

Sistema multiestático para la suplantación (*spoofing*) de señales GPS

Núñez-Ortuño, José M.^{1,*}, González-Coma, José P.¹, Nocelo López, Rubén¹,
Troncoso-Pastoriza, Francisco¹ y Álvarez-Hernández, María¹

¹ Centro Universitario de la Defensa en la Escuela Naval Militar. Plaza de España s/n. 36920 Marín, Pontevedra, España.
Correo electrónico: [jnunez@cud.uvigo.es](mailto:jnunez@ cud.uvigo.es) (JMNO), jose.gcoma@cud.uvigo.es (JPGC), rubennocelo@cud.uvigo.es (RNL),
ftroncoso@cud.uvigo.es (FTP) maria-alvarez@cud.uvigo.es (MAH).

* Autor Principal y responsable del trabajo; Correo electrónico: jnunez@cud.uvigo.es (JMNO)

Resumen

Actualmente, los sistemas y plataformas que emplean nuestras Fuerzas Armadas, tienen gran dependencia de datos procedentes de fuentes GNSS (Global Navigation Satellite System). En un ataque tradicional de suplantación (spoofing) de señales de sistemas GNSS, la emisión de las señales suele realizarse desde un mismo punto, radiando una señal que resulta ser el agregado de las señales que emitirían los satélites suplantados de la constelación original en la ZOI (Zona de Interés). Este tipo de ataque resulta fácilmente detectable en el emplazamiento de la víctima mediante el empleo de técnicas de DOA (Direction of Arrival) por cualquier equipo de guerra electrónica moderno o una antena CRPA (Controlled Reception Pattern Antenna). Una de las técnicas que complican la detección en este tipo de escenario es la de realizar un ataque simultáneo desde varias ubicaciones (ataque multiestático). El demostrador que se presenta en este trabajo, permite realizar este tipo de ataque que, ejecutado desde varios nodos atacantes de manera sincronizada, complica la detección de un ataque de GNSS Spoofing.

1. Introducción

El aseguramiento de los datos de PNT (Posición, Navegación y Tiempo) es vital para nuestras Fuerzas Armadas y Cuerpos de Seguridad del Estado. Vivimos en un momento de gran dependencia de sistemas y plataformas basadas en PNT de fuentes GNSS [1]. De hecho, el Servicio de Posicionamiento Preciso (PPS) de GPS es la principal fuente de PNT en la OTAN [2].

Los receptores de GNSS dependen de la recepción de señales débiles de radiofrecuencia débiles lo que los hace muy vulnerables a interferencias involuntarias e intencionadas. El ataque más extendido contra este tipo de sistemas es el denominado GNSS *jamming*, que consiste en perturbar el receptor para bloquear su funcionamiento y denegar así el servicio de PNT que presta. El GNSS *spoofing*, por el contrario, es una técnica que busca suplantar las señales que emitirían los satélites de la constelación original en la ZOI [3][4].

Un ataque de *spoofing* asíncrono o no coherente consiste en la creación de una señal que sea lo suficientemente robusta como para que el receptor se “ancla” a ella creyendo que es la señal GPS real. Esta técnica crea una

señal muy parecida en pseudodistancia y en doppler que la señal GNSS original. Dependiendo del grado parecido entre la señal real y la señal suplantada, el atacante podría conseguir su propósito. Si el parecido no es mucho, el receptor GNSS de la víctima podría interpretar la señal suplantada como ruido o incluso como *multipath*, que siendo severo podría degradar el funcionamiento del receptor convirtiéndose, en el peor de los casos, en un ataque de *jamming* en lugar de *spoofing*. Este ataque es fácilmente detectable monitorizando en el receptor cambios bruscos en la solución PNT o en la relación portadora a densidad de ruido (CN0) o en la frecuencia doppler de cada satélite.

El ataque de *spoofing* síncrono o coherente, es un ataque mucho más robusto que el asíncrono, principalmente porque la señal emitida no se diferencia prácticamente de la señal GNSS original en tiempo, coordenadas, doppler y pseudodistancia. Por lo general, en este tipo de ataques, el receptor GNSS víctima se encuentra anclado a la constelación de satélites real de la ZOI (visible). En este escenario, el nivel de la señal de suplantación se aumenta progresivamente hasta que el receptor se engancha a dicha señal, abandonando la señal original.

