Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Desarrollo de un sistema multiestático para la suplantación (spoofing) de señales GPS

Grado en Ingeniería Mecánica

ALUMNO: D. Marcos Pérez Vilda

DIRECTORES: D. José María Núñez Ortuño

D. Francisco Troncoso Pastoriza

CURSO ACADÉMICO: 2022-2023

Universidade Vigo

Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Desarrollo de un sistema multiestático para la suplantación (spoofing) de señales GPS

Grado en Ingeniería Mecánica

Intensificación en Tecnología Naval

Cuerpo General

Universidade Vigo

RESUMEN

Este trabajo fin de grado es una contribución a la investigación en el ámbito naval y militar de la explotación de las vulnerabilidades de los sistemas de navegación por satélite (GNSS) y en concreto del GPS. Durante el trabajo de desarrolla un sistema multiestático para la suplantación de la señal GPS (spoofing), que está compuesto por múltiples nodos de ataque que se comunican entre sí de forma inalámbrica, se dividen el espacio y se reparten los satélites de la constelación visible del GPS. De forma sincronizada ejecutan un ataque de spoofing sobre GPS suplantando la señal real por una falsa en una posición que establece el atacante. Dentro de la organización del ataque existe un nodo maestro, que unifica los datos de posición de los nodos y de los satélites visibles, reparte la esfera celeste en tantos sectores como nodos existan en el sistema y coordina el ataque según los parámetros introducidos por el usuario. Los nodos esclavos, ejecutan las órdenes del nodo maestro, trasfiriendo su posición cuando se le requiera o llevando a cabo el ataque en las condiciones que se dispongan. La comunicación entre los nodos de ataque se establece mediante la tecnología LoRa, de baja potencia, baja tasa de transferencia de datos y largo alcance, y la generación de las señales de suplantación del GPS se realiza mediante radio definida por software (SDR). Finalmente se muestran los resultados de diversas pruebas en el que el sistema es capaz de suplantar la señal GPS de forma efectiva.

PALABRAS CLAVE

GPS, *spoofing*, Perturbación, Satélite, Suplantación, *Jamming*, GNSS.

AGRADECIMIENTOS

En primer lugar, agradecer a mis tutores, el Sr. Núñez Ortuño y el Sr. Troncoso por su labor de tutorización y guía a lo largo de este trabajo. Al Sr. González Prieto por su inestimable ayuda.

A mis padres por la educación que he recibido, por fomentar mi pensamiento crítico y el interés por las ciencias y por su apoyo incondicional en las decisiones que he tomado a lo largo de mi vida.

Y a mis hermanos por el apoyo y los ánimos constantes durante los 5 años de formación.

"Toda guerra se basa en el engaño."

Sir Basil Liddell Hart

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

"Toda guerra se basa en el engaño"

Sir Basil Liddell Hart - Militar inglés

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Introducción

En el siglo XVI, también llamado de los descubrimientos, numerosos hombres se echaban a la mar en busca de tierras desconocidas, grandes riquezas y la promesa de un mundo maravilloso al otro lado del océano sin saber la derrota a seguir basando sus decisiones en suposiciones y cálculos muchas veces erróneos. Estimaban su situación y la corregían mediante la observación de astros. Pues era la astronomía la única forma de situarse en la mar.

Hoy en día los sistemas de navegación global por satélite (GNSS por sus siglas en inglés) permiten a cualquier persona situarse en cualquier parte del mundo sin necesidad de tener conocimientos sobre astronomía u orientación. Prácticamente todo el mundo dispone de un dispositivo que usa estos sistemas: móviles, navegadores, relojes… Se usan a diario cuando se quiere conocer el camino para llegar a este o aquel sitio, sin embargo, la importancia de estos sistemas es mucho mayor.

Gracias a los sistemas de navegación global por satélite el mundo es como se conoce. El trasporte comercial depende de estos sistemas para funcionar, especialmente el transporte marítimo, que supone más del 90% del comercio mundial según la UNCTAD[1]. No obstante, sus usos no se reducen al posicionamiento y navegación civil y militar, sino que son imprescindibles para actividades de rescate, rastreo o minería.

La rentabilidad que genera es de alrededor de 300.000 millones de dólares en el año 2017 y las ganancias acumuladas en el sector privado desde la existencia del GPS son de aproximadamente 1,4 billones de dólares según el estudio del NIST[2] [1].

Además, sus cada vez más implicaciones en sistemas e infraestructuras críticas de empresas y gobiernos los convierten en brechas de seguridad que son fácil y, sobre todo, económicamente explotables para perjuicios de gobiernos, empresas y particulares. Más aún si cabe cuando la mayor parte de sistemas militares dependen imprescindiblemente de los sistemas de navegación satélite y, especialmente el GPS, pueden convertir la negación o engaño de los sistemas de posicionamiento por satélite en armas de guerra de gran efectividad disuasoria como se reflexiona de forma interesante en [2].

[1] Conferencia de las Naciones Unidas sobre Comercio y Transporte
[2] Instituto Nacional de Estandarización y Tecnologías de EEUU.

1.2 Objetivos

El objetivo principal del presente trabajo fin de grado es el de desarrollar un sistema multiestático para la suplantación de la señal GPS o *spoofing*.

Determinados ataques de *spoofing* son fácilmente detectables, por ello el fin último será tratar de crear un sistema capaz de atacar desde varios vectores (múltiples transmisiones) que deberán dividirse acimutalmente el cielo de forma dinámica para suplantar cada uno un grupo de satélites. Además, y donde radica la mayor dificultad de este trabajo, el ataque debe ser simultáneo de esta manera detectar el ataque será mucho más complicado y efectivo.

Un objetivo secundario es comprender como se pueden realizar ataques, no solo de negación de uso (*Jamming)*, sino de suplantación (*spoofing)* de la señal GPS para poder variar la posición y el tiempo que recibe un usuario y un uso combinado de ambos.

Por último, se pretende realizar una serie de experimentos para validar la capacidad del sistema desarrollado sobre un receptor GPS víctima real.

1.3 Motivación

El autor como alumno del Centro Universitario de la Defensa y su condición de militar enfoca su interés hacia el ámbito más cercano al desempeño de su actividad personal y profesional presente y futura. Es decir, temas y campos relacionados con el mundo naval y militar o que puedan tener una aplicación directa o indirecta en estos mismos campos.

La motivación para la elección de este Trabajo Fin de Grado se fundamenta en tres puntos principalmente:

- El primero por tratarse de un trabajo relativo al ámbito de las Telecomunicaciones, por el que el autor siente predilección y ha desarrollado mayor interés durante el estudio del grado y por considerar que el futuro de esta tecnología es prometedor.

- El segundo y de mayor peso porque el trabajo tiene una clara finalidad militar y con expectativa de poder ser usado de forma real por unidades de la Armada en operaciones reales.

- Finalmente, por tratarse de un trabajo que ahonda en uno de los sistemas que, a criterio del autor, más ha revolucionado el mundo tal y como se conoce en la actualidad. Por la dependencia de tantos sistemas e infraestructuras hacia el GPS y por ser un problema de actualidad en el contexto de los conflictos armados donde el uso de la tecnología de *spoofing* sobre GPS ya está documentada con resultados satisfactorios (para las fuerzas empleadoras).

1.4 Estructura de la memoria

Después de presentar los objetivos a alcanzar con este trabajo de fin de grado y la motivación para su elección y realización se expone la estructura de la memoria para recoger a modo de resumen que contenidos se podrán encontrar en la misma. Está compuesta por seis apartados que pretenden presentar la información necesaria para la comprensión del trabajo.

1. En apartado 1 “Introducción y objetivos” se presenta un pequeño marco del porqué de el tema de este trabajo, los objetivos a alcanzar durante el desarrollo de este, la motivación del autor para llevarlo a cabo y una breve descripción de la estructura de la memoria.
2. En el segundo apartado “Estado del arte” se encuentra una contextualización teórica breve que pretende aportar una serie de fundamentos para comprender el desarrollo posterior del

trabajo en sí y hacer una descripción somera de las tecnologías que van a ser utilizadas en el trabajo.

3. En el tercer apartado “Desarrollo del TFG”, se presentan las herramientas tanto de software como de hardware que son necesarias para la realización del trabajo fin de grado, y el cómo se han resuelto los diferentes problemas necesarios para la consecución de los objetivos previamente mencionados. Así como de las condiciones en las que se han llevado a cabo los experimentos realizados para la validación del sistema.
4. El apartado 4 “Resultados” presenta el análisis de los resultados obtenidos durante los experimentos realizados.
5. En el apartado 5 se presentan las conclusiones alcanzadas por el autor del trabajo tras el desarrollo de este. Así como las líneas futuras a seguir para continuar, mejorar e implementar nuevas tecnologías, herramientas o procedimientos al sistema.

Tres Anexos complementan el contenido de la memoria, el Anexo I presenta las implicaciones sociales, económicas y ambientales del uso de la tecnología de suplantación de señales GPS, el Anexo II recoge una reflexión ético-social relativa al uso de esta tecnología y el Anexo III expone una recopilación de siglas y términos que aparecen de alguna u otra forma a lo largo del trabajo.

2 ESTADO DEL ARTE

2.1 Sistemas GNSS

Aunque el GPS, sistema GNSS (*Global Navigation Satelite System*) de los Estados Unidos de América, es el más reconocible de ellos, existen varios de estos sistemas desarrollados por diferentes gobiernos alrededor del mundo. La Unión Soviética desarrolló el sistema GLONASS que actualmente opera la Federación Rusa, plenamente operativo desde 2007 y compuesto por 24 satélites. La Unión Europea tras un largo proceso de desarrollo de su propio sistema GNSS, GALILEO, alcanzó la plena capacidad operacional en el año 2020 con una constelación de 27 satélites. Año en que también finalizó el despliegue de la constelación de 35 satélites del sistema chino BeiDou. Adicionalmente otros países cuentan con sistemas de cobertura regional como la India con el IRNSS o Japón con el QZSS.

Figura 2-1 Logotipos de los GNSS: GPS, GLONASS, BeiDou, GALILEO. [Fuente: páginas oficiales]

2.2 Fundamentos del GPS

El *Global Positioning System (GPS)* es un sistema de posicionamiento global por satélite propiedad del gobierno de los Estados Unidos de América que permite el posicionamiento, la navegación y cronometría en todos los puntos del planeta. Fue puesto en marcha en los años 70 y aunque su uso fue inicialmente militar, sus prometedoras aplicaciones pronto lo abrieron al mundo civil y comercial. Está compuesto de tres segmentos: el segmento espacial, el segmento de control y el segmento usuario. Los dos primeros están operados y mantenidos por la USSF[3] dependiente del Departamento de la Fuerza Aérea. [3]

[3] United States Space Force (Fuerza Espacial de Estados Unidos)

2.2.1 Segmento espacial

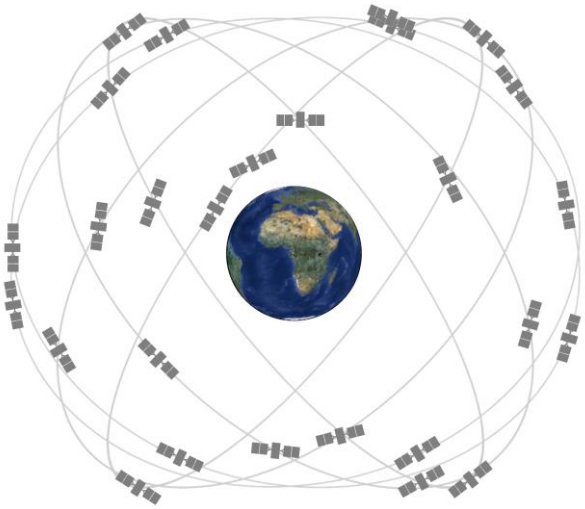

Figura 2-2 Constelación GPS de 24 ranuras. [1]

El segmento espacial del GPS debe estar compuesto por una constelación (Figura 2-2) de, como mínimo, 24 satélites divididos en 6 órbitas (nombradas con las primeras 6 letras del alfabeto), con una inclinación de 55º respecto al Ecuador, de 4 ranuras o "*slots*" cada una. Esta disposición asegura la cobertura de un mínimo de 4 satélites en cualquier punto del planeta en cualquier momento, que son los necesarios para el proceso de trilateración que permite el posicionamiento, como se expondrá en el apartado 2.4. Si bien es cierto, en la actualidad la constelación GPS está conformada por 31 satélites (Tabla 2-1) de los cuales 27 están operativos y 4 en reserva.

Estos satélites extra mejoran el desempeño general del sistema, aunque no se les considera parte del núcleo de la constelación. Las orbitas de los satélites del GPS son MEO[4] con una altura aproximada de 20.200 km. A esta altura los satélites orbitan la Tierra 2 veces cada 24 horas.

La esperanza de la vida operativa de los satélites que se diseñó en un principio ha sido ampliamente superada por las diferentes versiones de satélites de la constelación, lo que permite mantenerlos por más tiempo y la convivencia de hasta 4 versiones diferentes de satélites. Desde los más antiguos del *Bloque II* hasta los más modernos del *Bloque III* (Figura 2-3). Cada satélite porta 4 relojes atómicos de Rubidio o Cesio.

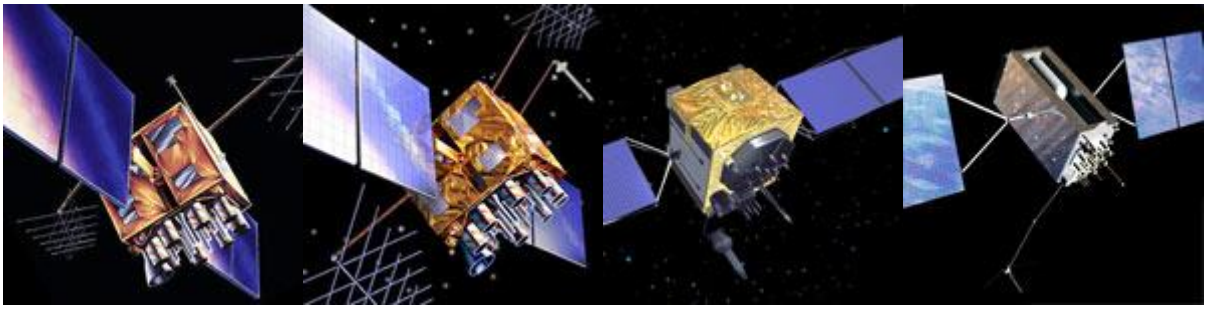

Figura 2-3 Satélites GPS: Bloque IIR, IIRM, IIF y III. [3]

Los satélites están compuestos por diferentes módulos con diferentes funciones, que se encargan de controlar la altitud o de posicionar los arrays solares. Sin embargo, la parte del astro artificial que aporta la funcionalidad GPS es el módulo de misión. El módulo de misión o navegación del satélite (Figura 2-4) es el que se encarga de la generación y transmisión de los mensajes de adquisición y datos de navegación las frecuencias determinadas para ello, las denominadas L1 y L2, a partir de los satélites

[4] Medium Earth Orbit (Entre 1.200 km y 36.000 km)

IIF, también la L5 para el ámbito civil. Este módulo de misión es controlado mediante las predicciones de navegación del satélite y datos de corrección de trayectoria que cada satélite recibe mediante los enlaces de seguimiento, telemetría y control con el Segmento de control (apartado 2.2.2). El módulo está compuesto por varios (aunque sólo funciona uno simultáneamente) relojes atómicos o *Atomic Frecuency Standards (AFS)*, generalmente de rubidio, aunque también los hay de cesio. Los AFS mantiene la base de la precisión y estabilidad de las frecuencias portadoras y códigos distancia que transmiten los satélites. Un sintetizador de frecuencias sincronizado en fase con los AFS genera la frecuencia de 10,23 MHz que sirve de referencia temporal. La *Navigation Data Unit (NDU)* contiene el código rango que genera el *C/A Code* (civil) y el *P(Y)* code (militar) con los datos de navegación que requieren los elementos del segmento usuario para calcular su posición. Disponen de antenas para la banda L, necesarias para la transmisión de mensajes de navegación y por último un sistema de comunicación (*crosslink)* entre satélites que permiten medir la distancia entre los mismos.

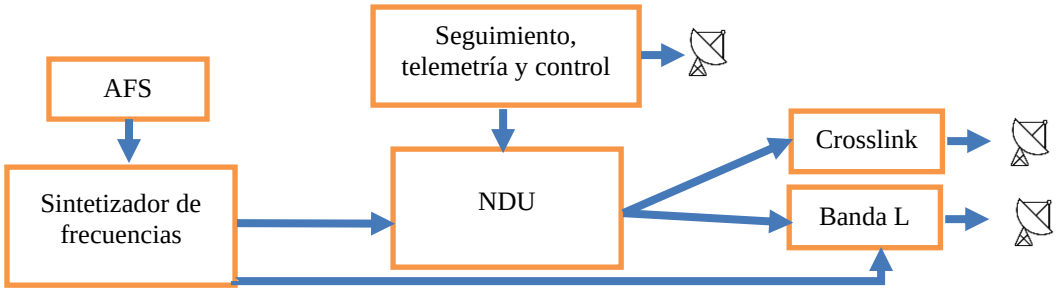

Figura 2-4 Módulo de navegación GPS (18/01/2023) [2]

Tabla 2-1 Estado de la constelación GPS (18/01/2023) [2]

Órbita	Ranura	SVN	PRN	Bloque
D	2	63	1	IIF
D	1	61	2	IIR
E	1	69	3	IIF
F	4	74	4	III
E	3	50	5	IIR-M
D	4	67	6	IIF
A	4	48	7	IIR-M
C	3	72	8	IIF
F	3	68	9	IIF
E	2	73	10	IIF
D	5	78	11	III
B	4	58	12	IIR-M
F	6	43	13	IIR
B	6	77	14	III
F	2	55	15	IIR-M
B	1	56	16	IIR
C	4	53	17	IIR-M

Órbita	Ranura	SVN	PRN	Bloque
D	6	75	18	III
C	5	59	19	IIR
E	4	51	20	IIR
D	3	45	21	IIR
F	5	41	22	IIR
E	5	76	23	III
A	1	65	24	IIF
B	2	62	25	IIF
B	5	71	26	IIF
C	2	66	27	IIF
C	1	57	29	IIR-M
A	3	64	30	IIF
A	2	52	31	IIR-M
F	1	70	32	IIF

2.2.2 Segmento control

El segmento de control es la parte de la infraestructura del GPS que se encarga de la monitorización, mando y control de los satélites, realiza su seguimiento y rastreo, actualiza las efemérides sobre el estado de los satélites y corrige los errores y anomalías que puedan detectarse en los mismos. Programa las maniobras relacionadas con el mantenimiento de la estación que les corresponde en las órbitas. Permite además comunicaciones por satélite para usuarios gubernamentales/militares. La red del segmento de control está compuesta por numerosas estaciones alrededor del mundo, en su mayoría en la zona intertropical.

La estación principal de control es la *Master Control Station (MCS)*, sita en la Base Aérea de Schriever en Colorado. En este centro de control se lleva a cabo la programación y la localización de los satélites, la generación del mensaje de navegación (*C/A code*), la monitorización del estado de cada satélite, la sincronización de la constelación y el análisis del desempeño y rendimiento del sistema.[4] Existe una MCS de reserva o alternativa en la Base Aérea de Vandenberg en el estado de California.[3]

Las estaciones de monitorización o *Monitor Stations (MS)*, están distribuidas por todo el planeta y se encargan de recopilar información atmosférica en las diferentes partes del mundo, de realizar el seguimiento a la señal (o mensaje) de navegación, de medir el rango y señal de la portadora y comprobar que la información proporcionada por los satélites a los usuarios es correcta. Existen 6 estaciones de monitorización situadas cada una de ellas en: Las Islas Hawaii, Schriever, Cabo Cañaveral (Florida), la Isla Ascensión en el Océano Atlántico, la Isla Diego García en el Índico y el Atolón Kwajalien en las Islas Marshall. Además de estas 6, que son administradas por las USAF[5], existen 10 adicionales administradas por la NGA[6]que han aumentado la precisión de los datos de las órbitas de la constelación (Figura 2-5).

[5] United States Air Force
[6] National Geospatial.Intelligence Agency

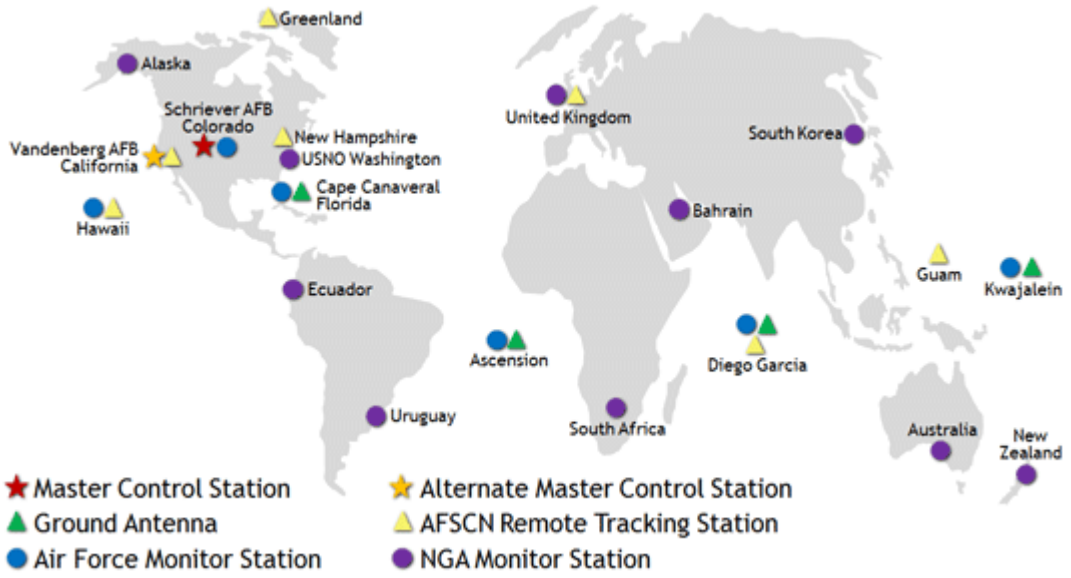

Figura 2-5 Mapa de las estaciones del Segmento Control. [3]

El último elemento del segmento de control son las antenas terrenas que se usan para comunicar con los satélites de la constelación, transmisiones de maniobra a los satélites, actualizaciones del mensaje de navegación y para recibir los datos de telemetría de los satélites que son luego analizados en las estaciones de control previamente mencionados. Son 4 y están situadas en Cabo Cañaveral, Isla Ascensión, Isla Diego García y Atolón Kwajalien. Además, existen 7 estaciones remotas de seguimiento

2.2.3 Segmento usuario

Este segmento engloba los receptores de señales GPS en banda L civil y militar y la computación para calcular posición estimada, velocidad y tiempo. Los receptores GPS están compuestos por una antena de polarización circular a derechas y cobertura hemisférica, un procesador y un interfaz para presentar los datos.

2.3 Señal GPS

La señal GPS hace uso del tipo de modulación *Binary Phase Shift Keying (BPSK)* que no es más que un esquema de señal digital por el cual una frecuencia portadora emite en fase (0º) o desfase de 180ª en función si se quiere enviar bits (símbolos) con valor 0 o 1 (Figura 2-6). Puede entenderse como el producto de la señal portadora por la señal de "datos" teniendo estos, valores de amplitud +1 o -1 según el valor del bit (0 o 1). Para evitar fallos en la transmisión de errores se hace uso de técnicas de *Foward Error Correction (FEC)* para que los receptores puedan detectar los posibles errores y subsanarlos.

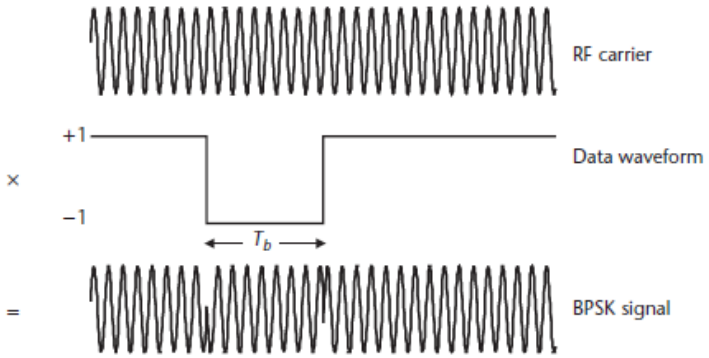

Figura 2-6 Señal modulada mediante BPSK. [4]

A este esquema de modulación se le añade otro tipo de modulación por cambio de fase conocido como *Direct Sequence Spread Spectrum (DSSS)* por el cual se añade a la señal BPSK una tercera componente (Figura 2-7): El código PRN, que es un concepto vital en este proyecto pues es único para cada satélite y por tanto permite identificar el o los satélites de los que un terminal GPS está recibiendo los datos. El término "Spread" hace referencia al gran ancho de banda de la señal una vez es modulada mediante este sistema.

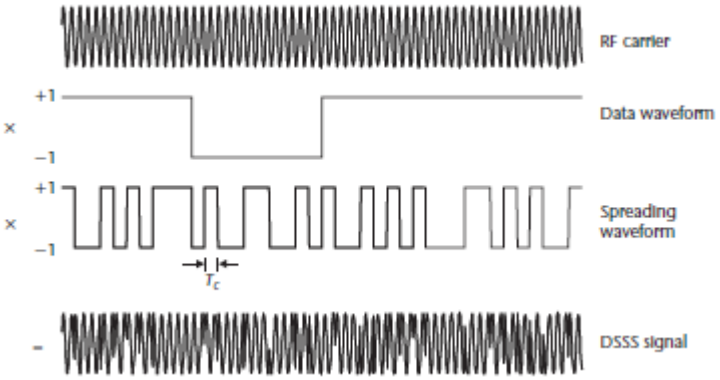

Figura 2-7 Señal modulada mediante DSSS. [4]

2.3.1 Adquisición

La adquisición de la señal GPS no es más que un proceso de búsqueda para encontrar la señal GPS de los satélites a la vista y estimar inicialmente la fase de la señal y el Doppler de la portadora (Figura 2-8). Este proceso necesita de replicar el código C/A y la frecuencia portadora de cada satélite. Existe un umbral de potencia y elevación para que los satélites sean adquiridos, por tanto, todo satélite con un valor mayor que este umbral son considerados a la vista y adquiribles.

La distancia se relaciona directamente con el desfase entre el código C/A recibido y la réplica del código C/A. El efecto Doppler de la réplica con la portadora permite calcular el movimiento del receptor. El receptor GPS, para buscar el código C/A inicial, replica las 1.023 fases distintas dentro de la frecuencia esperada de la señal GPS.

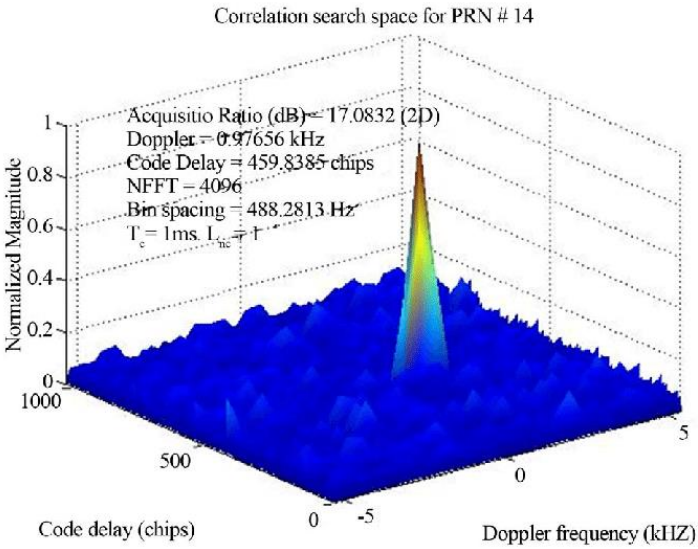

Figura 2-8 Pico de correlación (adquisición) respecto a Doppler y desfase del PRN 14. [5]

2.3.2 Seguimiento

El seguimiento es la monitorización continua de la señal GPS tras la adquisición, se divide en el seguimiento de código y el seguimiento de portadora. El seguimiento de código realiza una comparación constante de las señales con referencias internas del receptor GPS con el objetivo de mantener tanto el código réplica como las señales perfectamente alineadas. Para mantener la precisión el receptor aplica en tiempo real las correcciones de errores que se transmiten y detectan en estas mismas señales. En el seguimiento de frecuencia portadora, se detecta cualquier variación en el Doppler de la señal y se aplican las correcciones necesarias. Ambos dos tipos de seguimiento se realizan mediante bucles que se denominan "*Delay-Lock Loop"* (DLL) para el código y "*Phase-Lock Loop*" (PLL) para la frecuencia portadora.

Se puede apreciar en la Figura 2-9, que son tres las correlaciones que se llevan a cabo: la correlación "*prompt"*, la correlación "*late"* y la correlación "*early"*. El *DLL Discriminator* se obtiene comparando las tres correlaciones. A la salida de este se proporcionan las estimaciones de los errores de desfase y código que son introducidos al *DLL Loop Filter*, en este filtro se reduce el ruido de la señal para hacerla pasar por el *Numerical Controlled Oscillator, NCO* y obtener el desfase real de la señal que debe introducirse en el generador de código PRN para conseguir la alineación de ambas señales (sintética y real) como se ha mencionado anteriormente.

Una vez se alinea esta señal sintética con la señal real, el receptor es capaz de decodificar y leer la señal satélite y el mensaje de navegación que permite el posicionamiento GPS.

En cuanto al bucle de seguimiento de la frecuencia portadora, comienza tras la salida del correlador "*prompt"*, que de una forma parecida al seguimiento de fase-código, pasa por un discriminador que le proporciona el valor del error Doppler de la señal. A continuación, atraviesa un filtro para eliminar el ruido y el NCO tras lo cual se genera una réplica local de la frecuencia portadora.

Este esquema es el básico, aunque se pueden encontrar esquemas de seguimiento más complejos y robustos que hacen uso del filtro Kalman [6].

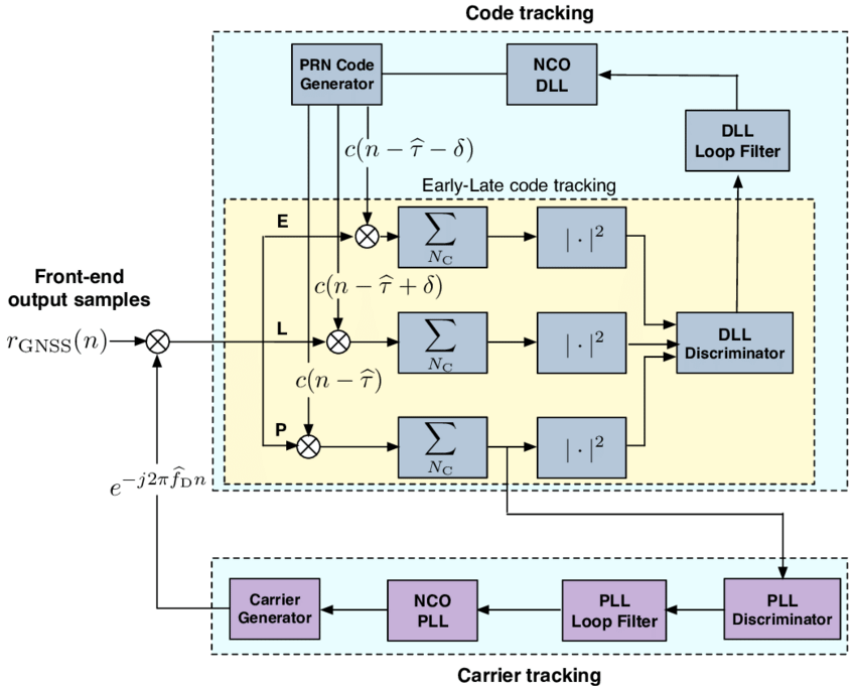

Figura 2-9 Arquitectura del módulo de seguimiento. [7]

2.3.3 PRN

El PRN (Pseudo-Random Noise) es una señal conocida por los receptores GPS y es finita y periódica. El intervalo entre cambios de la forma de onda del Código PRN es conocido como *Chip period* (T_C) y aquella parte de la onda dentro de este periodo es denominada *Chip*. El porqué del uso de PRN mediante DSSS se debe a tres factores principalmente: en primer lugar, porque los frecuentes cambios de fase inducidos por la señal PRN habilitan una medición de la distancia al satélite más precisa por parte de los receptores GPS. En segundo lugar, porque al estar claramente diferenciados los códigos PRN permite transmitir a múltiples satélites al mismo tiempo, en la misma frecuencia (*Code Division Multiple Access CDMA)* y ser el receptor GPS capaz de distinguir y diferenciar las señales de cada satélite. Por último, porque proporciona una protección efectiva ante las interferencias en banda estrecha (emisiones artificiales).

Actualmente la coexistencia de varios tipos de satélites diferentes permite que algunos de ellos tengan mayores prestaciones que otros más antiguos pero todos ellos emiten sus transmisiones haciendo uso de dos frecuencias portadores, denominadas L1 y L2, ambas dos, múltiplos de una frecuencia fundamental (f_0) de 10,23 MHz. La frecuencia L1 es 154 veces f_0 y por tanto tiene un valor de 1575,42 MHz, se modula mediante dos códigos PRN el código C/A[7] (civil) y el código P (militar) (Figura 2-10), además de los mensajes de navegación modulados a una velocidad de 50 bps. La frecuencia L2, con un valor de 1227,6 MHz ($120f_0$) también es de uso compartido civil-militar, sin embargo, sólo es modulada con una señal PRN al mismo tiempo y los mensajes de navegación correspondientes al satélite. En los satélites del Bloque III se ha añadido además una frecuencia portadora más, la L5 de 1176,45 MHz ($115f_0$) cuyo uso se reduce prácticamente al ámbito de la navegación aérea.[8]

[7] Coarse/acquisition code

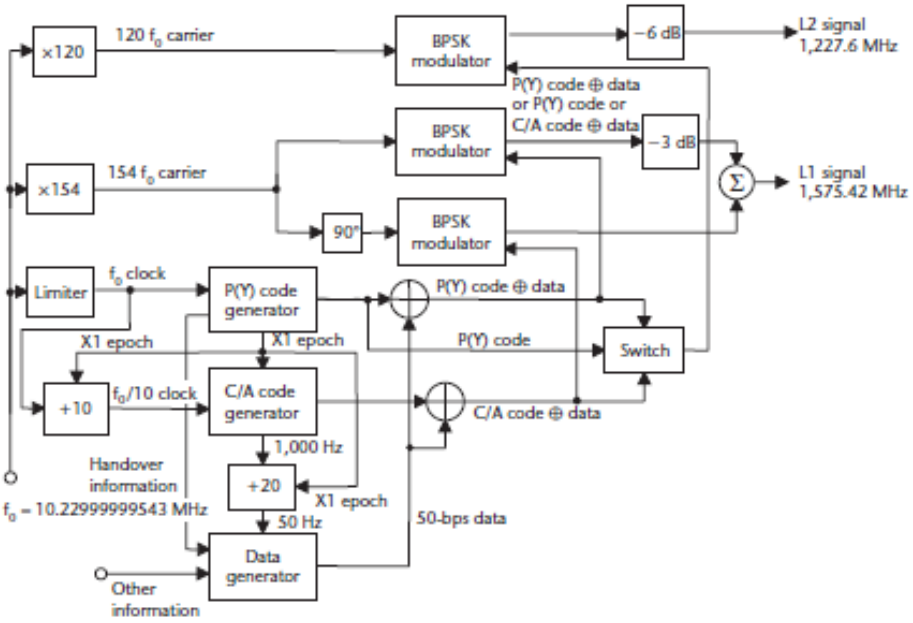

Figura 2-10 Esquema estructura señal satélite GPS. [4]

La diferencia entre el código P y el código C/A es que el primero es cifrado (tras lo cual se denomina código Y) y permite el acceso al *Precise Positioning Service (PPS)* [9], de uso gubernamental y militar y el segundo al *Standard Positioning Service (SPS)* [8] que es abierto al mundo civil.

