(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 871 256**

(51) Int. CI.:

G01S 19/09 (2010.01)
G01S 19/14 (2010.01)
G01S 19/36 (2010.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **02.05.2013 E 13002338 (5)**

(97) Fecha y número de publicación de la concesión europea: **03.03.2021 EP 2799907**

(54) Título: **Posicionamiento mediante la utilización de señales de navegación de GNSS cifradas**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.10.2021

(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:

ELZABURU, S.L.P

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Posicionamiento mediante la utilización de señales de navegación de GNSS cifradas

Campo técnico

La invención se refiere al posicionamiento mediante el uso de señales de navegación de GNSS cifradas.

Antecedentes

En el sistema europeo de navegación por satélite global (GNSS – Global Navigation Satellite System, en inglés) Galileo, el servicio público regulado (PRS – Public Regulated Service, en inglés) de Galileo ofrece una navegación segura para los usuarios autorizados. El control de acceso al servicio PRS se logra mediante el cifrado de códigos de distancia y datos, de modo que solo un receptor PRS pueda obtener y rastrear estas señales de navegación de GNSS cifradas y realizar un posicionamiento, particularmente calcular una Posición, Velocidad, Tiempo (PVT), si se encuentran disponibles las claves adecuadas para descifrar las señales de navegación de GNSS cifradas. El procesamiento de seguridad, tal como el descifrado, se realiza dentro del módulo de seguridad del receptor de PRS, que es un factor importante para la complejidad, el consumo de energía y el coste.

La necesidad de un módulo de seguridad dentro del receptor se puede superar si el receptor solo captura muestras digitales de GNSS sin procesar y las envía a través de un enlace de comunicación seguro a un servidor seguro que contiene un receptor de PRS de software y las claves de PRS adecuadas. El servidor seguro calcula un PVT a partir de estas muestras de GNSS sin procesar y devuelve el PVT, o simplemente una posición fija, al receptor. El inconveniente de este enfoque es la gran cantidad de datos que deben ser transferidos a través de la red de comunicación debido al gran ancho de banda de las señales de PRS: para calcular una posición fija, se requiere un tamaño de instantánea de entre varios milisegundos y más de un segundo, dependiendo de la sensibilidad requerida. Considerando, por ejemplo, la señal de PRS de BOCc (Portadora de compensación binaria - Binary Offset Carrier, en inglés) (15,2.5) en E1, se requieren muestras de banda base complejas a una velocidad mínima de 32,5 MHz para capturar los lóbulos principales de la señal. Con un ADC (convertidor de analógico a digital – Analog Digital Converter, en inglés) de 3 bits y un tamaño de instantánea de solo 100 ms, esto ya lleva a casi 20 Mbit de datos por cada instantánea.

El fabricante de receptores u-blox AG, Zürich, Suiza, ofrece una tecnología denominada “Capture & Process”. De este modo, el receptor obtiene 200 ms de muestras de banda base de GPS (Sistema de posicionamiento global – Global Positioning System, en inglés) sin procesar (NAVSTAR-) o IF (Frecuencia intermedia – Intermediate Frequency, en inglés), que son procesadas posteriormente en un PC (Ordenador personal – Personal Computer, en inglés) para generar una posición fija. La información adicional requerida, tal como los datos de efemérides, la proporciona un servidor a través de Internet. Esta técnica se utiliza, por ejemplo, para el geoetiquetado de imágenes, y ofrece la ventaja de que, cuando se toma una imagen para la que se desea un geoetiquetado, no es necesario esperar a que el receptor de GPS obtenga y rastree las señales de GPS, lo que llevaría entre segundos y minutos. Este enfoque no proporciona correcciones de posición en tiempo real o casi en tiempo real.

