

# Sistema de perturbación (*spoofing*) para receptores GPS embarcados

Núñez Ortuño, José María<sup>1\*</sup>; Troncoso Pastoriza, Francisco<sup>1</sup>

<sup>1</sup> Centro Universitario de la Defensa en la Escuela Naval Militar (CUD-ENM). Plaza de España s/n, 36920. Marín – Pontevedra. [\[jnunez|froncoso\]@cud.uvigo.es](mailto:[jnunez|froncoso]@cud.uvigo.es)

\* Autor principal; [jnunez@cud.uvigo.es](mailto:jnunez@cud.uvigo.es)

---

**Resumen:** Las pruebas de perturbación y suplantación de señal GNSS realizadas por el CUD-ENM en buques de la Armada y aeronaves del Ejército del Aire han revelado vulnerabilidades en estos sistemas, afectando tanto a equipos de navegación como a otros sistemas no previstos. El CUD-ENM ha desarrollado LOKI, un sistema capaz de realizar ataques de *jamming* y *spoofing* en múltiples bandas y constelaciones, suplantando posición y tiempo GPS con precisión. Esta herramienta permite evaluar y catalogar la resiliencia de los equipos receptores GPS y sistemas dependientes a bordo de los buques de la Armada. El sistema LOKI ha participado en las maniobras NEMO-22, MARSEC-22/23/24 y MINEX-23/24, creando ambientes GNSS degradados en los que se han realizado ataques efectivos sobre más de 15 unidades navales y aeronaves propias y de la coalición. En esta comunicación se describe la arquitectura *software* y *hardware* del sistema desarrollado, así como sus principales características.

**Palabras clave:** EW, Guerra electrónica, GPS, Perturbación, *Spoofing*.

---

## 1. Introducción

La protección de los datos de Posición, Navegación y Tiempo (PNT) es crucial para las fuerzas armadas y los cuerpos de seguridad del Estado. Hoy en día dependemos enormemente de sistemas y plataformas que se basan en la tecnología PNT de fuentes GNSS. De hecho, el Servicio de Posicionamiento Preciso (PPS) de GPS es la principal fuente de PNT en la OTAN [1-2]. Las grandes amenazas de los receptores de sistemas GNSS son los ataques de *jamming* [3] y *spoofing* [4]. El *jamming* busca interrumpir el funcionamiento del receptor, mientras

que el *spoofing* suplanta las señales de los satélites originales. El *spoofing* síncrono es un ataque muy sofisticado que genera una señal falsa casi indistinguible de la real, y obliga al receptor a “engancharse” a una constelación suplantada.

Las pruebas de perturbación y suplantación de señal GNSS, realizadas por el CUD-ENM contra buques de la Armada y diversas aeronaves del Ejército del Aire durante la ejecución de diversos ejercicios MARSEC, NEMO y MINEX, revelaron la vulnerabilidad de algunas de estas unidades a este tipo de ataques, que no solo afectaron a los equipos de navegación, sino también a otros sistemas del buque que no eran el objetivo directo del ataque. Tanto la OTAN como nuestras FFAA, conscientes de esta nueva amenaza, han comenzado a tomar medidas [5-6].

Ante esta realidad, se hace necesario y urgente que la Armada catalogue, en todas sus unidades, el nivel de resiliencia y robustez de equipos, sistemas y subsistemas que empleen información PNT proporcionada por sistemas GNSS y que podrían verse afectados por este tipo de ataques. Por ello, deben realizarse pruebas de *jamming* y *spoofing* en todos los equipos receptores GNSS para verificar los efectos de estos ataques y determinar el alcance del daño que pueden causar. El CUD-ENM, consciente de esta necesidad, ha desarrollado un sistema, denominado LOKI, que permite realizar ataques de *jamming* y *spoofing* en varias bandas y constelaciones simultáneamente, suplantando posición y tiempo GPS con gran precisión.

## 2. Materiales y métodos

En el escenario de ataque de un sistema de *spoofing*, la víctima del ataque recibe tanto las señales reales de los satélites  $\{s_i\}, i \in \mathcal{S}$ , siendo  $\mathcal{S}$  el conjunto de satélites visibles desde la víctima, como la señal de suplantación enviada por el equipo *spoofers*,  $\hat{s}$ , construida como una combinación de las señales sintéticas,  $\{\hat{s}_i\}$ , generadas para cada satélite. La señal transmitida por el *spoofers* debe ser equivalente al conjunto de señales recibidas por la víctima en el momento de llegar al receptor [7]. Por tanto, a partir de cada señal  $x_i[n]$  generada por el  $i$ -ésimo satélite, se deberán reproducir los principales efectos de la transmisión, incluyendo el retardo de propagación,  $\delta_i$ , el desplazamiento frecuencial provocado por el efecto Doppler,  $\Delta f_i$ , y la atenuación de la señal,  $G_i$ :

$$\hat{s}_i[n] = \frac{1}{G_i} e^{j2\pi\Delta f_i n} x_i[n - \delta_i]. \quad (1)$$

