

Perturbación de GPS en cazaminas clase segura

Autor: Fernández de León, Miguel Rafael

Director/es: Núñez Ortuño, José María y Troncoso Pastoriza, Francisco Manuel.

Contacto: mferleo@fn.mde.es

Resumen: El Trabajo de Fin de Máster (TFM) se enfoca en los buques de guerra clase "Segura" de la Armada Española, dedicados a la detección, identificación y neutralización de minas marinas. Estos buques son clave para la seguridad marítima, operando cerca de costas, puertos, zonas de pesca y canales angostos, donde las minas marinas son un riesgo significativo. Es crucial que mantengan una posición precisa, especialmente en zonas con riesgo de minas o de poca profundidad.

Se abordan aspectos relevantes de los sistemas de posicionamiento global (GPS) en estos buques, analizando en detalle los equipos GPS y los ataques de perturbación GPS más comunes que afectan su funcionamiento. Se analizan ejercicios de perturbación de GPS realizados en estos buques para entender mejor los riesgos y vulnerabilidades asociados a las perturbaciones en los sistemas GPS.

Un aspecto crucial es la investigación de métodos para mitigar interferencias en el GPS con la tecnología actual. En caso de que el GPS haya sido degradado, se estudian técnicas existentes y se exploran alternativas para que los buques mantengan su posición y continúen con operaciones de medidas contra minas.

Finalmente se buscará responder a una pregunta esencial: ¿es posible continuar con las operaciones de medidas contra minas tras un ataque de perturbación del GPS usando la tecnología actual? La respuesta a esta pregunta es crucial, ya que una interrupción en la navegación y operación de estos buques en zonas minadas podría tener consecuencias desastrosas, tanto táctica como operativamente. Se evaluará la viabilidad de seguir con estas misiones críticas o, de ser necesario, retirarse de la zona minada de forma segura.

Palabras clave: GPS, Perturbación, Cazaminas, Operaciones, Tecnología

1. Introducción

Los cazaminas de la clase "Segura" (figura 1) pertenecientes a la Armada Española, que incluyen al Segura, Sella, Tambre, Turia, Duero y Tajo, son buques específicamente diseñados y construidos con características únicas que les permiten operar eficientemente en áreas de poca profundidad y muy cercanas a la costa. Esta particularidad en su diseño los hace idóneos para tareas en estas zonas específicas.

La misión principal de estos cazaminas, como se detalla en la Instrucción Permanente de Organización de la Flota, IPO FLOTA 0327/201 [1] es: “Prepararse y llevar a cabo misiones relacionadas con la libertad de acción en el ámbito de la Guerra de minas y en cualquier área geográfica, incluyendo teatros litorales y escenarios costeros alejados del territorio nacional integrado en una Fuerza Naval y contribuir, en su caso, al resto de capacidades de la Fuerza de Acción Marítima”.



Figura 1. Cazaminas clase “Segura”.

Basado en la definición de la misión propuesta, resulta claro que es esencial para este tipo de plataformas tener un conocimiento constante y preciso de su posición. Esta necesidad se debe a los riesgos inherentes de navegar en áreas cercanas a la costa donde la profundidad del agua es limitada. Estos riesgos se magnifican significativamente en el caso de que estas áreas también estén afectadas por la presencia de minas.

Por lo tanto, la capacidad de determinar la posición exacta en todo momento es crucial para la operación segura y efectiva de la plataforma, especialmente en entornos potencialmente peligrosos o comprometidos. La precisión en la localización no es solo una cuestión de navegación eficiente, sino una medida crítica de seguridad, considerando los desafíos adicionales que presentan las zonas minadas.

Con el auge reciente de ataques a sistemas de posicionamiento global (GPS), que cada vez son más avanzados y precisos, los modelos de GPS que se llevan a bordo de los cazaminas y la necesidad de conocer perfectamente la posición para realizar las misiones de estos buques. En este contexto surge la pregunta, ¿es posible, con la ayuda de la tecnología actual, continuar los cazaminas con operaciones

de medidas contra minas, en el teatro de operaciones ante un ataque de perturbación de GPS, o deben de abandonar la zona de operaciones y cancelar la misión?

2. Desarrollo

2.1 Operaciones de los Cazaminas

Para entrar en contexto es necesario conocer el tipo de misiones que realizan los cazaminas, en las cuales se observa la importancia de conocer la posición GPS en todo momento.

- Operaciones de Medidas Contra Minas (MCM): Incluyen el reconocimiento, exploración y limpieza de minas en zonas minadas para proteger territorios o impedir el movimiento del enemigo. Se suelen utilizar dos tipos de minas: de fondo y de orinque, ambas se fondean en zonas de poca profundidad. Estas operaciones son críticas y requieren una precisión en la posición del cazaminas, extrema.