El proyecto ULTRA tiene como objetivo el desarrollo de un receptor de PRS de muy bajo coste, basado en el enfoque descrito anteriormente: Las muestras de banda base o IF sin procesar se transfieren a través de un enlace de comunicación seguro a un servidor seguro que contiene un receptor de PRS de software. En el servidor protegido, las muestras de banda base o de IF sin procesar se utilizan para calcular una posición fija, que a continuación se envía de vuelta al receptor. Tal como se mencionó anteriormente, la carga de la red de comunicación conectada a la transferencia de muestras de banda base o de IF sin procesar desde el receptor al servidor seguro es extremadamente exigente para las señales de PRS, que tienen un ancho de banda significativamente mayor que, por ejemplo, la señal de apertura de SPS de GPS. El sitio web del proyecto se puede encontrar en http://www.ultra-prs.eu. Además, la publicación de Glen Gibbons: “Civil Galileo System Poses New Options for Secure Services”, Inside GNSS, 18 de diciembre de 2012 (2012-12-18), XP055089141, de Internet: URL:http://www.insidegnss.com/node/3326, describe el proyecto ULTRA.

Compendio de la invención

Un objeto de la invención es proporcionar posicionamiento utilizando navegación de GNSS cifrada, en la que se utiliza un servidor seguro y la cantidad de datos transmitidos a un servidor seguro se reduce en comparación con los métodos conocidos descritos al principio.

Este objeto se logra mediante el objeto de las reivindicaciones independientes. Las reivindicaciones dependientes muestran realizaciones adicionales.

La invención propone capturar solo una de las bandas laterales de una señal de navegación de GNSS cifrada, que se modula con un método de BOC, para reducir la cantidad de datos que deben ser transferidos desde un receptor de GNSS a un servidor seguro. Esto se puede lograr de diferentes maneras: mediante una combinación adecuada de conversión del lado del usuario, conversión a una frecuencia menor, filtrado y conversión de ADC (Conversión de digital a analógica), solo se muestrea una de las bandas laterales de la señal de navegación de GNSS cifrada, o la

señal de navegación de GNSS cifrada se muestrea completamente, y la reducción a una banda lateral que permite la reducción de la velocidad de muestreo se realiza mediante técnicas de procesamiento de señales. Con la invención propuesta, se pueden observar las siguientes ventajas:

- Se mantienen todas las ventajas de la arquitectura descrita en el proyecto ULTRA: No se requiere ningún módulo de seguridad en un receptor de GNSS, lo que permite reducir el coste, la complejidad y el consumo de energía del receptor de GNSS. Además, se evitan problemas de seguridad relacionados con el receptor.

- La cantidad de muestras de banda base o IF que deben ser transferidas desde un receptor de GNSS sin un módulo de seguridad a un servidor seguro para calcular un PVT se reduce significativamente. Alternativamente, para un volumen de transferencia de datos dado, el intervalo de tiempo durante el cual se pueden capturar las muestras aumenta, lo que permite una mayor sensibilidad.

Una realización de la invención se refiere a un método de posicionamiento mediante la utilización de señales de navegación de GNSS cifradas, que se modulan con un método de BOC y transmiten información cifrada en sus bandas laterales, que comprende los actos de: capturar solo una de las bandas laterales de una señal de navegación de GNSS cifrada, transmitir solo las muestras de la banda lateral capturada de la señal de navegación de GNSS cifrada a un servidor seguro para calcular un PVT a partir de las muestras recibidas, y recibir el PVT calculado desde el servidor seguro.

El acto de capturar solo una de las bandas laterales de una señal de navegación de GNSS cifrada puede comprender procesamiento del lado del usuario, conversión a una frecuencia menor, filtrado y conversión de analógica a digital de solo una de las bandas laterales de la señal de navegación de GNSS cifrada.

Alternativamente, el acto de capturar solo una de las bandas laterales de una señal de navegación de GNSS cifrada puede comprender muestrear la señal de navegación de GNSS cifrada completamente y reducir la señal muestreada a solo una de las bandas laterales realizando una técnica de procesamiento de señales.

La realización de una técnica de procesamiento de señales puede comprender la conversión a una frecuencia menor de la señal muestreada en una banda base, dividir la parte determinista de la señal muestreada convertida a una frecuencia menor en una señal de banda lateral superior e inferior, filtrar la señal convertida a una frecuencia menor, dividida, para eliminar la señal superior o la señal de banda lateral inferior, eliminando la modulación de subportadora de la señal de banda lateral filtrada para obtener una señal de banda lateral con una frecuencia central 0, y diezmando la señal de banda lateral con una frecuencia central 0 para obtener una señal de banda lateral capturada con una velocidad de muestreo menor.