2.4 Estimación de Posición, Velocidad y Tiempo (PVT)

EL GPS utiliza el concepto de *Time of Arrival (TOA)* para determinar la distancia de un satélite a un usuario. Este concepto se traduce en que conociendo la velocidad de propagación de la señal en la atmosfera y midiendo el tiempo que tarda en recorrer la distancia que separa al satélite del usuario, añadiendo que el receptor conoce la posición del satélite al momento de la transmisión (por la transmisión de las efemérides ver apartado 2.5.1), podemos averiguar el valor de esa distancia, haciendo uso del siguiente sistema de ecuaciones:

$$r_n = c \cdot \Delta t_n,$$

donde r_n es la distancia desde el satélite *n* hasta el receptor, *c* es la velocidad de propagación de la luz y Δt_n es el tiempo que tarda en llegar la señal al receptor desde el satélite *n*.

Sin embargo, el mayor problema del GPS, y en general de todos los GNSS, es que los relojes de los receptores del segmento usuario son menos precisos que los relojes atómicos de los satélites. Aunque los relojes de cuarzo que suelen llevar los recetores GPS tienen un error de exactitud de 5 partes por millón, lo que a priori puede parecer poco, al multiplicarlo por la velocidad de la luz obtenemos un error de precisión de 1500 metros, que es inaceptable para un sistema como el GPS. Por ello y conociendo que existe un error, las distancias que se calculan se denominan pseudodistancias.

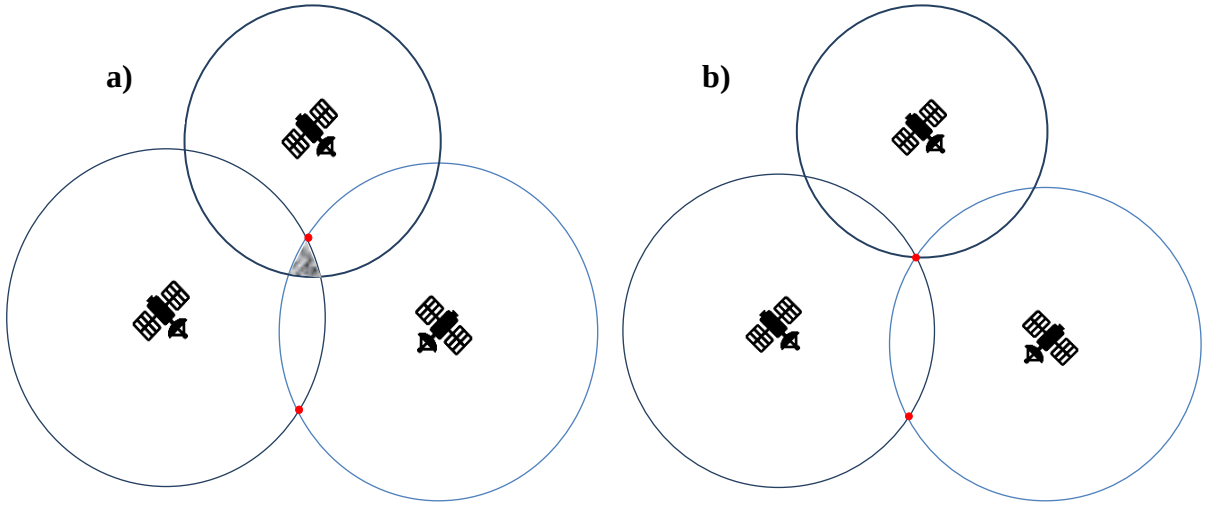

Figura 2-11 Trilateración en un sistema de 2 dimensiones a) Trilateración sin la corrección del reloj del receptor b) Trilateración con corrección. [Elaboración Propia]

Imaginando que se trabaja en un sistema de dos dimensiones. Con una sola pseudodistancia se halla una circunferencia, centrada en el satélite, de posibles posiciones donde puede encontrarse el receptor GPS. Si se añade una pseudodistancia más, es decir, otro satélite, los cortes de las dos circunferencias nos proporcionan dos puntos posibles. Por ello es necesaria una tercera distancia que resuelva la ambigüedad, proceso que se denomina trilateración[8]. Sin embargo, debido al error del reloj del receptor, esta tercera circunferencia de pseudodistancia no coincidirá de forma exacta con ninguno de los puntos de corte. El receptor está programado para adelantar o atrasar su reloj hasta hacer coincidir exactamente las tres pseudodistancias en el mismo punto (Figura 2-11). De esta forma no sólo se calcula la posición ansiada de forma precisa, sino que además se obtiene con exactitud.[10] El concepto es el mismo cuando es aplicado al sistema de tres dimensiones en el que trabaja, en vez de circunferencias, se obtienen cortezas esféricas (Figura 2-12). Y en vez de tres pseudodistancias, serán necesarias cuatro. Es por esto por lo que la disposición de la constelación del segmento espacial garantiza la cobertura de al menos cuatro satélites en todos los puntos del planeta (ver apartado 2.2.1).

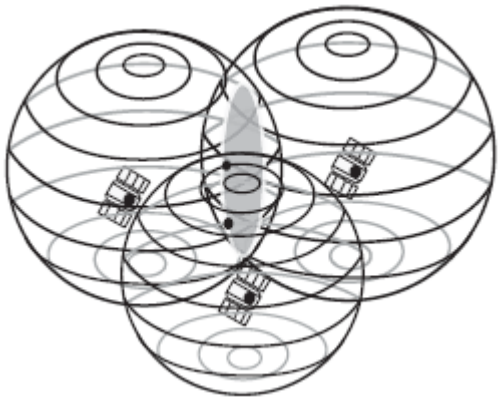

Figura 2-12 Trilateración en un sistema de 3 dimensiones. [4]

[8] Cálculo de la posición de un punto conocidas las posiciones de tres puntos de referencia y la distancia a estos.

2.5 Mensajes de Navegación

2.5.1 Legacy NAV Message (LNAV)

El mensaje de navegación proporciona información adicional que ayuda al receptor GPS a obtener la estimación PVT debido a que permite calcular de forma precisa la localización de cada satélite de la constelación visible y el tiempo que tarda en transmitirse cada señal de navegación. La información que aporta este mensaje incluye: el tiempo de vida del satélite, es decir desde cuando está en funcionamiento, la posición del satélite, la "salud" y estado del satélite, el estado de la constelación en su conjunto, las correcciones pertinentes aplicables al reloj satélite, los modelos de corrección del efecto de la ionosfera sobre las señales de frecuencia única, y el tiempo global UTC.

El mensaje o *master frame* está compuesto por 25 *data frames* que a su vez se dividen en 5 *subframes* (ver Figura 2-13) de una longitud de 300 bits cada una. Mientras las 3 primeras *subframes* se repiten en todas las *data frames*, la 4 y la 5 tienen 25 páginas, una por cada una de las frames que forman el mensaje. Por tanto, en la primera frame irán las páginas nº1 de las subframes 4 y 5, en la siguiente las páginas nº2, y así sucesivamente. Cada subframe está formada por 10 palabras de 30 bits y empiezan con una palabra telemétrica (TLM) y una "palabra de entrega" (HOW).[4], [8]

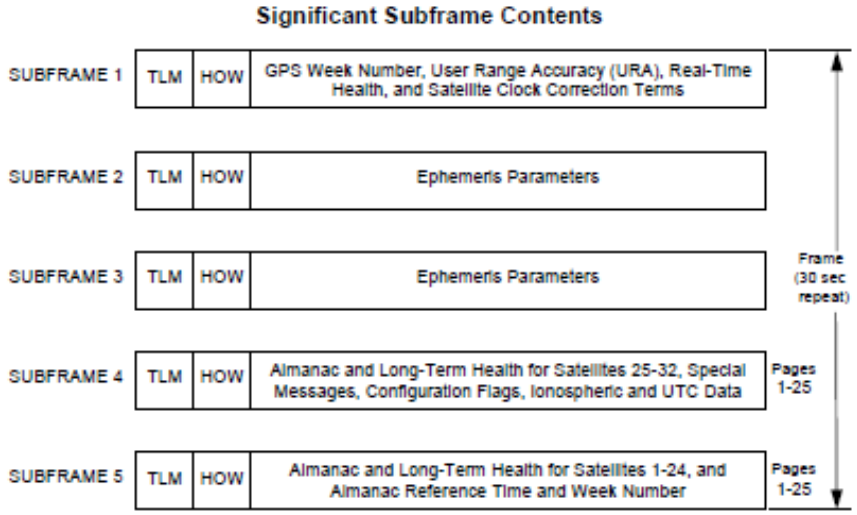

Figura 2-13 Estructura del mensaje de navegación LNAV. [8]

La subframe 1 proporciona el número semanal de transmisión, es decir el número de semanas que lleva en funcionamiento desde 1980 aunque como su valor máximo es 1024 ya han ocurrido dos reinicios, en 1999 y en 2019. También indica el tiempo del reloj atómico del satélite y sus correcciones, la salud del satélite, el indicador URA (*User Range Accuracy),* que es necesario cuando sólo se dispone de una de las dos bandas L1 o L2, e informa al usuario de la estimación de errores de distancia debidos al mismo satélite o al segmento de control (apartado 2.2.2).

La subframe 2 y 3 proporcionan las denominadas Efemérides, que no son más que parámetros de la órbita que está siguiendo el satélite en concreto y la posición en el momento de la transmisión.

En la subframe 4 y 5, se suministra el almanaque en cuyos datos se recogen efemérides simplificadas de todos los satélites de la constelación GPS, correcciones por el efecto ionosférico y los parámetros que permiten sincronizar la hora GPS a la hora UTC.

2.6 Degradación de GPS

Las señales GPS son susceptibles de diferentes fenómenos que degradan el rendimiento del sistema. Algunos de estos fenómenos están provocados por otras señales de radio, otros por la

reflexión de las propias señales del GPS y los últimos provocados por diferentes irregularidades en la atmósfera, concretamente en la ionosfera.

2.6.1 Interferencias

Las interferencias son provocadas por otras emisiones que no tienen como finalidad un ataque *Jamming* pero que sin embargo tienen un resultado parecido, es decir el *Jamming* explota este fenómeno de degradación del GPS (ver apartado **¡Error! No se encuentra el origen de la r eferencia.**). Pueden clasificarse en interferencias de banda ancha para las señales civiles en las bandas L1 y L2 y de banda estrecha para las señales militares de estas dos bandas y la banda L5 en general.

Generalmente cuando se trata de emisiones de un mismo tipo o de características similares siempre existe un nivel mínimo de interferencia entre señales, inclusive señales GPS de diferentes satélites hacen interferencia unas a otras en algún modo. Este tipo de interferencia entre señales de un mismo sistema se denomina interferencia propia o *self-interference*. La existencia de otros sistemas GNSS como Galileo, que hace uso de las mismas bandas que el GPS, supone un tipo de interferencias inter-sistemas o *intersystem interferences.*

Aunque en el presente grupo de degradación de GPS entrarían los ataques *Jamming* y *spoofing*, este apartado se centra en aquellas interferencias que no son intencionadas (como si lo son los ataques mencionados). Y es que es manifiesta la dependencia humana de las señales de radiofrecuencia. En el día a día, la cantidad de sistemas que, no solo hacen uso, sino que, además, dependen vitalmente de ellas es notable.

Para evitar las interferencias se han llevado a cabo medidas para reducir o prohibir determinadas emisiones en las bandas de frecuencia que pudiesen afectar a las emisiones GPS. Sin embargo, también se ha de tener en cuenta el tipo de señal que comparte banda con la del GPS, puesto que las señales de pulsos no suponen una interferencia real para los receptores GPS. Por tanto, sistemas militares como el TACAN[9], el Link 16[10] u otros sistemas para la navegación aérea, civil y militar, que usan señales pulsadas pueden convivir en un entorno que haga uso del GPS sin interferencias mutuas.

Pero no todos los problemas de interferencias son causados por transmisiones con las que comparte banda el GPS, sino que muchas otras son generadas por harmónicos de otras señales que se emiten en frecuencias diferentes con una intensidad alta.

Estas interferencias cobran especial importancia cuando consideramos que la intensidad de señal de los satélites al llegar al receptor está por debajo del nivel de ruido térmico (-174dB), por ello el receptor necesita una ganancia de alrededor de 100 dB para diferenciar el ruido térmico de la señal GPS.[4]

Es de especial relevancia la vulnerabilidad del código C/A a una interferencia de onda continua, que afecta especialmente a los procesos de adquisición, ya que perjudica a la identificación del PRN de los satélites.

2.6.2 Propagación multitrayecto (Multipath)

La degradación de la señal por propagación multitrayecto no es más que la refracción y/o reflexión de señales propias del GPS que sin embargo recorren un camino más largo entre satélite y receptor, precisamente, por esas reflexiones. Por tanto, las recepciones de camino múltiple llegan con retraso al receptor respecto a las de camino directo. Tienen gran importancia debido a que, en contraposición a otro tipo de degradaciones, estas contribuyen claramente a un gran número de los errores de GPS.

[9] Tactical Air Navitation System
[10] Tactical Data Link: Sistema de intercambio de datos tácticos militares en tiempo real

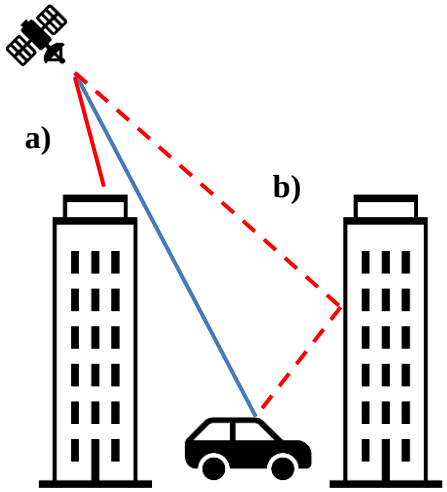

Figura 2-14 a) Shadowing, b) Multipath. [Elaboración Propia]

Cuando el retraso de las señales de propagación multitrayecto es mayor del doble del periodo que ocupa un símbolo de la modulación BPSK (ver apartado 2.3) el receptor puede detectarlas y eliminarlas fácilmente. Además, una vez el receptor está "anclado" a la señal de trayecto directo y la rastrea, estas señales retrasadas tienen muy poco efecto en el cálculo de posición. El problema aparece cuando este retraso es pequeño por el rebote en objetos cercanos o lejanos pero que llegan, del orden de, decenas o centenas de nanosegundos después, ya que afectan a la correlación de la señal original y las de referencia del receptor.

Puede deducirse que este problema viene dado en su mayoría por estructuras de gran tamaño, especialmente en las ciudades donde existen numerosas estructuras susceptibles de hacer "rebotar" la señal GPS. A colación de este problema aparece otro con un origen común, si los edificios, montañas o demás estructuras se interponen en la LOS[11] entre el satélite y el receptor tendremos un problema de *shadowing.*

El *shadowing* es una atenuación excesiva o total en el camino directo de la señal. Cuando estos dos tipos de degradación de señal se dan a la vez el efecto del camino múltiple debe ser tenido muy en cuenta (ver Figura 2-14). Porque si no es atenuado en la misma medida que la señal directa o incluso si el receptor sólo recibe señales de camino múltiple, tendremos un claro ejemplo de un cálculo de posición, que sin ser incorrecto respecto a las señales que se reciben, no se corresponden con la realidad.

La potencia tiene también mucho que ver en los errores producidos por el camino múltiple, si las señales de camino múltiple llegan al receptor con una potencia mucho menor a la de camino directo, producirán poca distorsión y por tanto errores casi despreciables. No así, si la potencia de ambas señales es similar o se diferencian escasamente.

El fenómeno del camino múltiple afecta en especial a las señales de rastreo y seguimiento, debido a que, en el caso de las señales de adquisición y datos de navegación, los efectos pueden subsanarse haciendo uso de diferentes técnicas implementadas en los receptores GPS, como comparar la potencia de las señales que le llegan y eliminar aquellas que llegan con menor potencia que otras idénticas a ellas, hecho que puede ser aprovechado para la realización de ataques de suplantación de la señal GPS.

[11] Line of Sight: Línea de visión

2.6.3 Centelleo (Scintillation)

Este tercer tipo de degradación de la señal GPS es producido por diferentes irregularidades en la ionosfera, que es la capa de la atmósfera que se encuentra entre los 80 km y los 400 km, sobre la superficie terrestre, aproximadamente. El fenómeno del *centelleo ionosférico* puede generar que un receptor GPS no sea capaz de seguir o rastrear uno o más satélites durante periodos temporales reducidos (Figura 2-15).

En esta capa de la atmósfera la radiación solar separa los elementos, normalmente de carga neutra, en iones cargados positivamente y electrones libres. Este fenómeno tiene el valor máximo de electrones libres a una altura de alrededor de 350 km sobre la superficie de la Tierra en las zonas diurnas. Y es que este fenómeno como se ha indicado previamente al depender de la radiación solar tendrá un efecto mayor en periodos diurnos que en periodos nocturnos. Por el mismo motivo puede deducirse que las zonas ecuatoriales sufren con mayor intensidad las degradaciones provocadas por el centelleo ionosférico.

La señal afectada por el centelleo ionosférico sufre principalmente un retraso temporal si se comparase con una señal idéntica sin centelleo. Sin embargo, las fluctuaciones en la densidad de electrones varían constantemente los efectos del centelleo. Es por ello por lo que es una de las degradaciones más difíciles de resolver, pues cada momento y lugar presenta unas condiciones diferentes que afectan a la señal GPS de forma distinta.

El centelleo ionosférico perturba tanto la amplitud de la señal como la fase en intervalos menores de tiempo por lo que se producen fluctuaciones de potencia de la señal.[11]

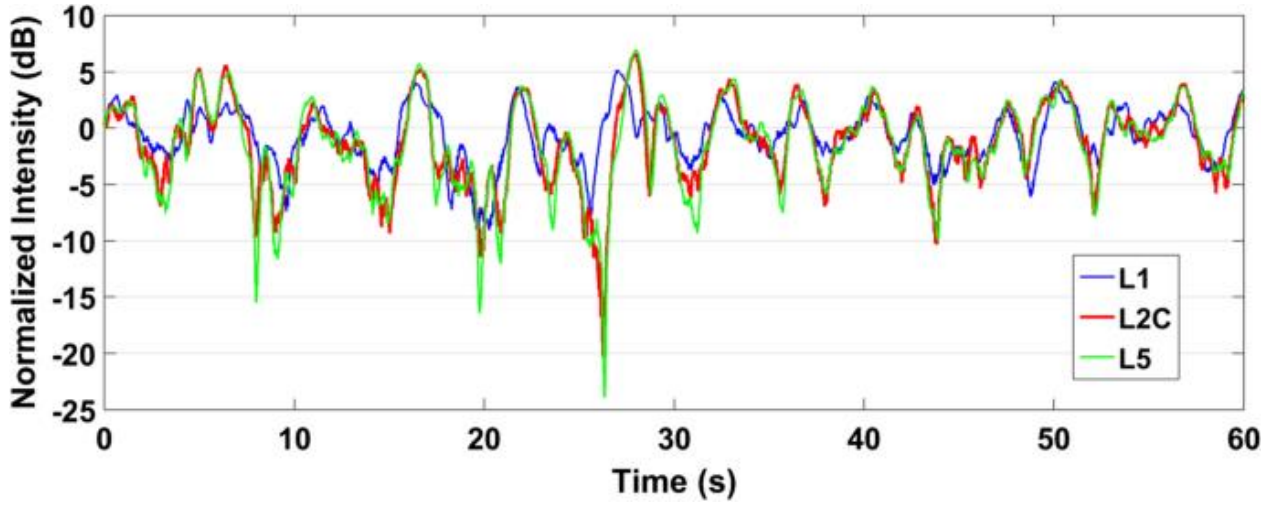

Figura 2-15 Ejemplo del efecto de centelleo ionosférico en la señal GPS. [11]

2.7 Ataques contra GPS

2.7.1 Jamming

El *jamming* GPS es una técnica de perturbación electromagnética que consiste en la emisión de una señal en la banda de frecuencia del GPS de mayor potencia con la finalidad de bloquear parcial o totalmente la recepción de la señal original. Puede simplificarse como la introducción de ruido en una determinada banda de frecuencias que evitan la recepción de la señal original. Es un método de ataque que busca la negación de uso (DoS) de una determinada parte del espectro electromagnético. Es especialmente peligro en el caso del GPS puesto que sistemas con relativa baja potencia son capaces de denegar la señal GPS en un área grande. Además, el ataque *jamming* puede ser selectivo, es decir,

quedan afectados solo los equipos que trabajen en el ancho de banda perturbado. A pesar de estar prohibida la realización de este tipo de ataques y la venta de sistemas capaces de llevarlos a cabo, la adquisición de la tecnología para poder construirlos no es difícil de adquirir. Se puede concluir que es una forma relativamente barata de negar el uso de GPS.[12]

2.7.2 Spoofing asíncrono

El *spoofing* por el contrario es una técnica de suplantación de la señal original. 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 "ancle" creyendo que es la señal GPS real. Esta técnica crea una señal distinta en pseudodistancia y en Doppler a la señal GPS original (Figura 2-16), por ello el receptor GPS la percibirá como ruido. Como consecuencia, debe interrumpirse la señal original aumentando la potencia de la señal de ataque entre 40 y 50 dB por encima de la original. En este caso el sistema que defiende al receptor del fenómeno *Multipath*, rebotes de la señal GPS, se aprovecha en beneficio del ataque de modo que el receptor se "engancha" a la señal de suplantación. La señal original llega con tan poca potencia comparada con la señal *spoofing* que el receptor la omite.[13], [14]

Este ataque es fácilmente detectable simplemente con percatarse de un salto importante de ganancia o de relación señal a ruido de la señal GPS recibida o por saltos bruscos de tiempo o coordenadas.

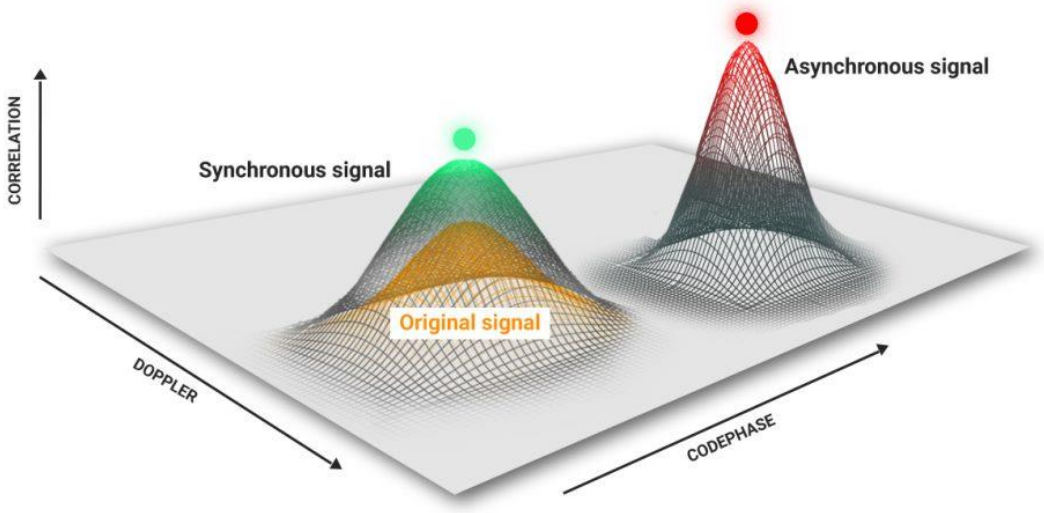

Figura 2-16 Doppler y Fase de las señales de ataques síncrono y asíncrono comparados a señal GPS real. [14]

2.7.3 Spoofing síncrono

El ataque de suplantación (*spoofing*) síncrono o coherente, es un ataque mucho más robusto que el asíncrono, principalmente porque la señal emitida es idéntica (ver Figura 2-16) a la señal GPS original en tiempo, coordenadas, Doppler y pseudodistancia. Por lo general en un escenario de ataque a GPS, partimos de que el receptor GPS víctima ya está anclado a los satélites de la constelación visible, por ello en este caso también será necesario aumentar ligeramente la potencia de la señal ataque, aunque si bien no tanto como en el ataque asíncrono.

Una vez el GPS víctima muda de la señal original a la señal ataque, el spoofer puede cambiar tiempo, distancias y, por tanto, coordenadas [15]. En este caso, la detección del ataque, si se realiza de

forma progresiva sin cambios de tiempo y distancia muy bruscos, es más complicada. Si bien si se dispone de la demora de la señal puede intuirse fácilmente que es un ataque, pues las señales de todos los satélites vendrán de una misma dirección. Problema para el atacante que puede ser subsanado mediante un ataque con transmisión múltiple desde diferentes demoras y que es el principal objetivo por alcanzar en este trabajo. Dentro de este tipo de ataques está el *meaconing*, en el que se retransmite una señal real en una posición determinada. La señal en este caso es muy robusta debido a que realmente es una señal GPS verdadera, sin embargo, el atacante no tiene apenas control sobre la posición de suplantación.

2.7.4 Spoofing multiestático

Los ataques spoofing GPS producidos por un solo emisor pueden ser fácilmente detectables si se dispone de equipos capaces de determinar la dirección de recepción de la señal de cada satélite, pues las señales de todos los satélites provendrían de la misma dirección. Este problema puede ser solventado mediante el uso de un sistema multiestático para la realización de estos ataques.

Este tipo de ataque puede ser síncrono o asíncrono, y trata de ejecutar un ataque con varios spoofers sincronizados entre sí de forma precisa para atacar de forma simultánea. Los spoofers se reparten la constelación visible y cada uno simula la señal de uno o más satélites, de esta forma el ataque llega desde varias demoras y por tanto es mucho más difícil de detectar a priori. Pudiéndose incluso diseñar un ataque más realista con una disposición de los spoofers cercana a la disposición real de la constelación visible GPS.

El principal problema del *spoofing* multiestático es que los Spoofers tienen que estar en contacto permanente para la sincronización del ataque además de ser capaces de repartirse los satélites de la constelación visible de forma autónoma o semiautónoma para mantener un ataque robusto. Este caso sólo interesaría cuando la motivación del ataque obligara a mantener el mismo sin detectar, pues es algo más costoso.

2.8 Casos de ataques mediante GPS *spoofing*

2.8.1 Spoofing en interdicción de drones

Es sin duda uno de los campos en los que más se utiliza el *spoofing* por la vulnerabilidad de los sistemas de navegación de los vehículos por control remoto. Los drones comerciales, pero también muchos militares, dependen del GPS para navegar acorde a las órdenes que le llegan desde el lugar donde se esté pilotando. Su pequeño tamaño y su asequible precio los convierte en armas fáciles de usar y de adquirir. A lo que se debe sumar la dificultad que se tiene actualmente en la detección y neutralización de amenazas de este tipo. Especialmente en bases militares o recintos de especial sensibilidad en los que su gran tamaño los convierte en muy vulnerables para ataque con drones. Países como Rusia en sus bases en Siria perturba los sistemas GNSS para evitar el vuelo de drones por encima de sus instalaciones. El problema de este tipo de ataques es que nos son selectivos, la perturbación afecta a todos los receptores que se encuentren en la zona lo que puede provocar que se vea afectado el tráfico marítimo y aéreo de la zona.[16]

La Federación Rusa ha desarrollado un gran abanico de sistemas de defensa anti-dron como expone C4ADS en [17] e instalado antenas, con capacidad de perturbar las señales GNSS, en numeroso edificios e instalaciones gubernamentales, bases militares y residencias de altos mandatarios como son las residencias gubernamentales en la costa de Crimea o edificios del gobierno en Moscú y otras capitales de Oblast rusos.

Pero no solo en cuestiones defensivas se han documentado ataques contra drones, en 2011 el gobierno iraní presumió de haber capturado una unidad del dron espía estadounidense RQ-170 que

operaba la CIA sobre la frontera entre Irán y Afganistán. Aparentemente y según [18], se usó un ataque de GPS *spoofing* contra el dron, que entró en modo autopiloto (como medida de seguridad prácticamente todos los drones tienen un modo de navegación autónomo en caso de perder la señal GPS real) pudiendo ser interceptado por los iraníes que lo hicieron aterrizar. Si bien esta información no ha sido reconocida oficialmente por los Estados Unidos de América.

2.8.2 Protección de autoridades: Puente del Estrecho de Kirch 2018

Es una de las situaciones en las que más se usa este tipo de ataques para evitar obtener la posición de personas VIP y/o inutilizar la capacidad de atentar contra ellas haciendo uso de armas de control remoto o que requieran de posicionamiento GPS.

Con motivo de la visita al puente del Estrecho de Kirch, tras su finalización, por parte del presidente de la Federación Rusa Vladimir Putin se detectaron graves interferencias en el GPS en la Península de Crimea y zonas cercanas a costa en el Mar Negro (ver Figura 2-17). Hecho que se ha vuelto habitual en las visitas sensibles que realizan los mandatarios de alto nivel de la Federación Rusa, que se ha convertido en pionera en estos ataques.

Aunque este caso, que se produjo en la inauguración del puente que unió territorio ruso con la península de Crimea, ha tenido relativa repercusión, el *think tank* C4ADS ha documentado hasta un total de 10.000 incidentes de interferencia del GPS provocados por Rusia recogidos en el estudio [17]. Aunque los incidentes recogidos terminan en 2018, podemos suponer que estos han aumentado considerablemente. Teniendo en cuenta el aumento de la tensión de Rusia con los países del bloque occidental OTAN y de los conflictos en los que está involucrado este país. Siendo uno de los países que más explota las vulnerabilidades de los sistemas GNSS en conflictos bélicos o de carácter híbrido.[19]

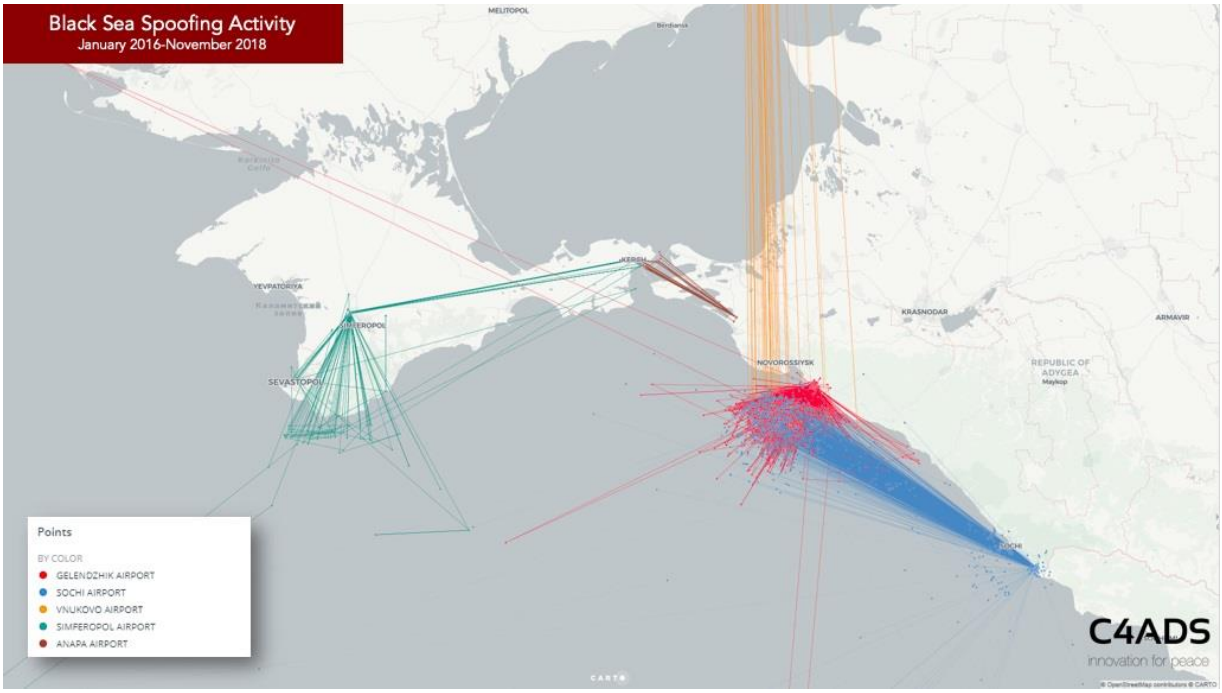

Figura 2-17 Casos documentados de *spoofing* de GPS en el Mar Negro entre enero 2016 y noviembre 2018. [17]

2.8.3 Aeropuerto internacional Ben Gurión 2019

El aeropuerto más grande de Israel y conocido también como el Aeropuerto de Tel Aviv sufrió en junio de 2019 un ataque de negación y suplantación de GPS, *Jamming* y *spoofing* que impidió a aeronaves y sistemas de control aéreo el uso de la localización GPS durante varios días, lo que supuso un impacto notable en las operaciones aéreas de este aeropuerto. Aunque, los sistemas de aproximación y rodaje en tierra dependen de otro tipo de señales y, por tanto, las aeronaves continuaron operando en el aeropuerto. No se produjeron accidentes, si bien, en el espacio aéreo circundante al aeropuerto no podía hacerse uso de sistemas GNSS.

Las autoridades israelíes acusaron de la autoría del ataque a la Federación Rusa en base a fuentes de "alto nivel" debido a la similitud entre las señales interferentes y los sistemas de guerra electrónica (EW) de los que Rusia dispone para la defensa de la base aérea Hmeimim en territorio sirio. A pesar de todo, las autoridades rusas han negado categóricamente la autoría de este ataque.[20]

2.8.4 Guerra de Ucrania 2022

Durante el conflicto tras la invasión rusa de Ucrania, han sido detectados numerosos casos de interferencias de distinto tipo en zonas concretas y relativas a este conflicto. Según la Agencia Europea de Seguridad Aérea, EASA por sus siglas en inglés, se registraron ataques al GPS en las regiones de Kaliningrado y zonas ribereñas del Mar Báltico, el Mar Negro, zonas de Finlandia fronterizas con Rusia y el Mediterráneo Oriental, en países como Egipto, Turquía, Siria, Israel, Irak, Chipre y Líbano.