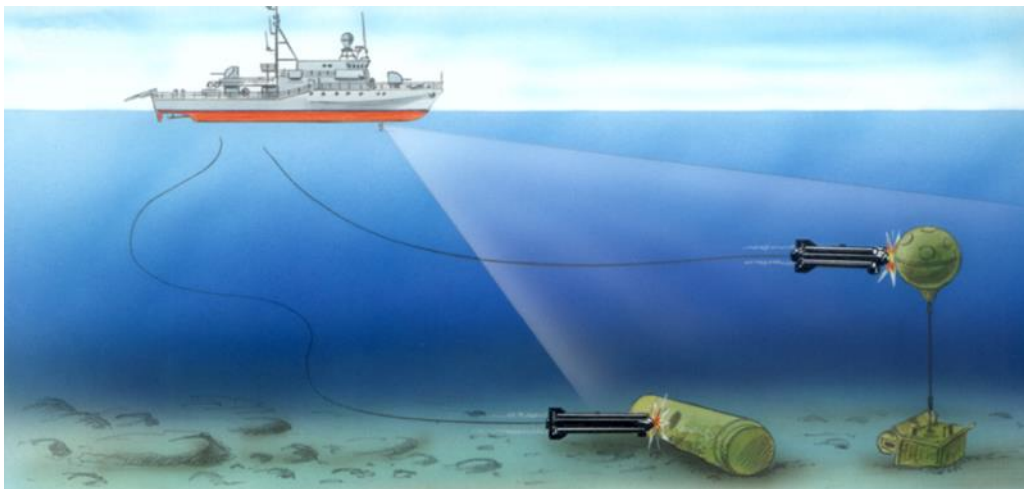


Figura 2. Operaciones MCM.

- Operaciones de Vigilancia de Rutas (*Route Survey*): Consisten en la vigilancia y protección marítima, especialmente en áreas de acceso a puertos. Estas operaciones incluyen el sondeo submarino y la recopilación de información medioambiental, siendo esenciales para la seguridad de las zonas portuarias.
- Operaciones Anfibias: Apoyan a las fuerzas anfibias en desembarcos militares, realizando el reconocimiento del fondo marino para identificar áreas óptimas para el desembarco.
- Otras Operaciones: Incluyen ejercicios nacionales e internacionales, participación en agrupaciones internacionales, presencia naval y colaboraciones con organismos civiles.

2.2 Tipos de GPS en Cazaminas

Se describen los sistemas GPS de los cazaminas con detalles sobre su precisión, tecnología, durabilidad, funcionalidades, facilidad de uso y soporte. Se realiza una comparativa de estos sistemas, destacando que cada uno tiene aplicaciones específicas y ventajas únicas.

2.3 Tipos de Perturbación GPS

Los tipos de perturbación los dividiremos en interferencias intencionadas, destacando las técnicas como el *jamming* y el *spoofing*, [2] y en interferencias no intencionadas, que serán mencionadas brevemente por su relevancia informativa.

- *Jamming* (Obstrucción): Consiste en la obstrucción deliberada de las señales GPS mediante señales de radiofrecuencia. Los *jammers* varían en potencia y pueden ser utilizados con fines ilícitos, como evitar el seguimiento o perturbar operaciones militares.
- *Spoofing* (Suplantación): Envía señales falsas a los receptores GPS, engañándolos sobre su ubicación real. Es particularmente peligroso ya que puede causar errores de navegación sin que el usuario se dé cuenta.
- Otras Perturbaciones: Incluyen reflexión de señales (*Multipath*), obstrucciones atmosféricas y problemas con la constelación de satélites. Todas ellas se tratan de interferencias no intencionadas.

2.4 Riesgos de Perturbar el GPS

Se enfatizan los riesgos de la navegación con un GPS degradado, las dificultades en las operaciones MCM, problemas de coordinación con otros buques y desafíos en la navegación bajo condiciones meteorológicas adversas cuando el GPS es perturbado.

2.5 Medidas para Mitigar Ataques al GPS

A continuación, se describen diferentes, medidas y técnicas para mitigar los ataques de perturbación al GPS. En caso de que estas medidas fueran efectivas en los cazaminas, significaría que el GPS no estaría afectado ante un ataque de GPS y los cazaminas podrían entonces continuar con las operaciones MCM.

- *Antenas Antijamming*: Se destaca la importancia de las antenas *antijamming* que utilizan tecnologías avanzadas como la formación de haces digitales y la información TLE de NORAD para combatir las interferencias. La antena GAJT-710ML (figura 3) es un ejemplo práctico que demuestra cómo estas tecnologías pueden integrarse en los sistemas existentes de los cazaminas para mejorar la resistencia frente a *jamming* y *spoofing*. La selectividad espacial y la inmunidad al ruido mejorada son aspectos clave de estas antenas. [3]



Figura 3. Antena antijamming.

