conjunto de signaturas de cliente 138 y el conjunto de signaturas de servidor 140 para generar un mensaje de decisión de autenticación 144. El servidor de autenticación 112 determina la validez de una ubicación declarada respecto de la ubicación 122 del cliente 108, en base al mensaje de navegación 134, y genera el mensaje de decisión de autenticación 144 que indica la validez o no validez de la ubicación declarada. La validez indica que hay una exactitud de que el cliente 108 está situado en la ubicación declarada y la no validez indica que no es aceptable la exactitud y/o certeza de que el cliente 108 está situado en la ubicación declarada.

Muchas transacciones financieras utilizan teléfonos celulares como el cliente 108 en un entorno "interior" o de "centro de una ciudad", donde ocurren en plataformas que son de bajo costo y operan en entornos de señales obstruidas. Pueden ser importantes dos criterios para un diseño de tal sistema de autenticación costo-efectivo basado en satélite de navegación. Primero, deben estar disponibles datos provenientes del receptor satelital de navegación 200 incluido en el teléfono celular. Segundo, el sistema de autenticación basado en satélite de navegación debe compensar las señales de navegación recibidas por el cliente 146 que se esperan, donde se congregan los usuarios de teléfonos celulares por ejemplo, "interior de edificios" y "centro de una ciudad". El primer criterio se refleja en la FIGURA 2, que muestra pasos básicos de procesamiento de señales en el receptor satelital de navegación 200. El segundo criterio respecto de un sistema de autenticación basado en satélite de navegación se ilustra en la FIGURA 3. La FIGURA 2 es una ilustración de un diagrama de bloques funcionales simplificado que es ejemplificativo del receptor satelital de navegación 200 mostrado en la FIGURA 1. El receptor satelital de navegación 200 puede comprender, por ejemplo pero sin limitación, un receptor GPS u otro receptor satelital. Tal como se muestra en la FIGURA 2, el receptor satelital de navegación 200 recibe señales de frecuencia radioeléctrica tal como las señales de navegación satelital de cliente recibidas del servidor 146 en la antena de cliente 110. El receptor satelital de navegación 200 después demodula las señales de navegación recibidas por el cliente 146 a partir de las señales satelitales de navegación 116-120 que se reciben en el cliente 108 provenientes de los satélites de navegación 102-108, respectivamente. El receptor satelital de navegación 200 demodula las señales de navegación recibidas por el cliente 146 a partir de las señales satelitales de navegación 116-120 recibidas en el cliente 108, cuando el conversor descendente 202 convierte hacia abajo las señales 146, de radiofrecuencia (RF) a banda base, y el filtro pasa banda efectúa el filtrado pasa banda de las señales de navegación recibidas por el cliente y convertidas hacia abajo 218.

Como ya se mencionó, puede perderse una fracción significativa de la potencia del componente de señal de código Y secreto en las señales satelitales de navegación 116-120 o las señales de navegación recibidas por el cliente 146, cuando éstas pasan a través del filtro pasa banda 204. En el caso del GPS, las señales moduladas por las señales de código Y secreto tienen un ancho de banda equivalente a ruido de 10 MHz, en tanto que el ancho de banda equivalente a ruido de las señales de código C/A civil (código C/A) es de aproximadamente 1 MHz. El receptor satelital de navegación 200 del cliente 108, tal como teléfonos celulares utiliza las señales de código C/A civil, no las señales del código Y secreto. Por ende, el filtro pasa banda 204 de los teléfonos celulares en general tiene un ancho de banda de sólo unos pocos MHz y así se pierde una apreciable fracción de potencia de las señales que comprenden los códigos Y secretos. La pérdida de potencia de señal degrada el desempeño en los entornos de baja proporción de señal a ruido (SNR). El desempeño degradado puede impedir o minimizar una capacidad del servidor de autenticación 112 de validar que es de buena fe un cálculo o una declaración basada en una posición global.

El receptor satelital de navegación 200 después convierte las señales de navegación recibidas por el cliente y filtradas por pasa banda 220 a partir de las señales convertidas de analógicas a digitales por un respectivo conversor de analógico a digital (ADC, por su sigla inglesa) 206 para proporcionar señales digitales de navegación recibidas por el cliente 222. El receptor satelital de navegación 200 después elimina mediante un borrado de código 210 el código de propagación de espectro 132 (código C/A) de las señales digitales de navegación recibidas por el cliente 222. El receptor satelital de navegación 200 después elimina mediante un borrado de portadora 212 la portadora en fase 130 de las señales digitales de navegación recibidas por el cliente 222 para proporcionar señales de navegación recibidas por el cliente que estén limpias 224.

El receptor satelital de navegación 200 después correlaciona las señales limpias de navegación recibidas por el cliente que son digitales 224 con una réplica de esas señales en el cliente 108 usando un módulo de correlación 214 para estimar la ubicación 122, una velocidad y un desplazamiento temporal del cliente 108 en una salida 216 basada en un pico de correlación 226. La ubicación 122 puede calcularse usando más que una cantidad mínima de satélites (4 satélites para calcular la latitud, longitud, elevación y hora del satélite de navegación/GPS).

La FIGURA 3 es una ilustración de un entorno de comunicaciones inalámbricas ejemplificativo (entorno 300) que muestra que los entornos de interior de edificios y centro de una ciudad pueden atenuar las señales satelitales de navegación 116-120. Una potencia de señal recibida nominal 304 de la señal GPS recibida es de aproximadamente -130 dBm (o 10E -16 vatios). El receptor satelital de navegación 200 del cliente 108 a cielo abierto puede esperar la potencia de señal recibida nominal 304. Sin embargo, el cliente 108, tal como un teléfono celular puede operar en el interior de un edificio de ciudad, donde una potencia de señal recibida atenuada 302 cae a -140 dBm o -160 dBm o es incluso más débil. Por eso, el servidor de autenticación 112 debe operar a esos niveles más bajos de potencia de señal recibida atenuada 302.

La FIGURA 4 es una ilustración de un diagrama ejemplificativo 400 que muestra una estructura de señales de los mensajes de navegación 134 del satélite de navegación 102. Los mensajes de navegación 134 modulan tanto la difusión del código conocido (P) como la del desconocido (Y) (que no se muestra) que efectúa por ejemplo el satélite de navegación 102, a través de la señal del satélite de navegación 116. Las formas de realización de la divulgación se basan en la información aleatoria (o pseudo aleatoria) contenida en la difusión de los mensajes de navegación 134 efectuada por el satélite de navegación 102 u otros transmisores de navegación. En el caso del sistema GNSS, El o los mensajes de navegación 134 se difunden a entre 50 y 1000 bits por segundo (bps) y de ese modo se diferencian de códigos de propagación de espectro tales como el código desconocido (Y) (que no se muestra) y el código C/A (código de propagación de código 132) que también modula las señales satelitales de navegación 116 provenientes del satélite de navegación 102. Los mensajes de navegación 134 varían lentamente a 50-1000 bits por segundo en comparación con el código de propagación de espectro (subyacente) 132 a 1.023 Mcps (código C/A) o código de propagación de espectro a 10.23 Mcps (código Y, que no se muestra).

El o los mensajes de navegación 134 del satélite de navegación 102 comprenden información, tal como ubicación y hora de dicho satélite, una ubicación común de los satélites de navegación 104, 106 diferentes del satélite 102 y otra información. A diferencia del código desconocido o secreto (Y), el filtro pasa banda 204 (FIGURA 2) no atenúa los mensajes de navegación 134 que pasan por allí cuando lo hace lo hace la señal del satélite de navegación 116. Así, usar los mensajes de navegación 134 en los entornos de baja proporción de señal a ruido (SNR) brinda confianza respecto de un sistema de autenticación basado en satélite para validar que es de buena fe un cálculo o una declaración basada en una posición global.

En comparación con los métodos existentes, las formas de realización de la divulgación proporcionan mejor cobertura en el interior de edificios de una ciudad, porque el mensaje de navegación 134 se superpone a la difusión tanto de los códigos C/A civil como de los códigos Y secreto que efectúan los satélites de navegación 102. Como ya se explicó, se pierde una fracción significativa de potencia de las señales del componente de código Y secreto cuando la señal del satélite de navegación 116 pasa a través del filtro pasa banda 204. En el caso de GPS, las señales moduladas por las señales del código Y secreto tienen un ancho de banda equivalente a ruido de 10 MHz, en tanto que el ancho de banda equivalente a ruido de las señales de código C/A civil es de 1 MHz. El receptor satelital de navegación 200 del cliente 108 utiliza las señales de código C/A civil, tal como un teléfono celular, no en general las señales del código Y secreto. Por ende, el filtro pasa banda 204 (por ejemplo, del teléfono celular) tiene anchos de banda de sólo unos pocos MHz, y así se pierde una apreciable fracción de potencia de señal de las señales del código Y secreto.

En comparación con los métodos existentes, las formas de realización de la divulgación mejoran significativamente la cobertura en el interior de edificios y en el centro de una ciudad del sistema de autenticación satelital basado en el receptor satelital de navegación 200 integrado al cliente 108, tal como un teléfono celular, y otras plataformas relativamente económicas. Las formas de realización logran esta ganancia usando la naturaleza aleatoria (o pseudo aleatoria) de los bits de datos de navegación 136 del o de los mensajes de navegación 134, y no la naturaleza aleatorio (o pseudo aleatoria) de las señales del código Y secreto. El mensaje de navegación 134 modula el código C/A civil y los códigos Y secreto, y así no se incurre en la precedentemente mencionada pérdida por el filtro pasa banda. Este ahorro de potencia puede ser de aproximadamente 6 dB.

Además, una capacidad de mensaje (por ejemplo, cantidad de bits de datos) ocupada por una signatura de ubicación (por ejemplo, 138 en la FIGURA 1 y 606 en la FIGURA 6) en base al código C/A civil es aproximadamente diez veces más pequeña es aproximadamente diez veces más pequeña que la capacidad de mensaje ocupada por una signatura de ubicación que deba incluir el ancho de banda de las señales del código Y secreto (código Y). Por ejemplo, si una signatura de ubicación que incluye un ancho de banda de las señales del código Y secreto ocupa aproximadamente 24 kBytes, el conjunto de signaturas de ubicación de cliente 138/606, de acuerdo con las formas de realización de la divulgación, puede ocupar aproximadamente 2,4 KBytes. Como alternativa, las formas de realización pueden poblar un mensaje de 24 KByte y usar una mayor longitud de bits de datos para mejorar el desempeño en entornos de baja proporción de señal a ruido (SNR).

Los mensajes de navegación 134 que modulan el código de propagación de espectro 132 varían entre a 50 y 1000 bits por segundo. Más aún, gran parte del mensaje de navegación 134 puede predecirse de antemano. Una baja velocidad y predictibilidad sugiere que una corriente de datos del mensaje de navegación 134 puede ser una fuente deficiente de signaturas de autenticación. Sin embargo, ciertas porciones del mensaje de navegación 134 pueden ser difíciles de predecir. Más aún, las formas de realización derivan una signatura de autenticación en base a una superposición del mensaje de navegación 134 en varios, preferentemente muchos, satélites tales como los satélites de navegación 102, 104 y 106.

La FIGURA 5 es una ilustración de un diagrama ejemplificativo 500 que muestra una superposición de mensajes de navegación 502, 504 y 506 provenientes de los satélites de navegación 102, 104 y 106, respectivamente. Tal como se muestra en la FIGURA 5, tal superposición no tiene una estructura compleja, porque los límites de los bits de navegación 508, 510 y 512 de cada uno de tales bits 520, 522 y 524 de los mensajes de navegación 502, 504 y 506 se desplazan en el tiempo 514 de satélite a satélite. El desplazamiento en el tiempo 514 de satélite a satélite puede ocurrir porque, por ejemplo, puede diferir apreciablemente un rango de cada uno de los satélites de navegación 102-

106 al cliente 108. Puede estimarse un desplazamiento en tiempo de satélite a satélite, tal como el 516, usando diversas técnicas. Una duración de bits de navegación 518 de los bits 520, 522 y 524 de los mensajes de navegación 502, 504 y 506 puede comprender, por ejemplo, 20 ms ~= 6000 km/velocidad de la luz.

La FIGURA 6 es una ilustración de un diagrama ejemplificativo 600 que muestra que los mensajes de navegación 502-506 provenientes de los satélites de navegación 102-106 mostrados en la FIGURA 5, se muestrean durante un período apenas mayor que un bit de navegación 518 (por ejemplo, 20 ms en la FIGURA 5), de acuerdo con una forma de realización de la divulgación. Una ventana de muestreo 602 de, por ejemplo, 25 ms es apenas más larga que la duración de bit de navegación 518 (por ejemplo, 20 ms) en un bit de navegación de cada uno de los mensajes de navegación 502-506. Una duración de la ventana de muestreo 602 más prolongada que la duración de bits de navegación 518 puede garantizar que la ventana de muestreo 602 traspase los límites de bits de navegación, tales como los límites 508, 510 y 512 mostrados en la FIGURA 5. Por ejemplo, pueden existir cuatro posibles secuencias para cada uno de los satélites de navegación 102, 104 y 106 que representan dos bits de navegación dentro de la ventana de muestreo 602 para cada uno de los satélites de navegación 102-106. Se distinguen por dos polaridades de bits "++", "+-", "-+" y "--". Si hay K satélites a la vista, una cardinalidad de una signatura de ubicación 606 que comprende todas las combinaciones de satélites respecto de un límite traspasado de bits de navegación es 22K. Si la ventana de muestreo 602 es más larga para cubrir una cantidad más grande de límites de bits de navegación, aumenta rápidamente una cardinalidad del conjunto de signaturas de ubicación 606 (por ejemplo, para 3 límites de bits de navegación 24K, para 4 límites de bits de navegación 25K, etc.)

En una forma de realización, el conjunto de signaturas de ubicación 606 comprende un ”O” excluyente (XOR) de series de bits de muestra, tales como las tramas de bits de muestra 616, 618 y 620 que comprenden los bits de datos de navegación 136 (por ejemplo, los bits de navegación 520, 522 y 524) de cada uno de los mensajes de navegación 502-506 de los satélites de navegación 102-106, respectivamente. Por ejemplo, las columnas de bits de muestra 608, 610, 612 y 614 de las tramas de bits de muestra 616, 618 y 620 comprenden un XOR para producir el conjunto de signaturas de ubicación 606. Cualquier función adecuada, tal como por ejemplo pero sin limitación, una función XOR lógica, una función OR lógica, una función AND lógica u otra función adecuada pueden producir el conjunto de signaturas de ubicación 606. En el cliente 108, las tramas de bits de muestra 616, 618 y 620 comprenden las tramas de bits de cliente 1030 (FIGURA 10), y el conjunto de signaturas de ubicación 606 comprende el conjunto de signaturas de cliente 138. En el servidor de autenticación 112, las tramas de bits de muestra 616, 618 y 620 comprenden tramas de bits sincronizadas por servidor 1032 (FIGURA 10), y el conjunto de signaturas de ubicación 606 comprende el conjunto de signaturas de servidor 140.