Una realización adicional de la invención se refiere a un programa informático, que implementa el método de acuerdo con la invención y, tal como se describe en el presente documento y que permite el posicionamiento utilizando señales de navegación de GNSS cifradas proporcionadas de acuerdo con la invención cuando es ejecutado por un ordenador. Un programa informático de este tipo podría ser utilizado por un ordenador equipado con un receptor de GNSS, por ejemplo, un teléfono inteligente o un ordenador de navegación portátil, permitiendo que el ordenador no solo procese señales de navegación de GNSS estándar, sino también señales de servicio de GNSS cifradas, tales como las señales de PRS de Galileo. El ordenador no debe estar equipado con un módulo de seguridad, sino que solo debe ser configurado para comunicarse con un servidor seguro a fin de realizar el posicionamiento con señales de navegación de GNSS cifradas.

De acuerdo con otra realización de la invención, se puede proporcionar un soporte de grabación que almacene un programa de ordenador de acuerdo con la invención, por ejemplo, un CD-ROM, un DVD, una tarjeta de memoria, un disquete o un soporte de datos similar, adecuado para almacenar el programa informático para acceso electrónico.

Otra realización más de la invención se refiere a un receptor de GNSS para posicionamiento mediante la utilización de señales de navegación de GNSS cifradas, que se modulan con un método de BOC y transmiten información cifrada en sus bandas laterales, que comprende medios para capturar solo una de las bandas laterales de una señal de navegación de GNSS cifrada., medios para transmitir muestras de la banda lateral capturada de la señal de navegación de GNSS cifrada a un servidor seguro que se proporciona para calcular un PVT a partir de las muestras recibidas, y medios para recibir el PVT calculado desde el servidor seguro.

Los medios para capturar solo una de las bandas laterales de una señal de navegación de GNSS cifrada pueden comprender un extremo del lado del usuario de RF para convertir una señal de navegación de GNSS cifrada recibida en una banda base, un filtro para eliminar la señal de banda lateral superior o inferior de la señal convertida a una frecuencia menor, un multiplicador y una unidad de eliminación de subportadoras para eliminar la modulación de subportadora de la señal de banda lateral filtrada, y una unidad de diezmado para obtener una señal de banda lateral capturada con una velocidad de muestreo más baja.

Los medios para transmitir solo las muestras de la banda lateral capturada de la señal de navegación de GNSS cifrada a un servidor seguro y/o los medios para recibir el PVT calculado desde el servidor seguro pueden ser configurados para establecer un enlace de comunicación seguro con el servidor seguro a través de una red de comunicación, en particular Internet.

Un ejemplo que no describe parte de la invención se refiere a un servidor seguro para calcular un PVT a partir de muestras de una banda lateral de una señal de navegación de GNSS cifrada recibida de un receptor de GNSS de la invención y tal como se describe en el presente documento, y que comprende una unidad de descifrado de PRS para descifrar las muestras recibidas de la banda lateral de la señal de navegación de GNSS cifrada, un receptor de software de PRS para calcular un PVT a partir de las muestras descifradas de la banda lateral de la señal de navegación de GNSS cifrada, y medios para transmitir el PVT calculado al receptor de GNSS. El servidor seguro puede ser implementado, por ejemplo, mediante un PC configurado para ejecutar un programa informático que implemente el receptor de software de PRS y la unidad de descifrado de PRS y equipado con un adaptador de red para establecer enlaces de comunicación particularmente seguros con los receptores de GNSS de acuerdo con la invención y tal como se describe en el presente documento.

Estos y otros aspectos de la invención resultarán evidentes y se aclararán con referencia a las realizaciones que se describen a continuación.

La invención se describirá con más detalle a continuación con referencia a realizaciones a modo de ejemplo. Sin embargo, la invención no está limitada a estos ejemplos de realización.

Breve descripción de los dibujos

La figura 1 muestra una realización de un diagrama de bloques de una implementación de posicionamiento del sistema mediante la utilización de señales de navegación de GNSS cifradas con un receptor de GNSS y un servidor seguro de acuerdo con la invención; y

la figura 2 muestra la densidad espectral de potencia de la señal de navegación de GNSS modulada de BOCc (15,2.5).

