(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 811 517**

(51) Int. CI.:

G01S 19/05 (2010.01)
G01S 19/25 (2010.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **20.12.2012 E 12008471 (0)**

(97) Fecha y número de publicación de la concesión europea: **10.06.2020 EP 2746810**

(54) Título: **Sistema de navegación segura asistida con GNSS**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.03.2021

(73) Titular/es:

AIRBUS DEFENCE AND SPACE GMBH (100.0%)
Willy-Messerschmitt-Straße 1
82024 Taufkirchen, DE

(72) Inventor/es:

WENDEL, JAN y
KOGLER, WOLFGANG

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Sistema de navegación segura asistida con GNSS

Campo técnico

La invención se refiere a un sistema de navegación segura asistida con GNSS.

Antecedentes

La navegación asistida sirve para mejorar las prestaciones de un sistema de posicionamiento basado en GNSS (Sistema Global de Navegación por Satélite). Mientras que los dispositivos autónomos de posicionamiento o navegación basados en GNSS sólo utilizan señales de radio de los satélites GNSS, los dispositivos de navegación asistida también utilizan recursos de red para mejorar las prestaciones de posicionamiento. En (NAVSTAR-) GPS, se introdujo el sistema GPS asistido (A-GPS) para mejorar las prestaciones del posicionamiento basado en GPS. A-GPS es un procedimiento bien conocido y establecido para mejorar las prestaciones de los receptores GPS proporcionando información a través de un enlace de comunicación al receptor GPS.

Este procedimiento se utiliza a menudo con los chips GPS integrados en teléfonos móviles, ya que para esta aplicación el enlace de comunicación ya está disponible. La información proporcionada al receptor por un servidor de asistencia consiste, por ejemplo, en una posición aproximada obtenida a partir del ID de célula de teléfono móvil u otros medios, datos de almanaque y/o efemérides e información de tiempo. Con esta información, el receptor puede calcular qué satélites podrían estar visibles y restringir el proceso de adquisición a estos satélites visibles.

Además, a partir de la posición de receptor aproximada, del tiempo y de la información de órbita de satélite de datos de almanaque o efemérides, el receptor puede calcular la frecuencia Doppler de señal de satélite esperada y, por lo tanto, reducir el espacio de búsqueda de frecuencia en el proceso de adquisición. Esto da lugar a una reducción significativa del tiempo hasta la primera determinación (TTFF), o de forma alternativa, con la misma complejidad computacional, los tiempos de correlación por tramo de frecuencia pueden aumentar en comparación con el caso no asistido, proporcionando una mayor sensibilidad en la adquisición.

Sin embargo, pueden lograrse otros beneficios; por ejemplo, proporcionando el mensaje de navegación completo al receptor, se supera la necesidad de desmodulación de mensajes, lo que permite utilizar señales de satélite para el posicionamiento cuando dicha desmodulación no sería posible debido a una baja relación de densidad de portadora a ruido.

En el sistema Galileo GNSS europeo se proporcionará un servicio público regulado (PRS) Galileo, restringido a usuarios autorizados por el gobierno, que se utilizará en aplicaciones sensibles que requieran un alto nivel de continuidad de servicio. Actualmente se está debatiendo el desarrollo de un servicio PRS Galileo asistido. En principio, un PRS asistido proporciona las mismas ventajas que A-GPS, como un TTFF reducido, etc. No obstante, el servicio PRS Galileo utiliza mensajes y códigos de medición de distancia cifrados para controlar el acceso a este servicio: Sin claves válidas necesarias para el descifrado, no es posible rastrear las señales PRS y obtener una determinación de posición. El descifrado de los mensajes PRS y la generación de los códigos de medición de distancia se realizan en el módulo de seguridad del receptor PRS, que es un factor importante del coste y el consumo de energía.

El fabricante de receptores u-blox AG, Zurich, Suiza, ofrece una tecnología denominada "captura y proceso". Mediante la misma, el receptor adquiere 200 ms de muestras sin procesar de IF o banda base GPS, que se procesan posteriormente en un PC para generar una determinación de posición. La información adicional requerida, como los datos de efemérides, es proporcionada por un servidor a través de Internet.