De ese modo, se reduce el tamaño del conjunto de signaturas de ubicación 606, a partir del tamaño de una combinación de las tramas de bits de muestra 616, 618 y 620. Si la ventana de muestreo 602 se elige para traspasar un límite de bits de navegación, el conjunto de signaturas de ubicación 606 que resulta de un XOR tiene una cardinalidad de 2K+1. Tal como se muestra en la Tabla 604 (N = K+1), la cardinalidad 2K+1 para XOR crece mucho más lentamente que la cardinalidad 22K (es decir, 22K = 4K) para todas las combinaciones de satélites respecto de un límite de bits de navegación. Por eso, la cardinalidad de un XOR de límites de bits de navegación satelital crece mucho más lentamente que la cardinalidad de todas las combinaciones de límites de bits de navegación satelital.

La FIGURA 7 es una ilustración de un diagrama ejemplificativo 700 que muestra que los mensajes de navegación 502-506 de los satélites de navegación 102-106 mostrados en la FIGURA 5 se muestrean durante un período de varios bits, de acuerdo con una forma de realización de la divulgación. En la forma de realización mostrada en la FIGURA 7, un conjunto de signaturas de ubicación 706 comprende un ”O” excluyente (XOR) (por ejemplo, a lo largo de una columna de bits de muestra 708) de series de bits de muestra, tales como las tramas de bits de muestra 710, 712 y 714, que comprenden bits de datos de navegación 136 (por ejemplo, los bits de navegación 520, 522 y 524) de cada uno de los mensajes de navegación 502-506 provenientes de los satélites de navegación 102-106.

Por ejemplo, las columnas de bits de muestra (por ejemplo, la columna de bits de muestra 708) de las tramas de bits de muestra 710, 712 y 714 comprenden XOR para producir el conjunto de signaturas de ubicación 706. Cualquier función adecuada, tal como por ejemplo pero sin limitación, una función XOR lógica, una función OR lógica, una función AND lógica u otra función adecuada pueden producir el conjunto de signaturas de ubicación 706. En el cliente 108, las tramas de bits de muestra 710, 712 y 714 comprenden las tramas de bits de cliente 1030 (FIGURA 10), y el conjunto de signaturas de ubicación 706 comprende el conjunto de signaturas de cliente 138. En el servidor de autenticación 112, las tramas de bits de muestra 710, 712 y 714 comprenden las tramas de bits sincronizadas por servidor 1032 (FIGURA 10), y el conjunto de signaturas de ubicación 706 comprende el conjunto de signaturas de servidor 140.

Una ventana de muestreo 702 de 65 ms es apenas más larga que 60 ms (tres bits de navegación a 20 ms cada uno). En ese caso, la ventana de muestreo 702 traspasa al menos tres límites de bits, y la cardinalidad del conjunto de signaturas es 24K. En general, el conjunto de signaturas 138 contiene posibles signaturas de 2K Ceiling[T/TB], donde T es una duración de la ventana de muestreo 602/702, y TB es la duración de bits de navegación 518 (FIGURA 5) de un bit de navegación 520. Ese resultado se traza en la FIGURA 8. Tal como se muestra en la FIGURA 8, el conjunto de signaturas 802 crece muy rápidamente a medida que T se expande más allá de TB. La FIGURA 8 es una ilustración

de un diagrama ejemplificativo que muestra una cantidad de signaturas de ubicación 802/804 (conjunto de signaturas de ubicación 802/804, similar al conjunto de signaturas de cliente 138) proporcionada de acuerdo con dos formas de realización de la divulgación para K = 10 satélites a la vista. La FIGURA 8 muestra una cantidad de signaturas de ubicación versus la ventana de muestreo 602/702. El conjunto de signaturas 802 se traza en base a la siguiente relación: DataCombos[T_,TB, K_] := 2K Ceiling[T/TB]. Tal como se muestra en la FIGURA 8, el conjunto de signaturas 802 se agranda muy rápidamente a medida que T se expande más allá de TB, donde DataCombos representa el conjunto de signaturas de ubicación 802 como una función de T, TB y K.

El conjunto de signaturas 804 se traza para la cardinalidad XOR en base a la siguiente relación: XORCombos[T_,TB, K_] := 2K Floor[T/TB], donde XORCombos representa el conjunto de signaturas 804 como una función de T, TB y K. Por eso, la combinación XOR de los datos de signatura logra simplicidad a un posible precio de seguridad. El uso de la combinación XOR depende de la aplicación. Cada aplicación puede dictar si tal intercambio es apropiado en base por ejemplo a un nivel de seguridad deseado.

La FIGURA 9 es una ilustración de un diagrama de bloques funcionales ejemplificativo de un sistema de autenticación 900 (sistema 900) de acuerdo con una forma de realización de la divulgación. Algunas formas de realización del sistema 900 pueden comprender componentes y elementos adicionales configurados para admitir características operativas conocidas o convencionales que no es necesario describir en detalle en la presente. En la forma de realización mostrada en la FIGURA 9, puede usarse el sistema 900 para transmitir y recibir datos en el entorno de comunicaciones inalámbricas 100. El sistema 900 puede tener funciones, material y estructuras similares a las de las formas de realización mostradas en las FIGURAS 1-8. Por lo tanto, las características, funciones y elementos que son comunes pueden no describirse de manera redundante aquí.

El sistema 900 en general comprende el cliente 108 y el servidor de autenticación 112.

El cliente 108 puede comprender un módulo de demodulación de cliente 942 que incluye el convertidor descendente 202 y el ADC 206. El cliente 108 además puede comprender un módulo de datos de muestra 902, un módulo de cifrado 904, un módulo procesador de cliente 906 (módulo procesador 906) y un módulo de memoria de cliente 908 (módulo de memoria 908). El conjunto de signaturas de cliente 138 enviado del cliente 108 al servidor de autenticación 112 comprende la signatura RF/IF 208. La signatura RF/IF 208 incluye muestras de las señales de navegación recibidas por el cliente 146 (señal de radiofrecuencia (RF) o frecuencia intermedia (IF)) capturadas por la antena de cliente 110 en el cliente 108. El módulo de datos de muestra 902 muestrea las señales digitales de navegación recibidas por el cliente 222 en el ancho de banda del código C/A (BWCA, por su sigla inglesa) para proporcionar el conjunto de signaturas de cliente 138.

En la forma de realización mostrada en la FIGURA 9, el cliente 108 no necesita rastrear las señales de navegación recibidas por el cliente 146 ni demodular los bits de datos de navegación 136 del mensaje de navegación 134. Tal como se muestra en la FIGURA 9, el rastreo y demodulación de bits son implementados por un módulo de rastreo y demodulación de bits 928 ubicado en el servidor de autenticación 112.

El servidor de autenticación 112 puede comprender la antena de servidor 114, un módulo de demodulación de servidor 940, un módulo de decisión de autenticación 924, un módulo de rastreo y demodulación de bits 922, un módulo de descifrado 930, un módulo procesador de servidor 932 (módulo procesador 932) y un módulo de memoria de servidor 934 (módulo de memoria 934).

El módulo de demodulación de servidor 940 comprende un conversor descendente 912 configurado para implementar la conversión de RF a banda base, un filtro pasa banda 914 configurado para implementar un filtrado pasa banda, un ADC 916 configurado para implementar la conversión de analógico a digital, un borrado de código 918 configurado para eliminar el código de propagación de espectro 132 (código C/A) y un borrado de portadora 920 configurado para eliminar la portadora en fase 130.

El módulo de rastreo y demodulación de bits 922 está configurado para estimar los bits de datos de navegación 136 del mensaje de navegación 134 proveniente de las señales de navegación recibidas por el servidor 148 a fin de proporcionar el conjunto de signaturas de servidor 140.

El módulo de rastreo y demodulación de bits 928 está configurado para estimar los bits de datos de navegación 136 del mensaje de navegación 134 contenido en la signatura RF/IF 208 del cliente 108 a fin de proporcionar el conjunto de signaturas de cliente 138.

El módulo de decisión de autenticación 924 compara el conjunto de signaturas de cliente 138 y el conjunto de signaturas de servidor 140 para generar el mensaje de decisión de autenticación 144 en base a la comparación. Esa comparación puede hacerse satélite por satélite o en base a una variada cantidad de funciones intermedias, tales como por ejemplo pero sin limitación, una función XOR lógica, una función OR lógica, una función AND lógica u otra función adecuada para la operación del sistema 900, como se explica con mayor detalle en el contexto de la reseña

de la FIGURA 10, a continuación. El módulo de cifrado 904 y el módulo de descifrado 930 se usan para reforzar más el desempeño de autenticación desempeño. Una clave única de cliente (o signatura de dispositivo) se concatena con un conjunto de signaturas GNSS del cliente (conjunto de signaturas de cliente 138). La clave única de cliente puede basarse por ejemplo pero sin limitación, en criptografía simétrica (por ejemplo, norma de cifrado avanzado (AES, por su sigla inglesa)), criptografía asimétrica (por ejemplo, criptografía pública-privada), funciones físicamente no clonables (PUF, por su sigla inglesa) u otra criptografía. La clave única de cliente se usa para modificar el conjunto de signaturas de cliente 138 de manera que la verificación de posición en el servidor de autenticación 112 requiere una copia de la clave única de cliente. El módulo de descifrado 930 puede usarse para descifrar la comunicación del módulo de cifrado 904. Como alternativa, la clave única de cliente puede usarse para modificar el conjunto de signaturas de servidor 140 de la misma manera que el conjunto de signaturas de cliente 138. Así, la comparación y autenticación del conjunto de signaturas de cliente 138 con el conjunto de signaturas de servidor 140 en general sólo son satisfactorias si el cliente 108 y el servidor de autenticación 112 utilizan la misma clave única de cliente.

Una signatura de satélite de navegación puede considerar texto plano en el cifrado de un dispositivo. La signatura de satélite de navegación también puede contener información subyacente de alimentación directa de tiempo de velocidad de posición de cliente (PVTF, por su sigla inglesa) que también se verifica correlacionando la signatura de satélite de navegación capturada por el cliente 108 con los correspondientes datos en un receptor de referencia del satélite de navegación. Por eso, se genera un sistema de seguridad concatenado.

Los módulos procesadores 906/932 pueden implementarse o plasmarse con un procesador de uso general, una memoria direccionable a contenido, un procesador de señales digitales, un circuito integrado específico de aplicación, una matriz de puertas programables en campo, cualquier dispositivo lógico programable adecuado, puerta discreta o lógica de transistor, componentes de hardware discretos o cualquier combinación de lo anterior, que se haya diseñado para implementar las funciones descritas en la presente. De esa manera, un procesador puede plasmarse como un microprocesador, un controlador, un microcontrolador, una máquina de estado o similar.

Puede implementarse un procesador como una combinación de dispositivos de computación, por ejemplo una combinación de un procesador de señales digitales y un microprocesador, una pluralidad de microprocesadores, uno o más microprocesadores conjuntamente con un núcleo procesador de señales digitales o cualquier otra configuración tal. En la práctica, los módulos procesadores 906/934 comprenden lógica de procesamiento configurada para llevar a cabo las funciones, técnicas y tareas de procesamiento asociadas con la operación del sistema 900.

En particular, la lógica de procesamiento está configurada para admitir el método de autenticación descrito en la presente. Por ejemplo, el módulo procesador de cliente 906 puede estar adecuadamente configurado para enviar el conjunto de signaturas de cliente 138 del cliente 108 al servidor de autenticación 112 por una antena de transmisión de cliente (que no se muestra). Como otro ejemplo, el módulo procesador de servidor 932 puede estar adecuadamente configurado para enviar el mensaje de decisión de autenticación 144 a otro servidor o al cliente 108 por una antena de transmisión de servidor (que no se muestra). Por otra parte, pueden implementarse directamente en un módulo de hardware, firmware o software ejecutado por los pasos de un método o algoritmo descrito en conexión con las formas de realización divulgadas en la presente, en los módulos procesadores 906/932 o una combinación de ellos.

Los módulos de memoria 908/934 pueden plasmarse como un dispositivo de almacenamiento no volátil (memoria de semiconductores no volátil, dispositivo de disco duro, dispositivo de disco óptico y similar), un dispositivo de almacenamiento de acceso aleatorio (por ejemplo, SRAM, DRAM) o cualquier otra forma de medio de almacenamiento conocido en la técnica. El módulo de memoria 908/934 puede estar acoplado a los módulos procesadores 906/932, respectivamente, de manera que los mismos puedan leer la información de los módulos de memoria 908/934 o grabar en ellos.

Como ejemplo, el módulo procesador 906 y el módulo de memoria 908, el módulo procesador 932 y el módulo de memoria 934 pueden residir en sus respectivos circuitos ASIC. Los módulos de memoria 908 y 934 también pueden estar integrados en los módulos procesadores 906 y 932, respectivamente. En una forma de realización, el módulo de memoria 908/934 puede incluir una memoria caché para almacenar variables temporales u otra información intermedia durante la ejecución de instrucciones que deben ejecutar los módulos procesadores 906/932. Los módulos de memoria 908/934 también pueden incluir memoria no volátil para almacenar instrucciones que deban ejecutar los módulos procesadores 906/932.

Por ejemplo, los módulos de memoria 908/934 pueden incluir una base de datos de ubicaciones (que no se muestra) para almacenar el conjunto de signaturas de ubicación 802/804 y otros datos, de acuerdo con una forma de realización de la divulgación. Como otro ejemplo, el módulo de memoria de cliente 908 puede almacenar la réplica de las señales digitales de navegación recibidas por el cliente 222 en el cliente 108. Los expertos en la técnica comprenderán que los diversos bloques, módulos, circuitos y lógica de procesamiento que se describen en conexión con las formas de realización divulgadas en la presente pueden implementarse en hardware, software legible por computadora, firmware o una combinación de ellos. Para ilustrar claramente el carácter intercambiable y la compatibilidad del hardware, firmware y software, se describen diversos componentes, bloques, módulos, circuitos y pasos ilustrativos, en general en términos de su funcionalidad.