Descripción de realizaciones

A continuación, los elementos funcionalmente similares o idénticos pueden tener los mismos números de referencia. Además, la siguiente realización de la invención se describe para el caso de Galileo de PRS, pero se debe tener en cuenta que la invención se puede aplicar a cualquier señal de navegación segura y servicios que utilicen mensajes y/o cifrado de códigos de telemetría.

A continuación, se describe en detalle una realización de la invención, en la que una señal de Galileo de PRS recibida se muestrea completamente y la reducción a una banda lateral que permite la reducción de la velocidad de muestreo se realiza mediante técnicas de procesamiento de señales.

La figura 1 muestra un receptor 10 que es un rover para un Galileo de SIS (señal en el espacio) 12. El SIS 12 está modulado por BOC y transmite información de PRS cifrada en sus bandas laterales.

En el receptor 10, el SIS 12 recibido está en un extremo del lado del usuario 14 de RF convertido a una frecuencia menor en una banda base compleja. Un modelo simplificado para una señal de BOC $s(t)$, que es emitida por el lado del usuario de RF 14, en la banda base compleja viene dada por

$$s(t) = \frac{A}{\sqrt{2}} \cdot c(t) \cdot b(t) \cdot e^{j\omega_{dop}t} + n(t)$$

Por la presente, A es una amplitud, $C(t)$ es el código de PRN, $B(t)$ es una subportadora rectangular con frecuencia angular ω_{sub}, ω_{dop} es la frecuencia angular Doppler, y $n(t)$ es un ruido complejo. Sin impacto en la validez de los resultados, la subportadora rectangular puede ser aproximada con una función coseno, lo que lleva a

$$s(t) = \frac{A}{\sqrt{2}} \cdot c(t) \cdot \cos(\omega_{sub}t) \cdot e^{j\omega_{dop}t} + n(t)$$

Utilizando algunas identidades trigonométricas, la parte determinista de este modelo de señal se puede dividir en una señal de banda lateral superior $s_u(t)$ y una señal de banda lateral inferior $s_l(t)$:

$$\begin{aligned} s(t) &= \frac{A}{2\sqrt{2}} \cdot c(t) \cdot \left(e^{j\omega_{sub}t} + e^{-j\omega_{sub}t}\right) \cdot e^{j\omega_{dop}t} + n(t) \\ &= \frac{A}{2\sqrt{2}} \cdot c(t) \cdot e^{j\omega_{sub}t} \cdot e^{j\omega_{dop}t} + \frac{A}{2\sqrt{2}} \cdot c(t) \cdot e^{-j\omega_{sub}t} \cdot e^{j\omega_{dop}t} + n(t) \\ &= s_u(t) + s_l(t) + n(t) \end{aligned}$$

El primer paso después de la conversión a una frecuencia menor de la señal de BOC a banda base es eliminar una banda lateral mediante un filtrado apropiado con un filtro 16. Por ejemplo, si se mantiene la banda lateral superior, la señal resultante después del filtrado viene dada por

$$s_{filt}(t) = \frac{A}{2\sqrt{2}} \cdot c(t) \cdot e^{j\omega_{sub}t} \cdot e^{j\omega_{dop}t} + n_{filt}(t)$$

Multiplicación mediante un multiplicador 18 con $e^{j\omega subt}$ proporcionada por una unidad de eliminación de subportadoras elimina la modulación de la subportadora, que desplaza el lóbulo lateral superior a la frecuencia cero:

$$s_{filt,wo}(t) = \frac{A}{2\sqrt{2}} \cdot c(t) \cdot e^{j\omega_{dop}t} + n_{filt,wo}(t)$$

La señal resultante tiene un ancho de banda que es igual al ancho de banda del código de PRN, y a continuación se puede aplicar un diezmado apropiado con un diezmador 22 para obtener una señal 24 con una velocidad de muestreo más baja. Alternativamente, se puede utilizar el lóbulo lateral inferior o muestras de IF en lugar de muestras de banda base.

La señal 24 con la velocidad de muestreo más baja es transmitida por el receptor de GNSS 10 a un servidor seguro 26 a través de un enlace de comunicación seguro bidireccional establecido entre el receptor 10 y el servidor 26, por ejemplo, un enlace de comunicación cifrado a través de Internet tal como una VPN (Red privada virtual - Virtual Private Network, en inglés), una SSL (Capa de puertos seguros - Secure Sockets Layer, en inglés) u otro enlace de comunicación cifrado.