La patente estadounidense US5952960A divulga un receptor de correlación retardada para el procesamiento de retardo de las señales de satélite cifradas. Una estación central está diseñada para recibir señales de satélite codificadas utilizando una antena de alta ganancia. La estación central extrae la información de satélite cifrada y la transmite al receptor de correlación retardada. El receptor de correlación retardada recibe la información de satélite cifrada utilizando la antena de satélite estándar y realiza la correlación completa con la información cifrada recibida desde la estación central sin requerir las claves de cifrado secretas.

La solicitud de patente internacional WO2010/105136A2 describe un sistema y un procedimiento para detectar la falsificación de señales mediante el procesamiento de ráfagas intermitentes de señales cifradas del Sistema Global de Navegación por Satélite (GNSS) con el fin de determinar si las señales no cifradas se están falsificando.

Resumen de la invención

Un objetivo de la invención es proporcionar un sistema mejorado de navegación segura asistida con GNSS.

Este objetivo se consigue mediante la materia objeto de las reivindicaciones independientes. Formas de realización adicionales se muestran en las reivindicaciones dependientes.

La presente invención se basa en el siguiente concepto básico: ampliando la idea antes mencionada de "captura y proceso", podría establecerse una arquitectura PRS asistida para la navegación segura asistida, donde el receptor PRS captura muestras de banda base, las transfiere a un servidor de asistencia que calcula una determinación de posición y transfiere esta determinación de posición al receptor PRS. El procesamiento de los mensajes PRS y la generación de réplicas de códigos de medición de distancia para la correlación con las muestras de banda base solo se llevarían a cabo en el servidor de asistencia; el receptor PRS no necesitaría tener un módulo de seguridad, no necesitaría descodificar mensajes PRS y no necesitaría generar códigos de medición de distancia. El control de acceso al servicio PRS podría aplicarse a través del enlace de comunicación; por ejemplo, TETRA proporciona mecanismos de autenticación y una identificación inequívoca de cada terminal mediante un código PIN que podría utilizarse para este fin. Sin embargo, los principales inconvenientes de este enfoque ampliado de captura y proceso son la enorme cantidad de datos que deben transferirse del receptor al servidor de asistencia, y el hecho de que la cantidad de datos que se transferirán y la potencia de procesamiento requerida en el servidor de asistencia crecen proporcionalmente al número de receptores a los que se dará servicio. Por lo tanto, la presente invención propone la provisión de fragmentos de código de medición de distancia de un servicio GNSS cifrado a través de enlaces de comunicación desde uno o más servidores de asistencia para que los receptores de señales de servicio GNSS cifradas puedan procesar estas señales cifradas mediante los fragmentos de código de medición de distancia proporcionados, que permiten correlacionar una señal de servicio GNSS cifrada recibida sin requerir ningún medio de seguridad como, por ejemplo, los requeridos para recibir y procesar señales PRS Galileo. En comparación con un enfoque de captura y proceso ampliado como el descrito anteriormente, la cantidad de datos a transferir a través de una red es significativamente menor: Los fragmentos de código de medición de distancia tienen una velocidad de datos mucho menor que las muestras de IF o de banda base. Las réplicas para la correlación con la señal recibida se generan en el receptor. Además, varios receptores podrían escuchar una radiodifusión de fragmentos de código de medición de distancia de un servidor de asistencia, por lo que la cantidad de datos a transferir a través de la red no aumenta necesariamente con el número de receptores que son atendidos por un servidor de asistencia.

Una forma de realización de la invención se refiere a un sistema de navegación segura asistida con un servicio GNSS cifrado y se define mediante la reivindicación 1 independiente.

Los detalles específicos de esta forma de realización se definen mediante las reivindicaciones 2 a 5 dependientes.

Una forma de realización adicional de la invención se refiere a un servidor de asistencia GNSS para su uso con un sistema de la invención y se define mediante la reivindicación 6 independiente.

Los detalles específicos de esta forma de realización adicional se definen mediante la reivindicación 7 dependiente.

Otra forma de realización de la invención se refiere a un receptor GNSS de navegación segura asistida con un sistema de la invención y se define mediante la reivindicación 8 independiente.

Los detalles específicos de esta otra forma de realización se definen mediante la reivindicación 9 dependiente.

Otra forma de realización adicional de la invención se refiere a un procedimiento para recibir fragmentos de código de medición de distancia de un servicio GNSS cifrado proporcionado por un sistema de la invención y se define mediante la reivindicación 10 independiente.