Una vez combinadas estas señales, deberá realizarse el proceso contrario para cancelar el efecto de la transmisión a través del camino directo entre *spoofers* y víctima, eliminando los tres efectos mencionados,  $\delta_d$ ,  $\Delta f_d$  y  $G_d$ , respectivamente:

$$\hat{s}_i[n] = G_d e^{-j2\pi\Delta f_d n} \sum_{i \in \mathcal{S}} s_i[n + \delta_d]. \quad (2)$$

Para alterar la percepción de la víctima, será necesario calcular los efectos incluidos en la Ec. 1 para una posición, velocidad y retardo diferentes de la real.

### 2.1 Esquema de funcionamiento y arquitectura software

A partir del modelo teórico presentado, el funcionamiento del sistema se ilustra en la Figura 1. En este esquema, por motivos de eficiencia, se combina la reproducción de los efectos de la propagación de la señal desde el satélite y la cancelación de los correspondientes a la señal enviada desde el *spoofers*. Además, se incluye un retardo adicional,  $\delta_t$ , para modificar la percepción temporal de la víctima. Estas modificaciones dan lugar a la siguiente señal generada:

$$\hat{s}_i[n] = \sum_{i \in \mathcal{S}} \frac{G_d}{G_i} e^{j2\pi(\Delta f_i - \Delta f_d)n} x_i[n - (\delta_i - \delta_d + \delta_t)]. \quad (3)$$

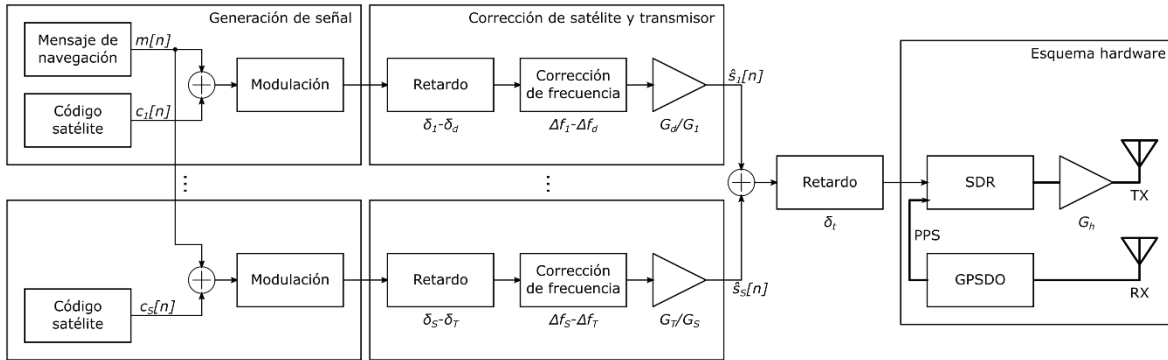


**Figura 1.** Diagrama de funcionamiento *software* y *hardware* del sistema LOKI.

La creación de la señal base,  $x[n]$ , incluye la generación del mensaje de navegación, común para todos los satélites, la generación del código correspondiente a cada satélite y el proceso de modulación.

La implementación de la parte *software* del sistema se ha realizado en el lenguaje Rust. Al inicio de la ejecución, el programa lee los parámetros de configuración de un archivo en formato YAML, obtiene los datos orbitales de la constelación de satélites a partir de un archivo en formato RINEX, sincroniza el inicio de la transmisión y comienza la generación de la señal. El bucle principal de funcionamiento actualiza los datos de PVT de los elementos del escenario y

recalcula los parámetros asociados a los tres efectos para cada satélite y para el *spoofers* cada 100 ms, siendo este intervalo configurable.

El *software* desarrollado incluye una interfaz gráfica de usuario (GUI), mostrada en la Figura 2, para la configuración de los parámetros del escenario de ataque y la visualización de la señal generada. Esta interfaz incluye: una barra de comandos en la parte superior, integrada junto con los controles de la ventana; un mapa ocupando la parte central para visualizar y modificar el punto de suplantación; un panel de configuración en la parte izquierda que permite modificar los parámetros de ejecución; un panel de filtrado y visualización de satélites en la parte derecha, indicando las posiciones relativas de todos los satélites involucrados en el ataque; y, por último, un registro de eventos en la parte inferior que permite analizar los puntos más relevantes de la ejecución.