Cualquiera de los ataques anteriores (*spoofing* asíncrono/síncrono o *jamming*), resulta fácilmente detectable en el emplazamiento de la víctima mediante el empleo de técnicas de DOA por cualquier equipo de guerra electrónica moderno o por una antena CRPA [5]. Una de las técnicas que complican la detección en este tipo de escenario es la de realizar un ataque simultáneo desde varias ubicaciones (ataque multiestático).

2. Descripción general del sistema

2.1. Realización de un ataque

Para la realización de un ataque de *spoofing* debe disponerse de, al menos, un nodo de ataque (ataque monosestático). En el caso de disponer de dos o más nodos, el ataque sería multiestático (Figura 1). De cara a la organización del ataque hay que designar un Nodo de Ataque Maestro (NAM), que unificará los datos de posición del resto de Nodos de Ataque Esclavo (NAS)

(etapa 1 de la Figura 1) y de los satélites visibles por cada uno de ellos (etapa 2). Con toda esta información, el nodo maestro, organizará el ataque dividiendo la constelación de satélites visibles en tantos sectores como nodos existan en el sistema (etapa 3) en un proceso denominado DAERS (División Acimutal del Espacio y Reparto de Satélites) y enviará a cada nodo el listado de satélites que debe suplantar (etapa 4). Por último, el nodo maestro indicará a los esclavos el resto de las condiciones (temporales o de cualquier otra índole) en la que debe iniciarse el ataque coordinado (etapa 5).

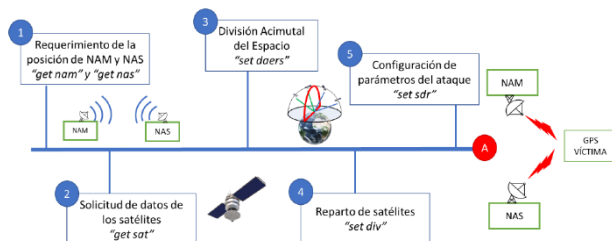


Figura 1. Secuencia de un ataque de spoofing multiestático.

2.2. Arquitectura

El sistema está compuesto por varios nodos de ataque. Existen dos tipos de nodo que tendrán diferentes funciones dentro del ataque, sólo uno de ellos actuaría como maestro (Nodo de Ataque Maestro, NAM) y el resto serían nodos esclavos (Nodo de Ataque Esclavo, NAS).

Los nodos disponen de una CPU, un receptor GPS, un módulo de comunicaciones y un transmisor SDR (*Software Defined Radio*) de bajo coste. El receptor GPS, modelo Ublox-6M [6], permite determinar la propia ubicación del nodo y la posición de cada uno de los satélites visibles de la constelación en esa ubicación, y permite obtener una sincronización temporal precisa común a todos los nodos (tiempo GPS).

Cada uno de los nodos está dotado con un módulo de comunicaciones basado en tecnología inalámbrica LoRa (*Long Range*) [7] con frecuencia de trabajo de 868 MHz en la banda libre ISM. Estos nodos permiten el intercambio de información entre nodos transmitiendo a muy baja potencia, pero consiguiendo gran alcance. Cada módulo de comunicaciones está conectado a un dispositivo Arduino UNO que actúa como intérprete de comandos entre dicho módulo y la CPU del nodo.

La CPU de cada nodo es una Raspberry Pi 4 con un procesador ARM Quad Core a 1.5 GHz y 4 GB de RAM.

El dispositivo SDR de cada nodo es un HackRF One [8] con un reloj TCXO de precisión $\pm 0,1$ ppm. La potencia de salida del SDR es ajustable ofreciendo un máximo de -15 dBm en el centro de la banda L1 de GPS (1575.42 MHz). Esta potencia es suficiente para el testeo en laboratorio empleando el concepto de HIL (*Hardware In the Loop*).

2.3. Comunicación entre nodos

Se ha establecido un protocolo que permita mantener la comunicación entre nodos de forma sencilla. Los comandos u órdenes que deben intercambiarse son muy pocos y se dividen en tres grupos: órdenes de solicitud de datos, órdenes de ejecución y órdenes misceláneas. Las primeras se ejecutan desde el NAM y solicitan a los NAS datos de posición y estado. Las órdenes de ejecución permiten realizar acciones y programar los ataques con diversos parámetros como satélites se deben suplantar y hora de inicio del ataque. Las órdenes misceláneas son las encargadas de ejecutar operaciones ajenas al propio ataque de *spoofing*, por ejemplo, reiniciar la CPU de un NAS.