Una forma de realización adicional de la invención se refiere a un programa informático, que implementa el procedimiento de acuerdo con la invención y se define mediante la reivindicación 11 independiente.

De acuerdo con una forma de realización adicional de la invención, un soporte de registro que almacena un programa informático de acuerdo con la invención se define mediante la reivindicación 12.

Estos y otros aspectos de la invención serán evidentes y se aclararán con referencia a las formas de realización descritas a continuación.

La invención se describirá con más detalle a continuación con referencia a formas de realización a modo de ejemplo. Sin embargo, la invención no se limita a estas formas de realización a modo de ejemplo.

Breve descripción de los dibujos

La Fig. 1 muestra una forma de realización de un diagrama de bloques de una arquitectura para un PRS asistido con un receptor A-PRS y un servidor de asistencia de acuerdo con la invención.

Descripción de formas de realización

En lo sucesivo, elementos funcionalmente similares o idénticos pueden tener los mismos números de referencia. Además, se describe la siguiente forma de realización de la invención para el caso de PRS Galileo, pero cabe señalar que la invención se puede aplicar a cualquier señal y servicio de navegación segura que use cifrado de mensajes y/o de código de medición de distancia.

La Fig. 1 muestra una arquitectura para un PRS asistido, donde uno o más servidores de asistencia 10 proporcionan, mediante enlaces de comunicación 12, fragmentos de código de medición de distancia PRS a uno o más receptores A-PRS 14.

El receptor A-PRS 14 es capaz de recibir una SIS (señal en el espacio) desde un satélite GNSS, donde la SIS puede comprender datos de un servicio GNSS cifrado tal como el PRS Galileo. El receptor A-PRS 14 no está equipado con medios de seguridad para descifrar por sí mismo el servicio PRS cifrado, es decir, sin los fragmentos de código de medición de distancia del servidor de asistencia 10.

El servidor de asistencia 10 comprende un receptor PRS 20, equipado con un módulo de seguridad completo y debidamente codificado, o cualquier otro medio, de modo que el receptor 20 puede recibir el servicio GNSS cifrado y descifrar la información transmitida por el servicio. A partir de la información de servicio GNSS descifrada, una generación de datos de asistencia 18 del servidor 10 genera fragmentos de código de medición de distancia adecuados para utilizarse para generar réplicas para su correlación con muestras de una señal de servicio GNSS cifrada recibida, es decir, con muestras SIS de esta señal. Al utilizarse estas réplicas para la correlación, no se requiere un descifrado adicional en el receptor A-PRS.

Los fragmentos de código de medición de distancia generados por la unidad de generación de datos de asistencia 18 pueden ser válidos, en un ejemplo útil para entender la invención, durante un intervalo de tiempo definido con anterioridad, en el que el receptor A-PRS 14 ha adquirido muestras de IF o de banda base de la SIS, o, de acuerdo con una forma de realización de la invención, durante un intervalo de tiempo definido en el futuro, donde el receptor PRS adquirirá muestras de IF o de banda base de la SIS. Los fragmentos de código de medición de distancia se pueden transmitir a través del enlace de comunicación 12 con una marca de tiempo que define su validez. El número de fragmentos de código de medición de distancia debe ser suficiente para permitir la generación de réplicas para su correlación con la señal recibida.

El enlace de comunicación 12 puede cifrarse de modo que solo los receptores A-PRS 14 puedan recibir los fragmentos de código de medición de distancia transmitidos con el enlace de comunicación 12, que pueden y están autorizados a descifrarlos.

La transmisión de fragmentos de código de medición de distancia a través del enlace de comunicación 12 se puede realizar mediante radiodifusión, es decir, a través de una comunicación de punto a multipunto. Por ejemplo, el servidor de asistencia 10 puede estar configurado para transmitir fragmentos de código de medición de distancia con un mensaje de radiodifusión a través del enlace de comunicación 12 de modo que la recepción de los fragmentos de código de medición de distancia no se restrinja a un receptor A-PRS.

El enlace de comunicación 12 puede ser un enlace de comunicación por cable y/o inalámbrico y también utilizar protocolos de transmisión estándar tales como TCP/IP. En particular, puede ser un enlace de comunicación móvil tal como el utilizado por dispositivos móviles con acceso a Internet, tales como teléfonos móviles o teléfonos inteligentes que usan UMTS, GPRS, HSDPA, de modo que un dispositivo móvil de este tipo que contiene el receptor A-PRS 14 pueda recibir y usar el PRS.