El servidor 26 protegido comprende un receptor 28 de software de PRS y una unidad 30 de descifrado de PRS correspondiente al módulo de seguridad de un receptor de PRS. El receptor de software de PRE 28 calcula con las muestras 24 recibidas después del descifrado por medio de la unidad 30 de descifrado de PRS a PVT. El PVT 32 calculado se transmite con un transmisor a través del enlace de comunicación cifrado bidireccional de vuelta al receptor de GNSS 10.

Puesto que solo se transfieren muestras de un lóbulo lateral de la señal de PRS desde el receptor 10 al servidor seguro 26, la cantidad de datos transferidos se reduce significativamente. Esto reduce la precisión alcanzable de la fijación de posición de lo que se puede lograr con la señal de BOC completa a aproximadamente la precisión de la señal de BPSK correspondiente. Por otro lado, el problema potencial de un falso bloqueo a un pico lateral de la función de correlación, que puede ocurrir con señales de BOC, ya no existe.

La densidad espectral de potencia de una señal de navegación de GNSS modulada con BOCc (15,2,5) se muestra a modo de ejemplo en la figura 2. La señal de PRS de Galileo en E1 es una BOCc (15,2,5) y requeriría una velocidad de muestreo de al menos 32,5 MHz para capturar ambos lóbulos laterales, dado que se utilizan muestras complejas de banda base. Con el enfoque de la invención, la reducción a un lóbulo lateral permite reducir la velocidad de muestreo a 2,5 MHz, es decir, el volumen de transferencia de datos se reduce en un factor de 13. Alternativamente, para un volumen de transferencia de datos dado, la duración de la instantánea se puede aumentar en un factor 13, que ofrece un aumento de sensibilidad de más de 11 dB.

Números de referencia

10 Rover con receptor de Galileo

12 Galileo de SIS con PRS

14 interfaz de RF

16 filtro

18 multiplicador

20 unidad de limpieza de subportadora

22 unidad de diezmado

24 muestras de PRS

26 servidor seguro

28 receptor de software de PRS

30 unidad de descifrado de PRS

32 PVT

REIVINDICACIONES

1. Un método de posicionamiento, mediante la utilización de Binary Offset Carrier cifrado, BOC, Sistema Global de Navegación por Satélite Modulado, GNSS, de señales de navegación (12), que transmiten información cifrada en sus bandas laterales, que comprende los actos de:

- capturar (14, 16, 18, 20, 22) solo una de las bandas laterales de una señal de navegación de GNSS modulada por BOC cifrada,

- transmitir solo las muestras (24) de la banda lateral capturada de la señal de navegación de GNSS modulada con BOC cifrada a un servidor seguro (26) para calcular (28, 30) una posición, velocidad y/o tiempo - PVT - (32) a partir de las muestras recibidas, y

- recibir el PVT (32) calculado del servidor seguro (26).

2. El método de la reivindicación 1, en el que el acto de capturar solo una de las bandas laterales de una señal de navegación de GNSS modulada con BOC cifrada comprende procesamiento del lado del usuario, conversión a una frecuencia menor, filtrado y conversión de analógica a digital de solo una de las bandas laterales de la señal de navegación de GNSS modulada con BOC cifrada.

3. El método de la reivindicación 1, en el que el acto de capturar solo una de las bandas laterales de una señal de navegación de GNSS modulada con BOC cifrada comprende muestrear la señal de navegación de GNSS cifrada por completo y reducir la señal muestreada a solo una de las bandas laterales mediante la realización de una técnica de procesamiento de señales.

4. El método de la reivindicación 3, en el que la realización de una técnica de procesamiento de señales comprende la conversión a una frecuencia menor de la señal muestreada en una banda base, dividiendo la parte determinista de la señal muestreada convertida a una frecuencia menor en una señal de banda lateral superior e inferior, filtrando la señal convertida a una frecuencia menor dividida para eliminar la señal de banda lateral superior o inferior (16), eliminando la modulación de subportadora de la señal de banda lateral filtrada (18, 20) para obtener una señal de banda lateral con una frecuencia central 0, y diezmando (22) la señal de banda lateral con una frecuencia central 0 para obtener una señal de banda lateral capturada con una velocidad de muestreo (24) menor.