Las interferencias o ataques contra el GPS en Ucrania no son nuevos de este conflicto pues se vienen reportando incidentes similares desde el comienzo de la Guerra del Donbass en 2014 que enfrentó al gobierno ucraniano con fuerzas separatistas pro-rusas, y que se intensificaron desde 2021 en la frontera ucraniano-bielorrusa hasta la invasión de Ucrania en febrero de 2022. [21], [22]

2.9 *Spoofing* en la Armada

Las Fuerzas Armadas españolas, como fuerza militar, son conscientes de la importancia de la explotación de lo que la OTAN denomina NAVWAR (Navigational Warfare), es decir, "aquellas acciones y/o medidas técnicas para asegurar la superioridad en el posicionamiento, la navegación y las señales de timing"[2]. En este campo se engloban todas las tecnologías que buscan la negación (*jamming*) o suplantación (spoofing) de la señal GPS y el resto de GNSS en general.

La OTAN y en concreto la Armada lleva varios años celebrando ejercicios de diversa intensidad en el que probar este ámbito de la guerra. El posicionamiento, la navegación y la adquisición de tiempo preciso puede ser una asimetría en el conflicto que de aprovecharse y explotarse puede suponer el cambio del curso del conflicto en un momento concreto.

Aunque los ejercicios y actores en estas maniobras son muchos, se expondrán aquellos en los que participó de alguna forma el Centro Universitario de la Defensa (CUD) de la mano de los tutores de este trabajo fin de grado.

2.9.1 MARSEC-22

La participación del CUD en los ejercicios MARSEC-22, ejercicios anuales de seguridad marítima organizados por ALMART en el escenario de ciberseguridad y NAVWAR, ponen de manifiesto la preocupación de la Armada ante este modo de hacer la guerra. Desde el 10 al 12 de mayo del año 2022 se llevaron a cabo pruebas por parte del personal del CUD con el objetivo de evaluar la eficacia de la perturbación y decepción de los sistemas GNSS, negando y suplantando la señal (Figura 2-18).

Observar las posibles consecuencias de un ataque sobre la capacidad de adquirir posición, navegación y tiempo (PNT), sobre otros equipos como las redes de comunicaciones y sistemas de enlace de datos tácticos como los sistemas LINK. Además de evaluar y analizar las medidas de mitigación ante ataques de este tipo.

Durante el desarrollo de las pruebas de *jamming* y spoofing, se realizaron ataque sobre diferentes plataformas navales y aéreas para la evaluación de los objetivos mencionados. Las víctimas de los ataques fueron: diversos buques mercantes civiles, el Buque de Acción Marítima "Furor" (P-46), el Patrullero "Formentor" (P-82) y diversas aeronaves del Ejército del Aire como el avión de transporte A400M, y aviones de caza F18 y Eurofighter.

Dada la naturaleza militar de los ejercicios , los resultados de los ataques y los análisis posteriores son materia clasificada y por tanto no se expondrán en este trabajo, si bien, se pone de manifiesto que la explotación de esta tecnología es parte en el presente y futuro de la Fuerzas Armadas y del conjunto de la OTAN.

Figura 2-18 Disposición sistema spoofer en los ejercicios MARSEC-22 en la Batería de la Parajola (Cartagena).[23]

2.9.2 NEMO-22

Los ejercicios NEMO (*Naval Electro-Magnetic Operations)* son unas maniobras OTAN que buscan optimizar la interoperabilidad de las fuerzas aliadas en escenarios de gran complejidad en el ámbito electromagnético. Se llevaron a cabo en aguas de la Bahía de Cádiz y fueron lideradas por España a través de COMANDES-31 del 31 de octubre al 4 de noviembre de 2022. El conjunto de estas maniobras permite avanzar en diversas líneas de investigación con actores civiles, militares y de la esfera de la industria de defensa. Además, tienen como objetivo evaluar la eficacia y validar las tácticas y técnicas de guerra electrónica de la OTAN utilizadas en la defensa antimisiles.

Las unidades participantes (Figura 2-19) fueron: el Buque de Aprovisionamiento de Combate Cantabria (A-15), la Fragata "Blas de Lezo" (F-103), la Fragata "Méndez Núñez" (F-104), la Fragata "Canarias" (F-86) y el Destructor "Andrea Doria" (D-553) de la Marina Militiare de la República Italiana. En un escenario combinado de ataques de *jamming* y spoofing.

Las conclusiones y propuestas del CUD señalan el valor de este nuevo campo de la guerra electrónica y manifiestan la importancia de tener equipos probados y resilientes lo máximo posible a este tipo de ataques. Además, señala que este, es un ámbito de la guerra en dos sentidos, esto es,

ofensivo y defensivo y que tiene un gran potencial en la defensa antiaérea con la posibilidad futura de desviar sistemas de armas cuyo guiado dependa se sistemas GNSS.[23]

Figura 2-19 Formación de unidades participantes en las maniobras de la OTAN NEMO-22. [24]

2.9.3 Ejercicios futuros

Durante el año 2023 la Armada realizará diversos ejercicios en los que la NAVWAR toma de nuevo relevancia y en concreto los ataques contra señales GNSS. Se prevé la participación del Centro Universitario de la Defensa en los ejercicios MARSEC-23, entorno probado para la realización de ataques de este tipo en un escenario de amplia cooperación entre instituciones relativas a la seguridad marítima en situaciones de crisis.

También se espera su participación en los ejercicios MINEX-23, un ejercicio de carácter multinacional en el ámbito de la guerra de minas organizados por la Armada en aguas del Mediterráneo anualmente. La edición de este año cuenta entre otras con las 6 unidades de la 1ª Escuadrilla de Medidas Contra Minas: los cazaminas “Segura” (M-31), “Sella” (M-32), “Tambre” (M-33), “Turia”, (M-34), “Duero” (M-35) y “Tajo” (M-36).

2.10 SDR: Software Defined Radio

La radio definida por software (SDR) es un conjunto de sistemas con los que la manipulación de señales radio, que tradicionalmente se ha realizado mediante elementos de hardware como filtros, moduladores, mezcladores, son realizadas mediante software.

El principio del SDR es el de sustituir la mayor parte posible de elementos físicos por esquemas de codificación y dispositivos programables que mediante convertidores de señal analógica-digital y viceversa disminuyan el tamaño de los sistemas de radio. Esto ha permitido por ejemplo que los teléfonos móviles sean capaces de recibir señales de radio y datos con tamaños difícilmente imaginables hace unos años.

Los receptores SDR están compuestos por dos módulos principalmente, el primero es un *Analog-to-Digital converter (ADC)*/ *Digital-to-Analog converter (DAC)* conectado a una antena que se encarga de convertir la señal analógica en digital en el caso de la recepción y al contrario en el caso de la transmisión. El segundo módulo, es el *Digital Signal Processor (DSP)* que extrae la información contenida en la señal analógica.[25]

2.11 LoRa

LoRa es el acrónimo de *Long Range*, y es la modulación de señales inalámbricas para lograr un gran alcance con baja potencia. Fue patentada por la empresa Semtech en el año 2012.

La técnica de modulación que utiliza LoRa es una combinación de el *Frecuency Shifting Keying (FSK)* o espectro ensanchado y una variación del espectro chirp extendido o *Chirp Spread Spectrum (CSS)*. Utiliza técnicas de corrección de errores como la *Forward Error Correction (FEC)* y las frecuencias y anchos de banda abiertos en las diferentes regiones denominados ISM (Industrial Scientific Medical), siendo en Europa la frecuencia 868 MHz. Al tratarse de una señal en banda ancha permite tener una mejor relación señal a ruido (SNR).[26]

Las transmisiones LoRa disponen de velocidad de transmisión variables pudiendo ajustar velocidad en detrimento de alcance y potencia. Actualmente es una tecnología ampliamente utilizada en el "*internet de las cosas"* (IoT).

2.12 NMEA

La National Marine Electronics Association (NMEA) desarrolló una interfaz entre distintos equipos electrónicos relacionados con la navegación y que permite aglutinar los datos de GPS, sondadores, navegadores inerciales, datos de viento, oleaje, etc. Y presentarlos en conjunto en cartas electrónicas o equipos de ayuda a la navegación. Los receptores GPS disponen del protocolo ASCII que es conocido como NMEA, por ser esta la organización que llevó a cabo su desarrollo. Cada bloque de datos se denomina sentencia y se presenta de forma independiente. En lo que ocupa este trabajo, son las sentencias GPS las que interesan. Este protocolo agrupa en diferentes sentencia o líneas de texto la información que el receptor GPS recibe del segmento espacial.[27]

Todas las sentencias de NMEA empiezan con el signo "$" y a continuación dos letras que identifican el sistema GNSS del que reciben los datos, en el caso del GPS son las letras "GP", a las que siguen tres letras que identifican la sentencia en sí y la información que contienen. La longitud máxima de las sentencias NMEA es de 80 caracteres de texto más los caracteres de finalización de sentencia que identifican el final de esta.

Tabla 2-2 Sentencias NMEA GPS [Elaboración Propia]

Sentencia NMEA	Significado
GPGGA	Correcciones de tiempo, posición y tipo de datos del sistema.
GPGLL	Posición geográfica, latitud y longitud.
GPVTG	Rumbo y velocidad sobre verdaderos.
GPRMC	Hora, fecha, posición, rumbo y velocidad verdaderos.
GPGSA	Modo de operación del receptor GPS, satélites usados en el cálculo de posición y valores Doppler.
GPGSV	Número de satélites a la vista y sus números de identificación, elevación, acimut y números del código PRN. (ver Tabla 2-1)
GPMSS	Relación señal a ruido, intensidad de la señal, frecuencia y velocidad de bit de baliza MSS.
GPTRF	Corrección de errores de tránsito.
GPSTN	Datos de identificación múltiple.
GPXTE	Medición del error en el cálculo de la trilateración.
GPZDA	Fecha y hora del PPS.

3 DESARROLLO DEL TFG

El escenario del ataque que se pretende realizar está compuesto por dos nodos de ataque separados entre sí que ejecutan a la vez un ataque asíncrono de suplantación de señales GPS sobre un receptor GPS víctima situado entre ambos nodos. Se plantea este escenario para localizaciones cercanas a costa o pasos angostos como pueden ser rías y estrechos.

En el desarrollo del proyecto se parte de la capacidad ya obtenida de perturbar mediante *spoofing* no coherente o asíncrono haciendo uso de un solo nodo. Como el objetivo es implementar esa capacidad en varios nodos, se deben comunicar estos nodos de ataque, que se repartan de forma autónoma, o a elección del operador, la constelación de satélites visibles y deben ser capaces de realizar un ataque coordinado.

Para esto deben hacerse una serie de consideraciones iniciales y dividir los diferentes problemas a resolver en módulos de trabajo independientes que serán analizados por separado y validados para su integración en el montaje o sistema final.

Los bloques de trabajo en los que se divide el proyecto son:

1. Capacidad de spoofing (spoofer).
2. Comunicación entre los nodos de ataque.
3. Recepción y lectura de datos GPS.
4. Preparación y envío de mensajes
5. División de constelación visible.
6. Coordinación de ataque.

Además, el proyecto requiere de numerosos recursos tanto hardware como software que serán reseñados brevemente en este apartado.

3.1 Enfoque inicial

El planteamiento inicial del proyecto en cuanto a hardware (ver Figura 3-1) es el de un sistema compuesto por dos nodos de ataque, ya que, de poder demostrar el correcto funcionamiento con dos nodos, podría implementarse en un número mayor. Estos dos nodos tendrían diferentes funciones dentro del ataque, uno de ellos actuaría como *Master (Nodo de Ataque Maestro, NAM)* y el otro como *Slave (Nodo de Ataque Esclavo, NAS)*, en el hipotético caso de añadir más nodos, estos nodos adicionales, tendrían la función *NAS.* Cada uno de ellos debe recibir la señal GPS real, por varios motivos:

- Sincronización del tiempo precisa.
- Obtener su propia posición.

- Obtener posición de la constelación visible de satélites.

Además, cada nodo debe estar conectado a un módulo de comunicación LoRa que permita la comunicación con los demás nodos. Por otra parte, también deberá haber un módulo SDR en cada nodo de ataque para sintetizar y transmitir la señal GPS falsa (*spoofing*) generada por el procesador (una Raspberry Pi) en el caso de un nodo de ataque de tipo *Slave* o del ordenador en el caso del *Master*.

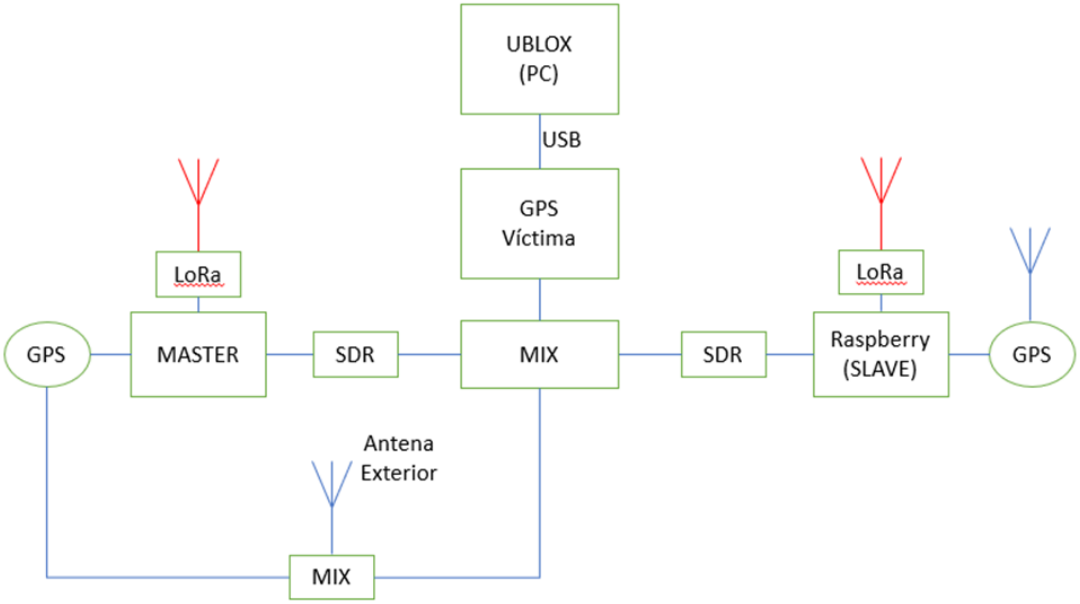

Figura 3-1 Esquema montaje. [Elaboración Propia]

El montaje para la prueba de laboratorio evita la radiación de señales GPS al aire, pues está prohibido, sustituyendo el medio radioeléctrico por un cable con atenuación para simular condiciones parecidas a las de propagación en espacio libre. Por tanto, el GPS víctima recibirá la señal GPS real de una antena exterior, y las señales *spoofing* de ambos nodos de ataque por cable (Figura 3-1). Mediante un combinador se simulará que el GPS víctima recibe todas las señales y podrá observarse el modo en que reacciona, es decir, si se ancla a la señal falsa o por el contrario mantiene el anclaje a la señal verdadera.

3.2 Hardware

3.2.1 Módulo LoRa

El hardware para la comunicación entre nodos está compuesto por módulos de Arduino con shields LoRa Dragino (Figura 3-2). Estos shields permiten comunicación a largas de distancias con baja velocidad de transmisión de datos y un mínimo consumo de corriente. Trabaja, como se indica en el apartado 2.11, en la frecuencia 868 MHz en Europa.

Tinen una sensibilidad de -148 dBm y permite, comunicaciones robustas y de gran alcance.

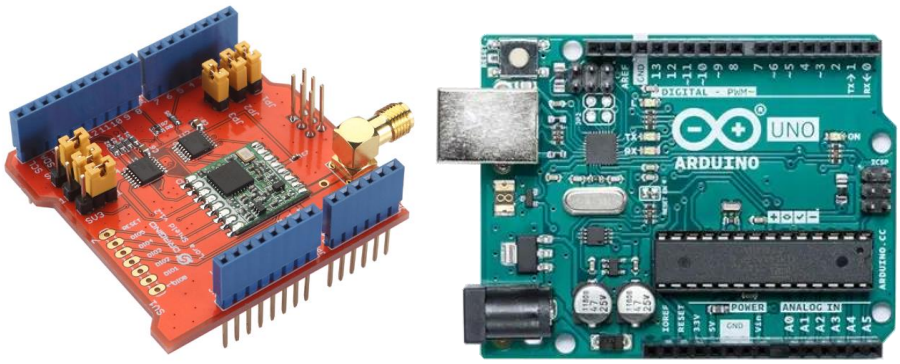

Figura 3-2 Shield LoRa Dragino [28] y placa Arduino Uno [29]

El shield LoRa se acopla a una placa Arduino Uno que se comunican mediante un protocolo de comunicación serie y una librería especifica de LoRa. También se encarga, mediante otra comunicación serie (en este caso un cable USB), de enviar los datos recibidos al ordenador o Raspberry.

3.2.2 Raspberry PI

La Raspberry Pi utilizada inicialmente para ejercer de NAS, es la Raspberry 3B+ (Figura 3-3), que es un ordenador de una sola placa con conexión bluetooth y LAN inalámbrica, dispone de 4 puertos USB, un puerto HDMI y uno de Ethernet. La alimentación de 2,1 A se produce mediante un puerto micro-USB y la memoria principal y el sistema operativo se encuentran en una tarjeta SD. Se instala el sistema operativo Raspberry Pi SO de 32 bits en una tarjeta de microSD de 16 GB.

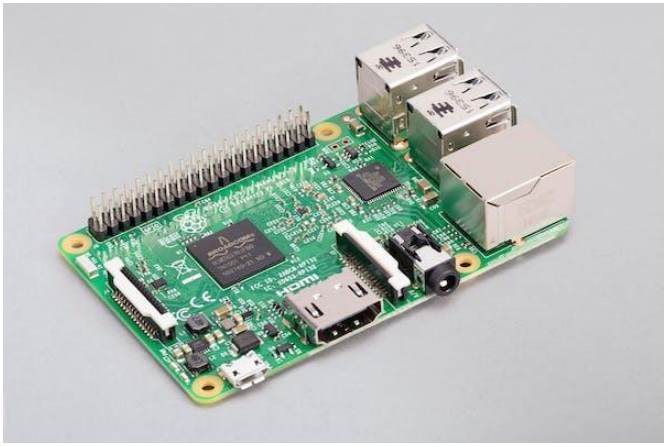

Figura 3-3 Raspberry Pi 3B+. [30]

Cuenta con una CPU Quad Core de 1.2 GHz Broadcom de 64 bits y una memoria RAM de 1 GB, dispone de conexión LAN, bluetooth de baja energía y una velocidad Ethernet de 100 Mbit por segundo.

Durante una fase de pruebas previas a las pruebas definitivas se hace evidente que la Raspberry Pi 3B+ utilizada durante todo el proceso de investigación y desarrollo no es capaz de procesar los programas requeridos en tiempo real lo que supone un criterio “NO-GO” claro. Se muda por tanto todo el sistema desarrollado a una Raspberry Pi 4 (Figura 3-4) de características físicas parecidas, pero con mayor capacidad de procesamiento y 4 GB de RAM.

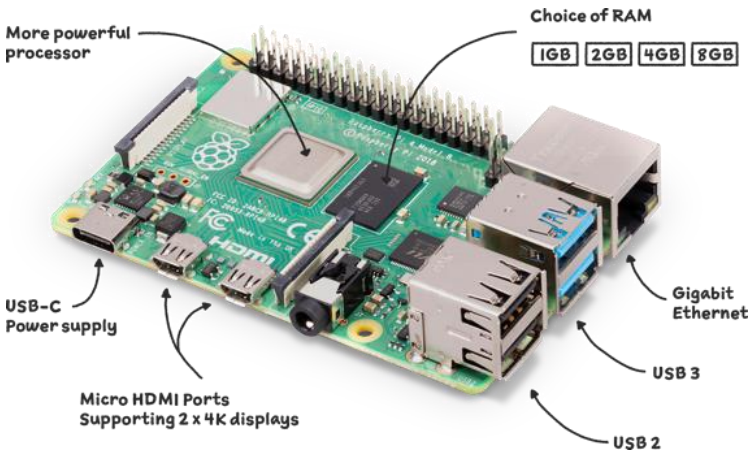

Figura 3-4 Raspberry Pi 4. [31]

Las especificaciones técnicas de la Raspberry Pi 4 utilizada son las siguientes:

El procesador es un Broadcom BCM2711, Quad Core Cortex-A72 (ARM v8) de 64-bit y 1.5GHz. Cuenta con una memoria RAM de 4 GB LPDDR4-3200 SDRAM, dos conexiones de USB 3.0 y otras dos de USB 2.0 además de dos conexiones HDMI y una fuente de alimentación tipo C de 2,5 A.

3.2.3 SDR

Debido a la disponibilidad de equipos, los módulos de radio definida por software del NAM y el NAS son distintos, hecho que hay que tener en cuenta pues el valor de ciertos parámetros de configuración no son los mismos. Es el caso de la tasa de muestreo. El NAM cuenta con el sistema USRP N200 cuya tasa de muestreo es de 16 bits. El NAS utiliza una SDR HackRF con una tasa de muestreo de 8 bits (Figura 3-5).

Figura 3-5 SDR HackRF (izquierda) y SDR USRP N200 (derecha). [Elaboración Propia]

3.2.4 GPS

Los módulos receptores GPS que se utilizan deben ser un mínimo de tres, uno por cada nodo de ataque y uno que ejerza de GPS víctima. Es la herramienta que permite leer esos datos transmitidos por los satélites y que calcula la posición cuando, como se ha mencionado anteriormente, recibe señales de un mínimo de cuatro satélites de la constelación GPS.

Los receptores GPS que se usan en el presente trabajo son dos módulos GPS modelo 6M UBlox (Figura 3-6), uno conectado a través de una plataforma Arduino al NAM y otro que actúa como GPS víctima. El tercer módulo GPS es el modelo 7M de UBlox y está conectado al NAS. Se ha elegido este

último para el NAS debido a que permite una conexión USB directa lo que simplifica la conexión y la programación del código.

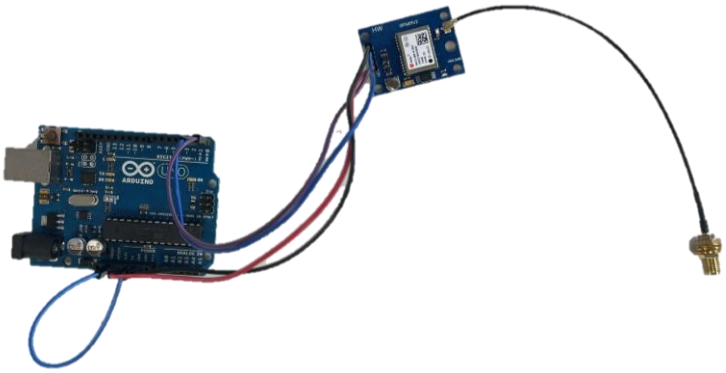

Figura 3-6 Módulo GPS 6M UBlox con Arduino. [Elaboración Propia]

3.2.5 Montaje

Así pues, los componentes que forman el NAS (ver Figura 3-7) son: la Raspberry Pi 4 que ejerce de "cerebro" del nodo de ataque y a ella están conectados mediante puertos serie USB los tres módulos periféricos del NAS, el módulo de comunicación LoRa que permite la recepción de órdenes por parte del NAM y transmisión al propio NAM de los datos de posición que requiera. Conexión que está representada por el color azul en la Figura 3-7. El módulo receptor GPS, de color amarillo y que permite posicionarse al NAS para poder comunicar su posición. Y el módulo SDR para la transmisión de la señal spoofer en color rojo.

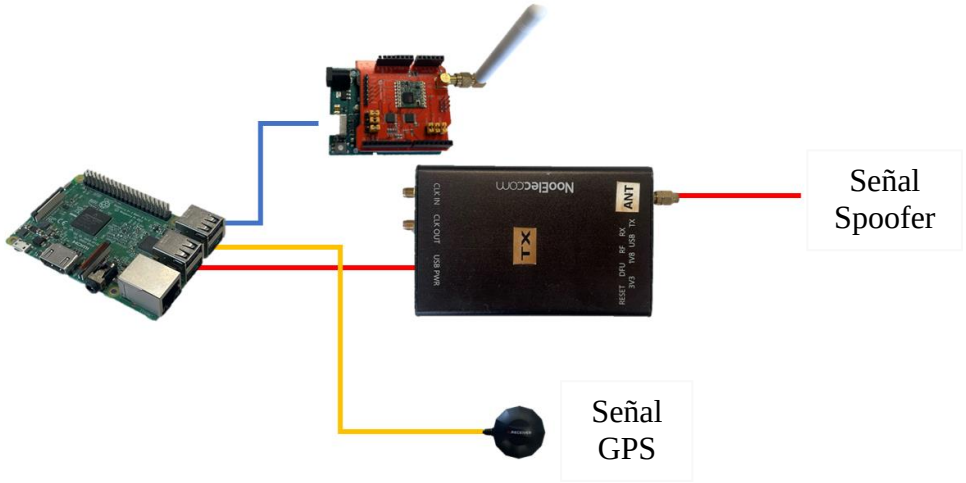

Figura 3-7 Esquema montaje del NAS. [Elaboración Propia]

De igual modo el montaje del NAM (Figura 3-8) es bastante parecido pues ambos dos nodos de ataque están compuestos por los mismos módulos. En este caso el trabajo de la Raspberry Pi es realizado por un ordenador que permite interactuar con el programa e introducir los comandos que se requieran. El módulo LoRa del mismo tipo que transmite las órdenes al NAS, los parámetros de configuración para el ataque y por el que se recibe la posición del NAS cuando esta es requerida por el usuario. El módulo GPS, en este caso diferente al del NAS, se trata del modelo de Arduino, pero cuya

misión es, eminentemente, idéntica y por último el módulo SDR, el modelo USRP N200 de Ettus Research que transmite la señal spoofer del NAM.

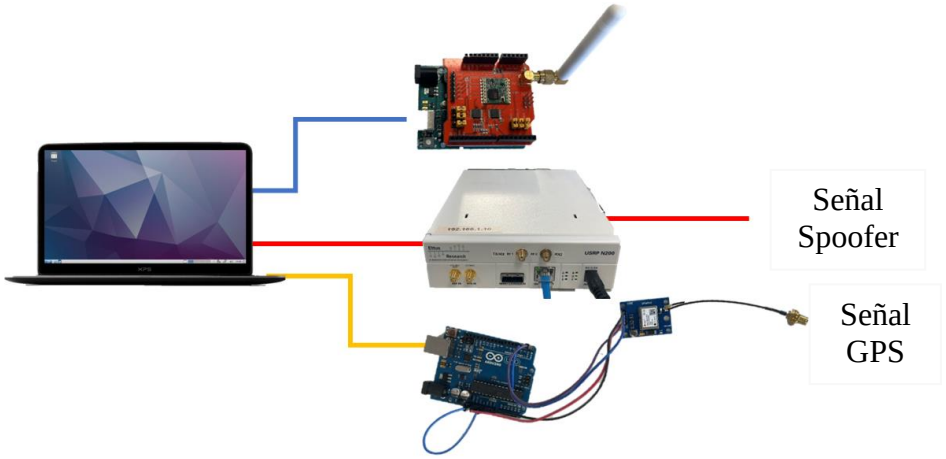

Figura 3-8 Esquema montaje NAM. [Elaboración Propia]

Debido a la prohibición de radiar señales spoofer contra el sistema GPS, el montaje debe hacerse sustituyendo esa radiación por conexiones alámbricas que quedan representadas en la Figura 3-9. Puede observarse siguiendo el código de colores que la señal GPS verdadera es compartida entre el NAM y el receptor víctima, que no es más que un ordenador con un módulo de recepción GPS. Debe combinarse esa señal GPS real que llega a la víctima con las dos señales spoofer provenientes de ambos nodos de ataque, NAM y NAS en color rojo.

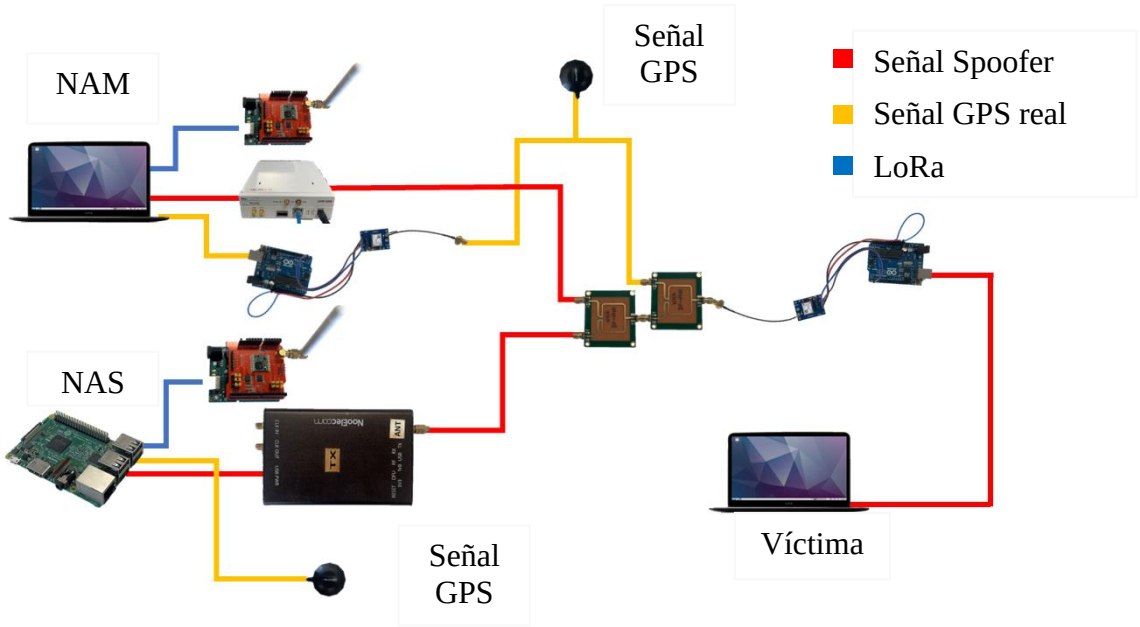

Figura 3-9 Esquema general del montaje. [Elaboración Propia]

3.3 Software

3.3.1 U-BLOX u-center

Este programa desarrollado por UBlox, una de las empresas más importantes a nivel mundial de desarrollo de módulos receptores de GNSS, es una interfaz de presentación visual de los datos GPS y otros sistemas GNSS y parámetros de las señales de estos sistemas. Permite entre otras muchas prestaciones conocer la relación señal a ruido de la señal de cada satélite que recibe el receptor GPS, si se usa o no para el cálculo de posición y la posición acimutal de cada satélite respecto al receptor GPS. Permite por tanto conocer de una forma visual y analítica la realidad GPS de cada momento en tiempo real.

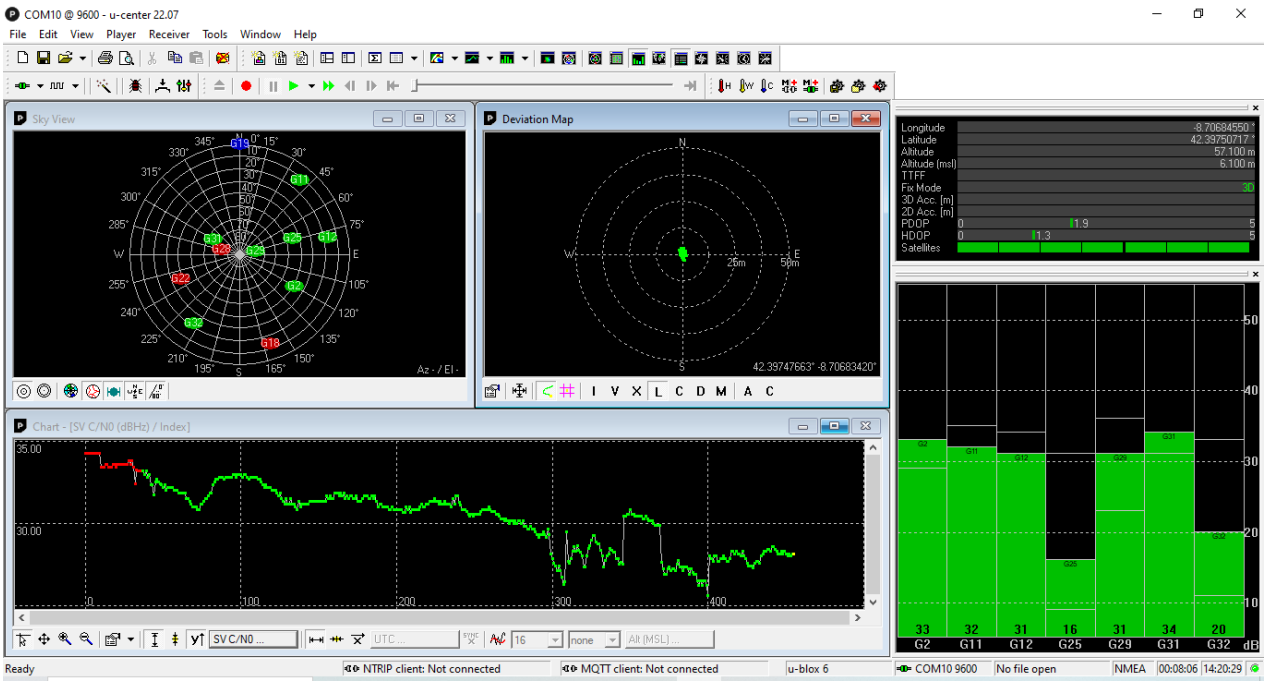

Figura 3-10 Pantalla u-blox con datos GPS 13/02/2023 a 14:22 UTC. [Elaboración Propia]

El interfaz de usuario es configurable con diferentes herramientas que permiten observar la variación de distintos parámetros, satélites a la vista, satélites usados para el cálculo de posición, relación señal a ruido, potencia recibida de cada satélite, etc.

En la configuración están, de izquierda a derecha y de arriba abajo en la Figura 3-10, el *Sky View*, que permite visualizar acimut y elevación de los diferentes satélites con un código de colores en el que verde significa que la señal es útil para el cálculo de posición. El azul, que significa que la señal llega con claridad, pero no está siendo usado para el cálculo de la posición y finalmente el rojo que indica que la señal no llega con la suficiente potencia o directamente que no se está recibiendo. La siguiente herramienta es el *Deviation Map*, que es útil para llevar el registro de posiciones calculadas por el receptor GPS y que permite comprobar que, efectivamente se ha realizado un ataque *spoofing* con éxito. La tercera herramienta es la presentación de la información general de la señal, posición y satélites que están siendo usados.