En algunas formas de realización, el sistema 900 puede comprender una variada cantidad de módulos procesadores, de módulos de memoria de módulos transmisores y de módulos receptores adecuados para su operación aquí descrita. El sistema 900 ilustrado representa una simple forma de realización que facilita la descripción. Esos y otros elementos del sistema 900 están interconectados entre sí, admitiendo la comunicación entre los diversos elementos del sistema 900. En una forma de realización, esos y otros elementos del sistema 900 pueden interconectarse entre sí por medio de un bus de comunicación de datos (que no se muestra).

Un módulo transmisor (que no se muestra) y un módulo receptor (que no se muestra) pueden estar ubicados en cada módulo procesador 906/932, acoplados a su respectiva antena compartida (que no se muestra). Aunque en un módulo simple sólo puede usarse una antena compartida, los módulos más sofisticados pueden estar provistos de múltiples antenas y/o de configuraciones de antena más complejas. Asimismo, aunque no se muestra en esta FIGURA 9, los expertos en la técnica reconocerán que un transmisor puede comunicarse con más de un receptor, y que múltiples transmisores pueden transmitir al mismo receptor. Que tal funcionalidad se implemente como hardware, firmware o software depende de la particular aplicación y las restricciones de diseño impuestas al sistema global. Quienes estén familiarizados con los conceptos descritos en la presente podrán implementar tal funcionalidad de manera adecuada en cada aplicación particular, sin que tal implementación deba interpretarse como desvío respecto del alcance de la presente invención.

La FIGURA 10 es una ilustración de un diagrama de bloques ejemplificativo que muestra un sistema de autenticación 1000 (sistema 1000), de acuerdo con una forma de realización de la divulgación. El sistema 1000 puede comprender un módulo selector de tramas de datos de cliente 1006, un módulo de operación de datos de cliente 1002, un módulo selector de tramas de datos de servidor 1010, y un módulo de operación de datos de servidor 1004.

El módulo selector de tramas de datos de cliente 1006 y el módulo de operación de datos de cliente 1002 pueden implementarse en el cliente 108 o en el servidor 112 como para recibir una pluralidad de señales de navegación recibidas demoduladas por cliente 1020, tales como los mensajes de navegación 502/504/506 como entrada, y generar el conjunto de signaturas de cliente 138 como salida. En las diversas formas de realización, el módulo selector de tramas de datos de cliente 1006 y/o el módulo de operación de datos de cliente 1002 pueden estar ubicados, por ejemplo, en el módulo de decisión de autenticación 924, el módulo de rastreo y demodulación de bits 928, un módulo selector de bits 1104 (FIGURA 11), un módulo de rastreo y demodulación de bits 1102 (FIGURA 12) u otra ubicación adecuada.

En las diversas formas de realización, el módulo selector de tramas de datos de servidor 1010 y/o el módulo de operación de datos de servidor 1004 pueden estar ubicados, por ejemplo, en el módulo de decisión de autenticación 924, el módulo de rastreo y demodulación de bits 922 u otra ubicación adecuada.

Por ejemplo pero sin limitación, las señales de navegación recibidas demoduladas por cliente 1020 pueden ser producidas por el módulo de rastreo y demodulación de bits 928. El módulo selector de tramas de datos de servidor 1010 y el módulo de operación de datos de servidor 1004 pueden implementarse en el módulo de decisión de autenticación 924 del sistema 900 como para recibir una pluralidad de señales de navegación recibidas demoduladas por servidor 1022, tales como los mensajes de navegación 502/504/506 como entrada, y generar el conjunto de signaturas de servidor 140 como salida. Por ejemplo pero sin limitación, el módulo de rastreo y demodulación de bits 922 puede producir y sincronizar las señales de navegación recibidas demoduladas por servidor 1022 con las señales de navegación recibidas demoduladas por cliente 1020.

El módulo selector de tramas de datos de cliente 1006 está configurado para seleccionar un subconjunto de las señales de navegación recibidas demoduladas por cliente 1020 y proporcionar una pluralidad de tramas de bits de cliente 1030. El subconjunto puede comprender, por ejemplo pero sin limitación, una subtrama, una selección aleatoria y una selección de bits entre los bits más dinámicos u otro subconjunto.

El módulo de operación de datos de cliente 1002 está configurado para calcular una función tal como un XOR 1008 de las tramas de bits de cliente 1030 a fin de proporcionar un conjunto de signaturas de cliente 138. La función puede comprender, por ejemplo pero sin limitación, una función XOR lógica, una función OR lógica, una función AND lógica u otra función adecuada.

El módulo selector de tramas de datos de servidor 1010 está configurado para seleccionar un subconjunto de las señales de navegación recibidas demoduladas por servidor 1022 sincronizadas con las tramas de bits de cliente 1030 a fin de proporcionar una pluralidad de tramas de bits sincronizadas por servidor 1032.

El módulo de operación de datos de servidor 1004 está configurado para calcular una función, tal como un XOR 1012 de las tramas de bits sincronizadas por servidor 1032 a fin de proporcionar un conjunto de signaturas de servidor 140.

El módulo de correlación de servidor 142 está configurado para comparar el conjunto de signaturas de cliente 138 y el conjunto de signaturas de servidor 140 a fin de proporcionar un resultado de comparación, tal como el mensaje de

decisión de autenticación 144. El módulo de decisión de autenticación 924 está configurado para generar el mensaje de decisión de autenticación 144 a fin de autenticar la ubicación 122 del cliente 108 en base al resultado de comparación. Esa comparación puede hacerse satélite por satélite o en base a una variada cantidad de funciones intermedias, tales como, por ejemplo pero sin limitación, una función XOR lógica, una función OR lógica, una función AND lógica u otra función adecuada.

La FIGURA 11 es una ilustración de un diagrama de bloques funcionales ejemplificativo de un sistema de autenticación 1100 (sistema 1100) de acuerdo con una forma de realización de la divulgación. El sistema 1100 puede tener funciones, material y estructuras similares a las de las formas de realización mostradas en las FIGURAS 1-9. Por lo tanto, las características, funciones y elementos comunes pueden no describirse aquí de manera redundante.

El sistema 1100 puede comprender el cliente 108 y el servidor de autenticación 112 (dispositivo servidor). El cliente 108 puede comprender un módulo de demodulación de cliente 1108 que incluye el convertidor descendente 202 configurado para implementar la conversión de RF a banda base, el filtro pasa banda 204 configurado para implementar un filtrado pasa banda, el ADC 206 configurado para implementar la conversión de analógico a digital, el borrado de código 210 configurado para eliminar el código de propagación de espectro 132 (código C/A) y el borrado de portadora 212 configurado para eliminar la portadora en fase 130. El cliente 108 también puede comprender el módulo de rastreo y demodulación de bits 1102 y el módulo selector de bits 1104.

El módulo selector de bits 1104 está configurado para elegir los bits de datos de navegación 136 de las porciones de los mensajes de navegación 134 que se sabe varían de manera impredecible. El módulo selector de bits 1104 identifica las tramas, subtramas y palabras del mensaje de navegación 134 y selecciona una multiplicidad de palabras que se sabe contienen datos variables. El módulo selector de bits 1104 evita los campos que cambian con poca frecuencia y que por eso pueden predecirse de inmediato. Por ejemplo, el módulo selector de bits 1104 evitaría los campos de datos que describen las efemérides de los satélites de navegación 102-106.

Una ventaja del sistema 1100 es que el cliente 108 puede usar el módulo selector de bits 1104 para elegir los bits de datos de navegación 136 de las porciones de los mensajes de navegación 134 que se sabe varían de manera impredecible. Alguna parte de los mensajes de navegación 134 puede ser muy predecible y por eso proclive a la falsificación. El uso de muestras de los mensajes de navegación 134 que son dinámicos, donde cambian a menudo los bits de datos de navegación 136, aleatoriza el conjunto de signaturas de cliente 138.

El sistema 1100 utiliza el módulo de rastreo y demodulación de bits 1102 que hay en general en muchos receptores GPS y que puede estar presente en diversos receptores GPS de teléfonos celulares. El cliente 108 rastrea las señales de navegación recibidas por el cliente 146 y demodula los bits de datos de navegación 136 del mensaje de navegación 134 usando el módulo de rastreo y demodulación de bits 1102 para estimar los bits de datos de navegación 136. El módulo selector de bits 1104 usa después los bits de datos de navegación estimados 1110 para elegir los bits de datos de navegación de las porciones de los mensajes de navegación 134 que se sabe varían de manera impredecible y proporcionar el conjunto de signaturas de cliente 138. El conjunto de signaturas de cliente 138 después se envía al servidor de autenticación 112 a los efectos de su comparación con el conjunto de signaturas de servidor 140.

La FIGURA 12 es una ilustración de un diagrama de bloques funcionales ejemplificativo de un sistema de autenticación 1200 (sistema 1200), de acuerdo con una forma de realización de la divulgación. El sistema 1200 puede tener funciones, material y estructuras similares a las de las formas de realización mostradas en las FIGURAS 1-11. Por lo tanto, pueden no describirse de manera redundante en la presente características, funciones y elementos que son comunes.

La FIGURA 12 muestra una forma de realización donde el servidor de autenticación 112 proporciona una forma de onda de prueba 1208 al cliente 108. En otras palabras, el servidor de autenticación 112 impulsa una signatura candidata al cliente 108. La forma de onda de prueba 1208 puede ser una secuencia binaria o una operación XOR del bit de datos de navegación 136 correspondiente a los satélites que se sabe están a la vista del cliente 108. El cliente 108 correlaciona o compara la forma de onda de prueba 1208 en el correlacionador de cliente 1204 con los bits de navegación 1206 demodulados en el cliente 108 por el módulo rastreador y demodulador 1120 y envía la información 1210 de esta correlación (o comparación) de vuelta al servidor de autenticación 112. El servidor de autenticación 112 toma la decisión de autenticación definitiva en base a la información de correlación 1210 del cliente 108.

En las formas de realización mostradas en las FIGURAS 9-12 y descritas precedentemente, la acción de autenticación puede iniciarse por cualquiera de los siguientes eventos:

- El cliente 108 desea completar una transacción o solicitud.

- Se promueve que el cliente 108 busque autenticación en base a su interacción con una terminal de punto de venta o comunicación de campo cercano (NFC).

• El cliente 108 está en una zona de seguridad pre-establecida, tal como su domicilio o trabajo, y desea pre-establecer la autenticación de transacciones o solicitudes anticipadas.

• El cliente 108 está en una zona de seguridad pre-establecida y desea post-autenticar una transacción o solicitud que ha tenido lugar en un pasado reciente.

• El cliente 108 detecta que las señales GNSS se vuelven cada vez más débiles y por eso desea pre-establecer la autenticación para potenciales transacciones o solicitudes en el interior de edificios.

• El servidor de autenticación 112 (dispositivo servidor) solicita una acción de autenticación.

La FIGURA 13 es una ilustración de un proceso de autenticación ejemplificativo, de acuerdo con una forma de realización de la divulgación. A las diversas tareas relacionadas con el proceso 1300 puede implementarlas el software, el hardware, el firmware, instrucciones ejecutables por computadora de un medio legible por computadora para plasmar el método del proceso o cualquier combinación de lo anterior. El proceso 1300 puede estar grabado en un medio legible por computadora, tal como memoria de semiconductores, disco magnético, disco óptico y dispositivos similares de una CPU, al que pueden acceder y ejecutar los módulos procesadores 906/932 en que está almacenado el medio legible por computadora.

Debe apreciarse que el proceso 1300 puede incluir una variada cantidad de tareas adicionales o alternativas; no es necesario implementar las tareas mostradas en la FIGURA 13 en el orden ilustrado y el proceso 1300 puede ser parte de un procedimiento más abarcador o tener una funcionalidad adicional que no se describa en detalle en la presente. En algunas formas de realización, diferentes elementos de los sistemas 900-1200, tales como: el cliente 108, el servidor de autenticación 112, etc., pueden implementar las porciones del proceso 1300. El proceso 1300 puede tener funciones, material y estructuras similares a las de las formas de realización mostradas en las FIGURAS 1-12. Por lo tanto, pueden no describirse de manera redundante en la presente características, funciones y elementos que son comunes.

El proceso 1300 puede comenzar con la recepción de las señales de navegación satelital de cliente recibidas de servidor, tales como las señales de navegación satelital de cliente recibidas de servidor 146 en un dispositivo de cliente, tal como el dispositivo de cliente 108 (tarea 1302).

El proceso 1300 puede continuar con la demodulación de las señales de navegación recibidas demoduladas por cliente, tales como los mensajes de navegación 502/504/506 de las señales de navegación satelital de cliente recibidas de servidor 146 que llegan al dispositivo de cliente 108 desde una pluralidad de satélites de navegación, tales como los satélites de navegación 102-106, respectivamente (tarea 1304). En algunas formas de realización, la demodulación de las señales de navegación recibidas demoduladas por cliente a partir de las señales de navegación satelital de cliente recibidas de servidor 146 puede comprender la conversión de RF a banda base y la conversión de analógico a digital. En algunas formas de realización, la demodulación de las señales de navegación recibidas demoduladas por cliente a partir de las señales de navegación satelital de cliente recibidas de servidor 146 además comprende el borrado de código y el borrado de portadora. Los satélites de navegación pueden comprender, por ejemplo pero sin limitación, un satélite del sistema global de navegación satelital (GNSS), un satélite del sistema de posicionamiento global (GPS™), un satélite del sistema Globalnaya Navigatsionnaya Sputnikovaya (GLONASS™), un satélite del sistema de navegación BeiDou (COMPASS™), un satélite Galileo™ u otro sistema de navegación satelital. En este documento, pueden usarse de manera intercambiable las señales de navegación recibidas demoduladas por cliente 502/504/506 y los mensajes de navegación 502/504/506.

El proceso 1300 puede continuar con la selección de un subconjunto de la pluralidad de señales de navegación entrantes recibidas por cliente para proporcionar una pluralidad de tramas de bits, tales como las tramas de bits de cliente 1030 (tarea 1306). El subconjunto puede comprender, por ejemplo pero sin limitación, una subtrama, una selección aleatoria, una selección de bits entre los más dinámicos u otro subconjunto.

El proceso 1300 puede continuar con la recepción de las señales de navegación satelital recibidas por el servidor, tales como las señales 148 en una de servidor, tal como la 114 (tarea 1308).