- **Detección y Filtrado de Señales:** Existen en desarrollo algoritmos avanzados para detectar y filtrar señales interferentes. Utilizando técnicas de procesamiento de señales y análisis espectral, junto con el aprendizaje automático, estos algoritmos pueden identificar eficazmente las señales anómalas y proteger los sistemas GPS. La implementación de estos algoritmos permitiría una evaluación continua de la autenticidad de las señales GPS, mejorando significativamente la seguridad y confiabilidad del sistema de navegación. [4]
- **Protección de GPS mediante Redes Neuronales:** La introducción de redes neuronales, como la NARX NN, en el campo de la navegación GPS ofrece una vía prometedora para mitigar los efectos del *spoofing*. Estas redes son capaces de aprender y adaptarse a patrones de señales, lo que les permite identificar desviaciones de las normas y responder en consecuencia. Su eficacia en la mitigación de ataques de *spoofing* es notable, y su aplicación podría revolucionar la seguridad del GPS en operaciones críticas. [5]
- **Criptografía:** Se explora la posibilidad de implementar la criptografía en las señales GPS para protegerlas contra ataques de *spoofing*. La criptografía simétrica y asimétrica ofrece diferentes ventajas y desafíos. La simétrica proporciona una fuerte resistencia a los ataques, pero presenta dificultades en la distribución de claves. Por otro lado, la criptografía asimétrica facilita la distribución de claves pero requiere más recursos computacionales. Ambas técnicas proporcionan un nivel adicional de seguridad para las señales GPS. [6]
- **Redundancia y Diversidad de Señales:** Esta estrategia implica el uso de varios sistemas de navegación satelital para proporcionar redundancia. En caso de interferencia en un sistema, el dispositivo puede cambiar a otro, asegurando la continuidad y precisión de la navegación. Esta diversificación aporta una seguridad adicional contra fallos o interferencias en cualquier sistema individual.

2.6 Medidas para Mantener Operaciones MCM

En caso de que no sea posible mitigar los ataques a los GPS de los cazaminas y estos queden degradados, es fundamental buscar una alternativa para intentar mantener la posición y poder continuar con las operaciones MCM, utilizando la tecnología actual.

- **Sistemas de Navegación Inercial:** Son una opción viable cuando el GPS falla, proporcionando datos de navegación independientes. Aunque su precisión disminuye con el tiempo, son útiles para maniobras a corto plazo, como la evacuación segura de una zona minada, pero no para continuar realizando operaciones MCM. [7]
- **Sistema eLoran:** Se presenta como una alternativa robusta al GPS, especialmente eficaz contra interferencias. Aunque su precisión no es tan alta como la del GPS, su robustez y fiabilidad lo hacen valioso para la navegación en situaciones críticas. Las señales de radio de baja frecuencia de eLoran ofrecen una cobertura efectiva y son menos susceptibles a interferencias, lo que lo convierte en una opción segura para la navegación y sincronización de tiempo en situaciones donde la integridad de la señal es crucial. Sin embargo, su precisión en decenas de metros puede no ser suficiente para realizar operaciones MCM. [8]

- Triangulación 5G: La posibilidad de usar la tecnología 5G para la localización precisa de buques representa un avance significativo. La capacidad de las antenas MIMO para una orientación precisa de la señal, combinada con la alta capacidad de transmisión de datos y baja latencia de 5G, ofrece un potencial considerable para la localización en el mar. Sin embargo, los desafíos de cobertura y penetración de la señal en entornos marítimos, junto con el alto costo y complejidad técnica de implementar redes 5G a gran escala, representan obstáculos significativos para utilizar esta técnica para mantener la posición y continuar con operaciones MCM. [9], [10]

3. Conclusiones

Ante la creciente amenaza de ataques de perturbación GPS y las limitaciones que ofrecen ante un ataque de perturbación, los GPS de los cazaminas, como se ha visto a lo largo del trabajo, es imperativo que se realicen esfuerzos para modernizar y mitigar estos posibles ataques para salvaguardar la integridad y disponibilidad de los sistemas GPS que son de vital importancia. Esta modernización incluye las técnicas descritas en apartados anteriores, como adopción de protocolos de encriptación, antenas *antijamming*, detección y filtrado de señales, protección de GPS mediante redes neuronales o redundancia de señales, todas ellas son medidas aplicables, excepto probablemente, las antenas *antijamming* por su elevado coste.