En la mitad inferior de la Figura 3-10 se posiciona la *Chart* con la relación señal a ruido global que permite comparar la diferencia de potencia entre la señal real y la señal *spoofing*. Y a la derecha la relación señal a ruido de la señal de cada satélite por separado.

3.3.2 Spyder (Python)

Spyder es un entorno de programación en código Python de fuente abierta orientado al ámbito científico, de la ingeniería y análisis de datos. Es el entorno del que se hace uso en este proyecto para la creación de los programas instalados en ambos nodos de ataque.

Es un entorno de programación sencillo que presenta el editor de código a la izquierda y la consola abajo a la derecha (ver Figura 3-11), donde también se tiene acceso al historial de dicha consola y al símbolo del sistema, para comprobar el funcionamiento del código que se desarrolla en el editor.

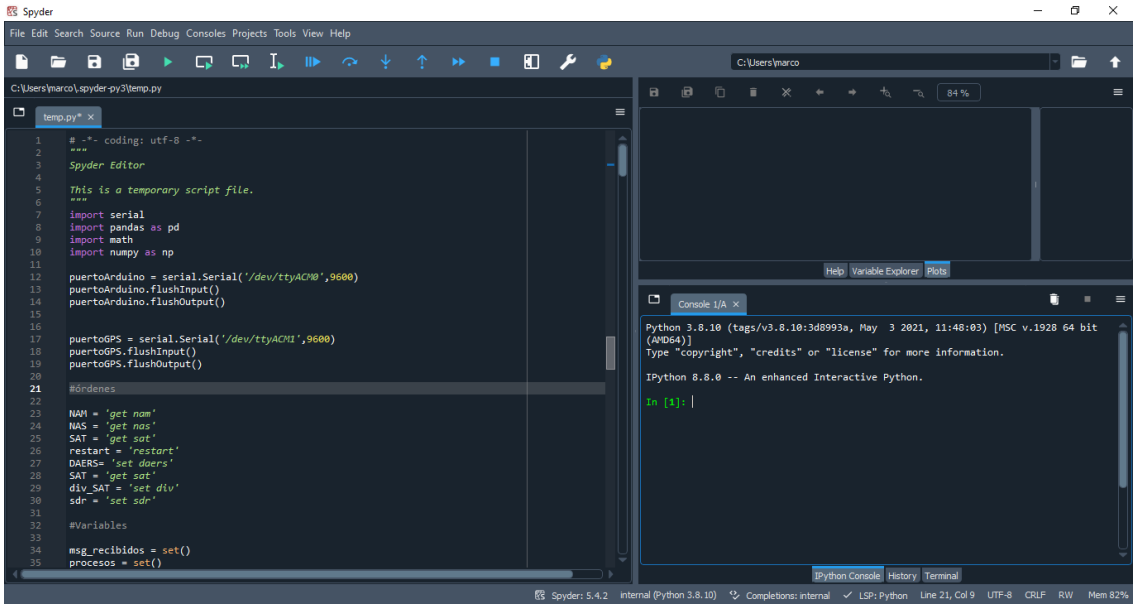

Figura 3-11 Presentación programa Spyder. [Elaboración Propia]

3.4 *Spoofing*

El *spoofing* en sí mismo se divide en dos etapas, la primera en la que se genera la señal GPS falsa y una segunda en la que se transmite esta señal mediante el módulo SDR.

3.4.1 Generación de señal spoofer

El programa empleado para la generación de los datos de la señal *spoofer* es el *gps-sdr-sim*. Este programa necesita acceso a los archivos de efemérides de los satélites que la NASA del gobierno de los Estados Unidos sube a internet diariamente a [32]. Las efemérides son usadas por este programa para sintetizar la señal falsa con las pseudodistancias y los Doppler de los satélites visibles en el momento del ataque. Esta señal que se genera corresponde a esa señal transmitida en la frecuencia L1 (1575,42 MHz) que permite el posicionamiento y es usada por todos los receptores GPS.

Existen ciertos parámetros que son necesarios para la creación de la señal Spoofer, que deben ser valorizados al introducir el comando de ejecución en el símbolo de sistema. Cuando se ejecuta el comando "*help*" del programa se despliega el siguiente texto exponiendo dichos parámetros.

```
gps-sdr-sim [options]
options:
  -e <gps_nav>     RINEX navigation file for GPS ephemerides (required)
  -u <user_motion> User motion file (dynamic mode)
  -g <nmea_gga>    NMEA GGA stream (dynamic mode)
  -c <location>    ECEF X,Y,Z in meters (static mode) e.g.
  -l <location>    Lat,Lon,Hgt (static mode) e.g., 30.286452,120.032669,100
  -t <date,time>   Scenario start time YYYY/MM/DD,hh:mm:ss
  -T <date,time>   Overwrite TOC and TOE to scenario start time
```

```
-d <duration>    Duration [sec] (static mode max: 86400)
-o <output>      I/Q sampling data file (default: gpssim.bin)
-s <frequency>   Sampling frequency [Hz] (default: 2600000)
-b <iq_bits>     I/Q data format [1/8/16] (default: 16)
-i               Disable ionospheric delay for spacecraft scenario
-v               Show details about simulated channels
```

Sin embargo, en lo que compete a este trabajo, los parámetros que deben ser especificados son: el archivo de efemérides (-e), la posición en latitud, longitud y altura para el ataque (-l), el momento concreto del ataque (-t), los satélites a suplantar por la señal (-x), la duración del ataque (-d) y el formato en bits de los datos de fase y amplitud (-b).

Gps-sdr-sim genera un archivo binario de la señal en banda base de Spoofer que es convertida a radiofrecuencia mediante SDR. En la infraestructura de este sistema de *spoofing* Multi-Nodal, el programa de generación de señal g*ps-sdr-sim*, debe ser instalado en todos los nodos que lo compongan. Además, para poder realizar ataques en tiempo real, se utilizarán *pipes* de Linux.

3.4.2 Radiación de señal Spoofer

La emisión de la señal generada por el programa *gps-sdr-sim* se lleva a cabo por dos programas diferentes debido a que los equipos SDR disponibles son de marcas diferentes que requieren sus propios programas. Sin embargo, el funcionamiento es, eminentemente, el mismo. Estos programas codifican esa señal generada en código binario, la convierten a radiofrecuencia y la transmiten de acuerdo con una serie de parámetros configurables que son: la frecuencia de transmisión que, evidentemente, debe coincidir con la frecuencia L1 del GPS de 1575,42 MHz, la frecuencia de muestreo que debe ser igual a la frecuencia de muestreo de la generación de la señal y que en el caso del HackRF es de 2600000 Hz y el del USRP N200 es de 2500000 Hz. Además, permite activar una amplificación de la señal en aproximadamente 15 dB y seleccionar un valor de ganancia.

Los equipos encargados de las emisiones del NAM y del NAS son respectivamente el USRP N200 y el HackRF, que utilizan sus softwares asociados.

3.5 Comunicación entre nodos de ataque

La comunicación entre los nodos de ataque como se ha indicado previamente se realiza mediante radioseñales LoRa a 868 MHz. Tanto el NAM como el NAS disponen de un módulo compuesto por una placa de Arduino con un shield LoRa que será el encargado de la comunicación entre ambos. Es de importancia que la velocidad o tasa de transmisión y recepción de los nodos sea igual en ambos, por ello se escoge el estándar de 9600 baudios o bits por segundo.

3.5.1 Protocolo de comunicación

Al tratarse de un sistema remoto, debe crearse un protocolo que permita la comunicación entre nodos de forma sencilla (Tabla 3-1). Realmente los comandos u órdenes que deben intercambiarse son pocas y pueden ser divididas en tres grupos:

- Órdenes de solicitud de datos.
- Órdenes de ejecución.
- Órdenes misceláneas.

Las primeras son aquellas que, desde el NAM, solicitan al NAS datos de posición y estado o datos del propio NAM. Las órdenes de ejecución permiten realizar acciones y programar los ataques con

diversos parámetros como satélites a suplantar u hora de ejecución de los ataques. Las órdenes misceláneas son las encargadas de ejecutar operaciones ajenas a los ataques *spoofing* como puede ser reiniciar la Raspberry de forma remota.

Tabla 3-1 Protocolo comunicación Nodos de Ataque. [Elaboración Propia]

Tipo	**Orden**	**Objeto**
Solicitud	get nas	Obtener posición NAS
Solicitud	get nam	Obtener posición NAM
Solicitud	get sat	Obtener datos de satélites.
Ejecución	set daers	Realizar la DAERS[12]
Ejecución	set div	Repartir los satélites en los sectores.
Miscelánea	restart	Reiniciar el NAS
Ejecución	set sdr	Configurar parámetros de la señal Spoofer

Las órdenes que tengan como objetivo la interactuación de ambos nodos de ataque ya sea por requerimiento del NAM de datos del NAS o para la configuración de los parámetros del ataque o ejecución de este, ejecutarán el envío de un código binario por parte del NAM que el NAS reconocerá y realizará las tareas que corresponda (Tabla 3-2).

Tabla 3-2 Códigos interactuación NAM-NAS. [Elaboración Propia]

Orden	**Código**
get nas	‘111’
set sdr	‘333’
restart	‘777’

3.6 Recepción y lectura de datos GPS

3.6.1 NMEA GPRMC

Como se ha visto en el apartado 2.12, esta sentencia NMEA proporciona fecha, hora, latitud y longitud. Se selecciona pues esta sentencia como referencia de tiempo y posición. Para hacer la selección y que se obvien el resto de las sentencias que no son de utilidad para el programa que ocupa, se introduce en el código del programa el siguiente comando:

[12] División Acimutal del Espacio y Reparto Satelital

```
if nmea_sentence.startswith(b'$GNRMC'):
```

A continuación, un ejemplo de una sentencia NMEA GPRMC.

$GPRMC, 114615.000, A, 4027.7896, N, 00338.6130, W, 0.13, 309.62, 110223,·, *10

A leer cada posición entre comas (‘,’):

1. Hora (hhmmss. milésimas de segundo),
2. Conexión (A sí, V no).
3. Latitud.
4. N o S.
5. Longitud.
6. W o E.
7. Velocidad verdadera.
8. Rumbo verdadero.
9. Fecha (ddmmyy).
10. Declinación magnética.
11. Modo.
12. * Cheksum.

En caso de no obtener alguno de los datos o parámetros de la sentencia en la posición en la que debe ocupar aparecen las comas juntas (“,,”).

3.6.2 NMEA GPGSV

La sentencia NMEA GPGSV proporciona información de los satélites a la vista, elevación, acimut y si están siendo seguidos por el receptor GPS y usados por tanto para el cálculo de la posición. Los datos recogidos en esta sentencia son de vital importancia para el problema que ocupa este proyecto. Principalmente porque debe conocerse el acimut de cada satélite al GPS Víctima o al menos un acimut aproximado al punto medio PM (ver apartado 3.8.2) para realizar una división de la constelación visible real. También es importante la elevación para descartar satélites que en situaciones normales serían descartado por el propio receptor. A continuación, un ejemplo de sentencia GPGSV y la lectura de cada término.[20]

$GPGSV,3,2,12,04,05,141,35,03,15,260,00,08,01,088,00,14,02,252,00*74

1. Número total de mensajes GPGSV
2. Número de mensaje
3. Satélites a la vista
4. Identificación del PRN del satélite.
5. Elevación del satélite (hasta 90º)
6. Acimut del satélite (0-360º)
7. SNR (0 si no se está realizando seguimiento ni usándose para el cálculo de posición)

- 8-11 Información del segundo satélite. (Igual que del 4-7).
- 12-15 Información del tercer satélite. (Igual que del 4-7).
- 16-19 Información del cuarto satélite. (Igual que del 4-7).

El presente ejemplo en su posición ‘1’ y ‘2’ indica que son 3 los mensajes que completan la información de toda la constelación visible y que éste es el segundo de ellos. Los satélites visibles expuestos en esta sentencia son: 04, 03, 08 y 14 con sus respectivas elevaciones, acimuts y valores de la relación señal a ruido (SNR).

Para su selección por parte del programa se usa el mismo comando que en el apartado 3.6.1:

```
if nmea_sentence.startswith(b'$GPGSV'):
```

3.7 Preparación y envío de mensajes

Cuando la Raspberry Pi, que actúa como NAS, realiza la lectura de datos GPS y encuentra la sentencia NMEA GPRMC, como se ha visto en el apartado 3.6.1, no es necesario tratarla en la propia Raspberry y se envía directamente al NAM mediante el siguiente comando:

```
puertoArduino.write(nmea_sentence)
```

Siendo `puertoArduino` la denominación del puerto donde esté conectado el Arduino con el *shield* LoRa, que funciona como transmisor y receptor de datos. Y `nmea_sentence` que es la variable donde se guarda la sentencia NMEA correspondiente. Es en el NAM donde se extraen los datos necesarios de la sentencia NMEA y se guardan en las variables correspondientes.

3.8 División de constelación visible

Para la división de la constelación visible se plantea un sistema sencillo al que se nombra División Acimutal del Espacio y Reparto Satelital (DAERS). Por el cual cada NAS, tras hacer lectura de los mensajes de posición GPS, reporta su posición al NAM. Se realiza el cálculo de tres conceptos para la división de la constelación visible (ver Figura 3-12).

- **PM:** Punto medio. Es el punto que 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. Es la línea de demora o acimut del nodo correspondiente partiendo del punto medio.

- **LDC:** Línea división de constelación. Es la 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 a dos de nodos en el sistema.

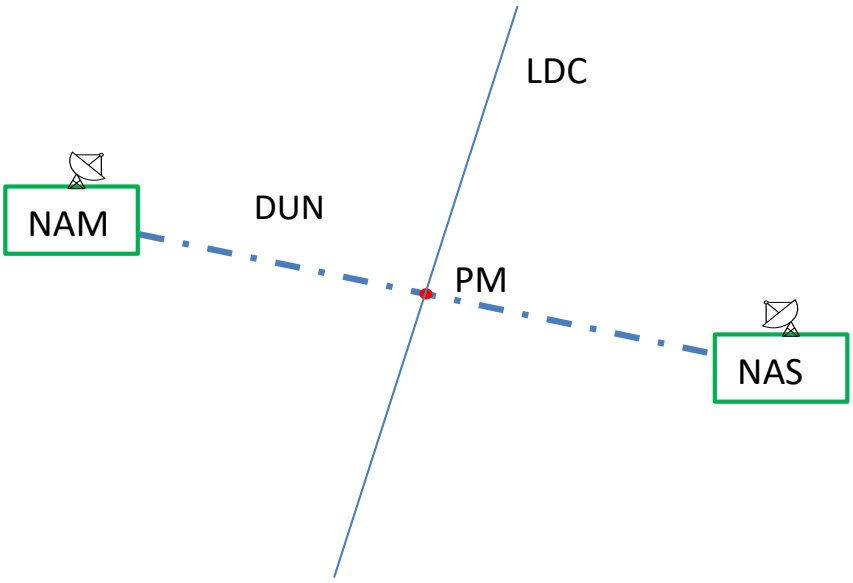

Figura 3-12 Esquema cálculo DAERS. [Elaboración Propia]

Aunque se trata de un sistema en dos dimensiones, realmente para dividir la constelación visible de satélites GPS, no se necesita la altura en ningún momento. El sistema de cálculo de la división simplemente calcula la demora verdadera desde el punto medio PM hasta cada uno de los satélites visibles. Conocida las líneas de división LDC cada nodo de ataque asumirá la responsabilidad de los satélites de su mitad de bóveda celeste a la hora de llevar a cabo el ataque (Figura 3-13).

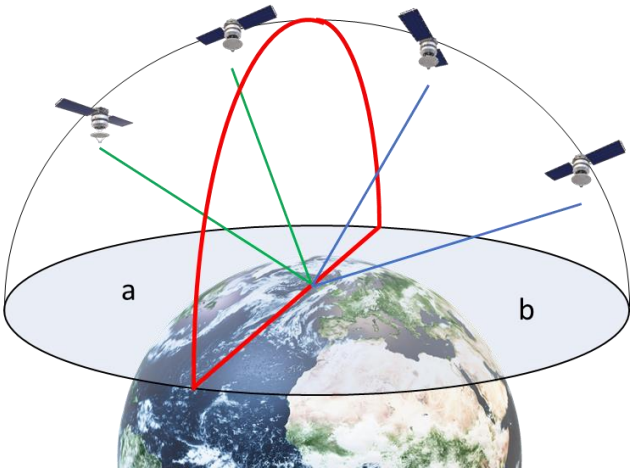

Figura 3-13 Esquema DAERS en tres dimensiones [Elaboración Propia]

3.8.1 DAERS: División Acimutal del Espacio y Reparto de Satélites

Para la realización del cálculo mediane este sistema, es de importancia que cada nodo de ataque realice una lectura de su posición, latitud y longitud reales, y la comunique al NAM. Dentro del mensaje GPS y después de una traducción de datos del formato NMEA, en concreto en la línea RMC, donde se encuentran los datos de tiempo, latitud y longitud del nodo. Cuando el NAM dispone de la posición suya y la del NAS, realiza el cálculo de los elementos indicados en el apartado 3.8.

Deben tenerse en cuenta las siguientes consideraciones:

Sean φ_M y φ_S la latitud del NAM y el NAS respectivamente.

Sean L_M y L_S la longitud de NAM y NAS respectivamente.

Para el cálculo de las coordenadas del punto medio PM, deben realizarse la media de las latitudes y la media de las longitudes. Debe tenerse en cuenta que las coordenadas terrestres tienen dos componentes en latitud, Norte (N) y Sur (S), y dos en longitud, Oeste (W) y Este (E). Por ello, debe asignarse un signo distinto a cada componente en latitud y en longitud. En este proyecto se considerarán negativas las latitudes S y las longitudes E.

3.8.2 Cálculo coordenadas PM

El cálculo de la latitud y longitud del PM no es más que el cálculo de las medias de la latitud y la longitud.

$$\varphi_{PM} = \frac{\varphi_M + \varphi_S}{2},$$

$$L_{PM} = \frac{L_M + L_S}{2},$$

siendo las coordenadas del punto medio PM (φ_{PM} , L_{PM}). Este sencillo proceso podría aplicarse con más nodos de ataque en la red, simplemente se hallaría la media de las latitudes de todos los NA (nodo de ataque) disponibles o presentes en el dispositivo para realizar el ataque mediante suplantación de señal GPS.

$$\varphi_{PM} = \frac{\varphi_M + \varphi_{S1} + \cdots + \varphi_{Sn}}{n+1},$$
$$L_{PM} = \frac{L_M + L_{S1} + \cdots + L_{Sn}}{n+1}$$

3.8.3 Cálculo de la Demora de Unión de Nodos (DUN)

El cálculo de esta demora permitirá posteriormente calcular la Línea de División de Constelación sumando 90 grados a la DUN. El problema es un ejemplo sencillo de trigonometría esférica.

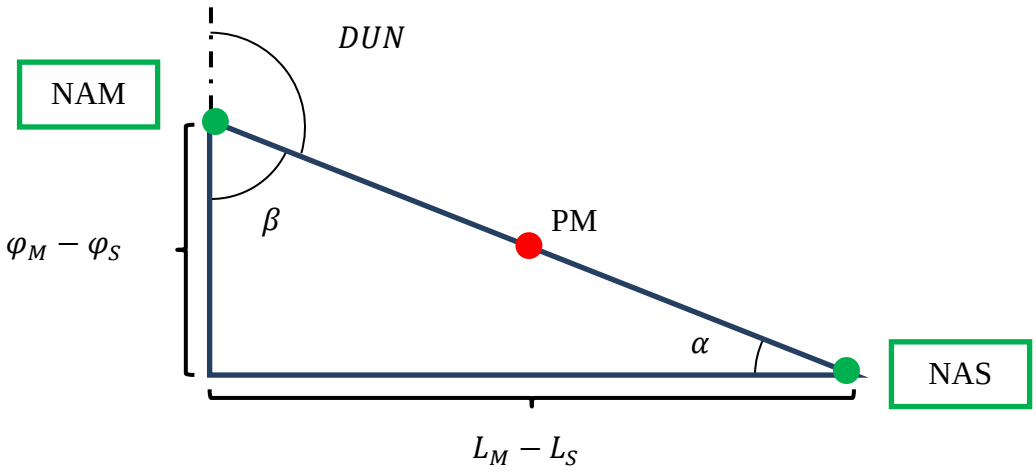

Figura 3-14 Representación plana del cálculo de DUN. [Elaboración Propia]

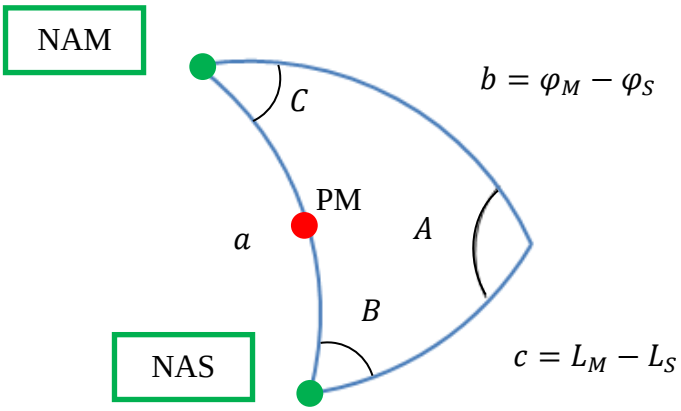

Figura 3-15 Triángulo esférico. [Elaboración Propia]

La ecuación que se expone a continuación relaciona los elementos del triángulo esférico (Figura 3-15) donde "b" es la diferencia de latitudes entre NAM y NAS, "c" la diferencia de longitudes y "a" la distancia entre ambos nodos de ataque. [33], [34]

$$\cos a = \cos b \cdot \cos c + sen\ b \cdot sen\ c \cdot \cos A \quad \text{¡Error! Marcador no definido.}$$

Debemos tener en cuenta que la latitud y la longitud forman un ángulo de 90º que correspondería al ángulo A. Al tener el coseno de 90º un valor de 0, la ecuación quedaría simplificada.

$$\cos a = \cos b \cdot \cos c$$

La relación entre ángulos y lados opuestos:

$$\frac{sen\ a}{sen\ A} = \frac{sen\ b}{sen\ B} = \frac{sen\ c}{sen\ C}$$

Para calcular la DUN debe tenerse en cuenta si la diferencia de longitudes y la diferencia de latitudes y si estas son positivas o negativas.

Tabla 3-3 Cálculo de la DUN [Elaboración Propia]

Diferencia de Longitudes	Diferencia de Latitudes	Método de cálculo de la DUN
Positiva	Positiva	1. $DUN = 180° - \left\lvert arcsen\left(\frac{sen\ c}{sen\ a}\right)\right\rvert$
Negativa	Positiva	2. $DUN = 180° + \left\lvert arcsen\left(\frac{sen\ c}{sen\ a}\right)\right\rvert$
Negativa	Negativa	3. $DUN = 270° + \left\lvert arcsen\left(\frac{sen\ b}{sen\ a}\right)\right\rvert$
Positiva	Negativa	4. $DUN = 90° - \left\lvert arcsen\left(\frac{sen\ b}{sen\ a}\right)\right\rvert$

3.8.4 Cálculo de la Línea de División de Constelación

Por último, debe calcularse la Línea de División de Constelación LDC sumando y restando a la DUN 90 grados. Son pues en realidad dos demoras separadas 180º.

$$LDC = DUN \pm 90°$$

Debe tenerse en cuenta que las demoras (ángulos) no pueden ser mayores de 360º ni negativos, por tanto, debe aplicarse en el código una corrección de darse uno de estos dos casos. En el primero de restar 360 grados y en segundo de sumar esos mismos 360º.

3.8.5 Ejemplo práctico

Se supone un escenario de ataque *spoofing* en la Ría de Pontevedra y se eligen dos situaciones para los nodos de ataque, uno en cada ribera (Figura 3-16). El NAM se colocará en la Isla de Tambo con coordenadas 42º24'37"N, 8º42'29"W y el NAS en Cabo Udra con coordenadas 42º20'18"N, 8º50'10"W, por tanto:

$$\varphi_{PM} = \frac{\varphi_M + \varphi_S}{2} = \frac{42°24'37"N + 42°20'18"N}{2} = 42°22'27{,}5"N,$$

$$L_{PM} = \frac{L_M + L_S}{2} = \frac{8°42'29"W + 8°50'10"W}{2} = 8°46'19{,}5"W,$$

$$b = \varphi_M - \varphi_S = 42°24'37"N - 42°20'18"N = 4'19" \ (+),$$

$$c = L_M - L_S = 8°42'29"W - 8°50'10"W = -7'41" \ (-),$$

$$a = \arccos(\cos b \cdot \cos c) = arcos(cos(4'19") \cdot \cos(-7'41")) = 8'48{,}77".$$

Al ser la diferencia de longitudes "c" negativa y la diferencia de latitudes "b" positiva debe utilizarse el método 2 de cálculo de la DUN (ver Tabla 3-3).

$$DUN = 180º + arcsen\left(\frac{sen\ c}{sen\ a}\right) = 180° + \left|arcsen\left(\frac{sen\ (-7'41")}{sen\ (8'48{,}77")}\right)\right| = 240{,}67°,$$

$$LDC = DUN \pm 90° = \begin{Bmatrix} LDC = 150{,}67° \\ LDC = 330{,}67° \end{Bmatrix}.$$

Por tanto, la Línea de División de la Constelación será circulo máximo que pasa por el PM en dirección 150,67º-330,67º.

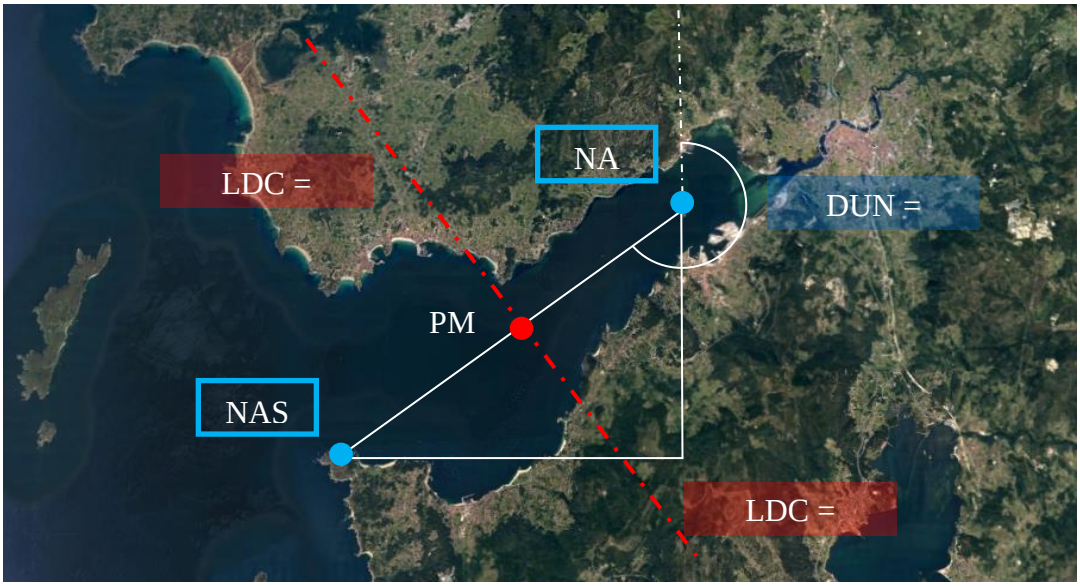

Figura 3-16 Representación gráfica del ejemplo práctico. [Elaboración Propia]

A continuación, deben sacarse los acimuts de cada satélite visible (ver apartado 3.6.2) y en función si quedan a la derecha o a la izquierda de la LDC serán asignados al NAM o al NAS.

3.8.6 Código

En el código general del programa se establece una función que realiza los cálculos pertinentes para obtener la posición del PM y los acimuts que corresponden a las LDC. También se calculan los acimuts de cada posición (del NAS y del NAM) desde el punto medio, para relacionar cada sector con el nodo de ataque que corresponda.

Cabe destacar que el código de esta función está diseñado y preparado para asumir el cálculo de la división acimutal del espacio y reparto satelital para "n" NAS, aunque si bien debería desarrollarse un método para identificar cada uno de ellos al intercomunicarse y que puede formar parte de las líneas futuras de este trabajo. Sin embargo, la función DAERS (Figura 3-17) está preparada para asumir más de dos nodos de ataque como es el caso del presente trabajo.

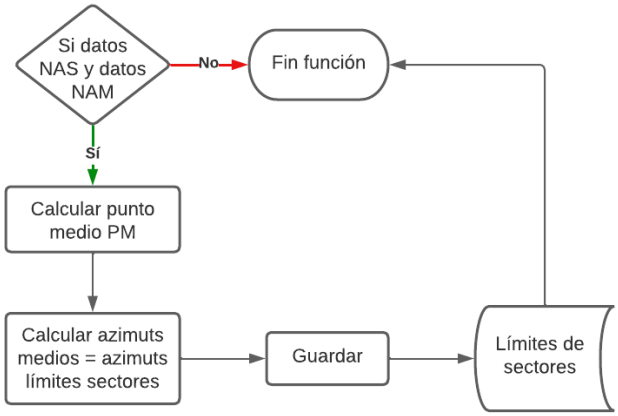

Figura 3-17 Diagrama de flujo función DAERS [Elaboración Propia].

3.9 Coordinación y secuencia del ataque

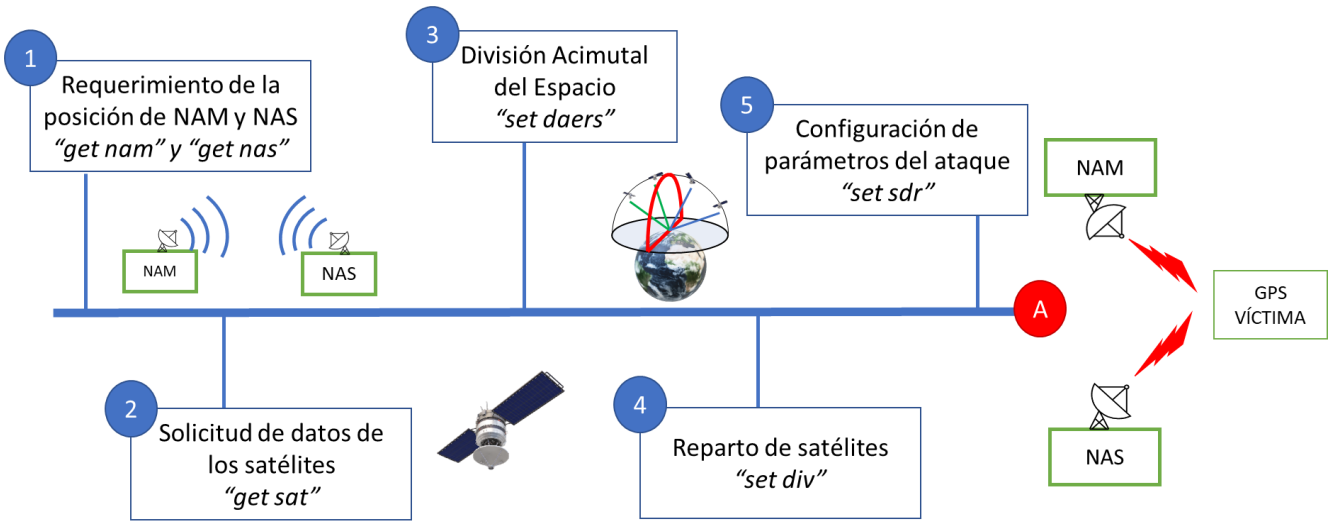

Figura 3-18 Esquema de la secuencia del ataque [Elaboración Propia]

3.9.1 NAM

El control del ataque se lleva a cobo desde el NAM donde se ejecuta el programa DAERS y se requieren ciertos comandos (ver apartado 3.5.1). En función de las órdenes que se vayan impartiendo el programa requerirá o no respuesta del NAS e irá obteniendo los datos necesarios para ejecutar el ataque, configurando los parámetros de este y finalmente llevándolo a cabo (Figura 3-18).

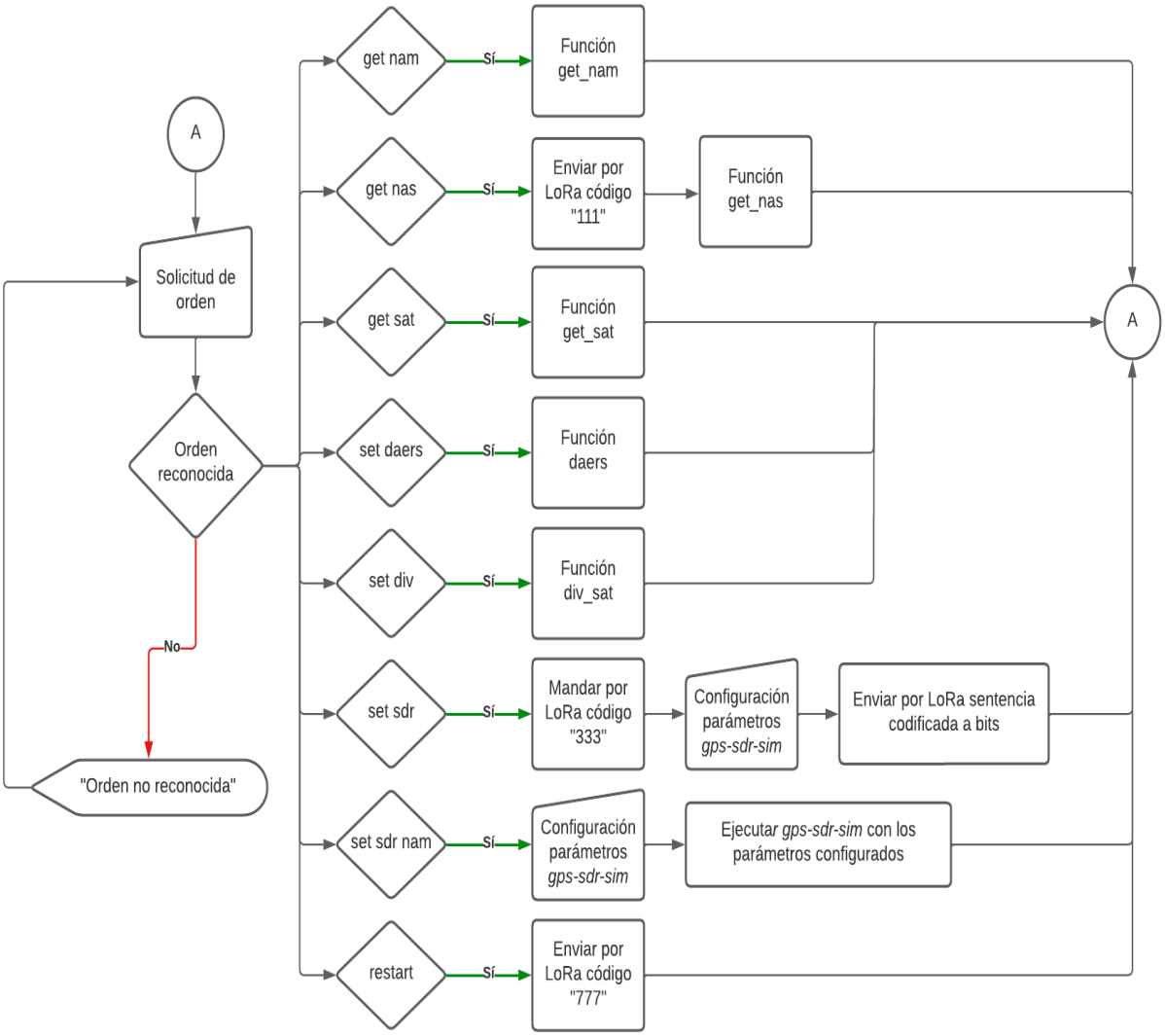

Figura 3-19 Diagrama de flujo del Programa DAERS [Elaboración propia].