El proceso 1300 puede continuar con la demodulación de las señales de navegación recibidas demoduladas por servidor, tales como los mensajes de navegación 502/504/506, a partir de las señales 148 recibidas en la antena de servidor 114 provenientes de los satélites de navegación 102-104, respectivamente (tarea 1310). En algunas formas de realización, la demodulación de las señales de navegación recibidas demoduladas por servidor, tales como los mensajes de navegación 502/504/506, a partir de las señales 148 comprende la conversión de RF a banda base, el filtrado pasa banda, la conversión de analógico a digital, el borrado de código y el borrado de portadora. En este documento también pueden usarse de manera intercambiable las señales de navegación recibidas demoduladas por servidor 502/504/506 y los mensajes de navegación 502/504/506.

El proceso 1300 puede continuar con la selección de un subconjunto de las señales de navegación recibidas demoduladas por servidor, tales como los mensajes de navegación 502/504/506, sincronizadas con las tramas de bits de cliente 1030 para proporcionar una pluralidad de tramas de bits sincronizadas por servidor, tales como las tramas de bits sincronizadas por servidor 1032 (tarea 1312).

El proceso 1300 puede continuar con el cálculo de una función de las tramas de bits de cliente 1030 para proporcionar un conjunto de signaturas de cliente, tal como el conjunto de signaturas de cliente 138 (tarea 1314). La función puede comprender, por ejemplo pero sin limitación, una función XOR lógica, una función OR lógica, una función AND lógica u otra función.

El proceso 1300 puede continuar con el cálculo de la función de las tramas de bits sincronizadas por servidor 1032 para proporcionar un conjunto de signaturas de servidor, tales como el conjunto de signaturas de servidor 140 (tarea 1316).

El proceso 1300 puede continuar con la comparación del conjunto de signaturas de cliente 138 y el conjunto de signaturas de servidor 140 para proporcionar un resultado, tal como el mensaje de decisión de autenticación 144 (tarea 1318).

El proceso 1300 puede continuar con la autenticación de una ubicación, tal como la ubicación 122 del dispositivo de cliente 108 en base al resultado de comparación (tarea 1320). La autenticación indica una validez de que hay exactitud y/o certeza aceptable en cuanto a que el cliente 108 está situado en la ubicación 122 o bien, indica la no validez de tal cosa.

La FIGURA 14 es una ilustración de un proceso de autenticación ejemplificativo, de acuerdo con una forma de realización de la divulgación. Las diversas tareas ejecutadas en conexión con el proceso 1400 pueden implementarse en software, hardware, firmware, un medio legible por computadora con instrucciones ejecutables también por computadora para plasmar el método o bien, una combinación de lo anterior. El proceso 1400 puede estar grabado en un medio legible por computadora, tal como una memoria de semiconductores, un disco magnético, un disco óptico y otros dispositivos similares a los que puede acceder una CPU de computación, tal como los módulos procesadores 906/932 en que está almacenado el medio legible por computadora.

Debe apreciarse que el proceso 1400 puede incluir una variada cantidad de tareas adicionales o alternativas; las tareas mostradas en la FIGURA 14 no necesitan ejecutarse en el orden ilustrado y el proceso 1300 puede estar incorporado en un procedimiento o proceso más abarcador con funcionalidad adicional que no se describe en detalle en la presente. En algunas formas de realización, las porciones del proceso 1300 pueden implementarse mediante diferentes elementos del sistemas 900-1200, tales como: el cliente 108, el servidor de autenticación 112, etc. El proceso 1400 puede tener funciones, material y estructuras similares a las de las formas de realización mostradas en las FIGURAS 1-12. Por lo tanto, pueden no describirse de manera redundante en la presente características, funciones y elementos que son comunes.

El proceso 1400 puede comenzar con la entrada de las señales de navegación satelital de cliente recibidas por el servidor, tales como las señales de navegación recibidas por el cliente 146, en un dispositivo de cliente tal como el dispositivo de cliente 108 (tarea 1402). El proceso 1400 puede continuar con la demodulación de las señales de navegación recibidas demoduladas por cliente, tales como los mensajes de navegación 502/504/506 provenientes de las señales de navegación satelital recibidas en el dispositivo de cliente 108 provenientes de una pluralidad de satélites de navegación, tales como los satélites de navegación 102-108, respectivamente (tarea 1404).

El proceso 1400 puede continuar con el envío de una forma de onda de prueba, tal como la forma de onda de prueba 1208 proveniente de un dispositivo servidor, tal como el dispositivo servidor 112, al dispositivo de cliente 108 (tarea 1406).

El proceso 1400 después puede continuar con la comparación de la forma de onda de prueba 1208 en el dispositivo de cliente 108 y las señales de navegación entrantes demoduladas por cliente en el dispositivo de cliente 108 para brindar información de correlación, tal como la información de correlación 1210 (tarea 1408).

El proceso 1400 después puede continuar con el envío de la información de correlación 1210 de regreso al dispositivo servidor 112 para proporcionar un mensaje de decisión de autenticación, tal como el mensaje de decisión de autenticación 144 (tarea 1410).

De esa manera, las formas de realización de la divulgación proveen un sistema de autenticación que admite una adecuada sensibilidad respecto de una señal satelital de navegación que debe recibirse en un dispositivo de cliente situado en un entorno de baja proporción de señal a ruido (SNR), tal como el interior de edificios y el centro de una ciudad.

Si bien en la descripción detallada precedente se ha presentado al menos una forma de realización ejemplificativa, debe apreciarse que existen una vasta cantidad de variaciones. Más bien, la descripción detallada precedente brindará a los expertos en la técnica un mapa de ruta conveniente para implementar la o las formas de realización expuestas.

En este documento, el término "módulo" tal como aquí se emplea, se refiere a software, firmware, hardware y cualquier combinación de esos elementos para implementar las funciones asociadas que se describen en la presente. Además, a los efectos de esta reseña, los diversos módulos se presentan como módulos discretos; sin embargo, tal como apreciará un experto en la técnica, pueden articularse dos o más módulos para formar uno solo que ejecute las funciones asociados, de acuerdo con las formas de realización de la presente divulgación.

En este documento, los términos "producto de programa de computación", "medio legible por computadora" y similares pueden emplearse en general para hacer referencia a medios tales como por ejemplo memoria, dispositivos de almacenamiento o unidad de almacenamiento. Estas y otras formas de medios legibles por computación pueden estar implicadas en el almacenamiento de una o más instrucciones que usan los módulos procesadores 906/932 para producir las operaciones especificadas. Tales instrucciones, en general referidas como "código de programa de computación " o "código de programa " (que pueden estar agrupadas en la forma de programas de computación u otros agrupamientos), al ejecutarse, habilitan un método para usar un sistema tal como el sistema 900-1200.

La descripción precedente se refiere a elementos o nodos o características “conectados/as” o “acoplados/as” entre sí. Como aquí se emplean, a menos que se especifique otra cosa, "conectado/a/s" significa que un elemento/nodo/característica está unido/a directamente (o se comunica directamente) a otro elemento/nodo/característica y no necesariamente lo hace de manera mecánica. Del mismo modo, a menos que expresamente se manifieste otra cosa, "acoplado/a/s" significa que un elemento/nodo/característica está directa o indirectamente unido/a (o que se comunica directa o indirectamente) a otro elemento/nodo/característica y no lo hace necesariamente de manera mecánica. Por eso, aunque las FIGURAS 1-12 ilustran disposiciones ejemplificativas de elementos, en una forma de realización de la divulgación, pueden haber e intervenir más elementos, dispositivos, características o componentes.

Los términos y frases usados en este documento y sus variaciones, a menos que expresamente se indique otra cosa, deben interpretarse como de final abierto en lugar de limitativos. Como ejemplos de lo anterior: el término "que incluye/n" debe entenderse que significa "que incluye/n sin limitación" o algo similar; el término "ejemplo" se emplea para proporcionar instancias ejemplificativas del elemento en cuestión, no una lista exhaustiva o limitativa de tales elementos; y adjetivos tales como "convencional/es", 'tradicional/es", "normal/es", "estándar", "conocido/s" y de significado similar no deben interpretarse como limitativos del elemento descrito a un determinado período de tiempo o disponible como de un determinado período de tiempo, sino en cambio como abarcador de tecnologías convencionales, tradicionales, normales o estándar que pueden estar a disposición o ser conocidas ahora o en cualquier momento del futuro.

Del mismo modo, un grupo de elementos vinculados con la conjunción "y" no deben interpretarse como que estén presentes cada uno y todos en el agrupamiento, sino más bien como “y/o”, a menos que expresamente se indique otra cosa. De manera similar, un gripo de elementos vinculados con la conjunción "o" no deben interpretarse como que requieren mutua exclusividad en dicho grupo, sino más bien como “y/o” a menos que expresamente se indique otra cosa.

Por otra parte, aunque los elementos o componentes de la divulgación se describan o reivindiquen en singular, se contempla que esté incluido el plural en su alcance, a menos que se manifieste explícitamente el singular. La presencia de palabras o frases ampliadoras como "uno/a o más", "al menos", "pero sin limitarse a ello " u otras por el estilo en algunas instancias, no debe interpretarse como que, en su ausencia, se pretenda o requiera que el caso o los casos se entiendan como más reducidos. El término "aproximadamente", si se refiere a un valor o rango numérico, se entiende que abarca los valores resultantes de errores experimentales que pueden ocurrir al efectuar las mediciones.

Tal como se emplea en la presente, a menos que expresamente se indique otra cosa, "operable" significa que se puede usar, ajustar o estar listo para uso o servicio, ser utilizable para una finalidad específica y apto/a para ejecutar una función mencionada o conveniente que aquí se describe. En relación con sistemas y dispositivos, el término "operable" significa que el sistema y/o el dispositivo son totalmente funcionales y están calibrados, comprenden elementos y cumplen con requisitos de operabilidad aplicables para plasmar una función mencionada al activarse. En relación con sistemas y circuitos, el término "operable" significa que el sistema y/o el circuito son plenamente funcionales y están calibrados, comprenden elementos y cumple requisitos de operabilidad aplicables para plasmar una función mencionada al activarse.

**REIVINDICACIONES**

1. Un método para autenticar ubicaciones, que comprende los pasos de:

demodular una pluralidad de señales de navegación satelital de cliente recibidas de servidor (146) en un dispositivo de cliente (108) provenientes de una pluralidad de satélites de navegación (102-106), respectivamente, para proporcionar una pluralidad de señales de navegación entrantes demoduladas por cliente (1020);

seleccionar un subconjunto de la pluralidad de señales de navegación entrantes demoduladas por cliente (1020) para proporcionar una pluralidad de tramas de bits de cliente;

calcular una función de la pluralidad de tramas de bits de cliente para reducir el tamaño de una combinación de la pluralidad de tramas de bits de cliente a fin de proveer un conjunto de signaturas de cliente (138);

demodular una pluralidad de señales de navegación satelital recibidas por el servidor (148) en una antena de servidor (114) provenientes de los satélites de navegación (102-106), respectivamente, a fin de proveer una pluralidad de señales de navegación entrantes demoduladas por servidor (1022);

seleccionar un subconjunto de la pluralidad de señales de navegación entrantes demoduladas por servidor (1022) sincronizadas con una pluralidad de tramas de bits de cliente (1030) para proporcionar una pluralidad de tramas de bits sincronizadas por servidor (1032);

calcular una función de la pluralidad de tramas de bits sincronizadas por servidor para reducir el tamaño de una combinación de la pluralidad de tramas de bits sincronizadas por servidor a fin de proveer un conjunto de signaturas de servidor (140);

recibir el servidor el conjunto de signaturas de cliente (138);

comparar el conjunto de signaturas de cliente y el conjunto de signaturas de servidor para proveer un resultado; y

autenticar una ubicación (122) de un dispositivo de cliente (108) en base al resultado de la comparación.

2. El método de la reivindicación 1, donde la función comprende una de: una función XOR lógica, una función OR lógica y una función AND lógica.

3. El método de la reivindicación 1, donde demodular las señales de navegación satelital de cliente, recibidas por servidor, (146) para proporcionar las señales de navegación entrantes demoduladas por cliente (1020) comprende:

la conversión de RF a banda base;

el filtrado pasa banda; y

la conversión de analógico a digital.

4. El método de la reivindicación 3, donde demodular las señales de navegación satelital de cliente, recibidas por servidor, (146) para proporcionar las señales de navegación entrantes demoduladas por cliente (1020) además comprende:

el borrado de código; y

el borrado de portadora.

5. El método de la reivindicación 3, el paso de autenticar además comprende:

enviar una forma de onda de prueba (1208) de un dispositivo servidor (112) al dispositivo de cliente (108);

comparar la forma de onda de prueba en el dispositivo de cliente con las señales de navegación recibidas demoduladas por cliente (1020) en el dispositivo de cliente para proporcionar la información de correlación (1210); y

enviar la información de correlación de regreso al dispositivo servidor a fin de proporcionar un mensaje de decisión de autenticación (144).

6. El método de la reivindicación 1, que además comprende entrar las señales de navegación satelital de cliente recibidas de servidor (1020) en el dispositivo de cliente (108).

7. El método de la reivindicación 1, donde demodular las señales de navegación satelital (148) para proporcionar las señales de navegación entrantes demoduladas por servidor (1022) comprende:

la conversión de RF a banda base;

el filtrado pasa banda;

la conversión de analógico a digital;

el borrado de código; y

el borrado de portadora.

8. El método de la reivindicación 1, donde el subconjunto comprende una de:

una subtrama;

una selección aleatoria; y

una selección de bits de entre los bits más dinámicos.