5. Un receptor de GNSS (10) para posicionamiento mediante la utilización de señales de navegación (12) moduladas mediante el Sistema de satélite de navegación global, GNSS con Binary Offset Carrier, BOC, cifrada, que transmiten información cifrada en sus bandas laterales, que comprende

- medios (14, 16, 18, 20, 22) para capturar solo una de las bandas laterales de una señal de navegación de GNSS modulada con BOC cifrada,

- medios para transmitir solo las muestras (24) de la banda lateral capturada de la señal de navegación de GNSS modulada con BOC cifrada a un servidor seguro (26) que se proporciona para calcular (28, 30) una posición, velocidad y/o tiempo - PVT - (32) de las muestras recibidas, y

- medios para recibir el PVT (32) calculado del servidor seguro (26).

6. El receptor de GNSS de la reivindicación 5, en el que los medios (14, 16, 18, 20, 22) para capturar solo una de las bandas laterales de una señal de navegación de GNSS cifrada comprenden

- una interfaz de RF (14), para convertir una señal de navegación de GNSS cifrada recibida en una banda base,

- un filtro (16), para eliminar la señal de banda lateral superior o inferior de la señal convertida a una frecuencia inferior,

- un multiplicador (18) y una unidad de eliminación de subportadoras (20), para eliminar la modulación de subportadora de la señal de banda lateral filtrada, y

- una unidad de diezmado (22), para obtener una señal de banda lateral capturada con una velocidad de muestreo menor (24).

7. El receptor de GNSS de acuerdo con la reivindicación 5 o 6, en el que los medios para transmitir muestras (24) de la banda lateral capturada de la señal de navegación de GNSS cifrada a un servidor seguro (26) y/o medios para recibir el PVT (32) calculado del servidor (26) está configurado para establecer un enlace de comunicación seguro con el servidor (26) seguro a través de una red de comunicación, en particular Internet.

8. Un producto de programa informático que comprende instrucciones para hacer que el receptor de GNSS (10) de la reivindicación 5 ejecute las etapas del método de la reivindicación 1.