El servidor de asistencia 10 puede ser un servidor estándar de la industria al que se puede acceder a través de un protocolo de red estándar, en particular TCP/IP. Para permitir un acceso amplio y fácil, el servidor de asistencia 10 puede estar conectado a Internet y ser accesible a través de un URL en Internet desde cualquier dispositivo.

Con el fin de conceder acceso únicamente a los usuarios autorizados, el servidor de asistencia 10 puede comunicarse con un servidor de sistema de autenticación y/o identificación 16, que autoriza a los receptores A-PRS 14 a acceder a y recibir fragmentos de código de medición de distancia desde el servidor de asistencia 10. El control de acceso al servicio del servidor de asistencia 10 también podría aplicarse a través de las capacidades de autenticación e identificación del enlace de comunicación 12, por ejemplo, como las ofrecidas por las radios móviles profesionales (PMR) TETRA y TETRAPOL.

Usando los fragmentos de código de medición de distancia proporcionados a través del enlace de comunicación 12, que está cifrado o no cifrado, el receptor A-PRS 14 puede generar réplicas de código con una unidad de generación de réplicas 22 y puede correlacionar estas réplicas con las muestras de IF o de banda base adquiridas de la SIS que transmiten el PRS mediante una unidad de correlación 24.

La información contenida en los mensajes de navegación como efemérides, etc., que son requeridos por el receptor para calcular una determinación de posición, es proporcionada también por el enlace de comunicación 12 o ha sido almacenada en el receptor 14 con anterioridad.

Con las réplicas generadas a partir de los fragmentos de código de medición de distancia y la información de mensaje de navegación, una unidad PVT (Posición, Velocidad, Tiempo) 26 del receptor 14 es capaz de calcular una determinación de posición sin requerir un módulo de seguridad, gestionar mensajes PRS o claves PRS.

A continuación se resumen brevemente algunas ventajas de la presente invención con respecto a la forma de realización descrita anteriormente:

- El receptor A-PRS 14 no necesita tener un módulo de seguridad, no se requiere el procesamiento de mensajes PRS y no tiene que haber claves PRS disponibles en el receptor. Esto da lugar a una baja complejidad, un bajo consumo de energía, una mayor duración de la batería y una reducción de costes para el receptor. Además, se evitan problemas de seguridad relacionados con el receptor.
- En comparación con un enfoque de captura y proceso, la cantidad de datos a transferir a través de la red es significativamente menor: Los fragmentos de código de medición de distancia tienen una velocidad de datos mucho menor que las muestras de IF o de banda base. Las réplicas para la correlación con la señal recibida se generan en el receptor. Además, varios receptores podrían escuchar una radiodifusión de fragmentos de código de medición de distancia desde el servidor de asistencia, por lo que la cantidad de datos a transferir a través de la red no aumenta necesariamente con el número de receptores que son atendidos por un servidor de asistencia.

Números de referencia

10 Servidor de asistencia
12 Enlace de comunicación para transmitir fragmentos de código de medición de distancia y mensajes de navegación
14 Receptor A-PRS
16 Servidor de sistema de autenticación y/o identificación
18 Unidad de generación de datos de asistencia
20 Receptor PRS
22 Unidad de generación de réplicas
24 Unidad de correlación
26 Unidad de cálculo PVT

REIVINDICACIONES

1. Un sistema de navegación segura asistida con un servicio cifrado del Sistema Global de Navegación por Satélite, GNSS, donde el sistema comprende uno o más servidores de asistencia (10) configurados para proporcionar a través de enlaces de comunicación (12) fragmentos de código de medición de distancia del servicio GNSS cifrado junto con una marca de tiempo que define su validez a uno o más receptores (14) del servicio GNSS cifrado, donde los fragmentos de código de medición de distancia proporcionados son válidos durante un intervalo de tiempo definido en el futuro, donde el número de fragmentos de código de medición de distancia es suficiente para permitir la generación de réplicas para su correlación con una señal recibida del servicio GNSS cifrado.