9. Un sistema de autenticación de ubicaciones (1000), que comprende:

un módulo de demodulación de cliente (1108) operable para:

entrar una pluralidad de señales de navegación satelital de cliente recibidas por servidor (146) en el dispositivo de cliente (108) provenientes de una pluralidad de satélites de navegación (102-106), respectivamente; y

demodular la pluralidad de señales de navegación satelital de cliente recibidas por servidor para proporcionar una pluralidad de señales de navegación entrantes demoduladas por cliente (1020);

un módulo selector de tramas de datos de cliente (1006) operable para seleccionar un subconjunto de la pluralidad de señales de navegación entrantes demoduladas por cliente (1020) a fin de proporcionar una pluralidad de tramas de bits de cliente;

un módulo de operación de datos de cliente (1002) operable para calcular la función de la pluralidad de tramas de bits de cliente a fin de reducir el tamaño de una combinación de la pluralidad de tramas de bits de cliente y proveer un conjunto de signaturas de cliente;

un módulo de demodulación de servidor (940) operable para:

recibir una pluralidad de señales de navegación satelital recibidas por servidor (148) en un dispositivo servidor (112) provenientes de los satélites de navegación (102-106), respectivamente; y

demodular las señales de navegación satelital recibidas por el servidor para proporcionar la pluralidad de señales de navegación entrantes demoduladas por servidor (1022);

un módulo selector de tramas de datos de servidor (1010) operable para seleccionar un subconjunto de la pluralidad de señales de navegación entrantes demoduladas por servidor (1022), que se sincronizan con la pluralidad de tramas de bits de cliente (1030) para proporcionar una pluralidad de tramas de bits sincronizadas por servidor (1032);

un módulo de operación de datos de servidor (1004) operable para calcular una función de la pluralidad de tramas de bits sincronizadas por servidor a fin de reducir el tamaño de una combinación de la pluralidad de tramas de bits sincronizadas por servidor y proveer un conjunto de signaturas de servidor (140);

un módulo de correlación de servidor (142) operable para recibir el conjunto de signaturas de cliente (138) y comparar el conjunto de signaturas de cliente (138) y el conjunto de signaturas de servidora fin de proveer un resultado; y

un módulo de autenticación operable para autenticar una ubicación (122) de un dispositivo de cliente (108) en base al resultado de la comparación.

10. El sistema (1000) de la reivindicación 9, donde el módulo de demodulación de cliente (1108) además es operable para efectuar:

la conversión de RF a banda base;

el filtrado pasa banda; y

la conversión de analógico a digital.

11. El sistema (1000) de la reivindicación 9, donde el módulo de demodulación de cliente (1108) además es operable para efectuar:

el borrado de código; y

el borrado de portadora.

12. El sistema (1000) de la reivindicación 9, donde el módulo de demodulación de servidor (940) además es operable para efectuar:

la conversión de RF a banda base;

el filtrado pasa banda;

la conversión de analógico a digital;

el borrado de código; y

el borrado de portadora.

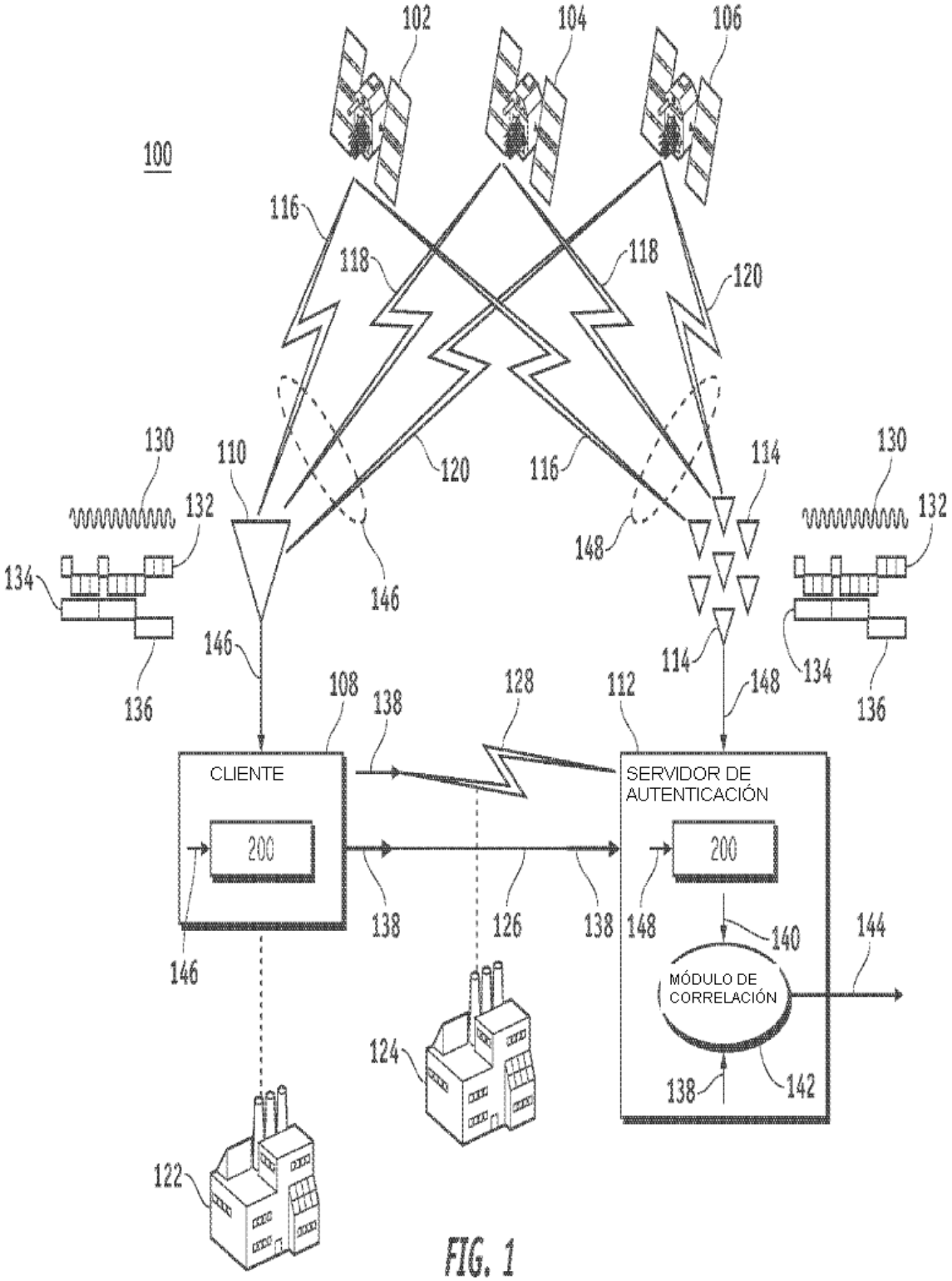
100
102
104
106
116
118
118
120
130
110
120
116
114
130
132
132
148
134
146
134
146
114
136
136
108
138
128
112
148
CLIENTE
SERVIDOR DE AUTENTICACIÓN
200
200
138
126
138
148
140
144
146
MÓDULO DE CORRELACIÓN
124
138
142
122

FIG. 1

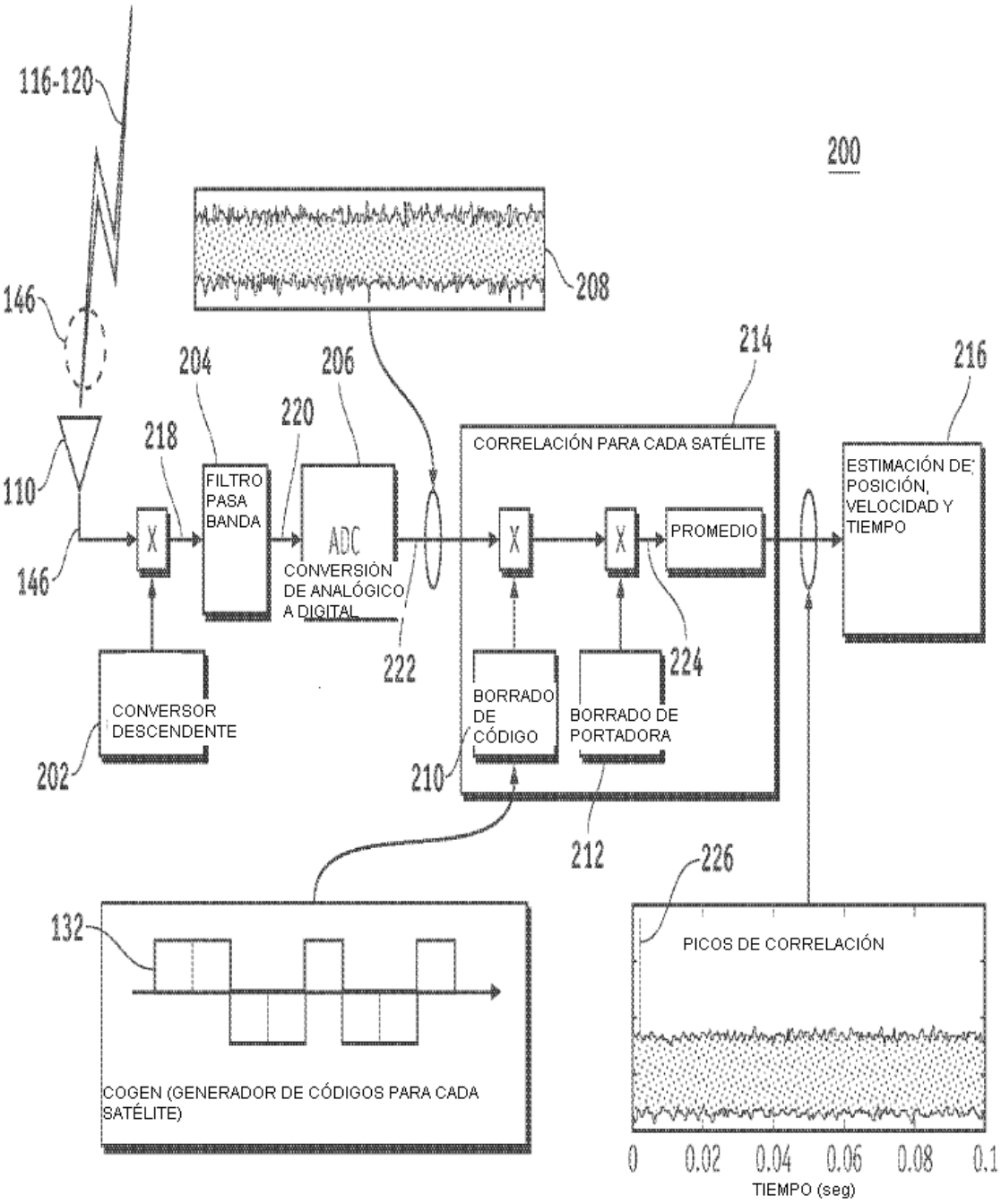
116-120
200
208
146
204
206
214
216
218
220
110
FILTRO PASA BANDA
CORRELACIÓN PARA CADA SATÉLITE
ESTIMACIÓN DE POSICIÓN, VELOCIDAD Y TIEMPO
X
ADC
X
X
PROMEDIO
146
CONVERSIÓN DE ANALÓGICO A DIGITAL
222
224
CONVERSOR DESCENDENTE
BORRADO DE CÓDIGO
BORRADO DE PORTADORA
202
210
212
226
132
PICOS DE CORRELACIÓN
COGEN (GENERADOR DE CÓDIGOS PARA CADA SATÉLITE)
0
0.02
0.04
0.06
0.08
0.1
TIEMPO (seg)