9. Un medio legible por ordenador que tiene almacenado en él el producto de programa informático de la reivindicación 8.

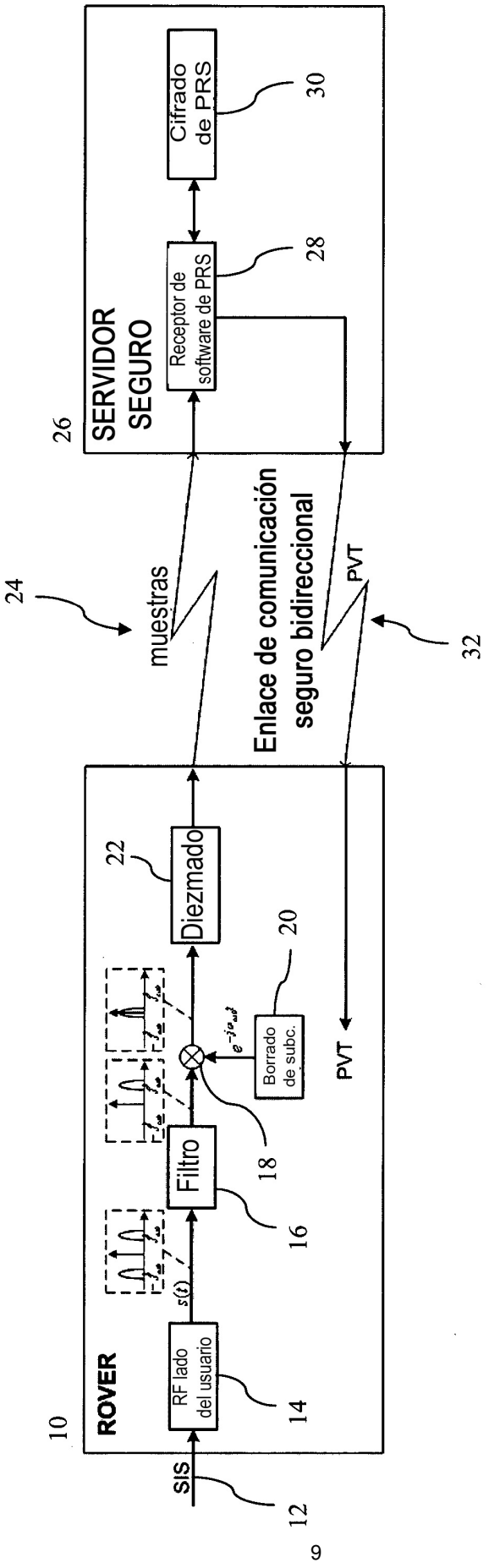

SERVIDOR SEGURO
Cifrado de PRS
Receptor de software de PRS
Enlace de comunicación seguro bidireccional
muestras
PVT
ROVER
RF lado del usuario
Filtro
Borrado de subc.
Diezmado
SIS
10
12
14
16
18
20
22
24
26
28
30
32

Fig. 1

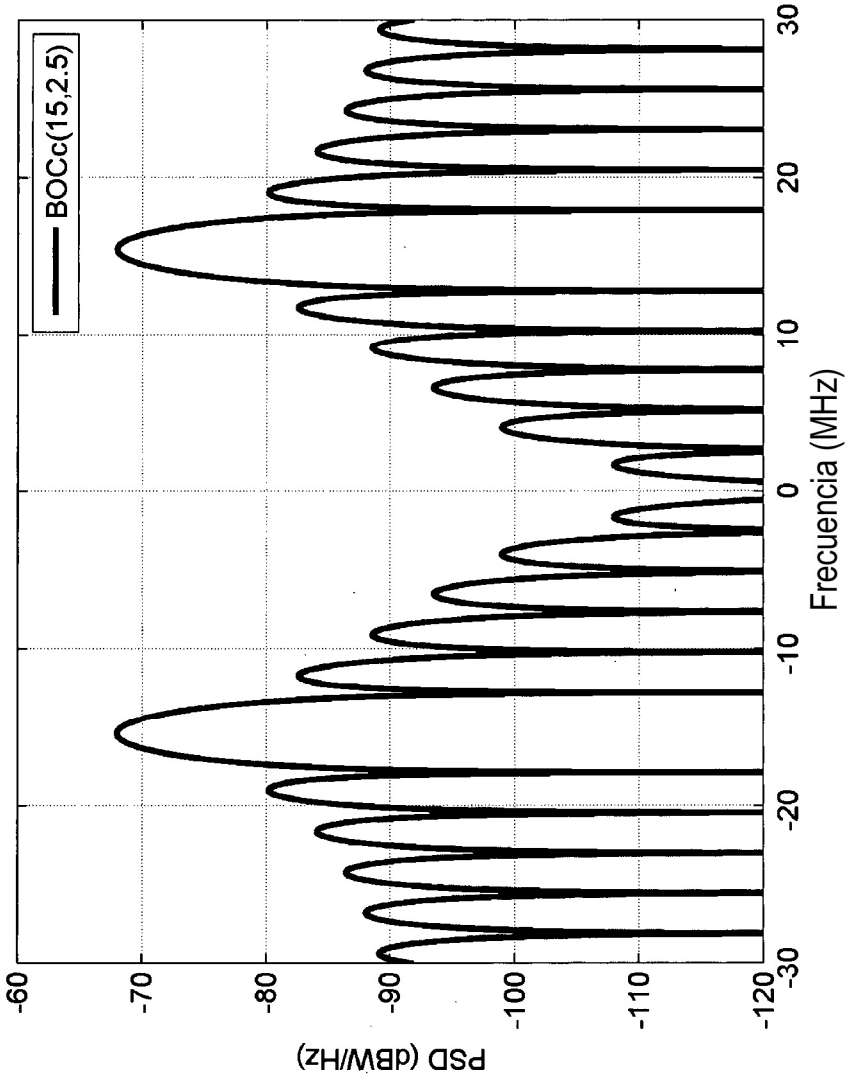

BOCc(15,2.5)
PSD (dBW/Hz)
-60
-70
-80
-90
-100
-110
-120
Frecuencia (MHz)
30
20
10
0
-10
-20
-30

Fig. 2