2.4. Generación de la señal

Para la generación de la señal de suplantación de cada nodo *spoofers*, se ha empleado una modificación *ad-hoc* del conocido software *gps-sdr-sim* [9]. Para ejecutar este programa es necesario proporcionar un archivo de efemérides de los satélites GPS que la NASA pone a libre disposición en internet diariamente [10]. El software emplea dichas efemérides para sintetizar la señal falsa con las pseudodistancias y los doppler de los satélites visibles durante el ataque. La señal generada en banda base es posteriormente elevada a la banda L1 (1575,42 MHz) por el SDR que alimenta directamente la antena.

2.5. Algoritmo DAERS

Para la división de la constelación visible, se ha planteado un algoritmo sencillo denominado División Acimutal del Espacio y Reparto Satelital (DAERS). Después de que cada NAS determine su posición GPS y la reporte al NAM, éste realizará el reparto de satélites atendiendo al concepto mostrado en la Figura 2. En dicha figura se plantean 3 conceptos:

- PM (Punto Medio): se encuentra equidistante a ambos nodos (o el número de nodos que existan en el sistema). Este punto pasará a ser el punto de referencia desde el que se calcularán las demoras a los diferentes satélites.
- DUN (Demora de Unión del Nodo): línea de demora o acimut del nodo correspondiente que parte del punto medio.
- LDC (Línea División de Constelación): línea que pasa por el PM y es perpendicular a las DUN, en el caso de dos nodos, o que separan los sectores en el caso de un número mayor de nodos.

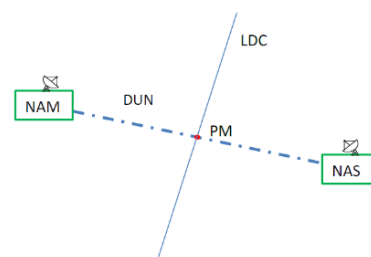


Figura 2. Esquema de cálculo DAERS.

Aunque se trata de un sistema en tres dimensiones, realmente para dividir la constelación visible de satélites GPS, no se precisa de la altura en ningún momento. El sistema de cálculo calcula la demora verdadera desde el PM hasta cada uno de los satélites visibles. Conocida las LDC, cada nodo de ataque asumirá la responsabilidad de suplantar las señales de los satélites de su mitad de bóveda celeste cuando se ejecute el ataque.

Dadas (φ_M, L_M) la latitud y longitud del NAM y (φ_{Si}, L_{Si}) la latitud y longitud del i-ésimo NAS, el cálculo de las coordenadas del punto medio PM (φ_{PM}, L_{PM}) se obtiene realizando la media de las latitudes y longitudes de los N nodos según las ecuaciones (1) y (2) respectivamente.

$$\varphi_{PM} = \frac{\varphi_M + \varphi_{S1} + \dots + \varphi_{SN}}{N + 1} \quad (1)$$

$$L_{PM} = \frac{L_M + L_{S1} + \dots + L_{SN}}{N + 1} \quad (2)$$

El cálculo de la Demora de Unión de Nodos (DUN) se realiza atendiendo a la figura 3, sumando 90° grados a la DUN. Para calcular la DUN debe tenerse en cuenta el signo de la diferencia de longitudes y latitudes.

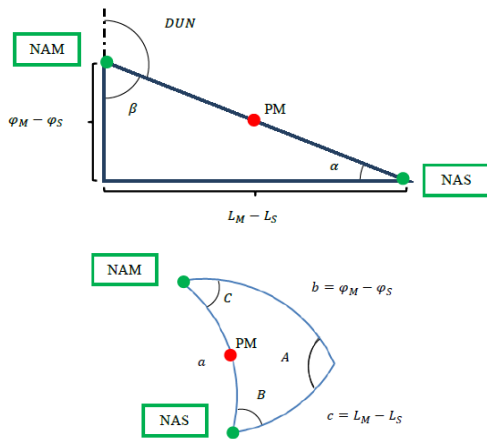


Figura 3. Determinación del DUN para nodo maestro y esclavo.

El cálculo de la Línea de División de Constelación (LDC) se realiza sumando y restando a la DUN 90° (ecuación (3)).

$$LDC = DUN \pm 90^\circ \quad (3)$$

A modo de ejemplo, en la figura 4 se muestra un escenario de ataque *spoofing* en la Ría de Pontevedra y se eligen dos situaciones para los nodos de ataque, uno en cada ribera. El NAM se instalaría en la Isla de Tambo con coordenadas $42^\circ 24' 37''\text{N}$, $8^\circ 42' 29''\text{W}$ y el NAS en Cabo Udra con coordenadas $42^\circ 20' 18''\text{N}$, $8^\circ 50' 10''\text{W}$. En este caso la LDC será el círculo máximo que pasa por el PM en dirección $150,67^\circ - 330,67^\circ$.