FIG. 2

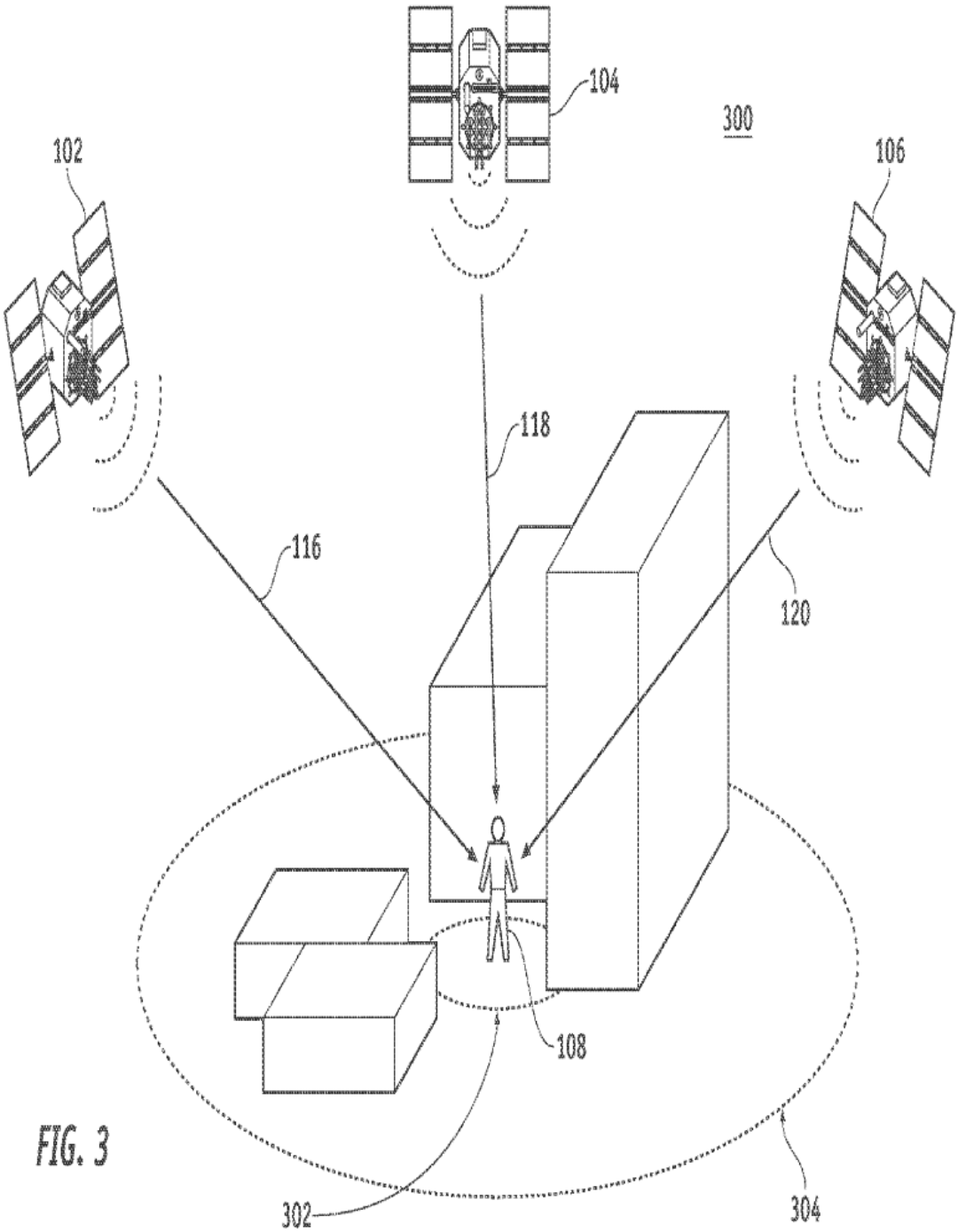


FIG. 3

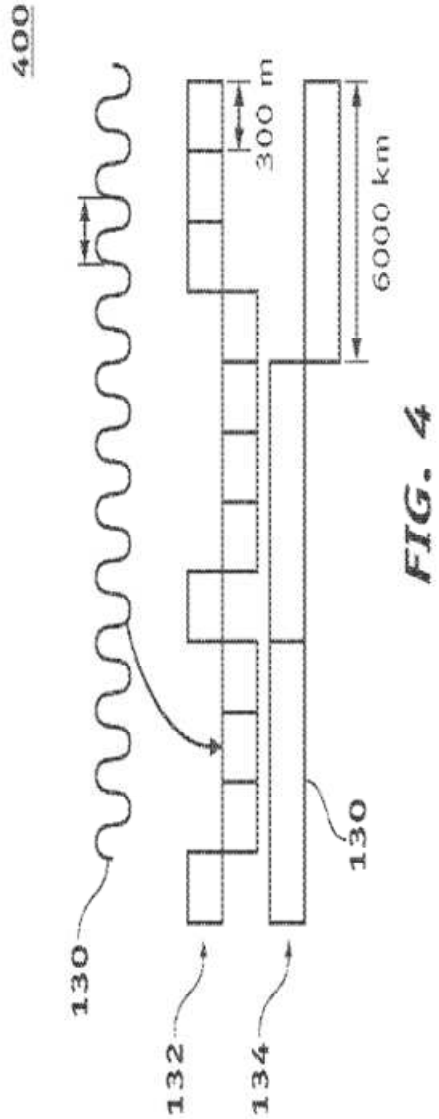
400
300 m
6000 km
130
132
134
130

FIG. 4

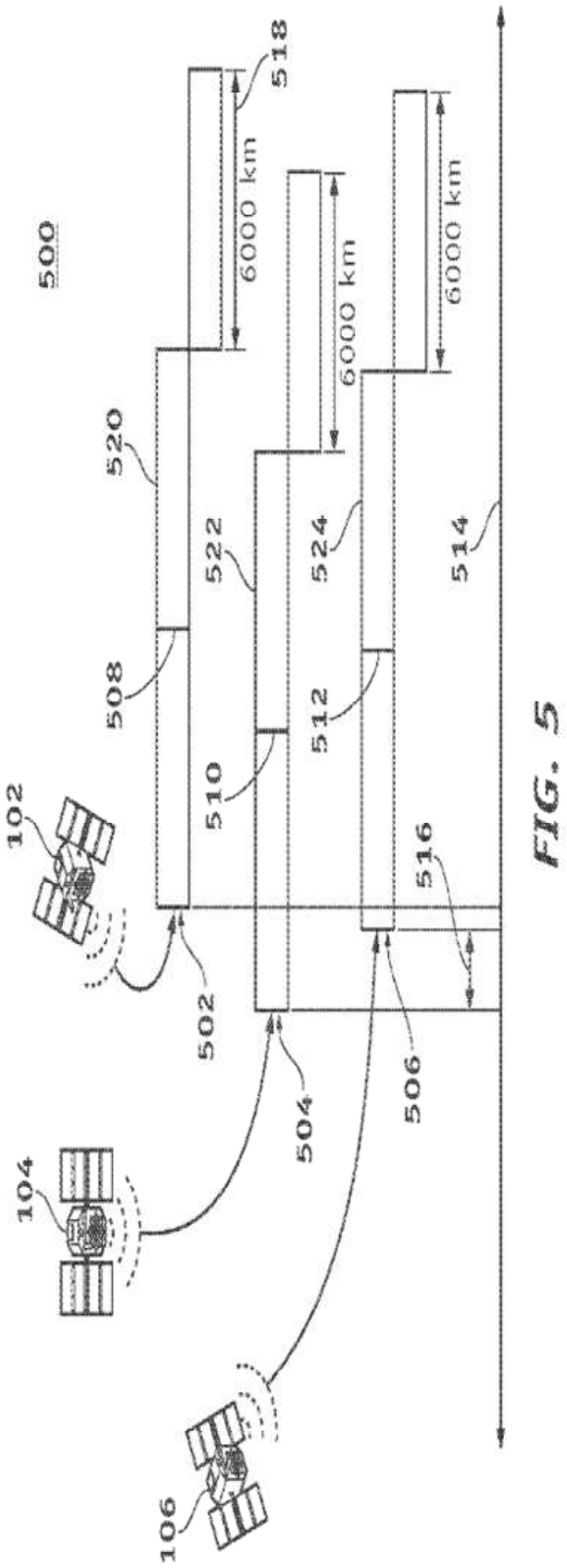
500
518
6000 km
520
6000 km
522
524
6000 km
514
508
512
510
102
516
502
504
506
104
106

FIG. 5

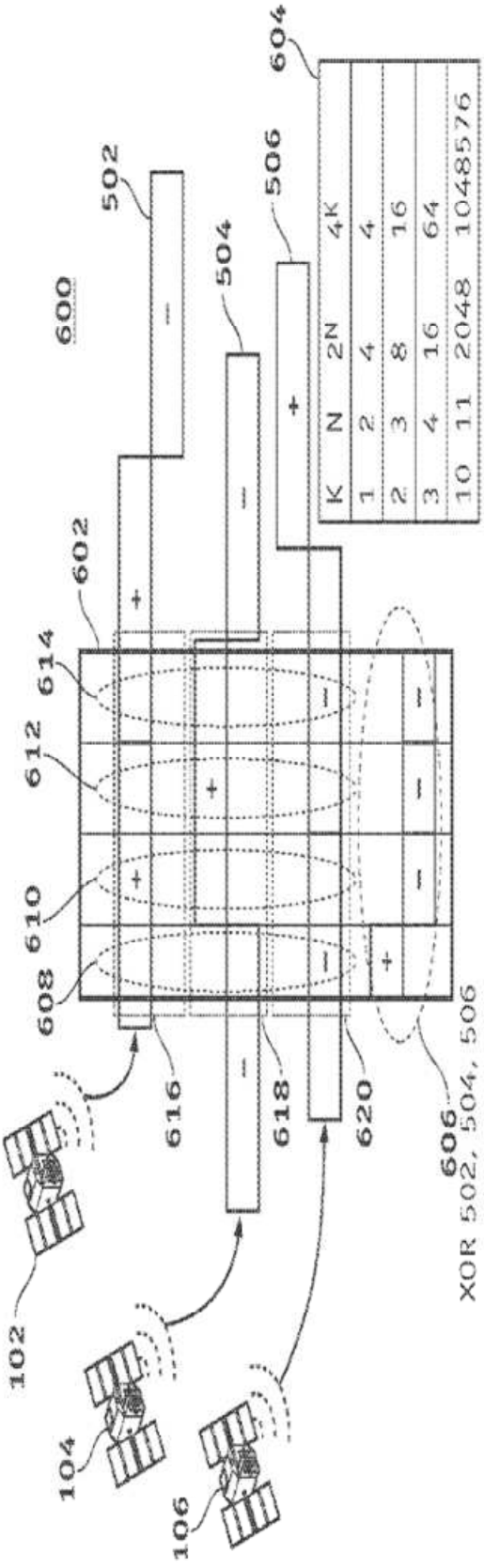
600
502
504
506
604
602
614
612
610
608
616
618
620
606
XOR 502, 504, 506
102
104
106
K N 2N 4K
1 2 4 4
2 3 8 16
3 4 16 64
10 11 2048 1048576

FIG. 6

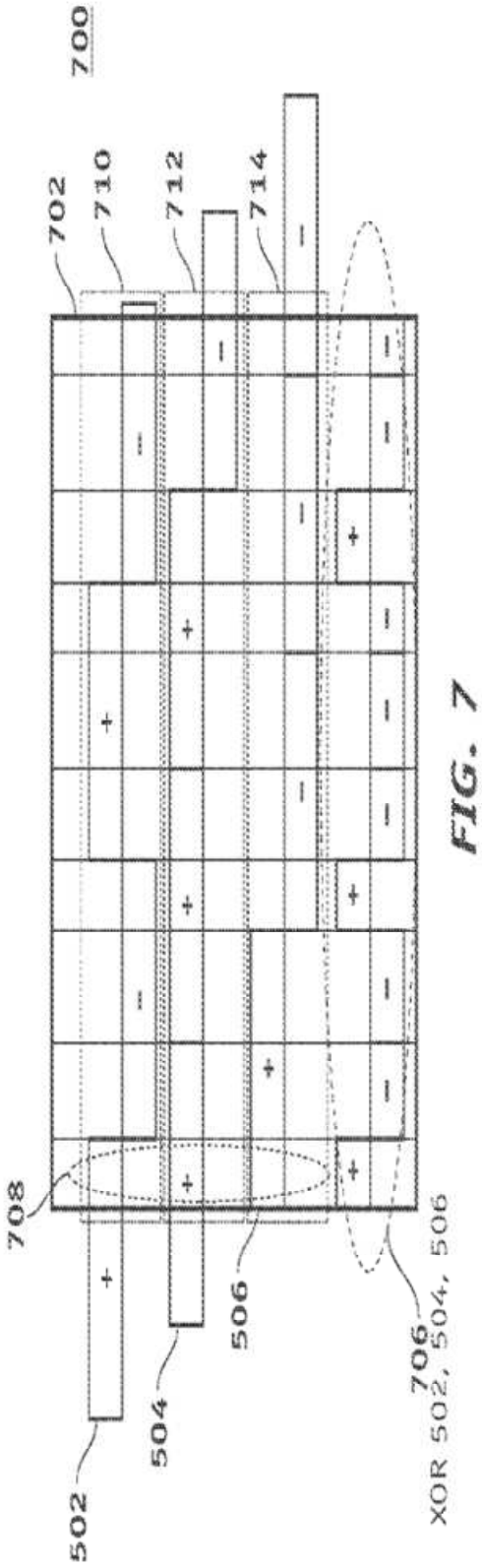
700
702
710
712
714
708
502
504
506
706
XOR 502, 504, 506

FIG. 7

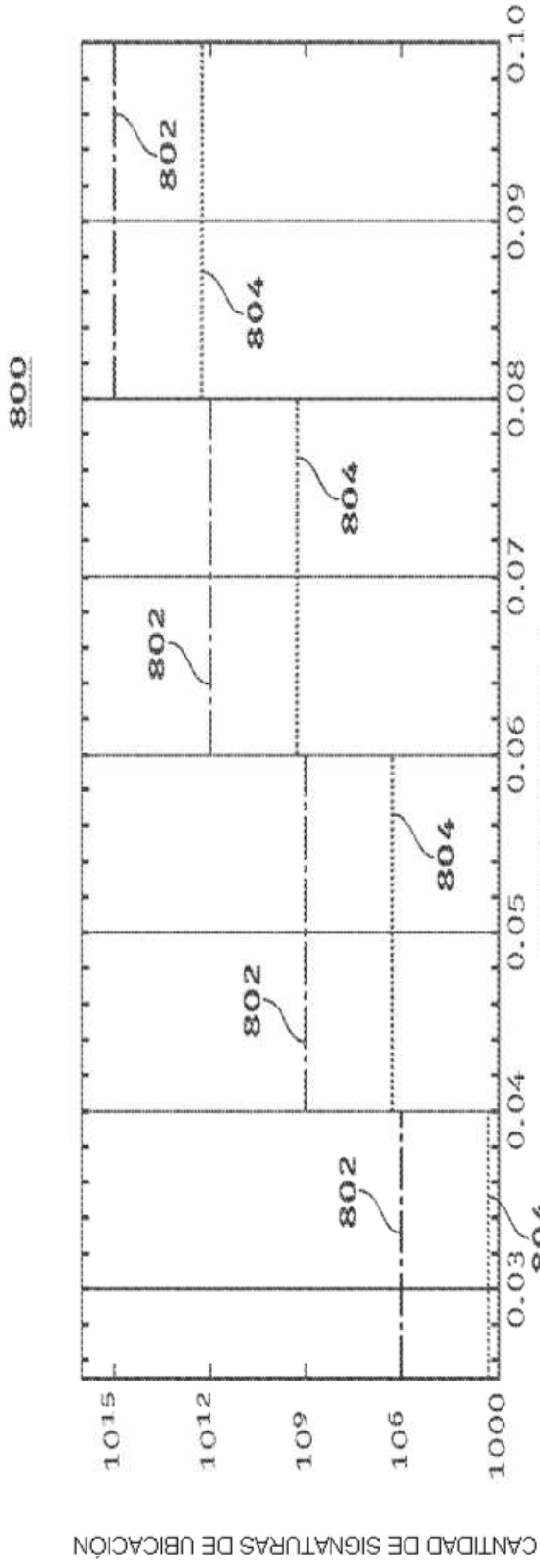
800
802
804
1015
1012
109
106
1000
0.03
0.04
0.05
0.06
0.07
0.08
0.09
0.10
VENTANA DE MUESTREO (seg)
CANTIDAD DE SIGNATURAS DE UBICACIÓN