El programa instalado en el NAM (Figura 3-19), como se ha mencionado, requiere de la interacción del usuario para realizar las diferentes acciones necesarias para configurar y parametrizar el ataque de *spoofing*.

Esta interacción debe comenzar por la adquisición de las posiciones de ambos nodos de ataque, ya que estas son necesarias para realizar los cálculos pertinentes. En la Figura 3-20 se observa la función "get_nam", que permite obtener la posición y tiempo del NAM, en forma de diagrama de flujo. Esta función se activa, como se ve en Figura 3-19, mediante el comando *get nam*. El modo en cómo se adquiere esta posición es mediante la lectura de las sentencias NMEA recibidas por el módulo GPS del NAM como se explica en el apartado 3.6.1.

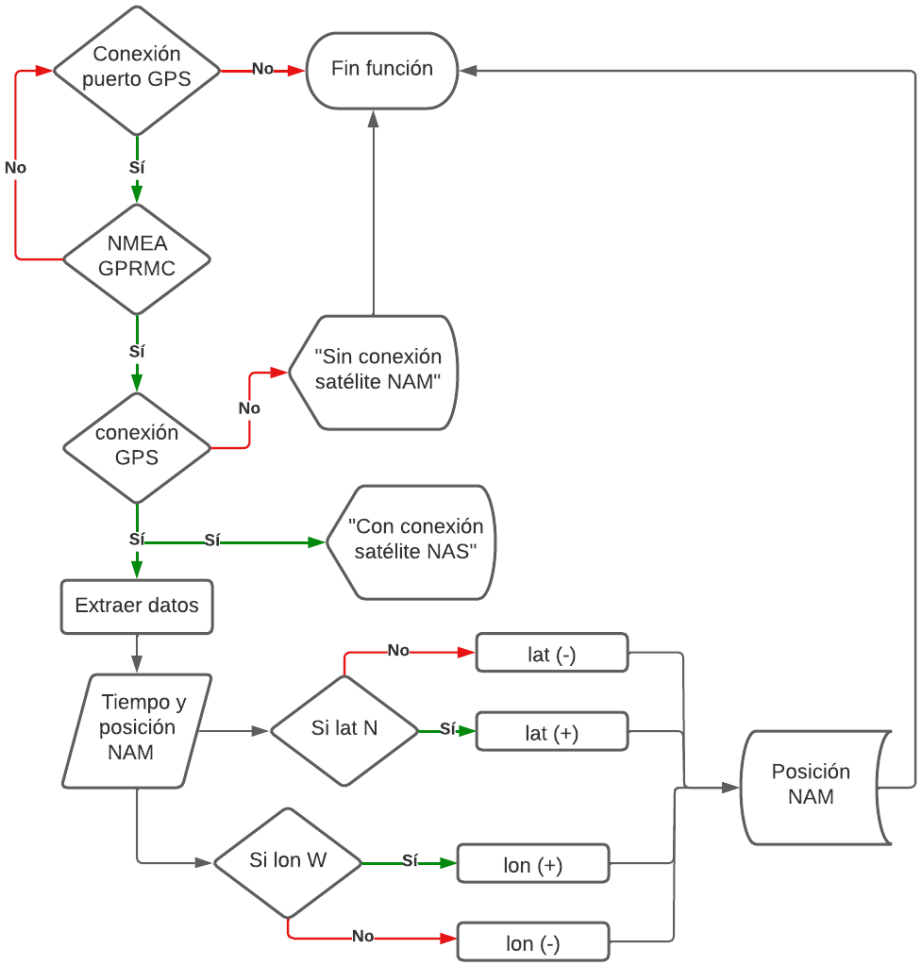

Figura 3-20 Diagrama de flujo de la Función "get nam". [Elaboración Propia]

La función "*get nam"* imprime por pantalla la disponibilidad o no de conexión GPS leyendo la segunda posición de la sentencia NMEA GPRMC, posición que ocupa la letra "A" si la conexión es positiva y la letra "V" si esta es negativa. De esta manera, el sistema puede saber si el receptor GPS ya ha sido capaz de calcular su posición y tiene al menos esos 4 satélites necesarios con los que realizar los cálculos de posición. El resto de las posiciones de la mencionada sentencia NMEA son leídas por la función y sus valores guardados en diferentes variables que permiten acceder a ellos de ser requeridos.

Es el caso de las posiciones 4 y 6 (ver apartado 3.6.1) que indican si la latitud es sur o norte y la longitud esta u oeste respectivamente. La función convierte los datos de latitud y longitud a grados pues vienen en grados y minutos, pero para simplificar los cálculos, se convierten a grados y se asigna el criterio de signos para las coordenadas que se ha decidido en el que las latitudes N y longitudes W son positivas por ser las componentes de las coordenadas donde se realizan los experimentos. Así pues, las latitudes S y las longitudes E son multiplicadas por -1.

A continuación, se guarda la latitud en la primera posición de un array que ira recogiendo todas las latitudes de los diferentes nodos de ataque (en este caso dos, el NAM y un NAS). La primera posición de este array está reservada para la posición del NAM. De igual manera, se guarda la longitud en otro array que recogerá las longitudes de los nodos de ataque y donde la primera posición del array guarda, también, la longitud del NAM.

La función que adquiere la posición del NAS (get_nas) tiene, en esencia, el mismo funcionamiento si bien la sentencia NMEA debe solicitarse al propio módulo NAS. Haciendo uso del protocolo de

comunicación entre nodos (apartado 3.5.1) se envía un código al NAS, que este identifica y envía la última sentencia NMEA GPRMC, recibida por el módulo receptor GPS, al NAM. Este último leerá los datos y de igual manera que la función get_nam, extraerá latitud y longitud. Del mismo modo que su función homóloga, aplicará el criterio de signos y guardará en los arrays mencionados latitud y longitud.

Los últimos datos necesarios para la realización del ataque son los de la constelación visible de satélites. La función "get_sat" mediante la orden *get sat* realiza la lectura y extracción de la sentencia NMEA GPGSV (ver apartado 3.6.2) en el NAM, que comprende algo más de dificultad que la sentencia GPRMC debido a que generalmente son más de una sentencia las necesarias para obtener los datos de toda la constelación visible.

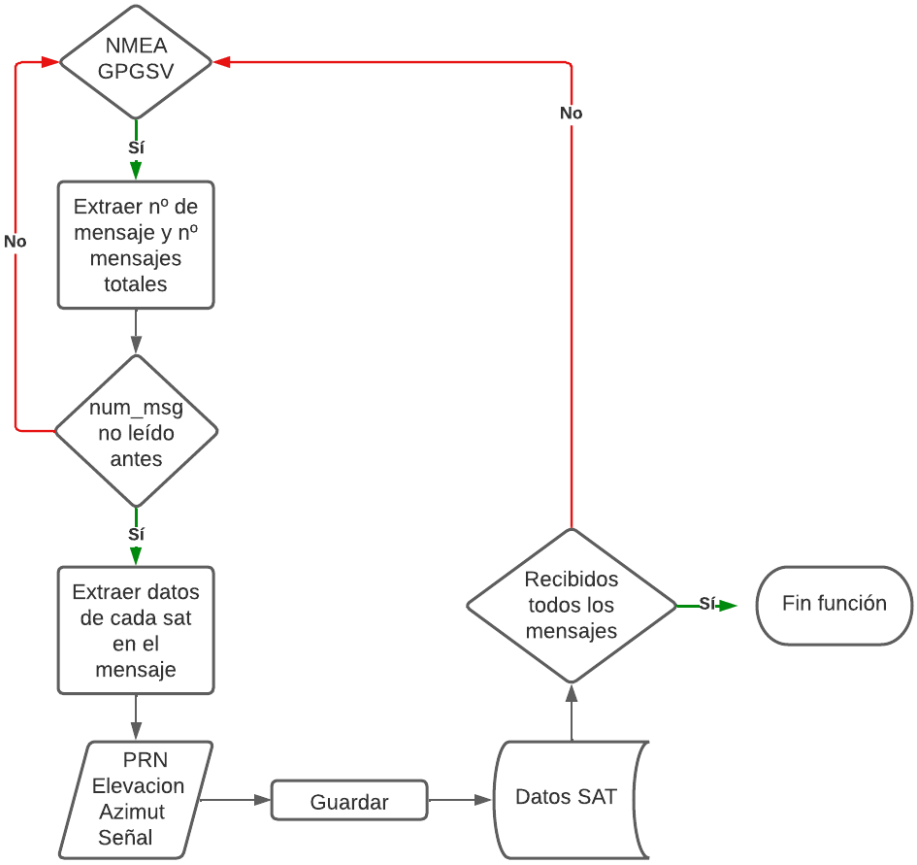

Figura 3-21 Diagrama de flujo de la Función get_sat. [Elaboración Propia]

Eminentemente el programa, mediante esta función (ver Figura 3-21), extrae de la sentencia el número de mensajes que contienen los datos de toda la constelación visible y guarda este valor en una variable que servirá para comparar y determinar si se han leído todos los mensajes diferentes de la sentencia GPGSV. Además, va guardando el identificador individual de cada mensaje en un array junto con los datos de los satélites presentes en dicho mensaje en una matriz. Finalmente compara si el número de identificadores diferentes que tiene guardados corresponde con el número de mensajes totales que componen los datos GPGSV, y si es así significa que ha extraído y guardado los datos de todos los satélites de la constelación visible. De no ser de este modo, continuará leyendo sentencias GPGSV hasta que se cumpla esta condición. Para entender esto se verá un ejemplo práctico.

Supóngase que la primera sentencia NMEA GPGSV que se recibe es la siguiente:

$GPGSV,**3**,2,12,04,05,141,35,03,15,260,00,08,01,088,00,14,02,252,00*74

Puede observarse que, en la segunda posición, resaltado en negrita y después del identificador de sentencia, se muestra el número total de mensajes portadores de los datos de los satélites de la constelación visible. A continuación, se observa el identificador de mensajes, en este caso el número 2. Así pues, se ha recibido el segundo mensaje de un total de tres. La función guarda en una variable de tipo entero el número 3 y en un array el identificador del mensaje. La siguiente sentencia NMEA GPGSV que se reciba se leerá de igual manera.

Si el identificador de mensaje coincide con alguno de los guardados previamente ene le array, esta sentencia es descartada. Si por el contrario no coincide con ninguno, es procesada y se añade al array este nuevo identificador. Supongamos que hemos recibido el mensaje número 1, el array quedaría de la siguiente manera (2,1). El proceso continúa hasta que el número de elementos distintos en el array es igual al número de mensajes totales, en el caso de este ejemplo, cuando el array contiene los tres identificadores distintos de los mensajes (2,1,3).

Los datos individuales de cada satélite son guardados finalmente en un DataFrame de cuatro columnas en que se recogen números de código PRN, elevación, acimut y relación señal a ruido de la señal de cada satélite (ejemplo Tabla 3-4).

Tabla 3-4 DataFrame ejemplo satélites. [Elaboración Propia]

PRN	Elevación (º)	Acimut (º)	SNR (dB)
27.0	57.0	293.0	23.0
31.0	8.0	181.0	24
2.0	5.0	44.0	0.0
7.0	10.0	323.0	15.0

De este modo es posible guardar los datos de una forma sencilla y poder seleccionar uno de los parámetros en función de otro de ellos, ya que permite mantener una asociación entre parámetros por pertenecer todos los de un mismo tipo a una misma fila. Esto cobra especial relevancia cuando deben seleccionarse los satélites que va a sustituir uno u otro nodo de ataque mediante el acimut o descartar satélites por una elevación insuficiente o una relación señal a ruido extremadamente baja.

Una vez recabados todos los datos necesarios, podemos ejecutar la función *daers* que realiza esa división acimutal del espacio, como se expone en el apartado 3.8. En primer lugar, se calculan la latitud y longitud del punto medio haciendo la media de las latitudes y de las longitudes guardadas de los diferentes nodos de ataque. Para la realización del resto de cálculos necesarios, expuestos durante el apartado 3.8 División de constelación visible, se convierten todos los datos necesarios a radianes para operar con funciones trigonométricas. Se calculan los acimuts de los nodos de ataque respecto al punto medio (DUN) y a continuación se calculan las líneas de división de constelación, que no son más que los acimuts medios entre los DUN. De este modo el programa calcula tantos sectores como nodos de ataque haya y está programado para el supuesto de que haya más de los dos que existen en este trabajo.

El resultado de esta función (para el caso de dos nodos) son dos sectores asociados cada uno a un acimut límite superior y un acimut límite inferior, que corresponden con las LDC que parten del Punto Medio. Estos datos se guardan en otro DataFrame como puede verse en la Tabla 3-5.

Tabla 3-5 DataFrame ejemplo Sectores Satelitales. [Elaboración Propia]

Sector	Límite inferior (º)	Límite superior (º)
1.0	163.0	343.0
2.0	343.0	163.0

En este punto se dispone de todos los acimuts de cada satélite y cada nodo de ataque al PM, por consiguiente, comparando estos acimuts con las LDC se agrupan los satélites y el nodo que se encuentren en un mismo sector. Esto es posible recorriendo la columna de *Acimut* del DataFrame de los satélites comparándolos con los límites de los sectores establecidos y guardados en las columnas del DataFrame *Sectores Satelitales*. De este problema se encarga la función *set div*, que divide la constelación de acuerdo con el valor de las LDC. Esta función realiza además dos modificaciones a los DataFrames de datos y que se imprimen por pantalla para tener el registro de los satélites asignados a cada sector y el nodo que se hace cargo de la suplantación de cada sector. Obteniéndose así las siguientes tablas de datos (Tabla 3-6 y Tabla 3-7).

Tabla 3-6 DataFrame ejemplo Reparto Satelital. [Elaboración Propia]

PRN	Elevación (º)	Acimut (º)	SNR (dB)	Sector
27.0	57.0	293.0	23.0	1.0
31.0	8.0	181.0	24	1.0
2.0	5.0	44.0	0.0	2.0
7.0	10.0	353.0	15.0	2.0

Tabla 3-7 DataFrame ejemplo asignación sector a nodo. [Elaboración Propia]

Latitud (º)	Longitud (º)	Acimut (º)	Sector
42.3967855	8.70986231	253.0	1.0
42.4263852	8.68965213	73.0	2.0

De igual modo se guardan en dos arráis los números PRN de los satélites asignados a cada uno de los sectores que después quedarán definitivamente asignados a un nodo de ataque tras comparar el número de sector con los datos recogidos en el DataFrame tipo de la Tabla 3-7.

A continuación, ya pueden configurarse los parámetros de la señal Spoofer, que será diferente para cada nodo ya que suplanta satélites distintos, mediante la función y orden *set sdr*. Esta función necesitará de otra interacción del usuario donde deberá introducir los valores de los parámetros que requiera como la posición de engaño, hora del ataque, satélites a suplantar y otros parámetros técnicos como la tasa de bits Fase/Amplitud. Esta configuración debe enviarse al NAS mediante LoRa y para ello se ha usado el sistema de las sentencias NMEA, es decir, cada parámetro a configurar se escribe en un orden concreto y es separado mediante una barra baja (“_”), a continuación, es codificado en binario y enviado a través del módulo LoRa.

La configuración de la señal de spoofer del NAM se realiza del mismo modo excepto que no es necesario enviarla por el módulo LoRa y es este mismo nodo el que ejecuta el programa *gps-sdr-sim* de acuerdo con la configuración.

Finalmente, la última fase consiste en ordenar y configurar el ataque en sí, para ello de forma parecida a la configuración de la señal sdr, se deben dar ciertos valores a parámetros para el ataque como la potencia de transmisión.

3.9.2 NAS

El programa instalado en el NAS es algo más sencillo debido a la menor capacidad del nodo de ataque esclavo. Este programa mantiene una escucha permanente por el puerto serie al que está conectado el módulo LoRa de Arduino y en función del código que reciba ejecutará una u otra acción (ver Tabla 3-2 en apartado 3.5.1). La recepción del código correspondiente a la solicitud de posición y estado del NAS hace que este discrimine entre las sentencias NMEA que recibe por su módulo GPS y envíe la sentencia GPRMC al NAM. Para evitar errores, se envía tres veces, aunque el NAM sólo leerá una de ellas, la primera que reciba completa.

Debido a la inaccesibilidad a un interfaz NAS-Usuario, se ha implementado la capacidad de reiniciar el NAS de forma remota ante la posibilidad de fallo del NAS. Para asegurar que tras el reinicio el programa vuelve a ejecutarse sin interacción con el operador, se ha integrado dentro de los programas ejecutables al inicio.

La otra orden que puede recibir el NAS y la última previa a la de ataque es la de configuración de la señal Spoofer mediante el programa *gps-sdr-sim* que, como se explica en los apartados 3.4.1 y 3.9.1, necesita de ciertos parámetros para ejecutarse. El valor de estos parámetros llega mediante un mensaje binario desde el NAM que es decodificado y cada parámetro al estar separado por una barra baja, es fácilmente separable al igual que se hace en la lectura de las sentencias NMEA en el apartado 3.6. Una vez tiene guardados cada parámetro por separado ejecuta el programa de generación de la señal Spoofer de acuerdo con la configuración indicada.

La orden de ataque se lleva a cabo de la misma manera, se recibe el código de ataque, la hora de la señal de suplantación y los parámetros necesarios para el mismo. Llegados a este punto, sólo cabe la comprobación de que el ataque *spoofing* es efectivo.

3.10 Dificultades encontradas

Realizando pruebas sobre el funcionamiento de los programas gps-sdr-sim y HackRF se hace evidente que la Raspberry Pi 3 que estaba siendo utilizada inicialmente carecía de la capacidad de procesamiento requerida para realizar los ataques (generar y transferir la señal al SDR) en tiempo real, obteniéndose un tiempo de procesamiento de 53 segundos para una señal ataque de muestra con una duración real de 10 segundos. Se toma la decisión de cambiar este modelo de Raspberry por un modelo superior, la Raspberry Pi 4 de 4GB de RAM, que si es capaz de procesar la señal en tiempo real.

4 RESULTADOS Y VALIDACIÓN

4.1 Resultados en laboratorio

Las pruebas de laboratorio se han llevado a cabo de una forma progresiva, según la cual, se han ido probando y validando las diferentes etapas, procesos, funciones y sistemas por separado y más adelante de forma conjunta para detectar en que punto del trabajo se hubiesen podido cometer errores o incoherencias. De esta forma podemos dividir las pruebas de funcionamiento en los siguientes bloques:

- Validación de comunicación inter-nodal entre el NAM y el NAS.
- Pruebas del funcionamiento del programa DAERS en sus múltiples funciones y etapas de desarrollo.
- Pruebas de suplantación de señal GPS (spoofing) sin integración en el sistema multiestático del programa generador de señal *gps-sdr-sim*.
- Pruebas de suplantación de señal GPS tanto generación como transmisión por parte de los dos nodos por separado.
- Prueba global del sistema multiestático desarrollado para la suplantación de señal GPS con la división acimutal del espacio y reparto de los satélites de la constelación visible.

4.1.1 Comunicación inter-nodal y programa DAERS

Los resultados de estos dos bloques se presentan juntos debido a que la comprobación efectiva de la comunicación entre el NAS y el NAM se ha realizado a la vez que el desarrollo del código del programa DAERS y se ha ido comprobando paulatinamente según se ha ido avanzando.

Esta validación del sistema se encuadra fuera de la suplantación de GPS y por tanto puede llevarse a cabo con los nodos de ataque incompletos, debido a que no requieren de la conexión del módulo SDR de cada uno de ellos.

Como se explica en el apartado 3.9, los primeros datos que se requieren son las posiciones de ambos nodos de ataque, que se solicitan mediante las mencionadas funciones *get nas* y *get nam*. En la Figura 4-1, su observa como al requerimiento de “orden: “ del programa, se escribe el comando de la primera de las funciones. La posterior impresión por pantalla de la sentencia “Con conexión satélite

NAS" y los posteriores parámetros, a saber, tiempo, latitud y longitud, prueban que la comunicación entre el NAM y el NAS es efectiva en ambos sentidos. La orden llega al NAS que responde enviando la sentencia NMEA GPRMC, pues de otro modo el programa no imprimiría nada por pantalla. Pues sólo lo hace si recibe una sentencia NMEA GPRMC por el puerto del módulo LoRa. Puede apreciarse que ambas posiciones no distan mucho la una de la otra, esto es debido a que ambas antenas estaban colocadas en posiciones muy cercanas durante esta prueba.

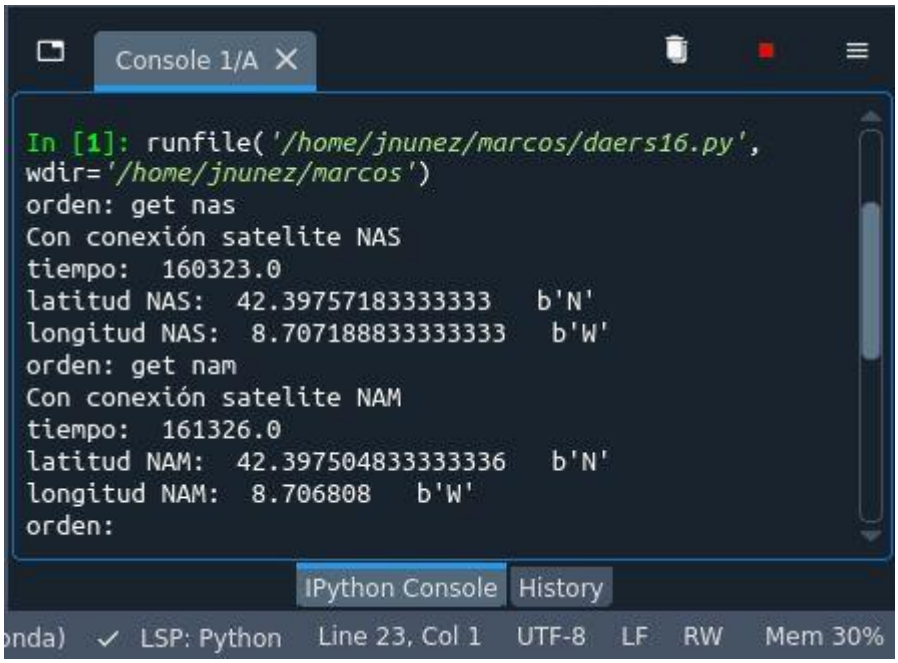

Figura 4-1 Validación funciones *get nas* y *get nam*. [Elaboración Propia]

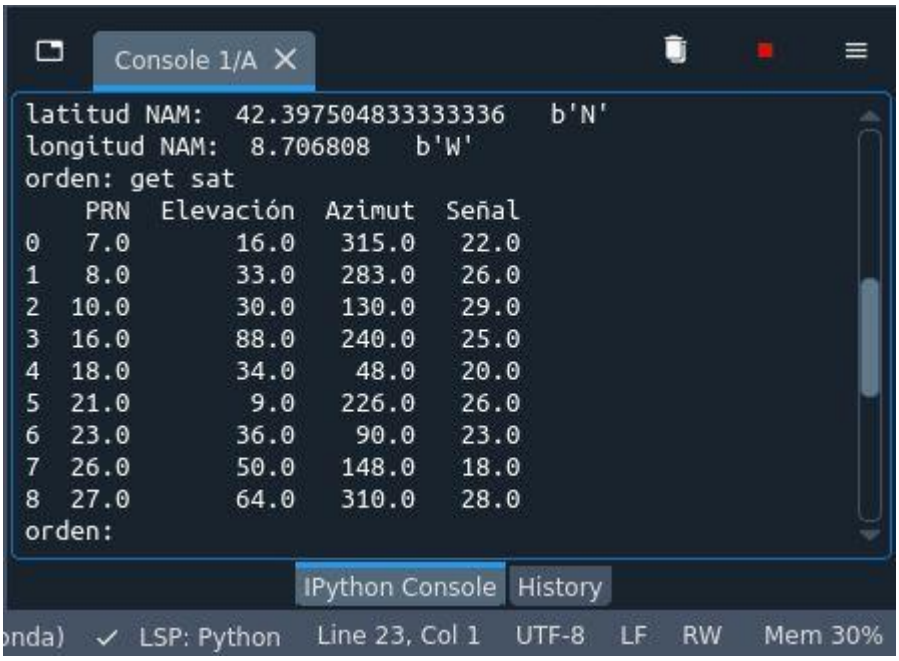

Figura 4-2 Validación función *get sat*. [Elaboración Propia]

En la Figura 4-2, se demuestra el funcionamiento de la función *get sat*, que recopila la información de los satélites de la constelación visible. Puede apreciarse que el programa realiza la lectura de las sentencias GPGSV y guarda los datos de los satélites de forma ordenada en un DataFrame que posteriormente imprime por pantalla. En este caso son 9 satélites los visibles de los que se recibe señal de todos ellos. Reseñar que la columna de "Señal" no es más que la relación señal a ruido (SNR) de la señal de cada satélite.

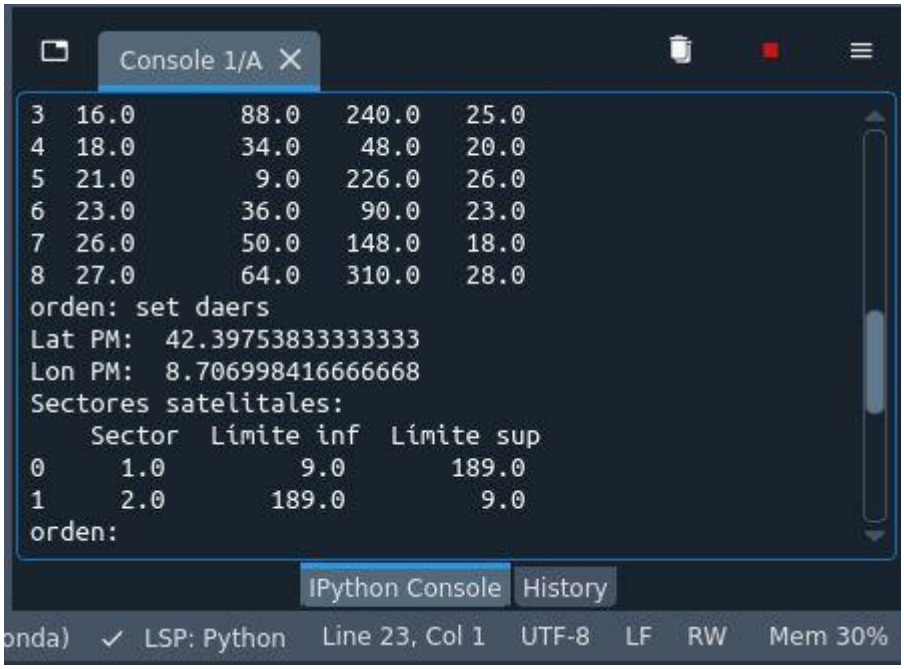

Figura 4-3 Validación función *set daers*. [Elaboración Propia]

En la Figura 4-3, se demuestra el funcionamiento del centro de gravedad del programa, la división acimutal del espacio. Puede observarse que ante el requerimiento del usuario de la función *set daers*, el programa calcula, efectivamente, las coordenadas del punto medio y las líneas de división de constelación LDC. De nuevo quedan guardados estos datos en un DataFrame que es impreso por pantalla para conocimiento del usuario y que relaciona el número de sector con los límites inferior y superior. Cabe destacar que el primer sector, sea el caso como este de dos nodos o de más, se corresponde siempre con aquel que comienza en la primera LDC después del Norte en sentido de acimut creciente u horario.

El reparto de los satélites y su asignación se lleva a cabo mediante la función *set div* como queda demostrado en la Figura 4-4, donde se aprecia una columna adicional en el DataFrame que contiene los datos de los satélites en la que se dispone el sector al que pertenecen (ver el funcionamiento de la función en el apartado 3.9.1).

Esta columna añadida que indica el sector también aparece en la tabla de latitudes y longitudes de los nodos de ataque, como se menciona en el apartado 3.9, la primera posición está reservada para el NAM y el resto de las posiciones las irían ocupando los NAS de los que se haga uso. Relacionando las columnas "Sector" de ambos DataFrames se obtiene la asignación de satélites a cada nodo que se imprimen en dos tablas denominadas respectivamente "Sat del NAM" y "Sat del NAS". Adicionalmente y para facilitar la lectura de los datos solución al usuario se imprimen los arrays (SatNAm y SatNAs) donde se guardan exclusivamente los números PRN de los satélites asignados a cada nodo y, en el caso de NAS, los que se envíen mediante el módulo LoRa para la ejecución del ataque.

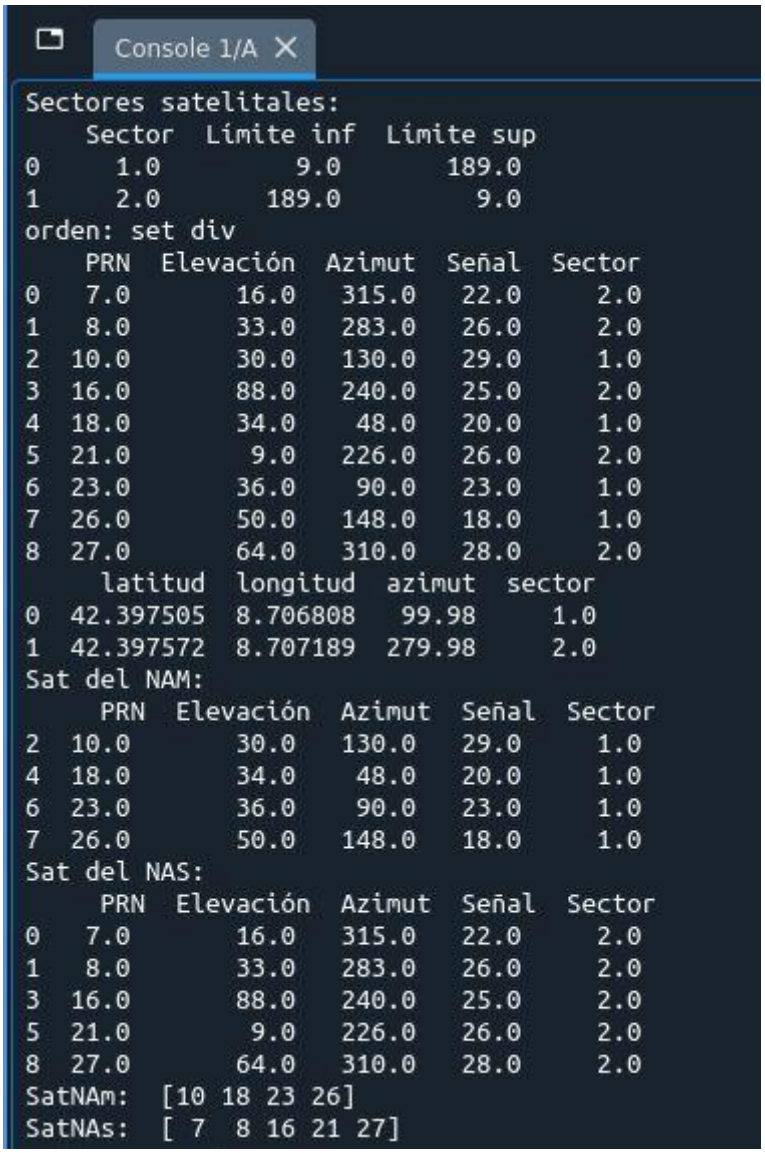

Figura 4-4 Validación función *set div*. [Elaboración Propia]

Por último y como acción previa al ataque, la función *set sdr* solicita la introducción por parte del usuario de valores de los parámetros de configuración de la suplantación de la señal GPS. Tras introducir el comando *set sdr*, se imprime en pantalla el orden y modo en que deben introducirse dichos parámetros. Puede observarse en la Figura 4-5 como tras la mencionada orden, aparece el nombre de cada parámetro y los símbolos que deben separarlos. Estos son esenciales para que, al enviarse esta sentencia al NAS, junto con el array de satélites asignados al NAS, este leerá la sentencia y separará el valor de cada parámetro en función del signo guion bajo ("_").

El funcionamiento de la recepción y lectura de esta orden de ataque y configuración del propio ataque sólo se puede validar si se observa que el programa *gps-sdr-sim* junto con el *HackRF_transfer* se ejecutan en las condiciones seleccionadas. Teniendo en cuenta que se ha demostrado el correcto funcionamiento de las comunicaciones inter-nodales, esta comunicación en concreto quedará validada en los siguientes apartados junto con los ataques de los nodos por separado y en su conjunto.

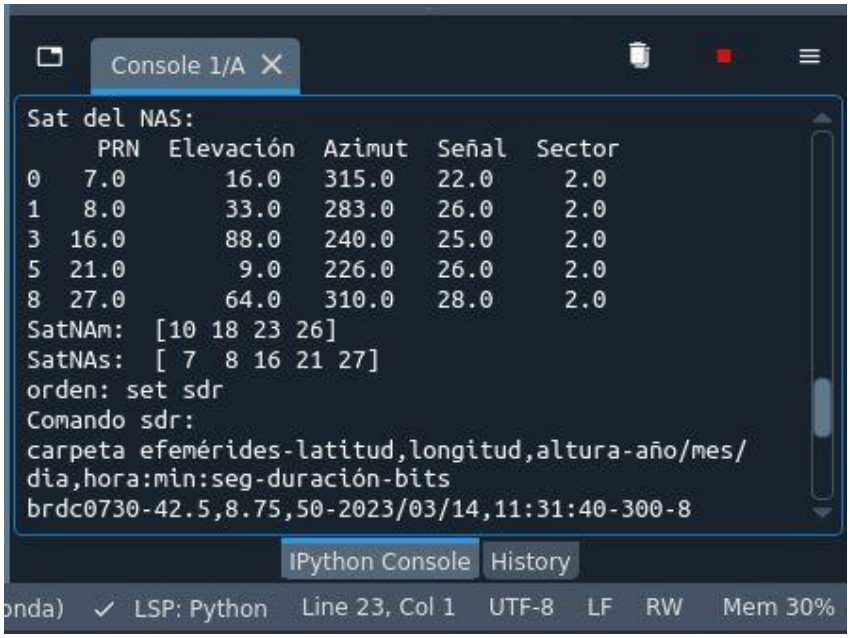

Figura 4-5 Validación función *set sdr.* [Elaboración Propia]

4.1.2 Generación de señal GPS falsa.

Este punto del trabajo ha sido un punto crítico para la continuación del mismo. La generación de la señal y su transmisión para la suplantación debían hacerse en tiempo real. Para esto es necesario que los nodos de ataque tengan la capacidad de procesamiento necesaria para que esto, sea así. En la Figura 4-6, se da la orden al NAS (Raspberry Pi 4) de ejecutar el programa que genera la señal (*gps-sdr*-sim) cuyos datos serán trasmitidos por el programa *HackRF_transfer* conectándolo mediante "*pipes*" de Linux.