En el siguiente paso se obtendrían los acimuts de cada satélite visible y, en función de si éstos quedan a la derecha o a la izquierda de la LDC, serían asignados al NAM o al NAS respectivamente. Este procedimiento se extrapola fácilmente al caso de un sistema compuesto por N nodos.

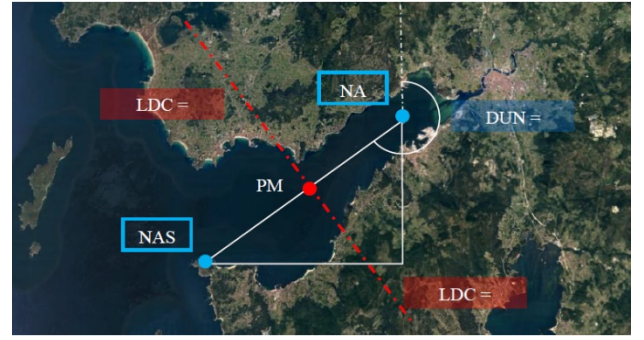


Figura 4. Ejemplo de cálculo de LDC con dos nodos de ataque.

3. Resultados y Discusión

3.1. Validación de la capacidad de proceso de un nodo

La generación de la señal y su transmisión para la suplantación deben hacerse en tiempo real. Para ello es necesario que las CPU de los nodos de ataque tengan capacidad de procesamiento suficiente. Se han realizado dos pruebas, para una CPU tipo Raspberry Pi 3B+ y para una Raspberry 4. La primera tuvo que descartarse por no cumplir requisitos de funcionamiento en tiempo real y la segunda resultó válida para la generación simultánea de señales de hasta 8 satélites (Figura 5).

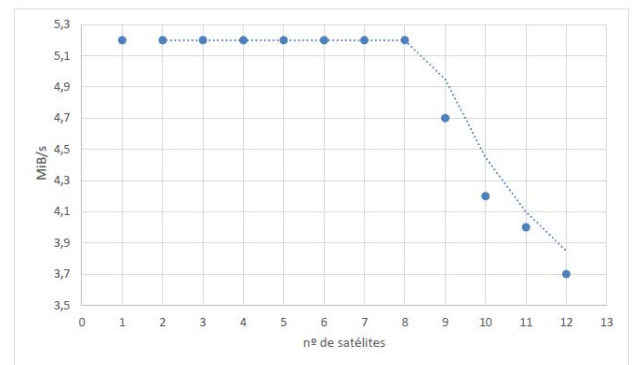


Figura 5. Capacidad de procesamiento del NAS en función del número de satélites suplantados.

3.2. Pruebas realizadas

El montaje para pruebas de laboratorio, mostrado en la Figura 6, ha sido realizado por sencillez únicamente con dos nodos: un NAM y un NAS. Este montaje evita la radiación de señales GPS al aire, pues además de estar prohibido, permite trabajar con un medio más controlado. Para ello, la atmosfera se ha sustituido por un cable coaxial y una serie de atenuadores de radiofrecuencia que tratan de simular así unas condiciones parecidas a las de propagación en espacio libre. La señal GPS real recibida por una antena exterior alimenta mediante un divisor al receptor GPS del nodo NAM y al receptor GPS víctima (Ublox-6M). Por otro lado, otra antena de GPS exterior entrega la señal real al receptor GPS del NAS. La víctima recibe, a través de un combinador, la señal GPS real y las señales de *spoofing* de ambos nodos de ataque.

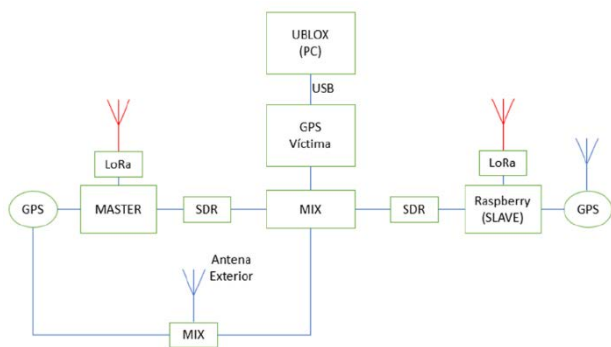


Figura 6. Montaje del demostrador con dos nodos de ataque.