FIG. 8

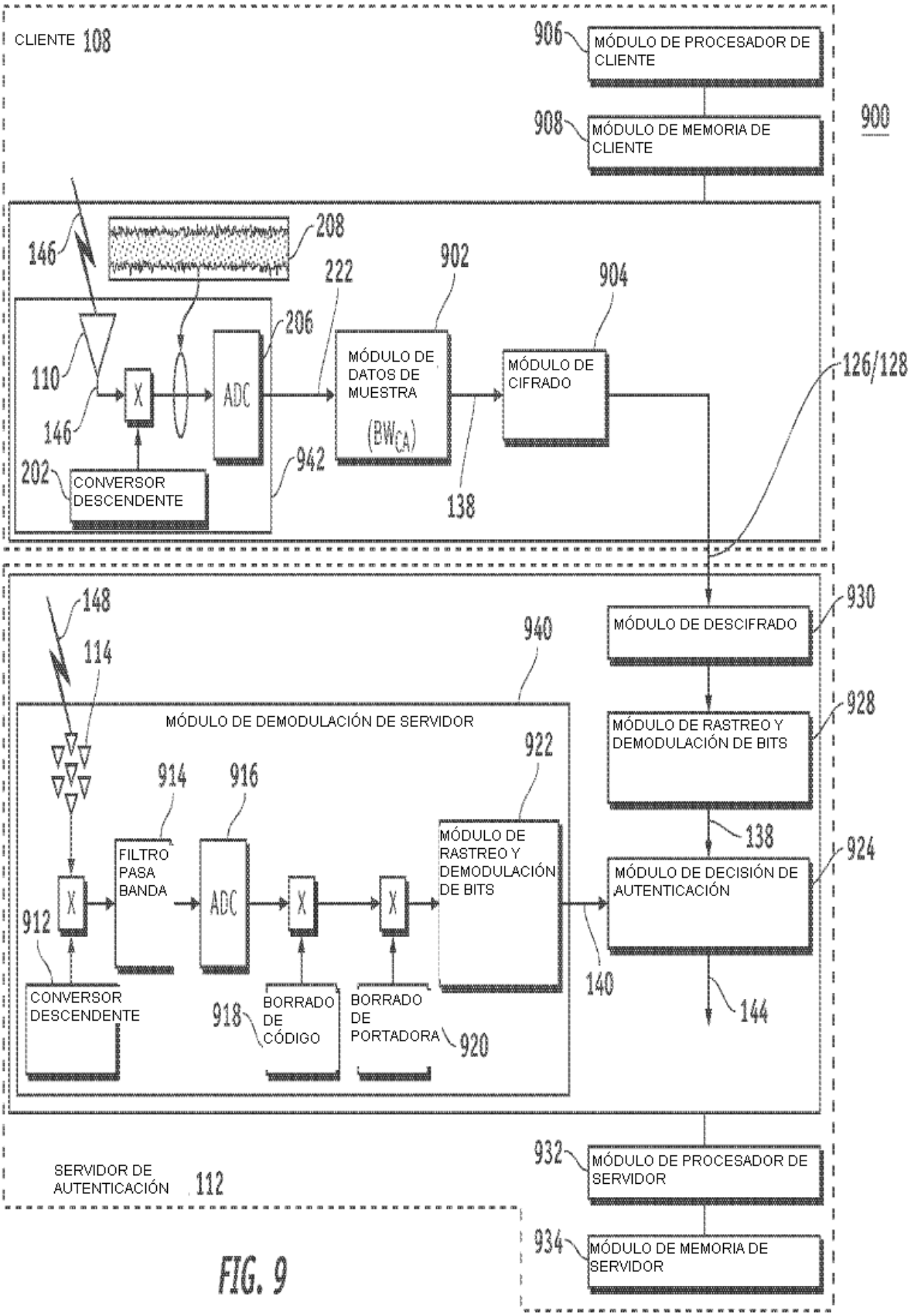
CLIENTE 108
906
MÓDULO DE PROCESADOR DE CLIENTE
908
MÓDULO DE MEMORIA DE CLIENTE
900
146
208
222
902
904
206
110
146
X
ADC
MÓDULO DE DATOS DE MUESTRA
(BW_CA)
MÓDULO DE CIFRADO
126/128
202
CONVERSOR DESCENDENTE
942
138
148
114
940
930
MÓDULO DE DESCIFRADO
MÓDULO DE DEMODULACIÓN DE SERVIDOR
922
928
MÓDULO DE RASTREO Y DEMODULACIÓN DE BITS
914
916
FILTRO PASA BANDA
MÓDULO DE RASTREO Y DEMODULACIÓN DE BITS
138
924
912
X
ADC
X
X
MÓDULO DE DECISIÓN DE AUTENTICACIÓN
140
144
CONVERSOR DESCENDENTE
918
BORRADO DE CÓDIGO
BORRADO DE PORTADORA
920
SERVIDOR DE AUTENTICACIÓN 112
932
MÓDULO DE PROCESADOR DE SERVIDOR
934
MÓDULO DE MEMORIA DE SERVIDOR

FIG. 9

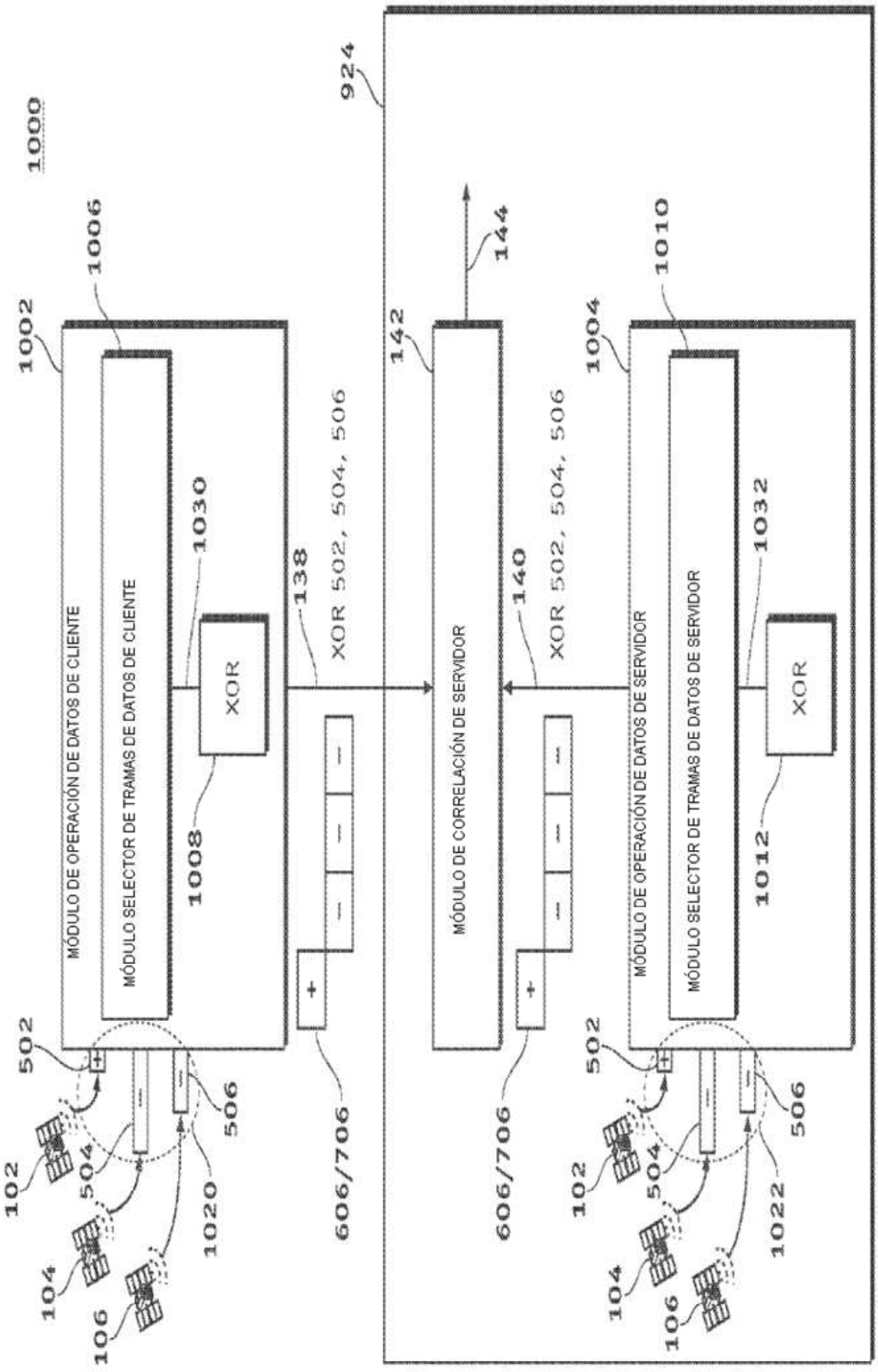
1000
924
1002
1006
1004
1010
142
144
MÓDULO DE OPERACIÓN DE DATOS DE CLIENTE
MÓDULO SELECTOR DE TRAMAS DE DATOS DE CLIENTE
1030
XOR
1008
138
XOR 502, 504, 506
MÓDULO DE CORRELACIÓN DE SERVIDOR
140
XOR 502, 504, 506
MÓDULO DE OPERACIÓN DE DATOS DE SERVIDOR
MÓDULO SELECTOR DE TRAMAS DE DATOS DE SERVIDOR
1032
XOR
1012
502
504
506
1020
1022
606/706
606/706
102
104
106

FIG. 10

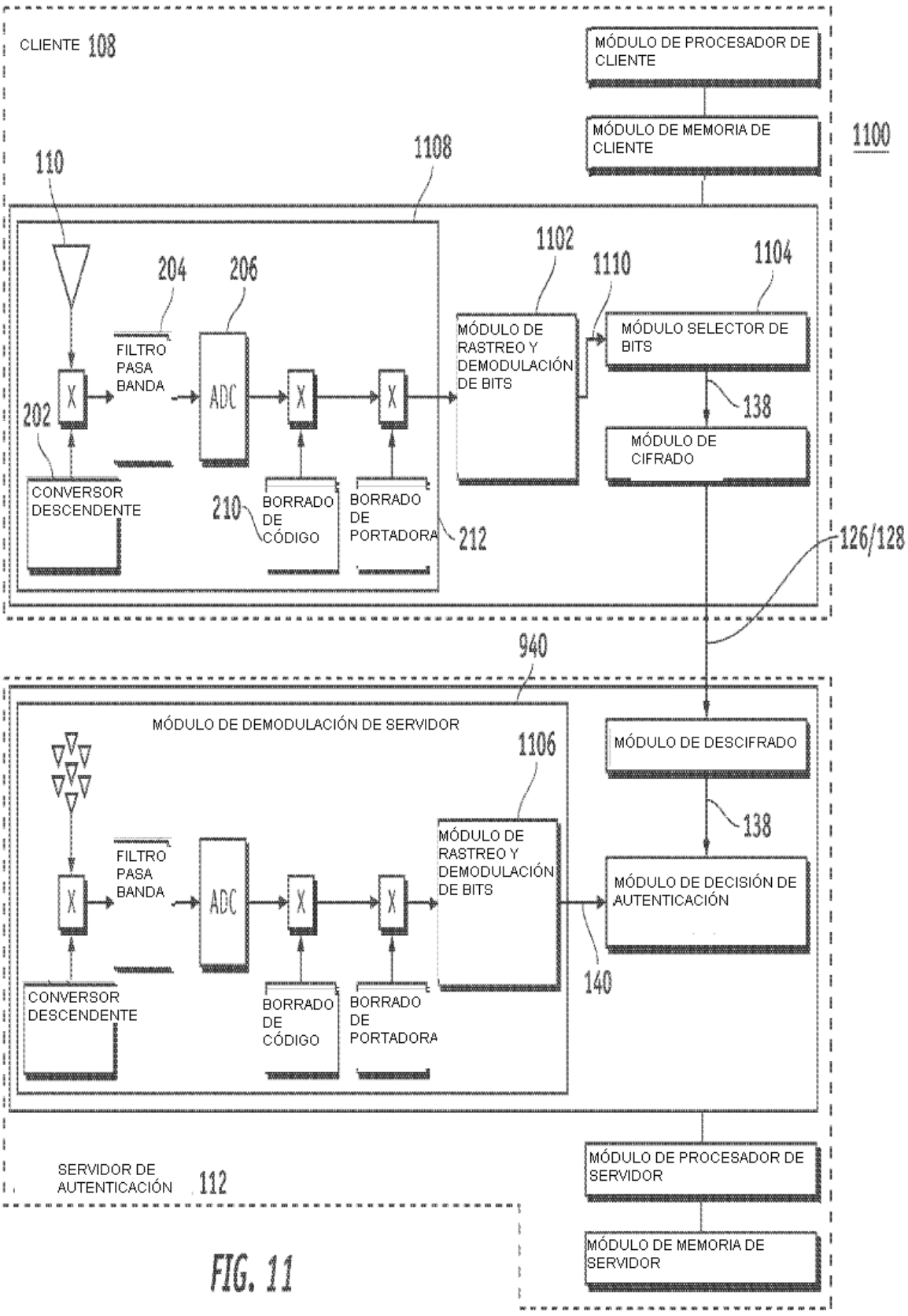
CLIENTE 108
MÓDULO DE PROCESADOR DE CLIENTE
MÓDULO DE MEMORIA DE CLIENTE
1100
110
1108
1102
1110
1104
204
206
FILTRO PASA BANDA
ADC
MÓDULO DE RASTREO Y DEMODULACIÓN DE BITS
MÓDULO SELECTOR DE BITS
202
138
MÓDULO DE CIFRADO
CONVERSOR DESCENDENTE
210
BORRADO DE CÓDIGO
BORRADO DE PORTADORA
212
126/128
940
MÓDULO DE DEMODULACIÓN DE SERVIDOR
1106
MÓDULO DE DESCIFRADO
138
MÓDULO DE RASTREO Y DEMODULACIÓN DE BITS
MÓDULO DE DECISIÓN DE AUTENTICACIÓN
140
SERVIDOR DE AUTENTICACIÓN 112
MÓDULO DE PROCESADOR DE SERVIDOR
MÓDULO DE MEMORIA DE SERVIDOR