2. El sistema según la reivindicación 1, que comprende además un sistema de autenticación y/o identificación (16), donde el sistema de autenticación y/o identificación (16) está adaptado para controlar el acceso a los fragmentos de código de medición de distancia proporcionados del servicio GNSS cifrado.

3. El sistema según la reivindicación 1 o 2, en el que uno o más de los enlaces de comunicación (12) que proporcionan fragmentos de código de medición de distancia del servicio GNSS cifrado a uno o más receptores (14) del servicio GNSS cifrado están protegidos mediante un cifrado.

4. El sistema según cualquiera de las reivindicaciones anteriores, en el que el servicio GNSS cifrado es un servicio GNSS con señales y/o servicios de navegación seguros, que utiliza cifrado de mensajes y/o de código de medición de distancia.

5. El sistema según cualquiera de las reivindicaciones anteriores, en el que el GNSS es Galileo y el servicio GNSS cifrado es el servicio público regulado Galileo.

6. Un servidor de asistencia GNSS (10) para su uso con un sistema según cualquiera de las reivindicaciones anteriores, que comprende

- una unidad de generación de datos de asistencia (18) configurada para proporcionar fragmentos de código de medición de distancia de un servicio GNSS cifrado a través de un enlace de comunicación (12) junto con una marca de tiempo que define su validez a uno o más receptores (14) del servicio GNSS cifrado, donde los fragmentos de código de medición de distancia proporcionados son válidos durante un intervalo de tiempo definido en el futuro, donde el número de fragmentos de código de medición de distancia es suficiente para permitir la generación de réplicas para su correlación con una señal recibida del servicio GNSS cifrado.

7. El servidor de asistencia GNSS según la reivindicación 6, que comprende además un receptor (20) adaptado para recibir y descifrar señales del servicio GNSS cifrado.

8. Un receptor GNSS (14) para la navegación segura asistida con un sistema según cualquiera de las reivindicaciones 1 a 6, que comprende

- una unidad de recepción configurada para recibir fragmentos de código de medición de distancia a través de enlaces de comunicación (12) desde un servidor de asistencia (10) de la reivindicación 6 o 7, donde los fragmentos de código de medición de distancia son proporcionados por el servidor de asistencia (10) y son válidos durante un intervalo de tiempo definido en el futuro, cuya validez está definida por una marca de tiempo proporcionada por el servidor de asistencia (10),
- una unidad de generación de réplicas (22) configurada para generar réplicas a partir de los fragmentos de código de medición de distancia recibidos, donde las réplicas son adecuadas para su correlación con una señal de servicio GNSS cifrada recibida,
- una unidad de correlación (24) configurada para correlacionar la señal de servicio GNSS cifrada recibida con las réplicas generadas y proporcionar una señal de servicio GNSS descifrada, y
- una unidad de cálculo (26) configurada para calcular una posición, una velocidad y/o un tiempo a partir de la señal de servicio GNSS descifrada.

9. El receptor GNSS según la reivindicación 8, que se adapta adicionalmente para descifrar los fragmentos de código de medición de distancia proporcionados a través de enlaces de comunicación cifrados desde uno o más servidores de asistencia del sistema según la reivindicación 3.

10. Un procedimiento para recibir fragmentos de código de medición de distancia de un servicio GNSS cifrado proporcionado por un sistema según cualquiera de las reivindicaciones 1 a 5, donde el procedimiento comprende recibir los fragmentos de código de medición de distancia a través de enlaces de comunicación (12) desde un servidor de asistencia (10) según la reivindicación 6 o 7, donde los fragmentos de código de medición de distancia recibidos son válidos durante un intervalo de tiempo definido en el futuro, cuya validez está definida por una marca de tiempo proporcionada por el servidor de asistencia (10), y generar réplicas a partir de los fragmentos de código de medición de distancia recibidos, donde las réplicas son adecuadas para su correlación con una señal de servicio GNSS cifrada

recibida, y proporcionar las réplicas generadas para correlacionar la señal de servicio GNSS cifrada recibida con las réplicas proporcionadas.

11. Un programa informático que comprende instrucciones que, cuando el programa es ejecutado por un receptor GNSS según la reivindicación 8 o 9, hacen que el receptor GNSS lleve a cabo el procedimiento de acuerdo con la reivindicación 10.