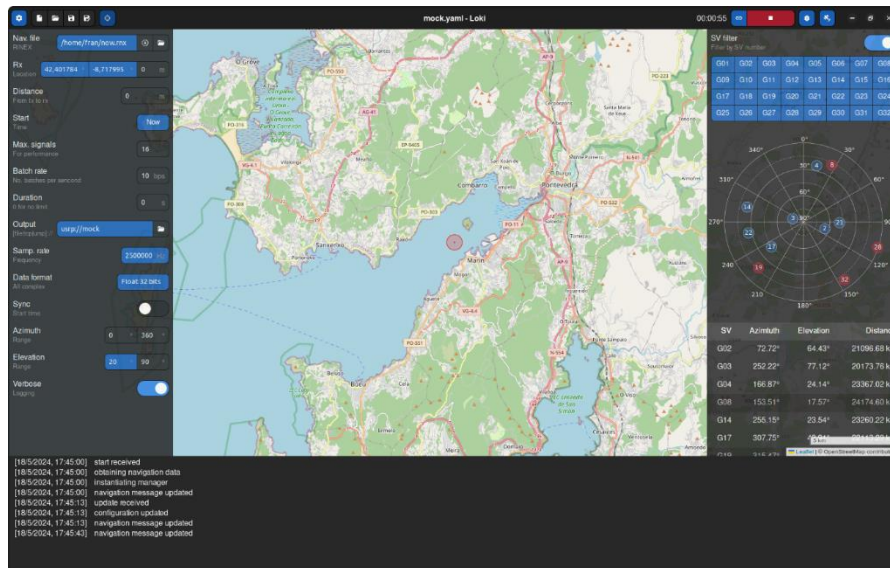


**Figura 2.** Interfaz gráfica de usuario del sistema LOKI.

## 2.2 Hardware utilizado

El *hardware* del sistema se ha integrado en un rack transportable (Figura 3), lo que permite desplazarlo a los ejercicios con un bajo impacto económico para la Armada. El *software*, que se ejecuta en un PC portátil, proporciona las muestras de la señal a un dispositivo SDR (*Software Defined Radio*) N200 de Ettus Research, que genera la señal de RF. Esta señal está sincronizada con el tiempo GPS, que se toma como referencia al inicio de cada ataque mediante un GPSDO (*GPS Disciplined Oscillator*), permitiendo realizar ataques de *spoofing* síncrono.

La señal de RF generada se conecta a un amplificador de banda L1 (1575 MHz) para incrementar la potencia de la señal transmitida y entregarla a la antena (Figura

3). Esta antena es de tipo helicoidal (*hélix*), de polarización circular a derechas (RHCP) con refuerzo del plano de tierra y garantiza una ganancia directiva de 15 dB, un ancho de haz relativamente estrecho y un lóbulo trasero muy reducido.



**Figura 3.** Equipamiento del sistema LOKI.

### 3. Resultados y discusión

Hasta la fecha, el sistema LOKI ha participado las maniobras NEMO-22, MARSEC-22/23/24 y MINEX-23/24, creando ambientes GNSS degradados en presencia de *jamming* y/o *spoofing*. En dichas maniobras se han realizado ataques (algunos con un alto grado de efectividad) sobre más de 15 unidades navales y aeronaves de la fuerza propia y también en diversos buques de la coalición. También se ha probado la vulnerabilidad de algunos receptores GNSS incluidos en equipos de comunicaciones de la FGNE (Fuerza de Guerra Naval Especial) durante su estancia en la ENM con motivo de las maniobras GNEX-24.

A modo de ejemplo, se muestra el efecto de un ataque de *spoofing* contra un buque concreto en las recientes maniobras MINEX-24. En la Figura 4a se muestra la ubicación del perturbador LOKI en las proximidades del Cabo Blanco en Mallorca. Las perturbaciones se realizaron en demora 135° mientras el buque víctima realizaba una maniobra de acercamiento a costa en *zigzag* empleando su GPS. Cuando el buque transitaba entre los puntos F y G (a unas 3 mn de distancia de costa) se inició un ataque de *jamming* de 3 min de duración con el objetivo de forzar al receptor GPS de la víctima a salir del modo de seguimiento y entrar en el modo de adquisición. Inmediatamente después, se realizó un ataque de *spoofing* suplantando una ubicación predefinida. Segundos después, el GPS del buque mostró una desviación inexistente de la ruta del barco (Figura 4b).