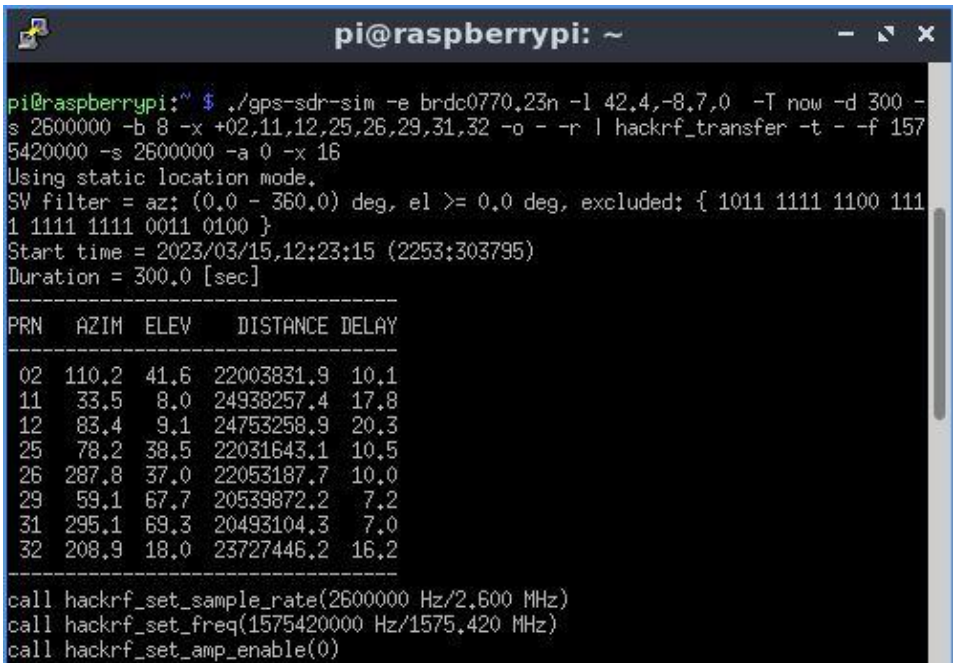

Figura 4-6 Prueba validación capacidad de procesamiento de la generación y transmisión de la señal spoofer. [Elaboración Propia]

Se observa que el programa selecciona los 8 satélites, de los que se indican en el comando, que están en ese momento en la constelación visible sobre la posición que suplanta la verdadera. En la Figura 4-7, se puede apreciar el llamamiento al programa trasmisor y el inicio del proceso de trasmisión que al ser en tiempo real avanza segundo a segundo por cada segundo de señal spoofer creada. Por tanto, se demuestra la capacidad de procesamiento de hasta 8 satélites por parte del NAS sin producirse retrasos en la generación o transmisión de la señal de suplantación GPS.

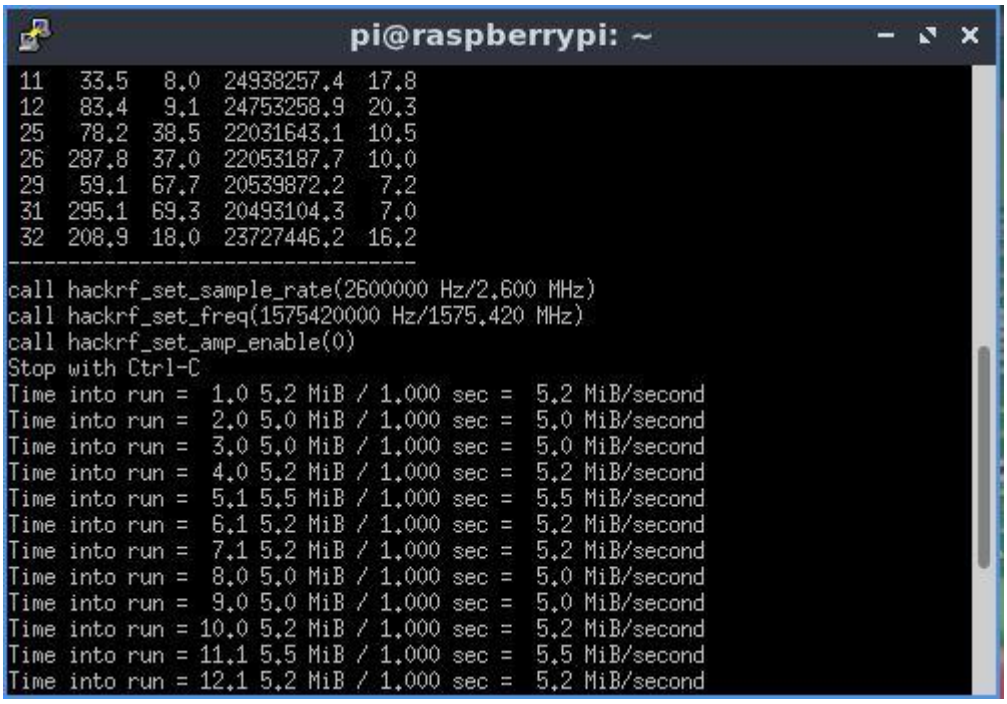

Figura 4-7 Prueba del procesamiento en tiempo real del programa spoofer. [Elaboración Propia]

4.1.3 Generación y transmisión del NAS

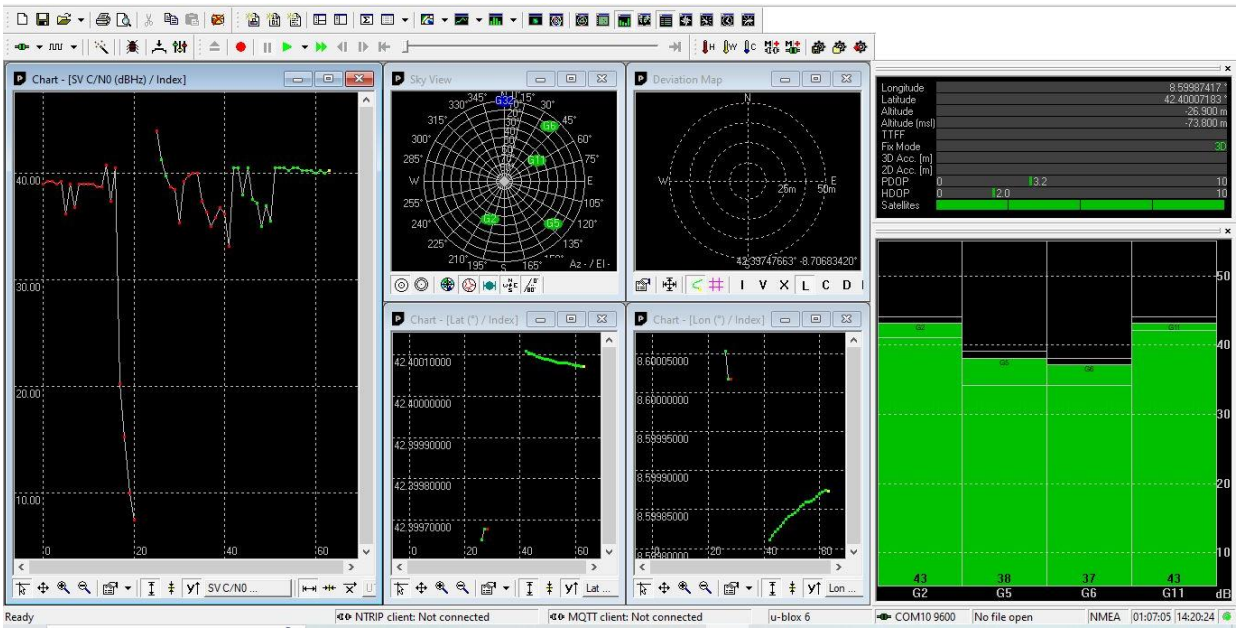

Figura 4-8 Suplantación de satélites 2, 5, 6 y 11 por parte del NAS y anclaje efectivo del GPS víctima. [Elaboración Propia]

Antes de probar el funcionamiento general del sistema multiestático se procede a comprobar la capacidad de procesamiento de la generación y transmisión de la señal que debe suplantar la verdadera señal GPS. En primer lugar, se comprueba en el NAS, donde se comprueba que la Raspberry Pi 3 que estaba siendo utilizada en un principio, como se ha mencionado, no tenía la capacidad necesaria. Es por ello por lo que se usa, finalmente, una Raspberry Pi 4.

En la Figura 4-8, se presenta la pantalla del programa uBlox durante la prueba de la capacidad de spoofing del NAS en la que se genera y emite un ataque para las coordenadas 42,4º N en latitud y 8,6º W en longitud. En ella se puede apreciar un anclaje positivo sobre la señal de suplantación durante la ausencia de señal GPS real. Los satélites seleccionados son cuatro, corresponden con los números PRN 02, 05, 06 y 11. Puede observarse en la gráfica de la izquierda de la figura que existe una fluctuación inicial de la relación señal a ruido durante el anclaje hasta que finalmente el receptor GPS reconoce todas las señales y es capaz de seguirlas y realizar el cálculo de posición. Momento en el que la gráfica pasa a color verde y se estabiliza.

En la parte superior de la Figura 4-8 en el mapa de satélites aparecen los cuatro mencionados en color verde, lo que significa que están siendo usados para el cálculo de posición y la señal suplantadora es tomada como real. Como se puede apreciar también en la parte derecha donde aparecen las SNR de cada satélite por separado en niveles cercanos a los que tendrían las señales de los satélites reales.

Queda validada, por tanto, la capacidad de procesar la generación y transmisión de la señal spoofer del NAS, pudiendo suplantar sin retrasos de procesamiento entre 7 y 8 satélites.

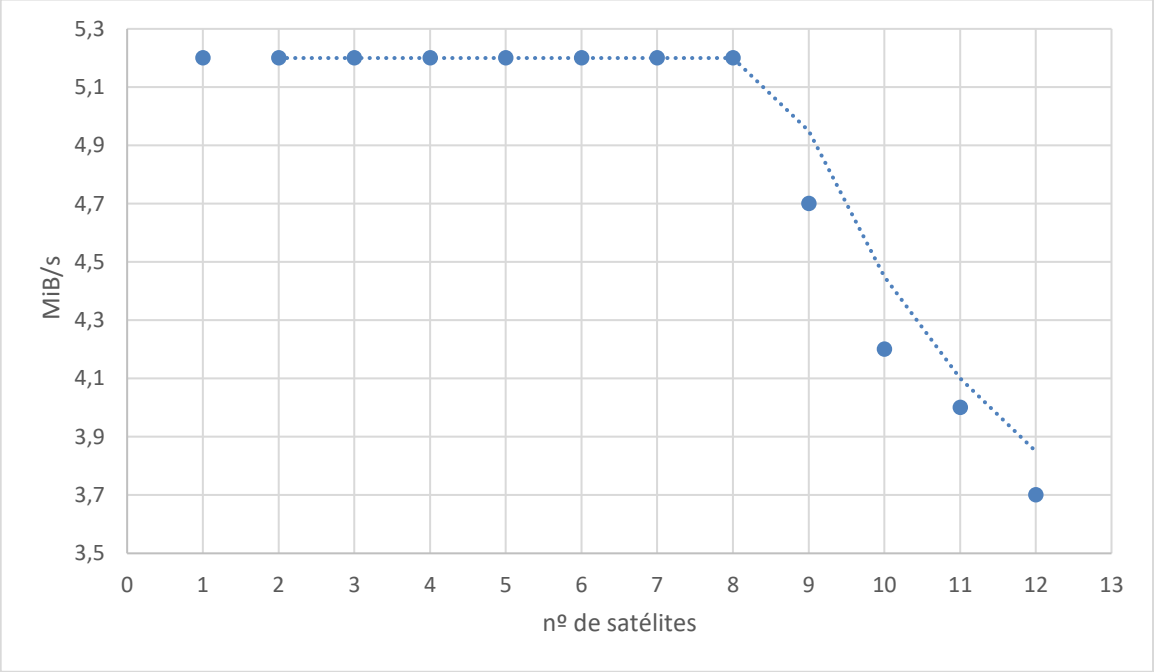

Figura 4-9 Relación de la capacidad de procesamiento del NAS con número de satélites suplantados. [Elaboración Propia]

Durante la realización de las pruebas de capacidad de procesamiento del NAS se realiza un estudio del volumen de satélites que puede soportar el NAS sin perder velocidad de procesamiento, que debe tenerse en cuenta, que debe ser en tiempo real. En la Figura 4-9 se expone la relación entre la velocidad de procesamiento y el número de satélites por ataque. Se puede ver que a partir de 8 satélites el rendimiento baja y la Raspberry no es capaz de procesar esos 5,2 mebibytes (1 MiB = 2^{20} bytes) por segundo que son preceptivos para que la señal se genere en tiempo real. A pesar de todo los ataques se

pueden seguir llevando a cabo con más satélites, si bien, no será capaz de suplantar la señal y únicamente será un ataque de *jamming*, es decir, de negación de la señal.

Esto demuestra que, realmente, un ataque puede llevarse a cabo únicamente con un nodo que cuente con la capacidad de procesamiento necesaria, sin embargo, la existencia de diferentes nodos en el sistema de ataque spoofer aporta versatilidad y robustez al ataque. Debido a que este continuaría en el caso de fallo de alguno de los nodos de la red.

4.1.4 Generación y transmisión del NAM

Del mismo modo que se ha validado la ejecución del NAS, debe comprobarse la actuación del nodo maestro en las mismas condiciones. En primer lugar, se ha realizado la comprobación de que la generación y transmisión de la señal de suplantación del NAM es, efectivamente, tomada como verdadera por un receptor GPS. Para esto dicho receptor no recibe señal GPS real para evitar interferencias en la validación.

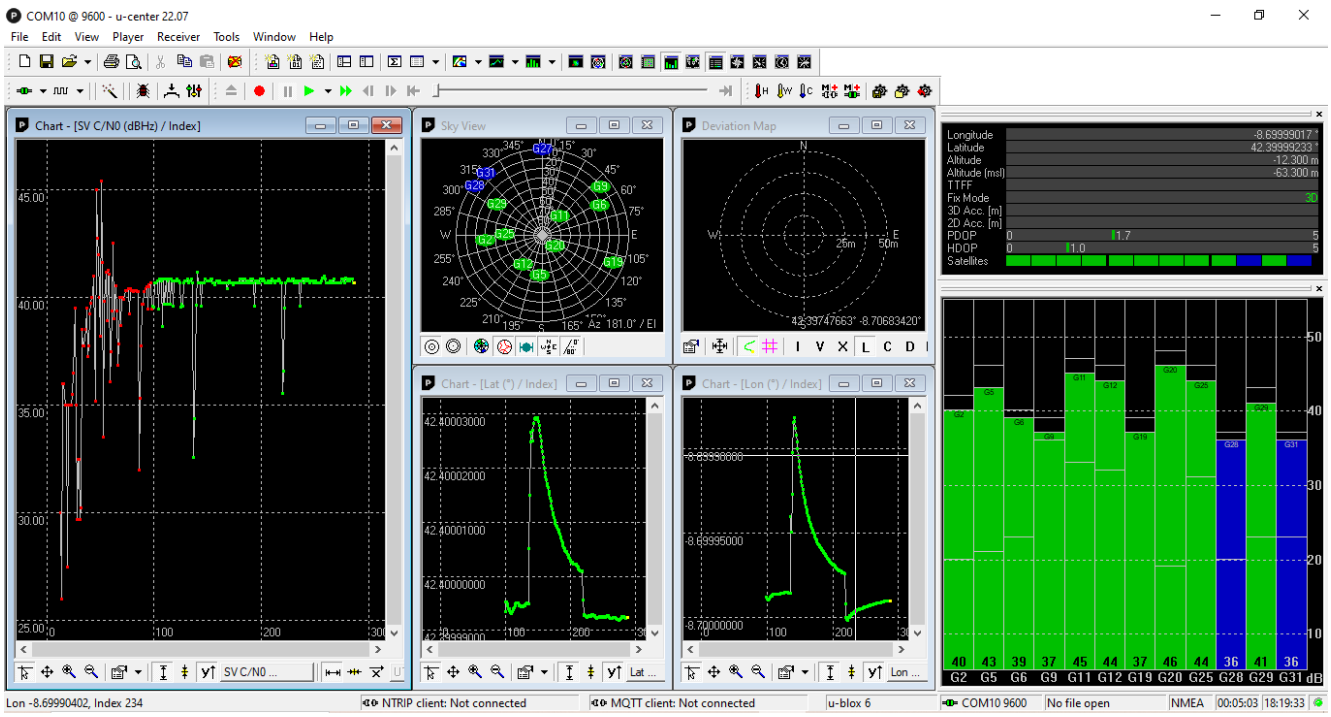

Figura 4-10 Validación generación y transmisión de señal válida por el NAM sin presencia de señal real. [Elaboración Propia]

En la Figura 4-10 se presentan los resultados obtenidos durante esta prueba. Destacar la mayor capacidad del NAM en el procesamiento de la señal y de la transmisión pues su módulo SDR es más avanzado que el del NAS. De hecho, puede apreciarse que es capaz de suplantar toda la constelación visible sin problemas y con relaciones señal a ruido superiores al NAS. Podría incluso deducirse que no son necesarios más nodos si se poseen los equipos de los módulos que conforman el nodo de ataque maestro. No obstante, el añadir un mayor número de nodos no se hace por una cuestión de capacidad spoofer sino por hacer el sistema atacante más robusto y versátil, como se ha mencionado anteriormente.

Durante la prueba se trasmite la señal correspondiente a 13 satélites, dos de ellos no usados para los cálculos de posición por encontrarse a una elevación insuficiente, generalmente por debajo de los 5º. Se aprecia una gran estabilidad en la relación señal a ruido media tras el enganche del receptor a esta señal.

4.1.5 Suplantación de señal GPS (spoofing) mediante sistema multiestático

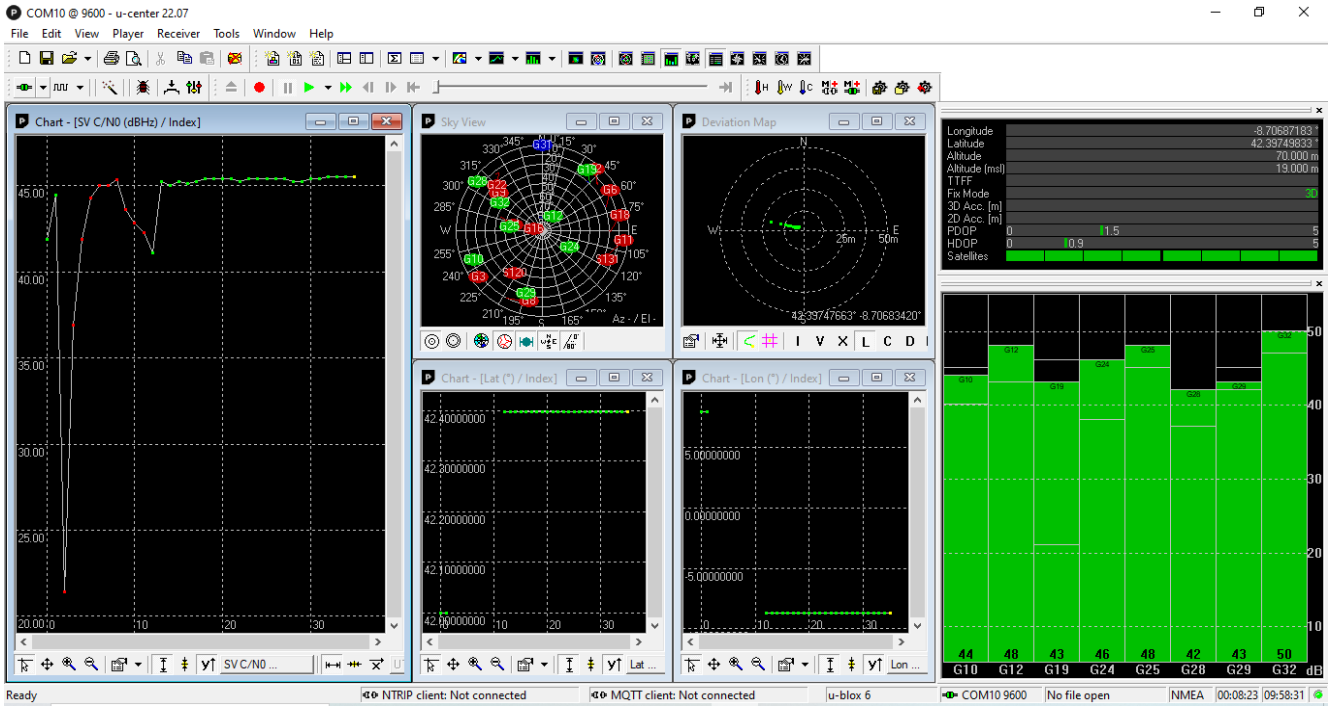

Figura 4-11 GPS víctima anclado a señal real. [Elaboración Propia]

Durante la prueba definitiva del sistema y tras repetir en numerosas ocasiones el intento de suplantar de forma efectiva la señal real GPS, se realizan modificaciones de potencia en la señal spoofer, pues se llega a la conclusión que la señal falsa debe ser ligeramente superior para romper el anclaje a la señal real y ser más "atractivas" para el receptor. En la Figura 4-11 se presenta el anclaje del receptor GPS víctima a la señal real de la constelación GPS, puede apreciarse una SNR general bastante estable de una constelación de 8 satélites que llega con bastante potencia.

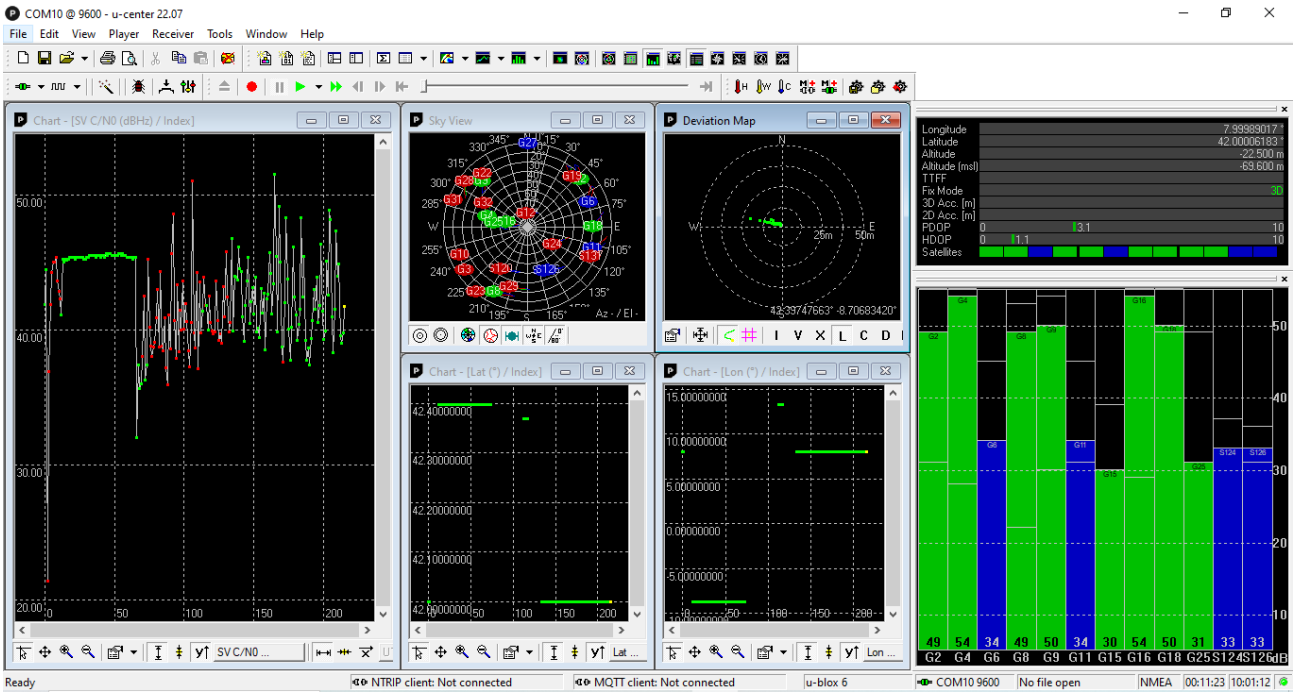

Figura 4-12 GPS víctima anclado a señal spoofer. [Elaboración Propia]

Una vez iniciado el ataque se puede detectar en la gráfica de la SNR de la Figura 4-12 un cambio en la tendencia (verde) de la señal real con el cambio de color a rojo y una gran fluctuación de la relación señal a ruido, lo que indica que ha perdido la señal real. Esta fluctuación continúa, aunque se puede apreciar que se vuelve de color verde, lo que quiere decir que la señal es tomada por el receptor víctima como verdadera y utilizada para los cálculos de posición, es decir, que es adquirida por el receptor GPS víctima. Se invita a comparar la Figura 4-11 y la Figura 4-12 y se verá que la posición de los satélites ha cambiado, lo que es lógico pues la posición del receptor "ha cambiado" y sobre ella, la disposición de la constelación visible es diferente.

A continuación, se observarán las variaciones de algunos parámetros durante el ataque, como pueden ser la diferencia de SNR entre los satélites reales y los que son suplantados. La Figura 4-13 muestra las SNR de los satélites de la señal real para la posición en la que se encuentra el receptor GPS víctima que como se puede leer en el cuadro rojo es 42,39744317º N y 8.70688200º W, además de otros datos como es el caso de la altura. Se destaca que las SNR de los satélites son relativamente parecidas, encuadradas en un intervalo pequeño, hecho que no pasará durante el ataque de suplantación.

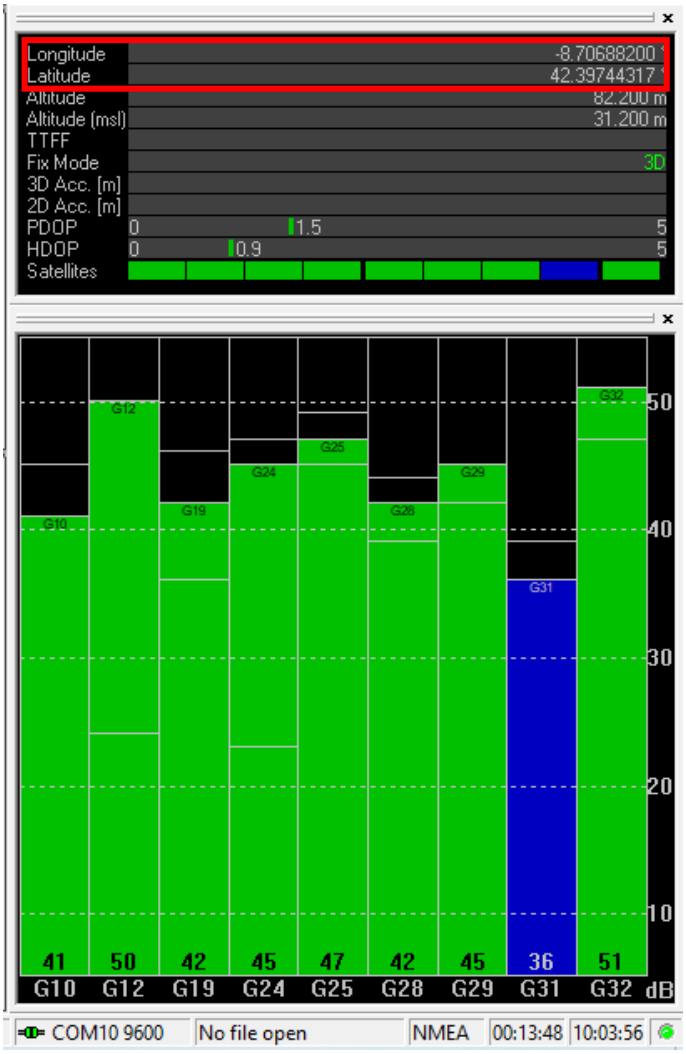

Figura 4-13 Satélites de la señal real antes de la suplantación. [Elaboración propia]

Como se ha mencionado previamente, la señal de la suplantación debe ser más potente que la real, realidad que puede observarse con claridad en la Figura 4-14, donde se diferencian los satélites que son suplantados, con un valor de la relación señal a ruido mayor, de los que se continúa recibiendo la señal real. En este caso los satélites suplantados se corresponden con los números de PRN 02, 04, 08, 09 y 18 que sobresalen sobre aquellos que no son suplantados.

Se observa pues, que aquellos que son señales falsas aparecen en verde, es decir, el receptor GPS víctima toma su señal como verdadera y el resto aparecen de color azul, lo que indica que su señal se considera errónea o al menos no válida para el cálculo de la posición "real", pues el receptor ha sido engañado completamente.

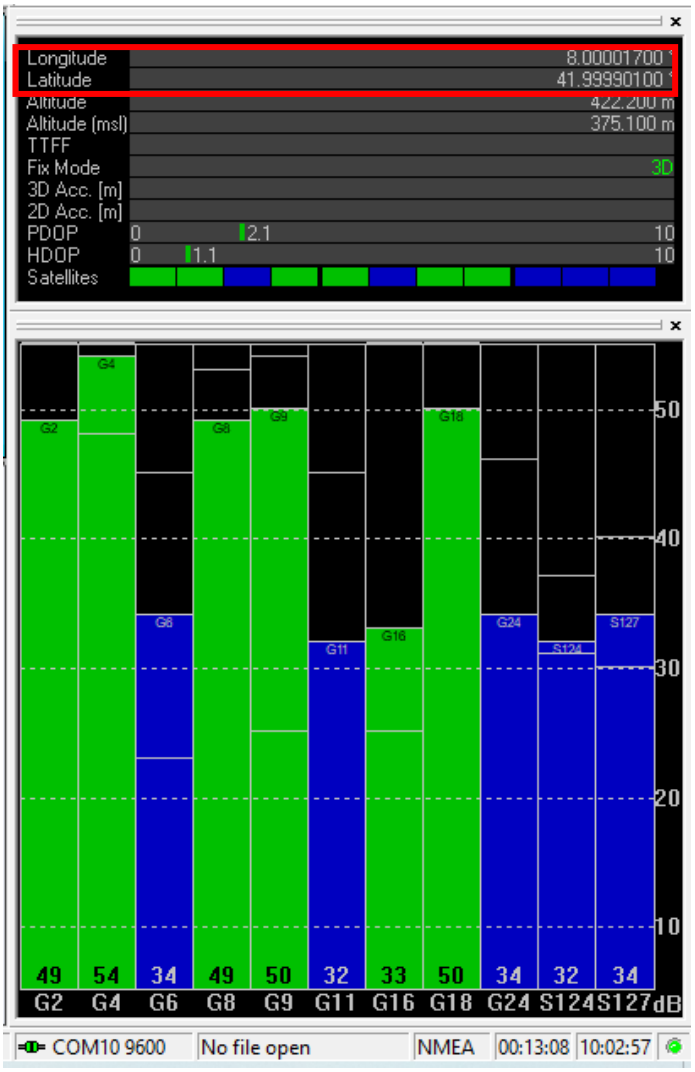

Figura 4-14 Satélites recibidos por GPS víctima durante la suplantación. [Elaboración Propia]

El análisis de la relación portadora a ruido (CNR) media de la señal GPS que capta el receptor GPS víctima permite detectar cambios de patrón en la recepción de las señales, ver cuando el receptor pierde la señal real o cuando se ancla a la señal suplantadora. La Figura 4-15 muestra la variación de la SNR durante toda la prueba. El eje de abscisas representa el tiempo en segundos y el de ordenadas la CNR en decibelios. Se observa que, tras unos segundos de adquisición de la señal, la CNR se estabiliza en una recta de color verde hasta el segundo 60 aproximadamente. En este punto comienza el ataque que hace que el receptor pierda la adquisición y seguimiento de la señal real, obsérvese en la amplia fluctuación de la CNR y la pérdida de la señal GPS señalada con el color rojo de los puntos de la gráfica.

La fluctuación continúa, pero cambia de color a verde alrededor del segundo 140, lo que indica que se ha anclado efectivamente a la señal suplantadora. Sin embargo, en este caso ocurre algo fuera de lo normal y es que la señal no se estabiliza como debería o como es el caso de la señal real. Este efecto se achaca a que el receptor no descarta del todo la señal que recibe de la constelación real y, por

tanto, aunque toma la falsa como verdadera sigue teniendo en cuenta la señal que recibe de los satélites reales de alguna manera, y aunque no los usa para el cálculo de la posición, generan conflicto en dicho cálculo y los tiene en cuenta para la media de la relación señal a ruido. Puede verse en la Figura 4-12, la Figura 4-13 y la Figura 4-14 que hay alguno de los satélites con un nivel de CNR correspondiente a la señal real que siguen usándose para el cálculo y que pueden generar esta anomalía. Es el caso del 15 y 25 en la primera y el 16 en la segunda.