12. Un soporte de registro que tiene almacenado en el mismo un programa informático de acuerdo con la reivindicación 11.

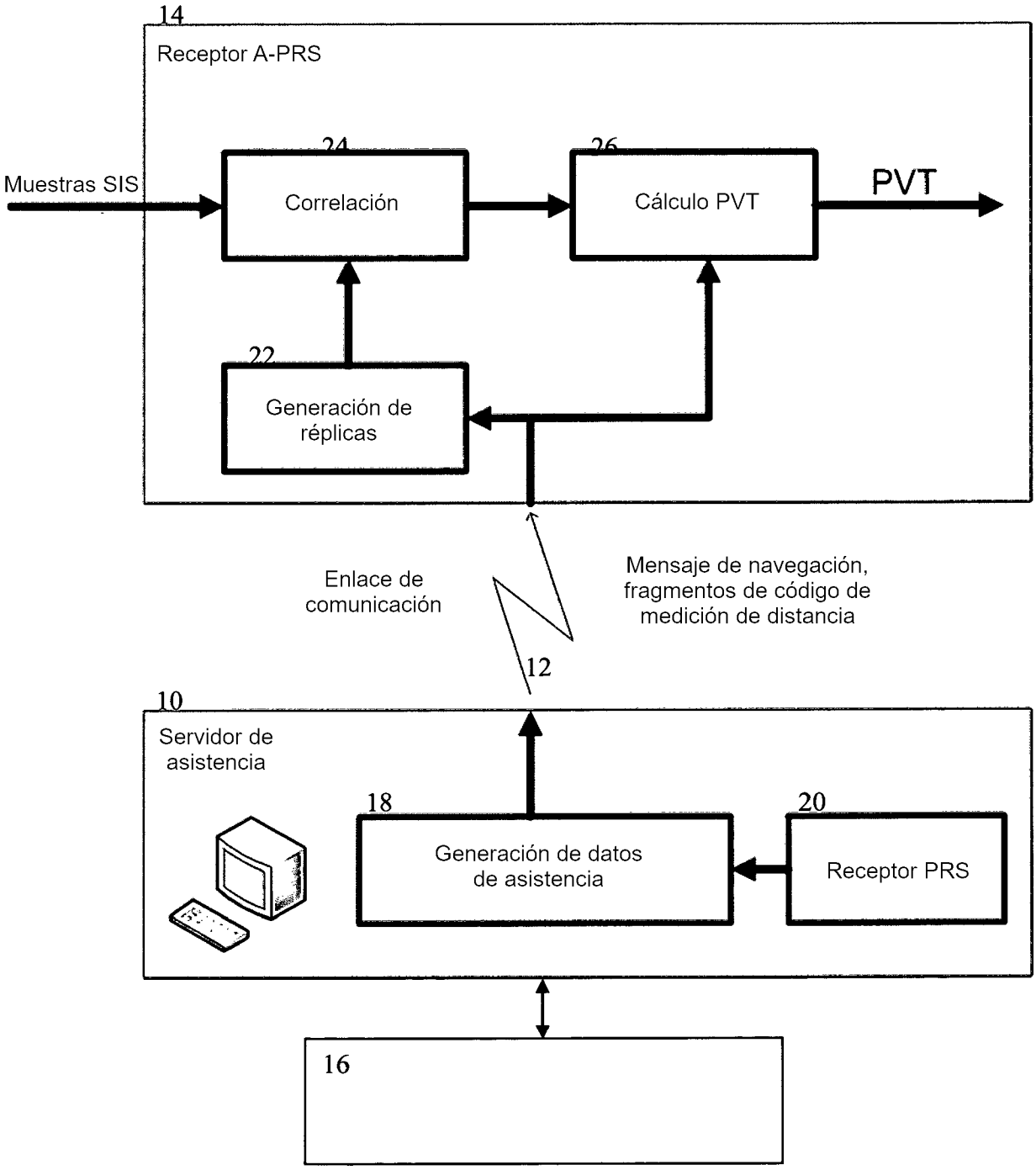
14
Receptor A-PRS
24
26
Muestras SIS
Correlación
Cálculo PVT
PVT
22
Generación de réplicas
Enlace de comunicación
Mensaje de navegación, fragmentos de código de medición de distancia
12
10
Servidor de asistencia
18
20
Generación de datos de asistencia
Receptor PRS
16

Fig. 1