FIG. 11

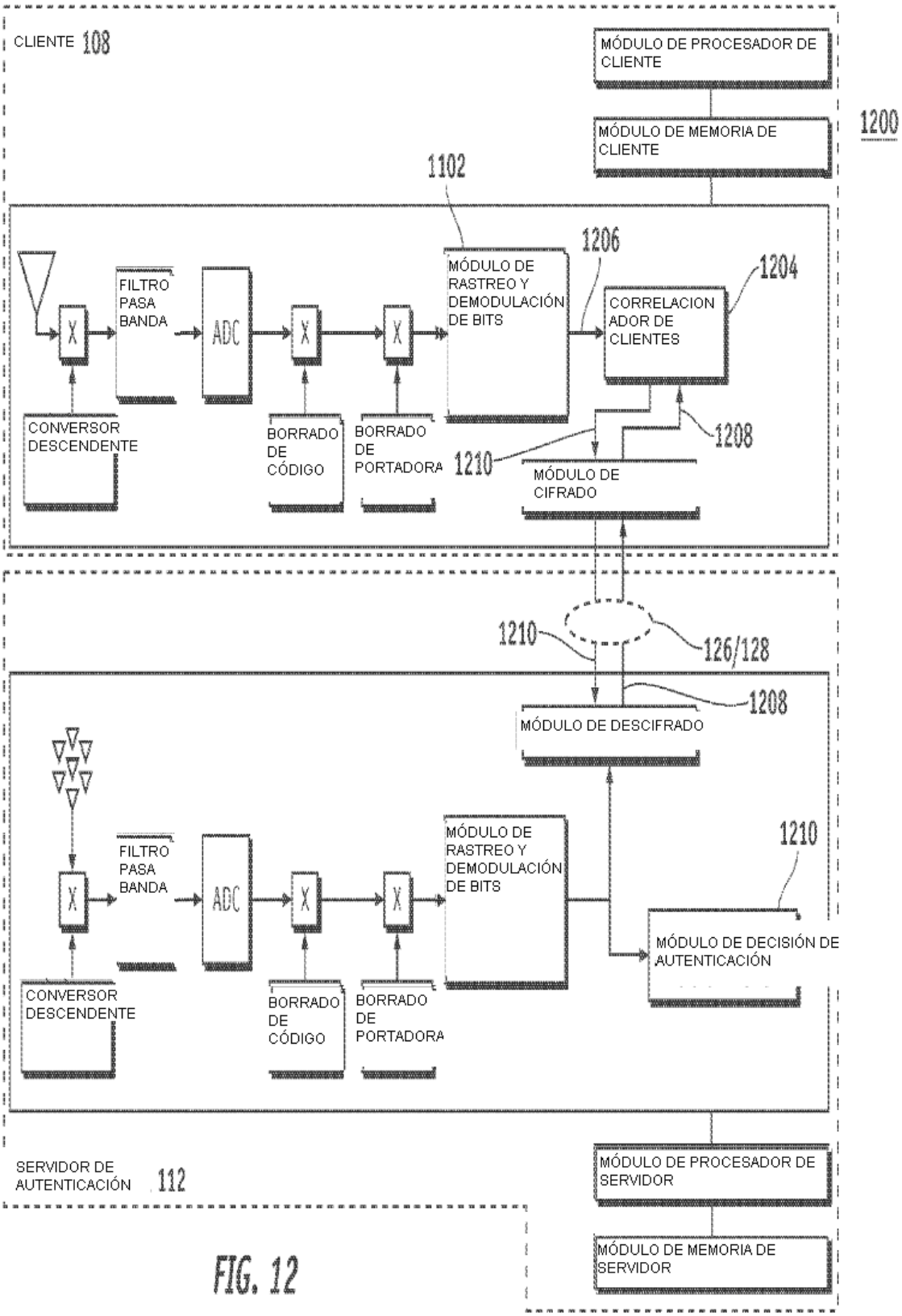
CLIENTE 108
MÓDULO DE PROCESADOR DE CLIENTE
MÓDULO DE MEMORIA DE CLIENTE
1200
1102
1206
1204
FILTRO PASA BANDA
ADC
MÓDULO DE RASTREO Y DEMODULACIÓN DE BITS
CORRELACIONADOR DE CLIENTES
CONVERSOR DESCENDENTE
BORRADO DE CÓDIGO
BORRADO DE PORTADORA
1210
1208
MÓDULO DE CIFRADO
126/128
MÓDULO DE DESCIFRADO
FILTRO PASA BANDA
ADC
MÓDULO DE RASTREO Y DEMODULACIÓN DE BITS
MÓDULO DE DECISIÓN DE AUTENTICACIÓN
CONVERSOR DESCENDENTE
BORRADO DE CÓDIGO
BORRADO DE PORTADORA
SERVIDOR DE AUTENTICACIÓN 112
MÓDULO DE PROCESADOR DE SERVIDOR
MÓDULO DE MEMORIA DE SERVIDOR

FIG. 12

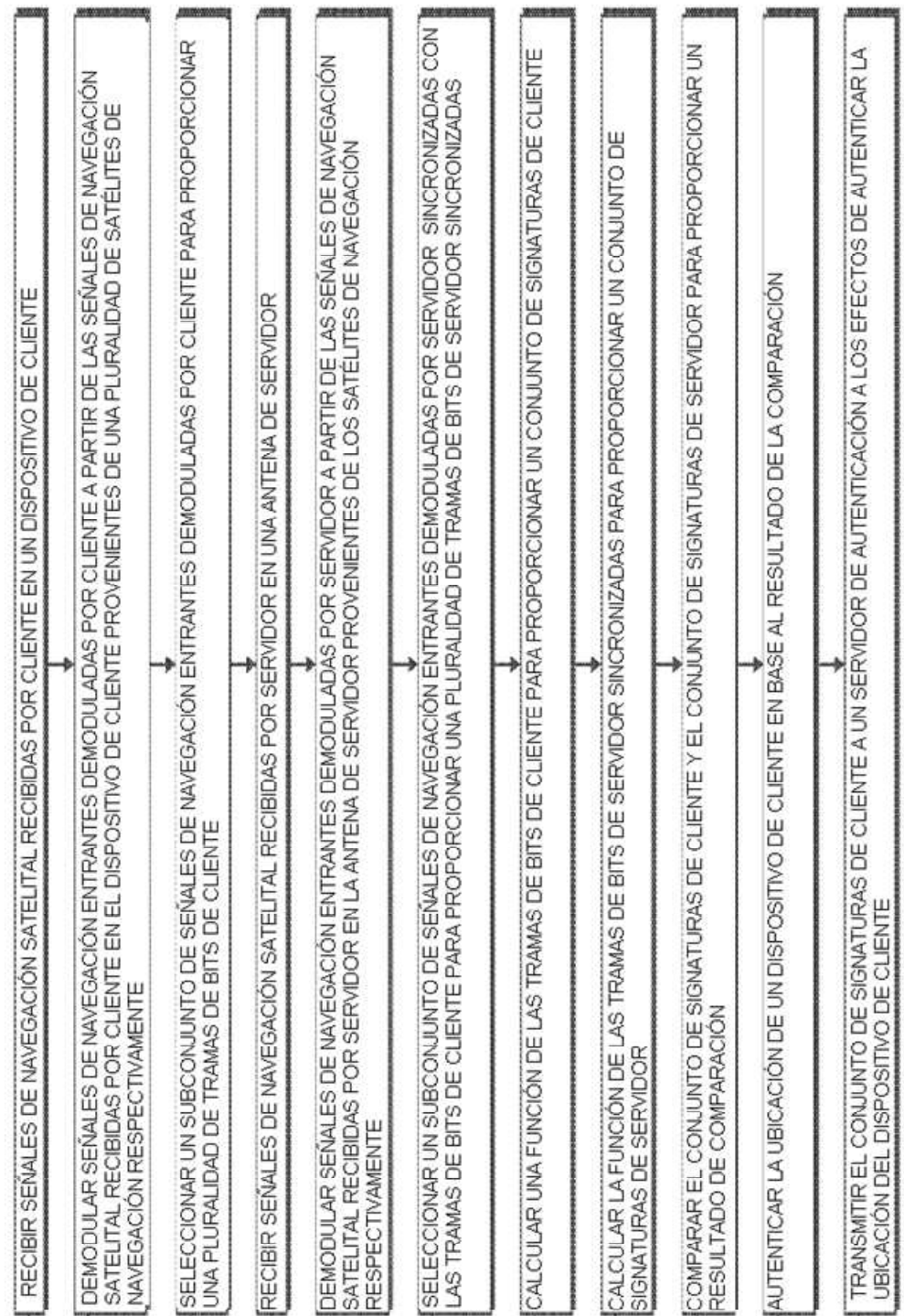
1300
1302
RECIBIR SEÑALES DE NAVEGACIÓN SATELITAL RECIBIDAS POR CLIENTE EN UN DISPOSITIVO DE CLIENTE
1304
DEMODULAR SEÑALES DE NAVEGACIÓN ENTRANTES DEMODULADAS POR CLIENTE A PARTIR DE LAS SEÑALES DE NAVEGACIÓN SATELITAL RECIBIDAS POR CLIENTE EN EL DISPOSITIVO DE CLIENTE PROVENIENTES DE UNA PLURALIDAD DE SATÉLITES DE NAVEGACIÓN RESPECTIVAMENTE
1306
SELECCIONAR UN SUBCONJUNTO DE SEÑALES DE NAVEGACIÓN ENTRANTES DEMODULADAS POR CLIENTE PARA PROPORCIONAR UNA PLURALIDAD DE TRAMAS DE BITS DE CLIENTE
1308
RECIBIR SEÑALES DE NAVEGACIÓN SATELITAL RECIBIDAS POR SERVIDOR EN UNA ANTENA DE SERVIDOR
1310
DEMODULAR SEÑALES DE NAVEGACIÓN ENTRANTES DEMODULADAS POR SERVIDOR A PARTIR DE LAS SEÑALES DE NAVEGACIÓN SATELITAL RECIBIDAS POR SERVIDOR EN LA ANTENA DE SERVIDOR PROVENIENTES DE LOS SATÉLITES DE NAVEGACIÓN RESPECTIVAMENTE
1312
SELECCIONAR UN SUBCONJUNTO DE SEÑALES DE NAVEGACIÓN ENTRANTES DEMODULADAS POR SERVIDOR SINCRONIZADAS CON LAS TRAMAS DE BITS DE CLIENTE PARA PROPORCIONAR UNA PLURALIDAD DE TRAMAS DE BITS DE SERVIDOR SINCRONIZADAS
1314
CALCULAR UNA FUNCIÓN DE LAS TRAMAS DE BITS DE CLIENTE PARA PROPORCIONAR UN CONJUNTO DE SIGNATURAS DE CLIENTE
1316
CALCULAR LA FUNCIÓN DE LAS TRAMAS DE BITS DE SERVIDOR SINCRONIZADAS PARA PROPORCIONAR UN CONJUNTO DE SIGNATURAS DE SERVIDOR
1318
COMPARAR EL CONJUNTO DE SIGNATURAS DE CLIENTE Y EL CONJUNTO DE SIGNATURAS DE SERVIDOR PARA PROPORCIONAR UN RESULTADO DE COMPARACIÓN
1320
AUTENTICAR LA UBICACIÓN DE UN DISPOSITIVO DE CLIENTE EN BASE AL RESULTADO DE LA COMPARACIÓN
1322
TRANSMITIR EL CONJUNTO DE SIGNATURAS DE CLIENTE A UN SERVIDOR DE AUTENTICACIÓN A LOS EFECTOS DE AUTENTICAR LA UBICACIÓN DEL DISPOSITIVO DE CLIENTE

FIG. 13

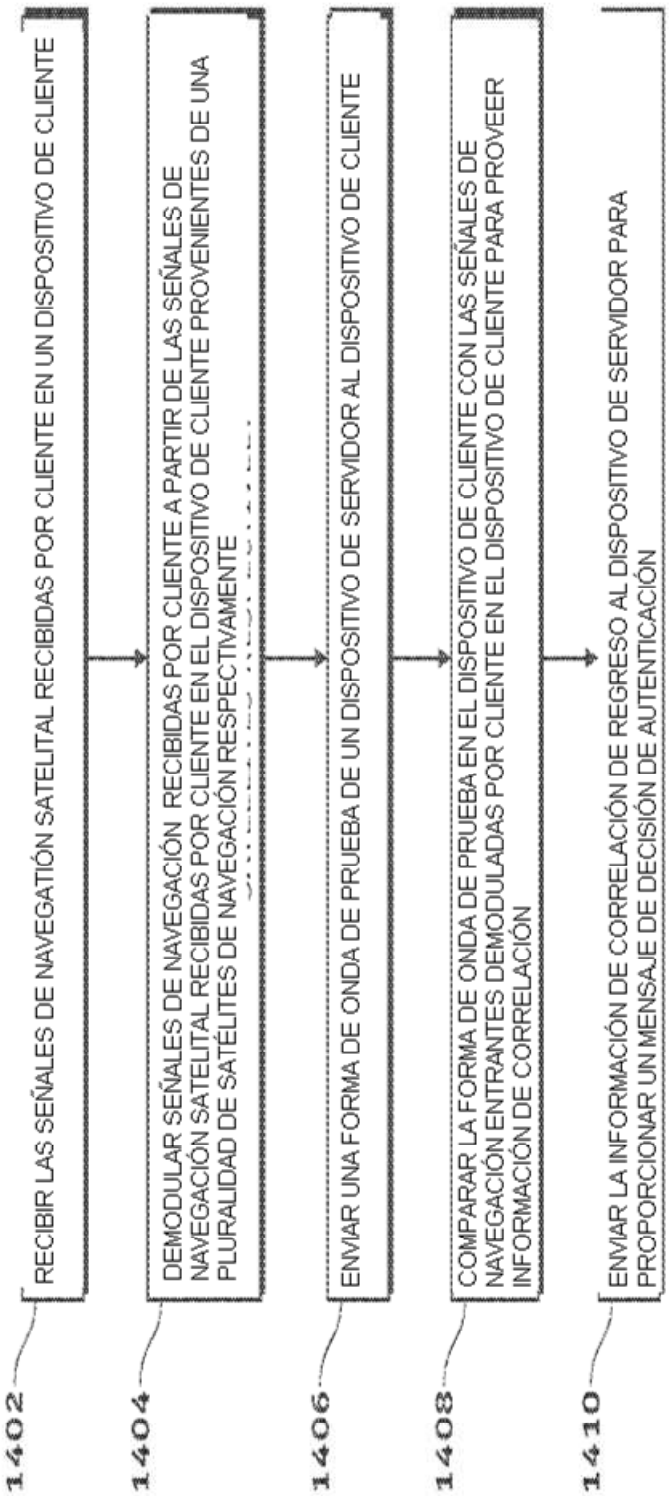
1400
1402
RECIBIR LAS SEÑALES DE NAVEGATIÓN SATELITAL RECIBIDAS POR CLIENTE EN UN DISPOSITIVO DE CLIENTE
1404
DEMODULAR SEÑALES DE NAVEGACIÓN RECIBIDAS POR CLIENTE A PARTIR DE LAS SEÑALES DE NAVEGACIÓN SATELITAL RECIBIDAS POR CLIENTE EN EL DISPOSITIVO DE CLIENTE PROVENIENTES DE UNA PLURALIDAD DE SATÉLITES DE NAVEGACIÓN RESPECTIVAMENTE
1406
ENVIAR UNA FORMA DE ONDA DE PRUEBA DE UN DISPOSITIVO DE SERVIDOR AL DISPOSITIVO DE CLIENTE
1408
COMPARAR LA FORMA DE ONDA DE PRUEBA EN EL DISPOSITIVO DE CLIENTE CON LAS SEÑALES DE NAVEGACIÓN ENTRANTES DEMODULADAS POR CLIENTE EN EL DISPOSITIVO DE CLIENTE PARA PROVEER INFORMACIÓN DE CORRELACIÓN
1410
ENVIAR LA INFORMACIÓN DE CORRELACIÓN DE REGRESO AL DISPOSITIVO DE SERVIDOR PARA PROPORCIONAR UN MENSAJE DE DECISIÓN DE AUTENTICACIÓN

*FIG. 14*