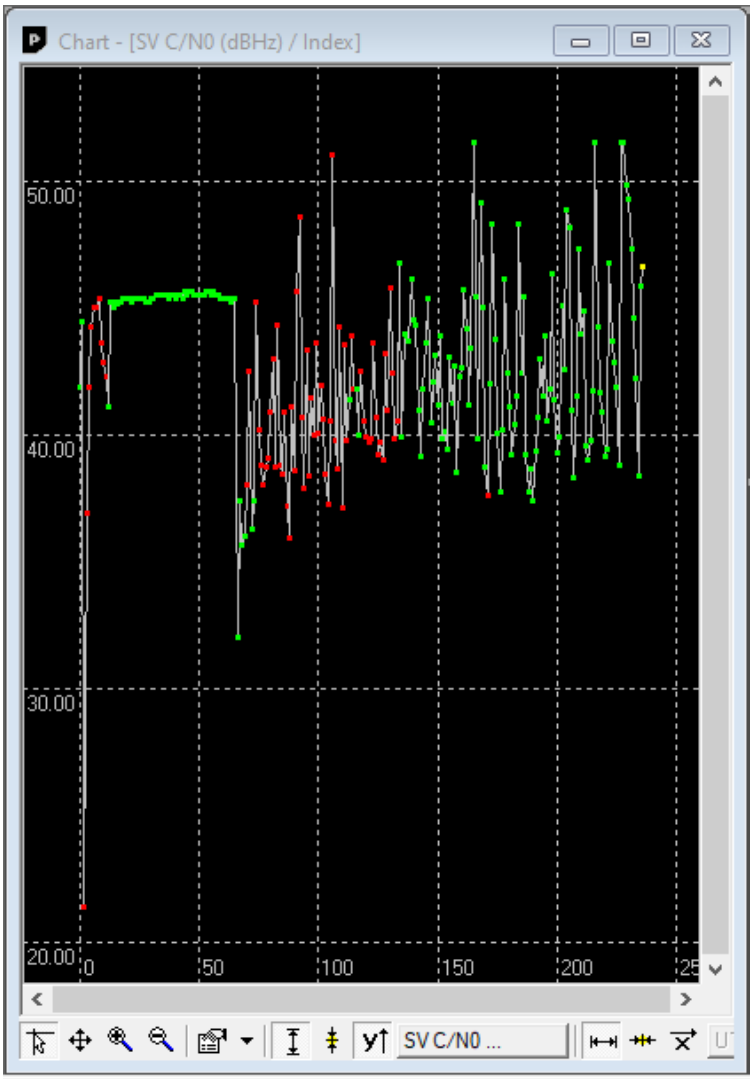

Figura 4-15 Variación de la CNR antes y durante la suplantación de la señal GPS. [Elaboración Propia]

La mayor prueba de la suplantación efectiva de la señal GPS real se aprecia en la Figura 4-16, donde se ofrece la latitud y longitud registrada durante toda la prueba. En ella se ven dos claras posiciones estables y diferenciadas separadas por ese periodo transitorio en que el receptor pierde la señal real hasta que se adquiere la señal falsa. La latitud pasa de 42,4º N a 42º N y la longitud de 8,7º W a 8º E. Cabe destacar la distancia tan grande con la que se consigue confundir al receptor GPS pues resolviendo el problema del triángulo esférico se obtiene una distancia entre posiciones de alrededor de 1321 km.

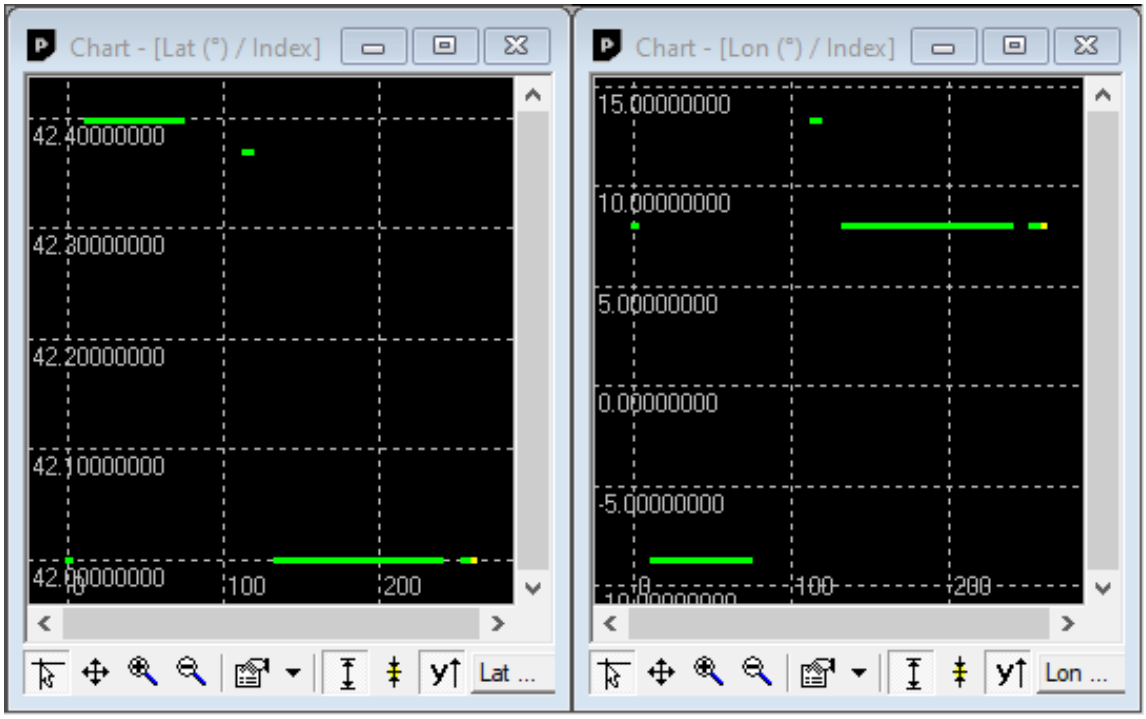

Figura 4-16 Variación de latitud y longitud antes y durante la suplantación de la señal GPS [Elaboración Propia].

Finalmente, y tras varias pruebas en diferentes escenarios se comprueba si el sistema puede enfrentarse a varios ataques consecutivos. También que, tras el primer ataque, en el que puede tardar más la rotura del seguimiento de la señal real y la adquisición de la señal suplantadora, el segundo ataque es mucho más rápido debido a que la memoria del receptor GPS víctima tiene esa señal falsa, que había adquirido en el primero, guardada y la vuelve a reconocer como útil y verdadera.

En la Figura 4-17 se expone el momento de adquisición de la señal falsa transmitida, como se puede apreciar en las gráficas de latitud y longitud, en las que el salto es evidente. Si se observa con detenimiento el "*Deviation Map*", pueden verse dos puntos verdes separados entre sí alrededor de 625 metros, ambos dos factores demuestran que el ataque ha sido efectivo.

En este caso, el ataque se ha diseñado de manera más realista y el cambio de posición es mucho menor, lo que ha llevado a concluir que cuanto menos ilógicos sean los cambios en los parámetros de la señal suplantadora respecto a la señal real, más fácil y rápido será que el receptor GPS víctima adquiera la señal falsa como verdadera.

La posición inicial y verdadera es la misma que en el resto de las pruebas, pues la antena de la víctima no varía su disposición en ningún momento. Esto es 42,39744317º N y 8.70688200º W aproximadamente. La posición de la suplantación en esta ocasión es 42,4º N y 8,7º W. Una variación pequeña comparada con el anterior ejemplo expuesto pero que puede tener consecuencias catastróficas en un lugar angosto como son las Rías Baixas donde se realizan las pruebas.

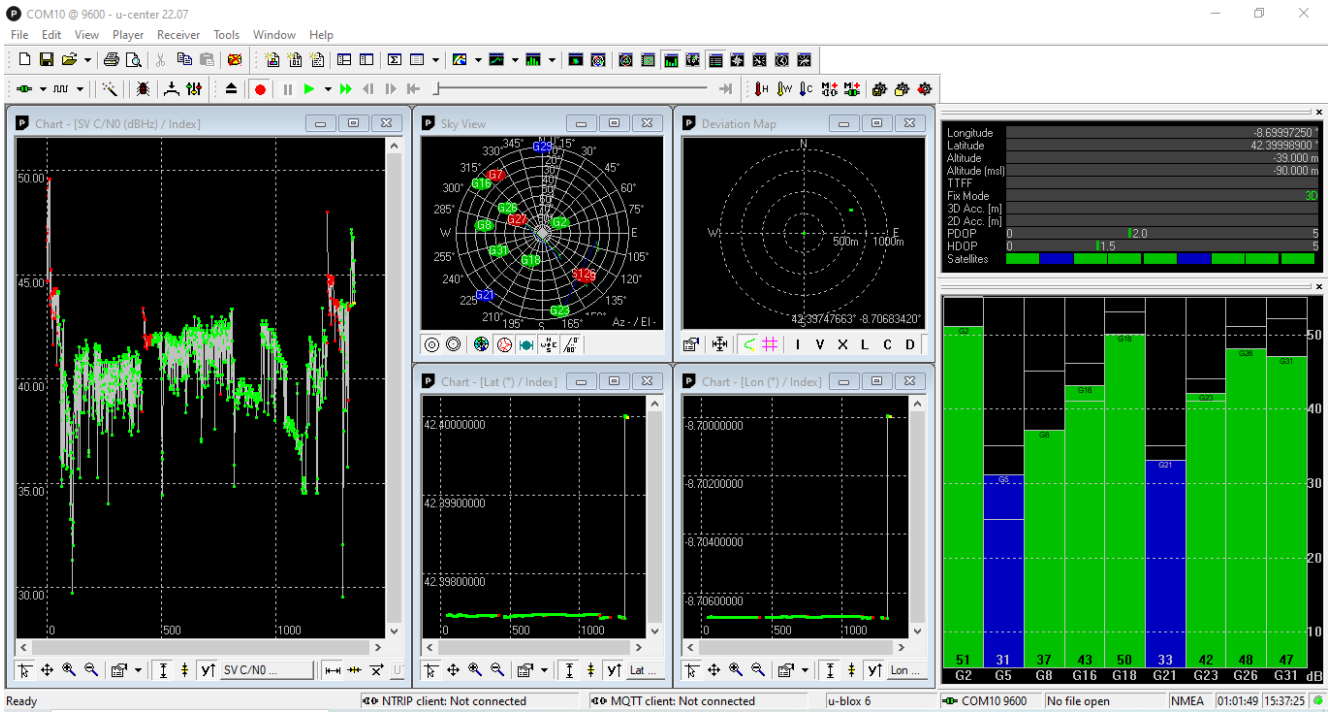

Figura 4-17 Momento de la adquisición de la señal suplantadora. [Elaboración Propia]

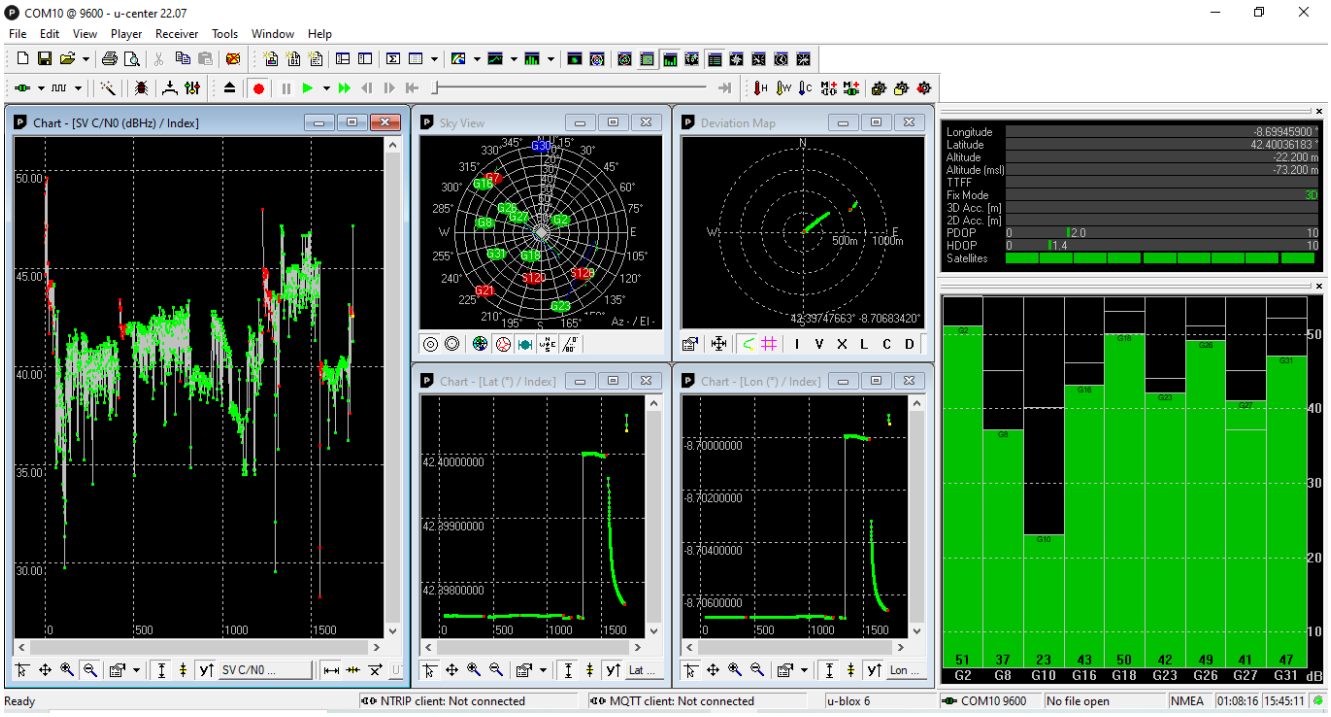

Figura 4-18 Segundo ataque consecutivo. [Elaboración Propia]

Para comprobar la respuesta del receptor GPS víctima a un ataque consecutivo al primero, se detiene el ataque y el receptor adquiere de nuevo la señal real de los satélites de la constelación visible. Puede apreciarse en las gráficas de latitud y longitud de la Figura 4-18, donde se puede observar la estabilización de latitud y longitud en la posición falsa y tras un corte, tanto latitud como longitud muestran una tendencia descendente hasta alcanzar la latitud y longitud inicial y verdadera.

Esta tendencia se debe a que, para el receptor víctima, no ha existido un cambio "violento" en la señal como en el caso del ataque. En este caso va corrigiendo la posición con la señal verdadera recuperada, de ahí esa gráfica descendente.

Se observa además en esta misma Figura 4-18 que el nuevo ataque es efectivo casi de inmediato, adquiriendo la señal spoofer pocos segundos después de perder la real. Hecho que puede apreciarse mejor en la Figura 4-19 donde se presenta la relación entre la relación señal a ruido en decibelios en el eje de ordenadas y el tiempo en segundos en el eje de abscisas.

En esta figura (Figura 4-19) se han marcado diferentes elementos que son de utilidad a la hora de valorar, validar y analizar los ataques de suplantación llevados a cabo por el sistema multiestático desarrollado. En color azul, se han marcado los dos periodos de tiempo en los que el receptor GPS víctima ha perdido el seguimiento de la señal GPS real hasta que ha adquirido la señal spoofer. Puede detectarse claramente que la diferencia de tamaño, es decir, de tiempo, es significativa. Esto se debe principalmente a que los receptores GPS disponen de medidas para evitar en lo posible ataques o perturbaciones indeseadas y entre ellas está la memoria de datos por la cual, señales poco correlacionadas con la que le llegaban en los momentos previos son desechadas, o se tarda mucho tiempo en adquirirlas. Por esto en el segundo ataque la señal ya no es considerada desconocida, sino que el receptor la reconoce como una posición lógica, ya que hacía poco tiempo que la había registrado.

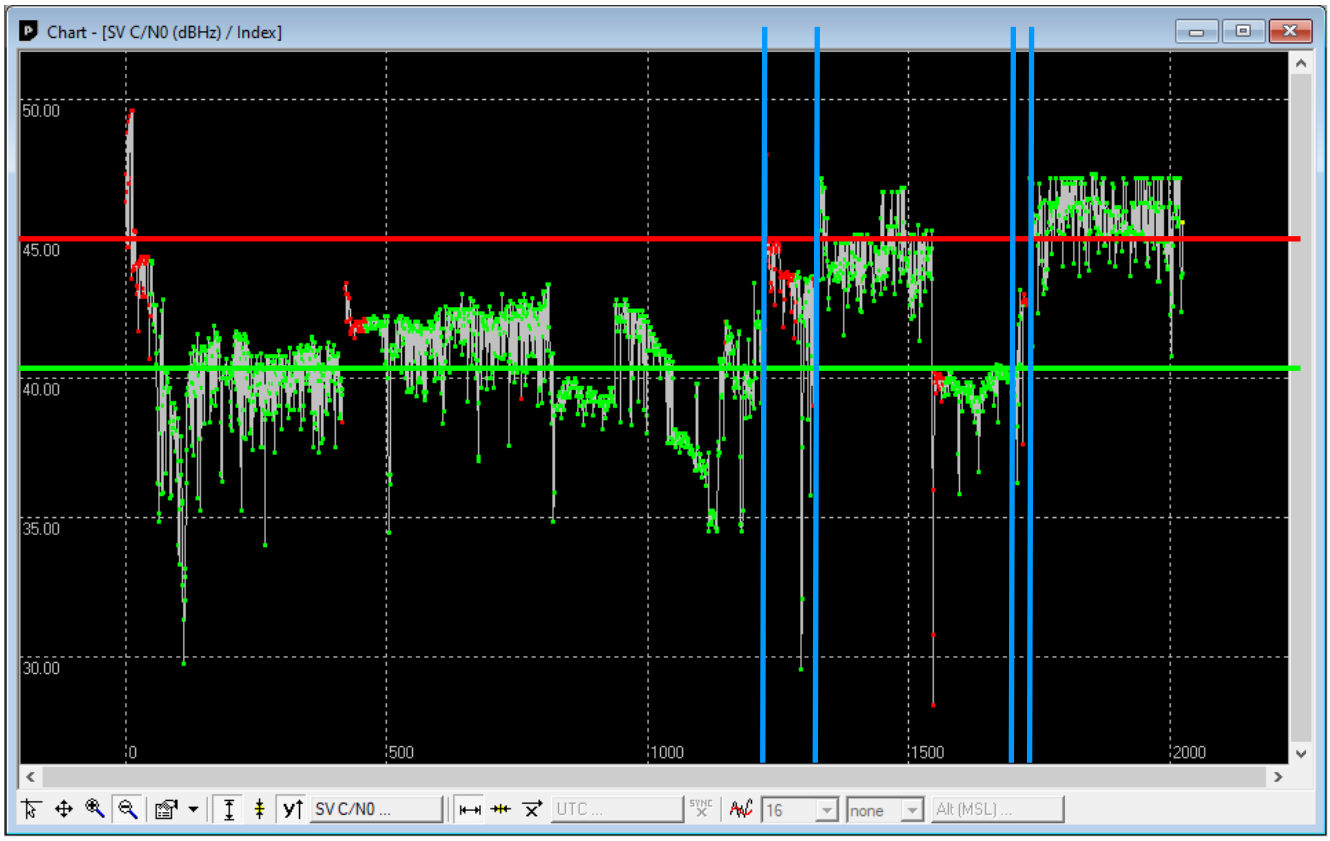

Figura 4-19 Análisis de la CNR de dos ataques consecutivos. [Elaboración Propia]

Los otros elementos marcados en la Figura 4-19 son las medias de relación portadora a ruido de ambas señales, la verdadera en color verde y la de suplantación en color rojo. Puede, por tanto, tomarse como referencia estos niveles de CNR para distinguir los periodos en los que el receptor tiene adquirida la señal real de aquellos en los que tenga adquirida la señal spoofer.

Se advierte que la relación portadora a ruido de la señal spoofer es alrededor de 5 dB mayor que la de la señal verdadera, lo cual es lógico, ya que la señal que pretende suplantar a la señal GPS verdadera debe romper el seguimiento de esta. Esto solo puede llevarse a cabo si la señal spoofer tiene un nivel de potencia mayor que la hace más "atractiva" para el receptor pues la recibe con mayor nivel de señal. 5 dB, además, es una diferencia adecuada para un ataque efectivo y no excesiva que pueda saturar el receptor GPS.

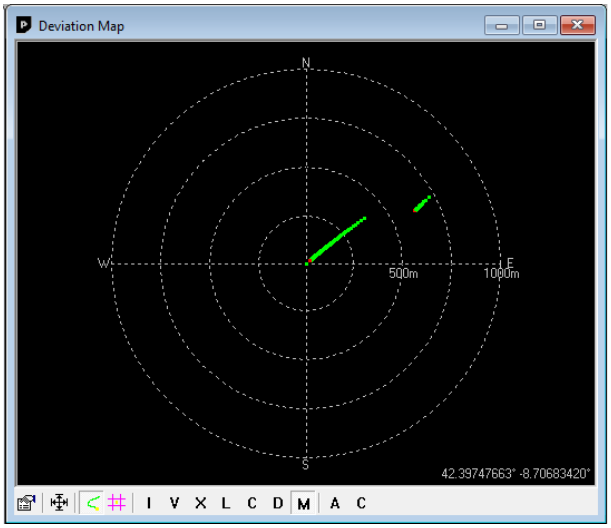

Figura 4-20 Separación entre la posición real y la señal falsa. [Elaboración Propia]

Por último, se analiza el mapa de desviación que demuestra el cambio de posición del receptor GPS víctima en la Figura 4-20. Se pueden observar dos estelas distintas, separadas entre si sus puntos finales sobre 625 metros. Que es la separación que existe entre ambas posiciones.

La forma de estela viene dada por la corrección de la señal falsa, por parte del receptor, una vez detenido el primer ataque. Así pues, quedan diferenciadas ambas posiciones, centrado el mapa de desviación en la situación inicial. La estela superior y de menor tamaño corresponde con la posición inducida por la señal spoofer, la más larga y centrada es la que corresponde con la señal GPS real.

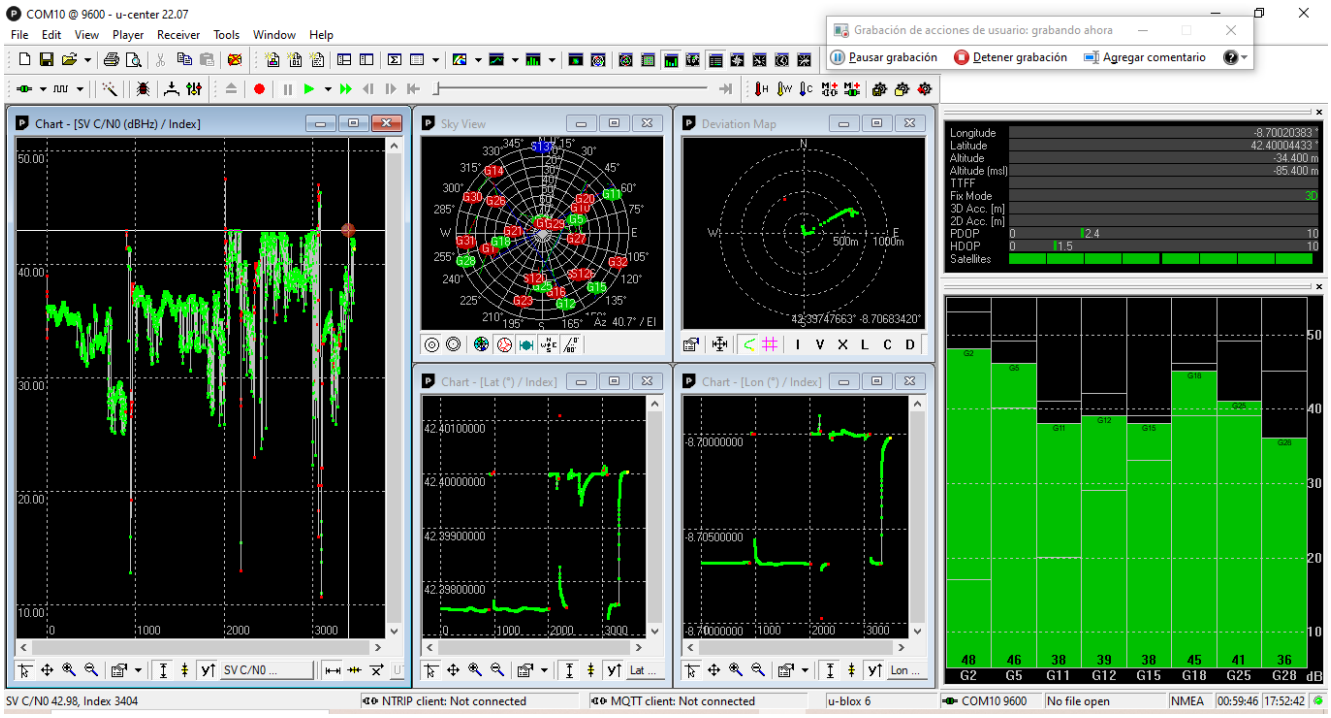

Figura 4-21 Ataques coordinados mediante sistema multiestático con suplantación efectiva. [Elaboración Propia]

Para finalizar se realiza una prueba de ataque en un escenario prolongado con una duración de alrededor de una hora. Donde se alternan periodos de adquisición y seguimiento de la señal GPS real, con ataques coordinados de ambos nodos, NAM y NAS. Queda patente en la Figura 4-21 que la calidad de los ataques mejora sustancialmente comparado con aquellos realizados exclusivamente con uno de los dos nodos.

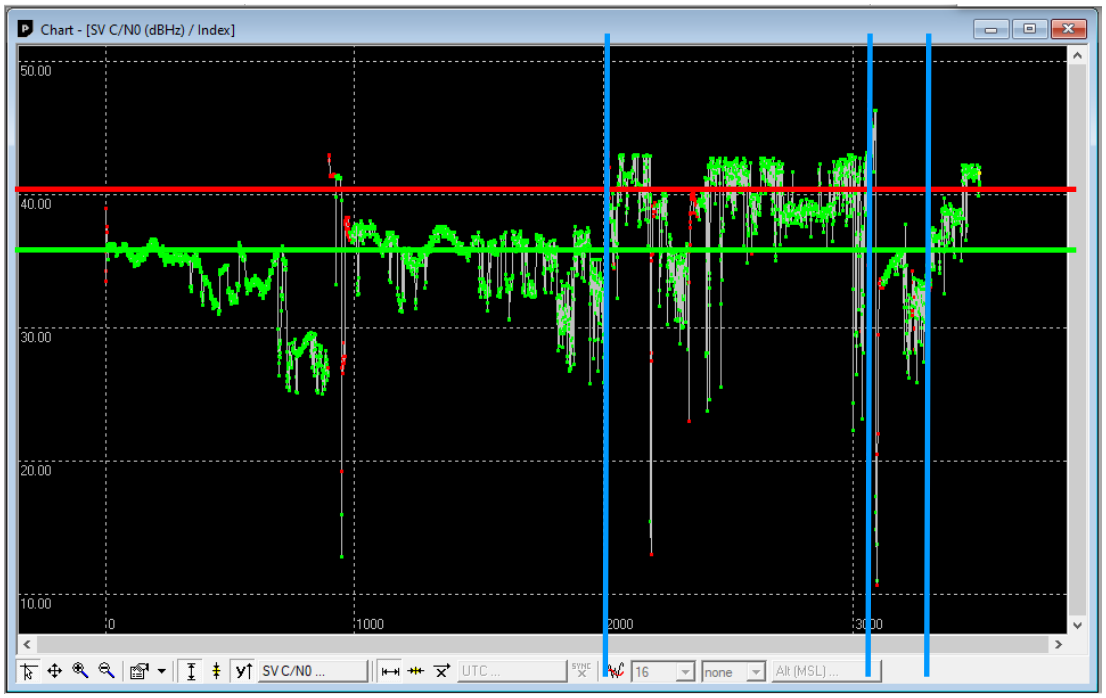

Figura 4-22 Variación de la relación portadora a ruido (CNR) durante los ataques de suplantación. [Elaboración Propia]

Analizando la variación de la relación portadora a ruido (eje de ordenadas en decibelios) respecto al tiempo (eje de abscisas en segundos), se observa que la duración del seguimiento a la señal real, con un valor medio de alrededor de 35 dB y marcada con una línea de color verde en la Figura 4-22, es de cerca de 35 minutos, aunque se aprecia un descenso antes de los 1000 segundos, punto en que hay un corte en la señal. Esto se explica como un intento fallido de ataque, que únicamente logra aumentar el ruido y por tanto bajar la CNR de la señal real, pero sin lograr la adquisición de la señal de suplantación por parte del receptor GPS víctima. Se toma la decisión de hacer un reinicio en frío o "*cold start*" para comprobar que la señal spoofer era adquirible por el receptor. De ahí el corte y discontinuidad de la gráfica.

Sin embargo, la señal de ataque no es adquirida por el receptor GPS, como era esperable. Por el contrario, vuelve a ser la señal real la que es adquirida. Tras comprobar los parámetros del ataque en ambos nodos se advierte que la ganancia del NAS está muy por debajo de la ganancia de la señal real. Tras realizar las correcciones en la configuración del ataque, se espera durante 15 minutos para generar un escenario difícil para el ataque, pues la información de los satélites de la constelación real está asentada y es más completa pues ha sido descargada de los mensajes de almanaque, que aportan información más precisa.

Finalmente, a los 2000 segundos se realiza el segundo ataque (señalado en la Figura 4-22 con la primera línea azul), y al poco tiempo es efectivo, adquiriendo, el receptor GPS víctima, la señal spoofer relativamente rápido y con una facilidad mayor a la esperada. Resaltar que los niveles de ganancia no son exageradamente altos (lo que generaría saturación en el receptor GPS), pues como se

aprecia la señal spoofer tiene una media de 40 dB (señalada la media con una línea roja), es decir, alrededor de 5 dB más que la señal real.

Tras un periodo de seguimiento de la señal de suplantación, se detiene el ataque, el receptor víctima recupera la señal GPS verdadera y el nivel de CNR vuelve a bajar hasta los niveles que rondan los 35 dB. Minutos después se lanza un segundo ataque y se observa, de nuevo, en la Figura 4-22 un aumento de la CNR.

Durante varios minutos se mantiene la señal suplantada y se detiene de nuevo el ataque. El periodo entre las dos líneas azules de la derecha en la Figura 4-22, supone el acaecimiento más interesante del trabajo y que permite extraer conclusiones. En este se permite la adquisición y seguimiento de la señal GPS real de nuevo y se ejecuta un tercer ataque. Esta vez, la adquisición de la señal spoofer y por tanto la suplantación es prácticamente inmediata. Podemos concluir que de algún modo el receptor GPS tiene en cuenta posiciones grabadas en un corto plazo que le permiten dirimir si las señales que le llegan son lógicas o no.

Por tanto, en el trascurso de estos tres ataques se extraen las siguientes conclusiones definitivamente:

- La ganancia de la señal que pretende suplantar la señal GPS real debe ser mayor que la propia señal GPS.
- El primer intento de ataque puede tardar excesivo tiempo o no llegar a ser efectivo si el receptor considera que la posición que le llega no es lógica comparándola con previas posiciones, considerar realizar los ataques spoofing tras un ataque de *jamming* que haga perder el seguimiento de la constelación real al receptor GPS puede aumentar la efectividad de los ataques notablemente.
- Una vez ha sido efectivo el ataque, de volver a realizarlo en un corto periodo de tiempo, la adquisición puede disminuir en tiempo, pudiendo llegar a ser prácticamente inmediata la adquisición de la señal de ataque.

En la Figura 4-23 se exponen las relaciones portadoras a ruido de los diferentes satélites por separado, pueden apreciarse dos niveles diferentes. Uno más alto que ronda los 45 dB y otro más bajo entre 35 dB y 40 dB. Esto se debe a que los satélites son suplantados por dos equipos diferentes, a saber, el NAS y el NAM. Puede, por consiguiente, deducirse cuales son suplantados por el NAM de mayor ganancia: 2, 5, 18, 25 y 29 y cuales lo son por el NAS: 11, 12, 15, 23 y 26 con menor ganancia. Lo que permite afirmar que el sistema multiestático funciona.

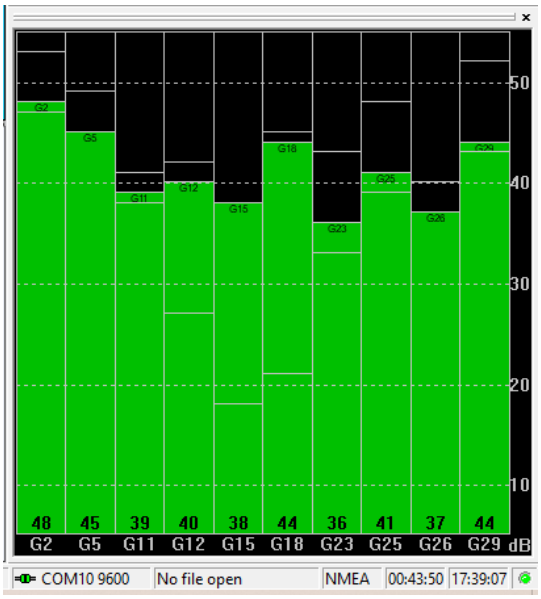

Figura 4-23 CNR de los satélites suplantados. [Elaboración Propia]

Los hitos expuestos en la Figura 4-22, pueden observarse también en la Figura 4-24, pues en esta se presentan las variaciones temporales (ordenadas en grados y abscisas en segundos) de la latitud y longitud durante el periodo del escenario de la prueba. Siendo los periodos con latitud 42,4º N y longitud 8,7º W los que corresponden con los ataques. Una prueba de la inmediatez del último ataque es que la señal no se llega a perder como en los anteriores, la posición simplemente es calculada y corregida como si el receptor GPS realmente realizase ese movimiento, pues sube de forma continua desde la latitud y longitud reales a las suplantadas. Por último, la Figura 4-25 recoge el registro de la posición relativa, centrada en la posición inicial (real), durante la duración de la prueba. En la que se aprecia que el cambio de posición, el desvío del receptor GPS víctima, ha sido de hasta 700 metros si tenemos en cuenta errores propios del cálculo de la posición tanto con la señal real o con la señal de ataque.

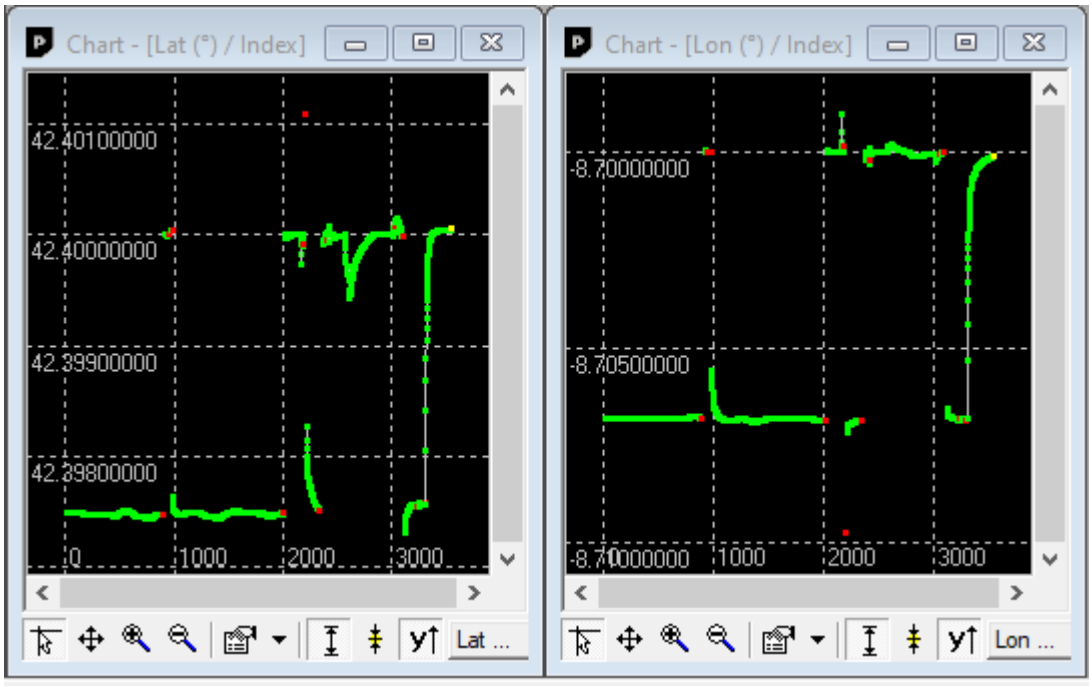

Figura 4-24 Variación de latitud (izquierda) y longitud (derecha) durante el ataque. [Elaboración Propia]

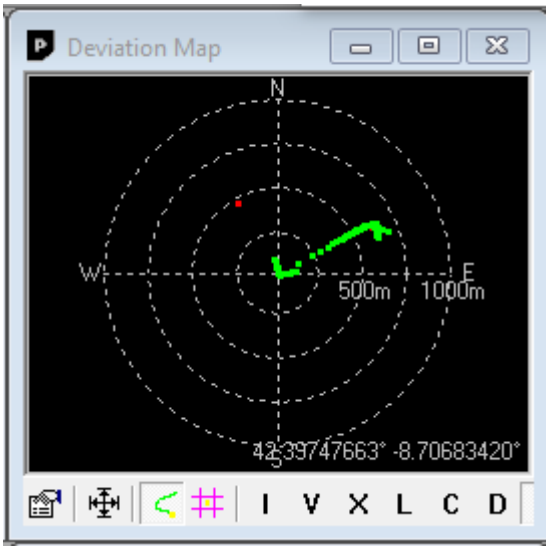

Figura 4-25 Variación de posición durante el ataque. [Elaboración Propia]

5 CONCLUSIONES Y LÍNEAS FUTURAS

5.1 Conclusiones

La dependencia actual de la sociedad a la tecnología es más que notable y significativa. La realidad es que una gran cantidad de servicios y modos de vida no serían posibles sin ciertas tecnologías que se dan por hechas y supuestas al haber estado presentes desde el inicio de la propia vida. El GPS y demás sistemas GNSS, especialmente, han pasado desapercibidos durante bastante tiempo porque a diferencia de otras tecnologías no han sufrido cambios significativos a nivel usuario desde su introducción al mercado civil. Sin embargo, es uno de los sistemas vitales para el modo de vida actual, las relaciones comerciales globales y el transporte entre otros.