Para comprobar la eficacia de los ataques se ha empleado el software *U-BLOX u-center*. En la figura 7 se evidencia una prueba de la suplantación efectiva de la señal GPS real, donde se muestra la latitud y longitud registrada durante dicha prueba. En ella se ven claramente dos posiciones estables y diferenciadas, separadas por un periodo transitorio en que el receptor pierde la señal real hasta y adquiere la señal falsa.

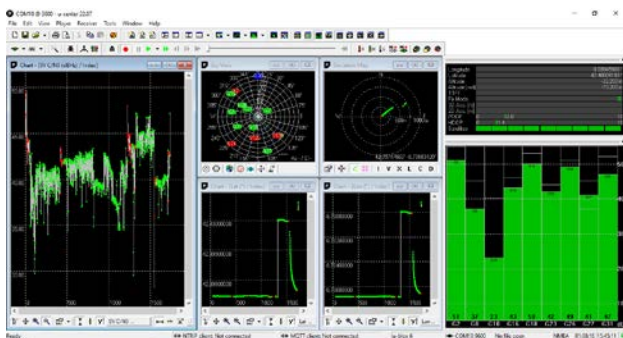


Figura 7. Ataque de spoofing evaluado con *U-BLOX u-center*.

En la figura 8 se muestra la evolución de la CN0 para otra prueba con dos ataques consecutivos. Las líneas verticales de color azul, definen los dos periodos de tiempo en los que el receptor GPS víctima pierde el seguimiento de la señal GPS real pero todavía no ha adquirido la señal suplantada. Ambos tiempos son relativamente grandes debido a que el receptor GPS empleado dispone de una medida básica para evitar perturbaciones indeseadas consistente en supervisar la coherencia histórica de las posiciones calculadas.



Figura 8. Evolución de la CN0 de dos ataques consecutivos.

En la figura 8 también se muestra la media de la CN0 evaluada por el receptor durante los ataques, en verde la señal real y en rojo la de la señal suplantada. Se puede observar una diferencia de alrededor de 5 dB entre ambas, lo cual resulta coherente, ya que la señal con la que se pretende suplantar a la señal GPS real deber ser de una potencia ligeramente superior a la primera.

4. Conclusiones

El ataque de suplantación (*spoofing*) de señales GNSS es técnicamente posible mediante el empleo de equipos de bajo coste. Este tipo de ataque resulta fácilmente detectable por cualquier equipo de guerra electrónica moderno o una antena CPRA debido a que la emisión de la señal suplanta se realiza desde una única ubicación. El demostrador presentado en este trabajo permite realizar un ataque multiestático, ejecutado por varios nodos atacantes de manera simultánea y sincronizada, complicando así su detección.

Agradecimientos

Este trabajo ha sido realizado bajo el marco del proyecto PICUD-2022-04 del Centro Universitario de la Defensa en la Escuela Naval Militar de Marín.

Referencias

- [1] M. A. Lombardi, "The Use of GPS Disciplined Oscillators as Primary Frequency Standards for Calibration and Metrology Laboratories," *Measure: The Journal of Measurement Science*, vol. 3, no. 3, 2008. <https://tf.nist.gov/general/pdf/2297.pdf>.
- [2] Resilient Positioning, Navigation, and Timing (PNT) Reference Architecture. Department of Homeland Security (DHS) Science and Technology Directorate (S&T).
- [3] M. L. Psiaki and T. E. Humphreys, "GNSS Spoofing and Detection," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258 - 1270, 2016. DOI: 10.1109/JPROC.2016.2526658.
- [4] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen and G. Lachapelle, "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques," *International Journal of Navigation and Observation*, vol. 2012, no. 127072, pp. 1-16, 2012. DOI: 10.1155/2012/127072.
- [5] J. A. Maloney, D. -H. Kwon, S. D. Keller and R. Janaswamy, "Realistic GPS Coverage Prediction for Dual-Polarized Controlled Reception Pattern Antennas," in *IEEE Antennas and Wireless Propagation Letters*, vol. 16, pp. 1907-1910, 2017, doi: 10.1109/LAWP.2017.2686581.
- [6] UBLOX. Neo-6 Series. <https://www.u-blox.com/en/product/neo-6-series>
- [7] SEMTECH. What is LoRa®? <https://www.semtech.com/lora/what-is-lora>
- [8] Great Scott Gadgets. HackRF One. <https://greatscottgadgets.com/hackrf/>
- [9] Takuji Ebinuma. GPS-SDR-SIM. <https://github.com/osqzss/gps-sdr-sim>
- [10] EOSDIS Earthdata. CDDIS Ephemerides data. <https://cddis.nasa.gov/archive/gnss/data/daily/>