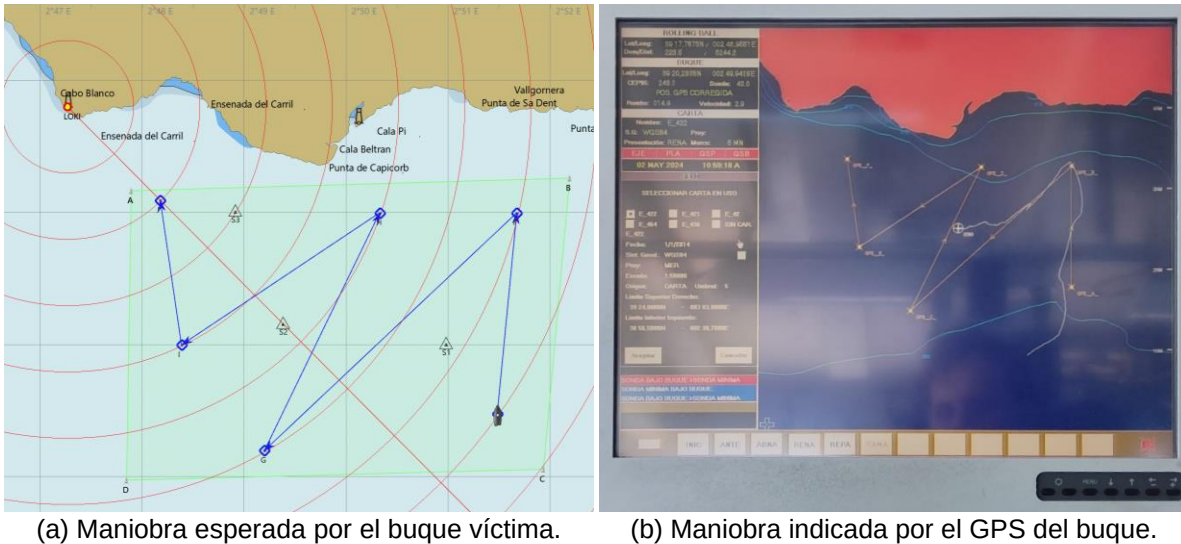


**Figura 4.** Efecto de un ataque combinado de *jamming* y *spoofing* contra un buque.

#### 4. Conclusiones

El sistema LOKI, desarrollado por el CUD-ENM, permite la realización de ataques de *jamming* y *spoofing* GPS, suplantando posición y tiempo GPS con gran precisión, tal y como ha quedado demostrado con su participación en los ejercicios navales MARSEC, NEMO y MINEX, afectando a más de 15 buques y aeronaves. La Armada dispone ahora de una herramienta que permitirá catalogar, en todas sus unidades, el nivel de resiliencia y robustez de los equipos que generan información PNT a partir de sistemas GNSS, lo que permitirá verificar los efectos de una decepción GPS y determinar el alcance del daño que puede causar.

#### Agradecimientos

Este trabajo ha sido realizado bajo el marco del proyecto PICUD-2023-05 del Centro Universitario de la Defensa en la Escuela Naval Militar. Se agradece la colaboración de la 1ª Escuadrilla de Medidas Contra Minas (MCM) y el INTA.

#### Referencias

- [1] Tim Vasen, "Is NATO Ready for Galileo?". Journal of the JAPCC (Joint Air Power Competence Centre), Dic. 2019, <https://www.japcc.org/>.
- [2] ANP-03 "The NATO Satellites Navigation Warfare (NAVWAR) Framework", NATO Restricted, Nov. 2004.
- [3] A. Grant, P. Williams, N. Ward and S. Basker, "GPS jamming and the impact on maritime navigation", The Journal of Navigation, vol. 62, no. 2, pp. 173-187, 2009
- [4] Bhatti, J., and Humphreys, T. E. (2017) "Hostile Control of Ships via False GPS Signals: Demonstration and Detection". J Inst Navig, 64: 51–66. doi: 10.1002/navi.183.
- [5] NATO Navigation Warfare (NAVWAR) Playbook Final Draf Rev1. Feb. 2021
- [6] SOP-03631 MOPS "Medidas de mitigación ante denegación de GNSS"
- [7] P. Bethi, S. Pathipati and A. P, "Impact of Target Tracking Module in GPS Spoofer Design for Stealthy GPS Spoofing," 2020 IEEE 17th India Council International Conference (INDICON), New Delhi, India, 2020, pp. 1-6, doi: 10.1109/INDICON49873.2020.9342285.