La suplantación de GPS es relativamente sencilla y barata de llevar a cabo, sin embargo, durante el desarrollo de este sistema se ha podido comprobar que cada vez los receptores GPS tienen mayores medidas anti spoofing no sólo de reacción (una vez se está produciendo el ataque) sino sobre todo de prevención con algoritmos para evitar engancharse a la señal de una posición ilógica comparando con el registro de posiciones pasadas. Por tanto, los ataques de suplantación requieren de algo de tiempo hasta conseguir engañar al GPS víctima.

A pesar de todo durante la fase de validación se han extraído una serie de conclusiones que permiten aumentar el potencial de esta tecnología. Esto no es más que la realización de ataques combinados de *jamming* y spoofing, ya que esto permite forzar la desconexión del receptor víctima de la señal GPS real y que la adquisición de la señal falsa se produzca en unas condiciones en las que el receptor no tiene con que comparar y por tanto no encontrará ilógica la señal spoofer que es más fácilmente adquirida al llega con mayor potencia, como se puede ver en la Figura 5-1.

La realización de este Trabajo Fin de Grado ha permitido obtener unas nociones básicas sobre el funcionamiento del GPS y la posibilidad de realizar *spoofing* sobre la señal de este sistema de posicionamiento global por satélite, consiguiendo que un receptor tome una señal GPS falsa transmitida desde dos terminales distintos que suplantan satélites distintos como verdadera y deseche la señal emitida realmente por la constelación de satélites GPS.

El objetivo principal del trabajo presentado en el apartado 1.2 ha sido satisfecho al haberse desarrollado un sistema multiestático que puede suplantar la señal del GPS mediante un reparto dinámico de la constelación visible de satélites y la configuración de los parámetros del ataque spoofing.

Para el desarrollo de este sistema ha sido necesaria la documentación e investigación sobre sistemas que a priori pudiese pensarse que no tienen relación con la suplantación de la señal GPS y que, sin embargo, han permitido desarrollar este sistema multiestático con nodos relativamente

autónomos que se comunican entre sí. Además, ha sido fundamental contar con conocimientos de trigonometría esférica para resolver el problema de la división acimutal del espacio.

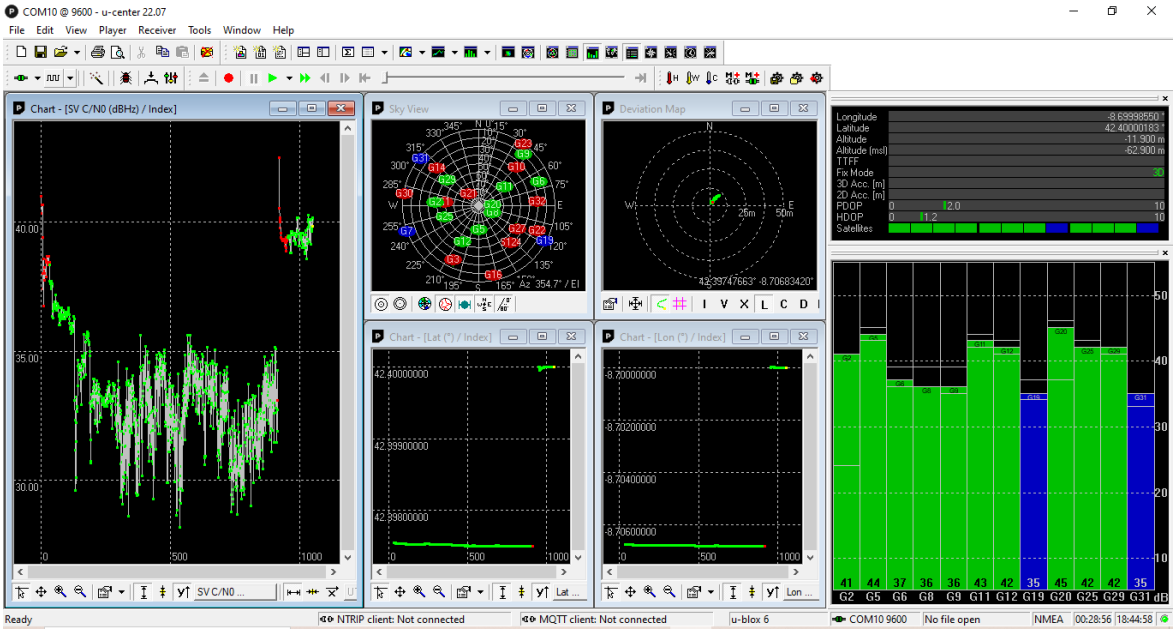

Figura 5-1 *spoofing* tras la simulación de un ataque *jamming*. [Elaboración Propia]

Se puede apreciar durante todo el trabajo que la dificultad en suplantar y mucho más negar la señal del GPS es relativamente baja si se tiene en cuenta que existen multitud de programas con capacidad de spoofing al alcance de cualquiera en internet y que realmente son necesarios equipos económicamente al alcance de todos. Lo que convierte esta tecnología en un modo barato y sencillo de cometer actos ilícitos o de gran impacto.

Las dificultades que se han presentado durante la realización de este trabajo fin de grado principalmente han sido:

La cantidad de equipos disponibles y especialmente el uso de modelos o equipos diferentes para la realización de tareas iguales o similares en los distintos nodos de ataque. Por ejemplo, el uso de distintos SDR o receptores GPS lo que ha supuesto un esfuerzo mayor en la conexión e interoperabilidad de estos equipos, teniendo que desarrollar diferentes funciones o modos de operación en los diferentes nodos.

El descubrimiento, una vez avanzado el trabajo, de que la Raspberry Pi que estaba siendo utilizada carecía de la capacidad necesaria de procesamiento para el programa Spoofer. Hecho que ha tenido que ser subsanado con su sustitución por otra Raspberry Pi de un modelo diferente y una capacidad superior.

En conclusión, el desarrollo de este trabajo fin de grado ha permitido al autor descubrir el mundo de los sistemas GNSS y la programación en Python además de aprender a desenvolverse en el entorno Linux del que era, prácticamente, desconocedor. Por ello puede decirse que ha tenido un efecto muy positivo en cuanto al aprendizaje de múltiples disciplinas relacionadas o no con el GPS y en el desarrollo de la autonomía necesaria a la hora de realizar un trabajo de esta magnitud. Enfrentarse a problemas que resolver y encontrar las soluciones en mayor o menor medida acertadas han permitido al autor disfrutar del proceso de desarrollo de este trabajo fin de grado.

5.2 Líneas futuras

Tras el desarrollo de un sistema multiestático para suplantar señales GPS se presenta un amplio abanico de oportunidades de explotación, mejora y evolución de este sistema. Además de la posibilidad de investigación de otras formas de explotación de esta tecnología o de implementación en

la Armada y sus unidades. Entre otras, se presentan las siguientes posibilidades de mejora y evolución del sistema:

- Implementación real de más de dos nodos de ataque mediante el desarrollo de un sistema de identificación de cada uno de ellos en las comunicaciones.

- Desarrollo de un sistema similar explotando otros sistemas GNSS o una conjunción de varios. Como el GLONASS ruso, el BeiDou chino o el GALILEO europeo.

- Desarrollo de un sistema multinodal dinámico en el que los nodos de ataque sean implementados sobre plataformas móviles como drones. Esta sería la línea ideal para la continuación de este trabajo fin de grado y que puede suponer una oportunidad real de crear un sistema con potencial para ser integrado como sistema de guerra electrónica y de NAVWAR en unidades de la Armada.

- Investigación y desarrollo de un sistema capaz de detectar ataques de suplantación de la señal GPS. Al poder usarse la investigación de sistemas de ataque spoofing con la finalidad de detectarlos e intentar evitarlos.

- Para la mejora del sistema desarrollado en este trabajo y que resultaría una posibilidad interesante sería la integración de alguna forma de un tercer actor que sería la posición de la víctima. En el entorno marítimo mediante, por ejemplo, trazas radáricas que permitiesen la división acimutal del espacio desde el propio receptor víctima y permitiese la disposición de los nodos de ataque (estáticos o dinámicos) de forma óptima para el reparto de la constelación visible y el ataque.

Fuera del ámbito académico y de investigación debe tenerse en cuenta la posibilidad de embarcar sistemas de suplantación de señales GPS, es decir, capacidad spoofing sobre GPS, en los buques y unidades de la Armada y otras unidades de las Fuerzas Armadas Españolas o Fuerzas y Cuerpos de Seguridad del Estado. Pues supone una herramienta económica y sencilla de manejar que permite al usuario de esta tecnología ejercer al enemigo la incapacidad sobre un sistema esencial para la navegación. No quizás en el caso de enemigos convencionales, que hacen uso de otros sistemas GNSS o de la versión militar y encriptada de estos sistemas, sino contra actores híbridos o del ámbito criminal que hacen uso de tecnología menos sofisticada de origen generalmente civil.

En esta dirección podría ser usada en el ámbito de las operaciones antipiratería como la Operación Atalanta en aguas del Océano Índico en la que el uso de receptores GPS civiles por parte de los piratas podría ser fácilmente contrarrestado mediante esta tecnología. O contra las actividades ilícitas de tráfico de estupefacientes, armas o personas en el ámbito marítimo pues en la mar la ausencia de puntos de referencia claros complica en gran medida la orientación sin sistemas de posicionamiento satélite.

En definitiva, puede llegar a ser una gran herramienta en el marco de las Operaciones de Seguridad Marítima (MSO) y escenarios de baja intensidad donde los sistemas GPS civiles no son adversario para sistemas potentes de negación o suplantación de señales GPS. Aunque no debe ser despreciado su potencial uso en escenarios de guerra convencional, donde numerosos sistemas de armas son guiados por GPS u otros sistemas GNSS, lo que podría hacer pensar en aplicaciones como la inhibición de la navegación de drones y vehículos no tripulados, desvío de misiles, aeronaves o unidades navales y la capacidad de negación de área en zonas como estrechos, fiordos, rías o pasos angostos.

6 BIBLIOGRAFÍA

[1] A. C. O'Connor *et al.*, «ECONOMIC BENEFITS OF THE GLOBAL POSITIONING SYSTEM (GPS)».

[2] I. N. Fernández, «NAVWAR. LA GUERRA EFICAZ DEL MENOS PODEROSO», *Rev. Gen. Mar.*.

[3] «GPS: The Global Positioning System». https://www.gps.gov/ (accedido 18 de enero de 2023).

[4] E. D. Kaplan y C. J. Hegarty, *Understanding GPS: principles and applications.*, Second Edition. Artech House, 2006.

[5] Mollaiyan, R. Santerre, y R. J. Landry, «Acquisition of Weak Signals in Multi-Constellation Frequency Domain Receivers», *Positioning*, vol. 4, pp. 144-152, ene. 2013, doi: 10.4236/pos.2013.42014.

[6] S. Locubiche-Serra, G. Seco-Granados, y J. A. López-Salcedo, «Performance assessment of a low-complexity autoregressive Kalman filter for GNSS carrier tracking using real scintillation time series», nov. 2022, doi: 10.13039/501100003329.

[7] R. Ferre, «Analysis of GNSS replay-attack detectors exploiting unpredictable symbols», 2018. doi: 10.5281/zenodo.3479303.

[8] «2020-SPS-performance-standard.pdf». Accedido: 30 de diciembre de 2022. [En línea]. Disponible en: https://www.gps.gov/technical/ps/2020-SPS-performance-standard.pdf

[9] «2007-PPS-performance-standard.pdf». Accedido: 30 de diciembre de 2022. [En línea]. Disponible en: https://www.gps.gov/technical/ps/2007-PPS-performance-standard.pdf

[10] *An Introduction to GNSS, GPS GLONASS, BeiDou, Galileo and other Global Navigation Satellite Systems*, Second Edition. Calgary, Alberta, Canada: NovAtel Inc., 2015.

[11] L. A. Salles, B. C. Vani, A. Moraes, E. Costa, y E. R. de Paula, «Investigating Ionospheric Scintillation Effects on Multifrequency GPS Signals», *Surv. Geophys.*, vol. 42, n.º 4, pp. 999-1025, jul. 2021, doi: 10.1007/s10712-021-09643-7.

[12] «Spoofing y jamming sobre los GNSS», *INCIBE-CERT*, 9 de julio de 2020. https://www.incibe-cert.es/blog/spoofing-y-jamming-los-gnss (accedido 26 de enero de 2023).

[13] P. Sokolenko, «Types of GNSS Spoofing | GPSPATRON.com», *GPSPATRON*, 26 de marzo de 2020. https://gpspatron.com/types-of-gnss-spoofing/ (accedido 4 de enero de 2023).

[14] *Types of basic GNSS spoofing attack scenarios*, (27 de septiembre de 2020). Accedido: 4 de enero de 2023. [En línea Video]. Disponible en: https://www.youtube.com/watch?v=5Mw-NKy1BOM

[15] *Coherent and non-coherent GPS spoofing in a live demo*, (6 de octubre de 2020). Accedido: 4 de enero de 2023. [En línea Video]. Disponible en: https://www.youtube.com/watch?v=Ws76xfJc1Pg

[16] «Hackeo de señales GPS en todo el mundo por parte de Rusia – Centro de Estudio Grl Mosconi». https://www.fie.undef.edu.ar/ceptm/?p=3922 (accedido 1 de febrero de 2023).

[17] «AboveUsOnlyStars-Report.pdf». Accedido: 31 de enero de 2023. [En línea]. Disponible en: https://c4ads.org/wp-content/uploads/2022/05/AboveUsOnlyStars-Report.pdf

[18] S. Ragan, «Reports Say U.S. Drone was Hijacked by Iran Through GPS Spoofing», *SecurityWeek*, 18 de diciembre de 2011. https://www.securityweek.com/reports-say-us-drone-was-hijacked-iran-through-gps-spoofing/ (accedido 12 de febrero de 2023).

[19] «Study maps "extensive Russian GPS spoofing"», *BBC News*, 2 de abril de 2019. Accedido: 17 de enero de 2023. [En línea]. Disponible en: https://www.bbc.com/news/technology-47786248

[20] «Russia denies role in Israeli airport GPS jamming», *BBC News*, 27 de junio de 2019. Accedido: 17 de enero de 2023. [En línea]. Disponible en: https://www.bbc.com/news/technology-48786085

[21] Marmer, «Interferencias GPS Mediterráneo Este | Bitácora – webmar.com». https://www.webmar.com/archives/12233 (accedido 30 de enero de 2023).

[22] C. D. V. López, «Suplantación de GPS -», 27 de febrero de 2020. https://www.revistaejercitos.com/2020/02/27/suplantacion-de-gps/ (accedido 30 de enero de 2023).

[23] J. M. Núñez Ortuño, «II Seminario de NAVWAR-MOPS Experiencia en la utilización de spoofers en la Armada», MOPS, noviembre de 2022.

[24] Armada, «Finalizan los ejercicios OTAN NEMO TRIALS-22, liderados por la Armada en el Golfo de Cádiz - Noticias de la Armada - Armada - Ministerio de Defensa - Gobierno de España». https://armada.defensa.gob.es/ArmadaPortal/page/Portal/ArmadaEspannola/conocenosnoticias/prefLang-es/00noticias--2022--11--NT-113-FINNEMO-es?_selectedNodeID=5345088&_pageAction=selectItem (accedido 22 de marzo de 2023).

[25] M. N. O. Sadiku y C. M. Akujuobi, «Software-defined radio: a brief overview», *IEEE Potentials*, vol. 23, n.º 4, pp. 14-15, oct. 2004, doi: 10.1109/MP.2004.1343223.

[26] M. A. M. Quimbita y C. E. P. Salvador, «Evaluación de pasarela LoRa/LoRaWAN en entornos urbanos».

[27] «GPS Sentences | NMEA Sentences | GPGGA GPGLL GPVTG GPRMC». https://www.rfwireless-world.com/Terminology/GPS-sentences-or-NMEA-sentences.html (accedido 11 de febrero de 2023).

[28] «Arduino Shield featuring LoRa® technology». https://www.dragino.com/products/lora/item/102-lora-shield.html (accedido 16 de febrero de 2023).

[29] «Arduino UNO | Arduino.cl - Compra tu Arduino en Línea», 14 de enero de 2019. https://arduino.cl/arduino-uno/ (accedido 16 de febrero de 2023).

[30] R. P. Ltd, «Buy a Raspberry Pi 3 Model B», *Raspberry Pi*. https://www.raspberrypi.com/products/raspberry-pi-3-model-b/ (accedido 16 de febrero de 2023).

[31] R. P. Ltd, «Raspberry Pi 4 Model B specifications», *Raspberry Pi*. https://www.raspberrypi.com/products/raspberry-pi-4-model-b/specifications/ (accedido 9 de marzo de 2023).

[32] «CDDIS | | Data and Derived Products | GNSS | broadcast ephemeris data». https://cddis.nasa.gov/Data_and_Derived_Products/GNSS/broadcast_ephemeris_data.html (accedido 5 de marzo de 2023).

[33] C. de navío Moreu Curbera y C. de navío Martínez Jiménez, *Primer Curso de Naútica*, 3ª Edición., vol. 1, 3 vols. Vigo, 1987.

[34] C. de navío Moreu Curbera y C. de navío Martínez Jiménez, *Segundo Curso de Naútica*, 3ª Edición., vol. 2, 3 vols. Vigo, 1987.

[35] «2020-civil-monitoring-performance-specification.pdf». Accedido: 30 de diciembre de 2022. [En línea]. Disponible en: https://www.gps.gov/technical/ps/2020-civil-monitoring-performance-specification.pdf

[36] *3. GP-Simulator. Time Manipulation*, (1 de mayo de 2022). Accedido: 17 de enero de 2023. [En línea Video]. Disponible en: https://www.youtube.com/watch?v=gKl0ln195_Q

[37] *2. GP-Simulator. Spoofing multi-constellation GNSS receiver*, (10 de abril de 2022). Accedido: 17 de enero de 2023. [En línea Video]. Disponible en: https://www.youtube.com/watch?v=quj0ASw2iOk

[38] *1. GP-Simulator Intro. SDR-based GPS spoofing resilience testing tool*, (4 de abril de 2022). Accedido: 17 de enero de 2023. [En línea Video]. Disponible en: https://www.youtube.com/watch?v=zL-u_BAb9ps

[39] «tecnicas_neutralizacion_drones_galileo.pdf». Accedido: 12 de febrero de 2023. [En línea]. Disponible en: https://www.fundacionayesa.org/wp-content/uploads/2017/03/tecnicas_neutralizacion_drones_galileo.pdf

[40] D. Carmena Cabanillas, «GNSS para aplicaciones críticas en entornos de transporte», septiembre de 2020. https://oa.upm.es/67491/ (accedido 9 de marzo de 2023).

[41] «Institute for the Study of War», *Institute for the Study of War*. http://dev-isw.bivings.com/ (accedido 13 de marzo de 2023).

[42] G. C. Von Clausewitz, *De la guerra*, 1.ª ed. Barcelona: Ediciones Obelisco, 2015.

[43] S. B. Liddell Hart, *Estrategia*, 1.ª ed. Madrid: Arzalia Ediciones, 2019.

ANEXO I: IMPLICACIONES SOCIALES, ECONÓMICAS Y AMBIENTALES

La investigación en este campo de la tecnología permite obtener una serie de conclusiones en mayor o medidas sorprendentes que afectan a los ámbitos social y económico si bien no casan excesivamente con el ambiental, por ser el impacto de esta tecnología prácticamente nulo en el medio ambiente.

Como se desarrolla en el Anexo II: Reflexiones Éticas y Sociales, existen numerosas consecuencias negativas del libre uso de esta tecnología con fines lucrativos o dolosos. Dejando los aspectos éticos para el mencionado anexo, se centra el tiro en aquellas de carácter social y económico.

El espectro posible de ataques de *spoofing* sobre GPS es tan amplio que se repasan estas implicaciones desde un enfoque generalista. Y se asumirá que el fin último del ataque es absolutamente negativo sin tener en cuenta aquellas ocasiones que pueda usarse de forma legítima por las autoridades competentes para ello.

La principal implicación social del uso extensivo de la tecnología *spoofing* GPS es la pérdida de confianza por parte de los usuarios hacia la tecnología GPS y por extensión a otros sistemas GNSS como ya ha ocurrido con otras tecnologías cuya fiabilidad o seguridad se ha visto comprometida. Evidentemente esto tiene su efecto en la economía pues numerosas empresas viven de la tecnología GPS de alguna u otra forma. A mayores de la gran cantidad de servicios públicos o privados que dependen actualmente de los sistemas GNSS. Y la sociedad no está preparada para perder la capacidad de posicionarse de forma tan precisa.

Esta pérdida de confianza cobra mayor importancia si pensamos en ella desde un punto de vista judicial. El posicionamiento por GPS u otros sistemas GNSS son actualmente una fuente importante de pruebas tanto inculpatorias como exculpatorias para demostrar la estancia o permanencia de los actores involucrados en un crimen por la presencia de dispositivos relacionados con estos mismos actores. Imaginemos que, precisamente haciendo uso de la suplantación de señales GPS, puedan generarse coartadas o pruebas falsas que son tomadas como verdaderas en un juicio penal. Las consecuencias pueden ser catastróficas pues las pruebas obtenidas del posicionamiento mediante GPS de estos dispositivos dejarían de tener validez y no podrían usarse en el enjuiciamiento criminal.

Sin embargo, el impacto económico puede llegar a ser aún mayor precisamente por la gran cantidad de comercio, transporte y tecnología que dependen de los sistemas GNSS. Las pérdidas millonarias que puede generar el desvío de un barco de mercancías que haga retrasar la fecha de llegada el puerto de destino multiplicado por ese 90 % del transporte que se hace por mar y sumado a ese uso extensivo del *spoofing* GPS, puede colapsar irremediablemente la economía global con las innumerables consecuencias humanitarias y de suministro que esto puede llegar a suponer. Para relativizar la magnitud de las perdidas, por ejemplo, el colapso de una semana del Canal de Suez por el accidente del buque portacontenedores Evergreen supuso en pérdidas una media de 10.000 millones de dólares diarios. A lo que hay que sumar la subida de precios por los problemas de suministros que ocasionó. Imagínese pues el escenario de un uso extensivo del *spoofing* de GPS teniendo en cuenta estas cifras.

Pero, y esto es más preocupante si cabe, la capacidad de realizar *spoofing* sobre GPS y en extensión todo tipo de ataques sobre todos los sistemas GNSS, es relativamente barata con el daño que puede llegar a hacerse. Lo que puede suponer un problema aún mayor pues hace que la capacidad de hacer *spoofing* esté al alcance de prácticamente cualquiera. Si tenemos en cuenta que tener un

ordenador, que no requiere una gran capacidad, en propiedad es lo usual en la sociedad actual, una inversión de menos de 200 euros permite realizar *spoofing* GPS de forma efectiva. Si bien para realizarlo a gran escala es necesaria tecnología y medios más caros.

Deben, pues, tenerse en cuenta estas implicaciones socioeconómicas a la hora de la publicación de trabajos de investigación que puedan permitir un uso inadecuado de esta tecnología, razón por la cual no se hará público el código del programa desarrollado para no fomentar o ayudar a la realización de actos en contra de la legalidad y con un posible impacto negativo tan grande en la economía y sociedad.

ANEXO II: REFLEXIONES ÉTICAS Y SOCIALES

Desde el principio de los tiempos las tecnologías no han estado necesariamente asociadas al bien o al mal. Es el uso que se hace de ella lo que las convierte en dañinas o malignas. Por tanto, no es el objeto sino el uso lo que convierte una determinada tecnología, ciencia o investigación en algo éticamente cuestionable o socialmente nocivo.

También se da el caso de que la posibilidad de alcanzar un bien que se cree mayor nuble la capacidad de discernimiento o de búsqueda de posibles males que pueda conllevar determinada tecnología. Problema actualmente presente en la tecnología de modificación y diseño genético. No se duda que la investigación en este campo de la ciencia no esté motivada por la más alta y noble de las intenciones y, sin embargo, puede acabar con la humanidad tal y como la conocemos. La sólo posibilidad de poder diseñar nuestra descendencia a la carta podría tener la capacidad de abrir una brecha todavía mayor entre los estratos económicos de la sociedad. Lo sano, inteligente, atractivo o fuerte que nazca un niño dependerá de la capacidad económica de sus padres. Es un ejemplo claro de como una tecnología diseñada y alcanzada para solucionar problemas de salud, evitar el sufrimiento y muerte se convierte en el motivo máximo de desigualdad que sin duda acabaría con la sociedad tal y como la conocemos. Pero ¿debemos pues abandonar una capacidad por los efectos negativos que pudieran derivarse de su uso? Por supuesto que no, de hecho, la respuesta está en la misma pregunta, "de su uso", lo que debe hacer la sociedad es velar porque se de buen uso de la ciencia y de la tecnología.

El *spoofing* GPS por el contrario no tiene esa repercusión positiva en la sociedad como tecnología pues su función no es otra que el engaño, la suplantación de un servicio oficial y público para la consecución de objetivos de dudables consecuencias. Como forma de engaño, es en sí mismo un atentado contra uno de los principios básicos de la ética, la verdad. Esta falta a la verdad concretamente puede tener efectos catastróficos que pueden ser explotados por usuarios con fines delictivos. El *spoofing* GPS permite falsificar posiciones que los dispositivos receptores se piensan verdaderas, y que actualmente tienen validez como prueba judicial, lo que podría permitir la creación de falsas coartadas para la realización de actos criminales.

El GPS y otros sistemas de posicionamiento global por satélite son utilizados extensivamente en los sistemas de seguridad de bases militares, instalaciones gubernamentales o infraestructura crítica. Principalmente para hacer frente a las amenazas de los drones. Actualmente los drones comerciales llevan incorporado de serie un registro de áreas por las que no pueden volar estos vehículos autónomos y si se intenta, el propio aparato no entrará en esa zona que tiene prohibida. Mediante el GPS *spoofing* esta medida de seguridad puede ser fácilmente ignorada, pues para el dron, no se estará violando ese espacio aéreo no autorizado.

Es en el sector de la navegación marítima y aérea, sin embargo, donde las consecuencias del uso del GPS *spoofing* pueden alcanzar las magnitudes más graves. Imagínense desviar la trayectoria de un buque mercante con la subsecuente pérdida económica millonaria que supondría o la catástrofe que supondría desviar aeronaves o buques de pasajeros en términos de vidas humanas.

Consecuentemente ante un uso generalizado de esta tecnología, se produciría una peligrosa socavación de la confianza en la tecnología GPS y de aquella que depende de los sistemas de navegación global por satélite por parte de la sociedad.

En definitiva, siendo un ataque tecnológico orientado contra usuarios de este sistema. ¿Por qué entonces considerarlo como una opción a investigar, por qué desarrollar esta capacidad si el objetivo es exclusivamente negativo?

La realidad es que la sociedad en que vivimos no es ideal y, si bien el hombre no es violento por naturaleza en su individualidad, sí que lo es en su colectividad. Las relaciones interpersonales dentro de la sociedad y entre los diferentes grupos que se conforman dentro de la humanidad tienen y deben tener un componente de violencia. Desde que el hombre se ha organizado de alguna forma en aquellas tribus primitivas (casi manadas animales) hasta las más complejas sociedades contemporáneas la violencia, los conflictos y las guerras ya fuese entre individuos o grupos de individuos han formado parte de la historia de nuestra especie. Nos guste o no es parte de nuestra naturaleza social y como lo define el teórico de la guerra, el General prusiano Carl Von Clausewitz, *"La guerra es, pues, un acto de fuerza para obligar al contrario al cumplimiento de nuestra voluntad"*. Si nos paramos a pensar y tomamos esta definición de Von Clausewitz como válida, estamos en un permanente estado de guerra pues la fuerza, al igual que la violencia, no tiene que ser necesariamente física.

Hay quien dice que la historia de la guerra es la historia misma de la humanidad, es una realidad latente que aun hoy en día, a pesar del progreso y modernidad que pensemos que pueda tener nuestra organización social, está a la orden del día en un porcentaje del mundo que asusta. Efectivamente la historia de la guerra es la historia de la humanidad, principalmente, porque la guerra acelera los procesos de investigación tecnológica y científica, aunque en este caso con la finalidad del ejercer el mal al enemigo. Eh aquí la paradoja de cuanto se decía al principio. Pues la cuestión del uso también puede encontrar en esa tecnología nociva finalidades positivas.

Tratando de responder a la pregunta del porqué GPS *spoofing*, afirmaré que en el ámbito militar sí que tiene sentido la investigación de tecnologías que en el ámbito civil son éticamente incorrectas debido a que en estrategia militar deben explotarse todas las posibilidades que puedan suponer una ventaja frente al enemigo y el engaño, en este caso de la señal GPS, forma parte de estos. Decía Sir Basil Liddell Hart teórico de la guerra británico en su libro Estrategia: El estudio clásico sobre la estrategia militar que: *"Toda guerra se basa en el engaño."*

Este engaño en modo de suplantación sobre la señal GPS no es más que una herramienta que añadir a esos elementos que, bien explotados en el ámbito del conflicto armado, permiten obtener una ventaja táctica significativa sobre el enemigo. Y que mejoran las opciones de alcanzar los objetivos, no sólo ofensivos en el conflicto abierto sino también defensivos y de seguridad fuera de ellos. Si bien es cierto que es una actividad y tecnología que debe estar regulada convenientemente para que sólo actores autorizados tengan acceso a ella y hagan un uso adecuado de la misma con el fin de evitar esos problemas que se mencionaban al principio que pueden aparecer como consecuencia de un mal uso de esta tecnología.

En conclusión, no es una tecnología que deba utilizarse a la ligera o que deba estar al alcance de cualquiera, pues un uso indebido puede tener consecuencias nefastas para multitud de actores como fuerzas gubernamentales, el transporte marítimo y aéreo e incluso usuarios particulares. Razón, entre otras, por la cual no se implementará el código del programa en este Trabajo Fin de Grado.

ANEXO III: GLOSARIO DE SIGLAS Y TÉRMINOS

ADC: Analog-to-Digital Converter.

AFS: Atomic Frequency Standards.

ALMART: Almirante de la Fuerza de Acción Marítima.

ASCII: American Standard Code for Information Interchange.

BPSK: Binary Phase Shift Key.

C/A: Coarse Acquisition.

CDMA: Code Division Multiple Access.

CIA: Central Intelligence Agency.

CNR: Carrier-to-Noise Ratio (Relación Portadora a Ruido)

COMANDES-31: Comandante de la 31ª Escuadrilla de Superficie.

CPU: Central Processing Unit.

CUD: Centro Universitario de la Defensa.

DAC: Digital-to-Analog Converter.

DAERS: División Acimutal del Espacio y Reparto de Satélites.

DLL: Delay-Lock Loop.

DoS: Denial of Service.

DSP: Digital Signal Processor.

DSSS: Direct Sequence Spread Spectrum.

DUN: Demora de Unión de Nodo.

EASA: European Union Aviation Safety Agency.

EW: Electronic Warfare.

FEC: Forward Error Correction.

GALILEO: GNSS de la Unión Europea.

GLONASS: Global'naya Navigatsionnaya Sputnikovaya Sistema (GNSS ruso).

GNSS: Global Navigation Satellite System.

GPS: Global Positioning System.

HDMI: High-Definition Multimedia Interface.

I/Q: Amplitud y fase.

IoT: Internet of Things.

IRNSS: Sistema regional de posicionamiento satélite de la India.

LAN: Local Area Network.

LDC: Línea de División de Constelación.

LNAV: Legacy Navigational Message.

LoRa: Long Range.

LOS: Line of Sight.

MCS: Master Control Station.

MS: Monitor Station.

MSO: Maritime Security Operations.

NA: Nodo de Ataque.

NAM: Nodo de Ataque Maestro.

NAS: Nodo de Ataque Spoofer esclavo.

NASA: National Aeronautics and Space Administration.

NAVWAR: Navigation Warfare.

NCO: Numerical Controlled Oscillator.

NDU: Navigation Data Unit.

NEMO: Naval Electro-Magnetic Operations.

NIST: National Institute of Standards and Technologies.

NMEA: National Maritime Electronics Association.

OTAN: Organización del Tratado del Atlántico Norte

PLL: Phase-Lock Loop.

PM: Punto medio.

PNT: Posición, Navegación y Tiempo.

PPS: Precise Positioning Service.

PRN: Pseudo-random Noise.

PVT: Positioning, Velocity and Time.

QZSS: Sistema regional de posicionamiento satélite de Japón.

RAM: Random Access Memory.

SCA: Semi-Constelación Asignada.

SD: Secure Digital (memoria de almacenamiento)

SDR: Software Defined Radio.

SNR: Signal-to-Noise Ratio (Relación Señal a Ruido)

SPS: Standard Positioning Service

TACAN: Tactical Air Navigation System.

TLM: Telemetry.

TOA: Time of Arrival

UHF: Ultra High Frequency.

UNCTAD: Conferencia de las Naciones Unidas sobre Comercio y Transporte

URA: User Range Accuracy.

USAF: United States Air Force.

USB: Universal Serial Bus.

USSF: United States Space Force.

UTC: Universal Coordinated Time.

VIP: Very Important Person.