Sistemas GNSS. Amenazas/Vulnerabilidades. Implantación PNT robusta en las FAS

Autor: Alejandro Ruiz Ruiz de Cortázar
Directora: Paula Gómez Pérez

I. INTRODUCCIÓN Y CONTEXTO

La gran mayoría de las capacidades militares dependen, en mayor o menor grado, de la obtención de una solución de posicionamiento, navegación y tiempo "*Positioning, Navigation and Timing* (PNT)" fiable para su correcto funcionamiento. Actualmente, las diferentes plataformas y sistemas en las Fuerzas Armadas (FAS) disponen solamente de receptores del sistema global de posicionamiento por satélite "*Global Navigation Satellite System* (GNSS)" americano "*Global Navigation System* (GPS)", bien del servicio protegido y abierto, o sólo abierto, por lo que cualquier indisponibilidad del mismo afectaría muy negativamente en la conducción de las operaciones.

Entre las vulnerabilidades y amenazas, se destaca el hecho de que se depende exclusivamente de las señales del GPS, y que estas señales son susceptibles tanto al "*spoofing*" (servicio abierto) como al "*jamming*" (servicio abierto y servicio protegido).

II. DESARROLLO Y RESULTADOS

En primer lugar, se analizan los cuatro sistemas de posicionamiento globales (GNSS) basados en satélites, y sus sistemas de aumentación (SBAS) asociados, en cuanto a sus programas de modernización con potencial interés en su implantación en las Fuerzas Armada (FAS). Por motivos estratégicos, se han centrado en los sistemas GPS y Galileo, especialmente en sus servicios militares protegidos, pero también en aquellos servicios abiertos que están previstos sean interoperables a nivel señal en el futuro.

En segundo lugar, se describen la naturaleza de las señales GNSS, así como los principios de funcionamiento de los receptores GNSS, lo cual es necesario para entender las amenazas ("*spoofing*" y "*jamming*") a las que están expuestos tanto en relación con los servicios abiertos como los servicios protegidos.

Posteriormente, se analiza la técnica de "*spoofing*" en cada uno de sus tipos, así como las diferentes técnicas de mitigación a los servicios abiertos, en la que las antenas "*Controlled Reception Pattern Antenna* (CRPA)" resultan el método más efectivo. Se resaltan, también, los distintos métodos de protección de la señal GNSS, tanto las militares/gubernamentales con sistemas de encriptación como las de servicio abierto con sistemas de autenticación.

En cuanto al "*jamming*", se describen los diferentes tipos, principalmente de banda estrecha y de banda ancha, a la que son vulnerables tanto los receptores de servicios protegidos como abiertos debido a la poca potencia en que la señal GNSS alcanza la superficie terrestre. Se analizan las diferentes técnicas de mitigación, en la que las antenas CRPA resultan, otra vez, el único medio efectivo.

Debido a la importancia de las antenas CRPA en la mitigación de ambas amenazas, se realiza un análisis detallado de sus diferentes tipos, teniendo en cuenta su evolución desde las más sencillas hasta las más avanzadas, así como su efectividad de mitigación tanto en lo relativo al número de señales "jamming" que pueden mitigar, así como en su efectividad en lo relativo tanto a las señales "jamming" de banda estrecha como de banda ancha.

En cuanto a las antenas CRPA, habría que distinguir dos tipos principales:

- Antenas CRPA con capacidad de realizar "*nulling*", las cuales se componen de varios (N) elementos radiantes con un algoritmo de formación de nulos, reduciendo la ganancia en la dirección de la señal interferente. Se destaca que estas antenas disponen de un límite de conformación de nulos relacionado con el número de elementos, así como con el comportamiento efectivo de la antena.
- Antenas CRPA con capacidad de conformado de haces en recepción, en las que la unidad de control de antena necesita información de la localización de los satélites para maximizar la ganancia hacia el satélite, la cual es obtenida tanto de los datos de las efemérides como del almanaque del receptor. En este caso, debido a que la antena dispone de información sobre la dirección de los satélites, no existen límites de conformación de haces, y vendrán delimitados por las entradas a cada uno de los elementos radiantes.

  Además, en este tipo de antenas, existe la posibilidad de implementar ciertos algoritmos para mitigar el "*jamming*" de banda ancha modulada, en la que se aborda la problemática dividiendo el ancho de banda en múltiples anchos de banda estrechos, en la que se considera que la señal no varía en fase y/o frecuencia, y por lo tanto sería efectiva su mitigación.

Posteriormente, se realiza un análisis de las diferentes doctrinas e iniciativas militares relacionada con la capacidad de posicionamiento PNT por satélite.

Finalmente, se realiza un análisis de las iniciativas de los países y organismos aliados en cuanto a la obtención de soluciones PNT robustas.

III. CONCLUSIONES

En primer lugar, y una vez analizados los sistemas GNSS, y sus SBAS asociados, se definen los requisitos generales de los receptores multiconstelación, multiservicio y multifrecuencia, los cuales se consideran como la primera capa de defensa ante las amenazas de "*spoofing*" y "*jamming*".

En segundo lugar, y analizados los dos tipos de amenazas ("*spoofing*" y "*jamming*"), se proponen diferentes requisitos de mitigación relacionadas con las antenas CRPA, así como con su nivel de integración entre los subsistemas que componen el sistema PNT.

Mas adelante, se detalla la considerable influencia de la capacidad PNT en las demás capacidades militares, y, por lo tanto, la importancia de obtener la superioridad PNT en el campo de batalla, en la que se persigue asegurarse la solución PNT basada en sistemas GNSS, y otras fuentes PNT, y denegársela a la fuerza oponente.

Posteriormente, y analizadas las iniciativas aliadas, se resalta que todas las soluciones PNT militares tienen en cuenta tanto el uso de receptores militares protegidos como diferentes tipos de antenas CRPA para la mitigación de las citadas amenazas ("*spoofing*" y "*jamming*").

Finalmente, se proponen los requisitos operacionales, junto con los requisitos técnicos asociados, de las diferentes soluciones según el nivel de resiliencia ante el "jamming" requerido para cada tipo de plataforma/sistema, los cuales podrían servir de punto de partida para la elaboración de los requisitos funcionales y técnicos de menor nivel en el proceso de obtención de la capacidad PNT robusta en las FAS.