A la respuesta de la hipótesis de este estudio; ¿es posible, con la ayuda de la tecnología actual, continuar los cazaminas con operaciones de medidas contra minas, en el teatro de operaciones ante un ataque de perturbación de GPS, o deben abandonar la zona de operaciones y cancelar la misión? Sí que es posible, utilizando una combinación de las técnicas descritas, evitar prácticamente al 100% un ataque de perturbación GPS y poder continuar con la misión. Pero en caso de que se produzca una degradación de la señal, con las técnicas actuales estudiadas, como la navegación inercial, la triangulación 5G o la navegación mediante el sistema eLoran, no sería posible continuar con las operaciones MCM en la zona minada debido a que la precisión que nos ofrecen estas técnicas no es suficiente para garantizar la seguridad de la plataforma y deberíamos cancelar la misión. Aunque cabe destacar, que las técnicas de navegación inercial y de navegación con el sistema eLoran, sí que garantizarían una salida segura de la zona de operaciones.

Por otro lado, los procedimientos operativos de los cazaminas están obsoletos y no recogen ninguna medida ni de mitigación, ni de medio alternativo de mantenimiento de posición en caso de que el GPS este degradado, por lo que se propone la actualización de dichos procedimientos con las técnicas descritas.

Por último, al no ser posible con las técnicas estudiadas mantener las operaciones de medidas contra minas en caso de ser efectiva la perturbación del GPS, planteo la opción como línea futura, de modificar el procedimiento de ejecución de operaciones MCM, evitando la entrada directa del cazaminas en áreas minadas y delegando esta labor a vehículos submarinos autónomos. Esto disminuiría significativamente los peligros asociados a la navegación en campos minados para la tripulación del buque y además, se evitarían los inconvenientes asociados a la perturbación del GPS en zona de minas al operar desde una zona segura.

Agradecimientos

En primer lugar, agradecer a mis directores de TFM que me han ayudado mucho para la realización de este trabajo.

A la primera escuadrilla de Cazaminas, segunda casa para mí, donde me han aportado mucha información útil para la realización de este trabajo de fin de Máster.

Y por último y más importante, a mi mujer Blanca, que después de unos duros años con TFG, TFM, mucho tiempo fuera de casa durante el mando del “Tarifa” y 4 niños en casa, todavía sigue animándome y apoyándome en todo lo que realizo.

Referencias

- [1] Armada Española. 2001. Instrucción Permanente de Organización de la Flota: IPO FLOTA 0327/2001.
- [2] INCIBE-CERT. (s.f.). Spoofing y jamming en los GNSS. Recuperado de <https://www.incibe.es/incibe-cert/blog/spoofing-y-jamming-los-gnss>
- [3] NovAtel. (s.f.). GAJT-410ML Anti-Jam Antenna. Recuperado de <https://novatel.com/products/anti-jam-antenna-systems-gajt/gajt-410ml-anti-jam-antenna>
- [4] Demir, M. Ö., Kurt, G. K., & Pusane, A. E. (2023). A Pseudorange-Based GPS Spoofing Detection Using Hyperbola Equations. IEEE Transactions on Vehicular Technology, 72(8). Recuperado de <https://ieeexplore.ieee.org/document/10068811>
- [5] Tohidi, S., & Mosavi, M. R. (2023). A Non-linear Autoregressive Exogenous Neural Network-based Predictor for Protecting the GPS Receiver's Tracking Loop from the Spoofing Attack. DOI: 10.21203/rs.3.rs-2657692/v1. Recuperado de https://assets.researchsquare.com/files/rs-2657692/v1_covered_a98ac407-ad0b-46b3-8f2c-bc1c846289b3.pdf?c=1698215234
- [6] Bybit Learn. (s.f.). What is Public Keys and Private Keys in Cryptography and How it Works. Recuperado de <https://learn.bybit.com/es/blockchain/what-is-public-keys-and-private-keys-in-cryptography-and-how-it-works/>
- [7] Dewesoft. (s.f.). ¿Qué es un sistema de navegación inercial? Recuperado de <https://dewesoft.com/es/blog/que-es-un-sistema-de-navegacion-inercial>
- [8] Ofcom. (s.f.). Enhanced Long-Range Navigation (eLoran). Recuperado de <https://www.ofcom.org.uk/manage-your-licence/radiocommunication-licences/enhanced-long-range-navigation>
- [9] Pointr. (s.f.). 5G Indoor Positioning. Recuperado de <https://www.pointr.tech/blog/5g-indoor-positioning>
- [10] Telecom Review. (s.f.). Emerging 5G Use Cases for the Maritime Industry. Recuperado de <https://www.telecomreview.com/articles/reports-and-coverage/4073-emerging-5g-use-cases-for-the-maritime-industry>