Universidad Zaragoza
1542

Trabajo Fin de Grado

SISTEMA DE CONTRAMEDIDAS ELECTRÓNICAS DE SEÑAL GPS BASADO EN SDR

José Antonio Ortiz Sánchez

Director académico: Eva Tresaco Vidaller

Director militar: Carlos Manuel Esteban Artero

Centro Universitario de la Defensa-Academia General Militar

2022

Agradecimientos

Todo el apoyo recibido para hacer posible este Trabajo de Fin de Grado no merece menos que una pequeña, pero muy importante mención. El trabajo individual aquí presente es un simple reflejo de todo lo aprendido gracias a la exquisita formación recibida en la Academia General Militar.

Pero las competencias aquí presentes no provienen de un mero esfuerzo individual si no que tienen su origen en la dedicación a lo largo de estos cinco años de todos los profesores, tanto civiles como militares, siempre comprometidos con la educación universitaria y castrense.

En primer lugar, me gustaría resaltar el nombre de la directora académica de este trabajo: la Dra. Dña. Eva Tresaco Vidaller que en todo momento ha estado dispuesta a ayudar tanto a dar forma como a perfeccionar el trabajo, gracias a su experiencia se ha podido encauzar y dirigir todos los esfuerzos realizados de este proyecto.

También me gustaría mostrar mi agradecimiento al director militar: Tte. de Transmisiones D. Carlos Manuel Esteban Artero por su gran disponibilidad, esfuerzo y dedicación. Hacer extensivo este agradecimiento al resto de personal del Regimiento de Guerra Electrónica nº 31, no sólo por su ayuda técnica sino por su abnegada labor humana y por mostrarme los inmaculados valores de la Unidad.

No puedo dejar fuera de estas palabras de agradecimiento al Cap. D. Indalecio Cazorla Aguirre jefe de la sección de cuarto curso de Transmisiones de la LXXVII promoción, el cual nos ha inculcado, entre otros muchos valores, el afán de superación personal siempre enfocado al servicio al Ejército y sus unidades.

Por último, dar las gracias a mis padres ya que sin su esfuerzo, dedicación y ayuda constante no hubiese podido superar los numerosos retos de mi formación militar.

En Zaragoza, a 10 de enero de 2022

Firmado por ORTIZ SANCHEZ JOSE ANTONIO - ***0642** el día 10/01/2022 con un certificado emitido por AC FNMT Usuarios

CAC. TRS. D. José Antonio Ortiz Sánchez

RESUMEN

El uso masivo de los medios de navegación por satélite (GNSS) y más concretamente del GPS ha llevado a la sociedad actual a depender en demasía de este medio, pero esto no afecta únicamente al ámbito civil. En el ámbito militar, con el paso de los años también ha crecido la dependencia en este tipo de tecnologías, tanto en el mando y control de las unidades como en la conducción de la maniobra.

La señal GPS, debido a sus características, es un blanco fácil dentro del espectro electromagnético para lo que se conoce en el ámbito de la Guerra Electrónica (EW) como ataque electrónico (EA). La inutilización de esta tecnología podría ser crucial para las operaciones militares, por ello en este trabajo se desarrolla un sistema de contramedidas que actúa contra la banda de frecuencias del GPS mediante el uso de Software Defined Radio (SDR).

Se entiende por contramedida toda aquella acción destinada para paliar o anular otra. El sistema de contramedidas desarrollado en el presente trabajo tiene como objetivo anular la señal GPS de sistemas enemigos, mediante acciones de perturbación y decepción. Por ello es importante aclarar que el sistema de contramedidas tiene un carácter puramente ofensivo, es decir, no está diseñado para proteger los sistemas propios de ataques contra su señal GPS.

Para la realización de dicho sistema se ha optado por el uso de SDR por dos razones principales. La primera, debido a que existen medios SDR en dotación en las unidades de EW del Ejército y la segunda, debido a su facilidad de uso debido a que estos medios son configurables vía software.

En este trabajo se ha desarrollado un sistema capaz de realizar acciones de perturbación (jamming) y decepción (spoofing) sobre la señal GPS cuyas capacidades han sido puestas a prueba en diferentes prácticas contra diferentes tipos de receptores GPS. Se han obtenido, por lo tanto, resultados acordes a los objetivos planteados. Además, se han planteado posibles soluciones a sus limitaciones, por ejemplo, el ensamblaje de amplificadores y filtros de paso banda al sistema para aumentar su alcance efectivo o la posibilidad de aumentar la portabilidad del sistema usando ordenadores de placa base reducida.

PALABRAS CLAVE

GNSS, GPS, Software Defined Radio (SDR), contramedidas, Guerra Electrónica (EW).

ABSTRACT

The massive use of satellite navigation (GNSS) and more specifically of GPS has led today's society to depend too much on this means, but this does not only affect the civilian sphere. In the military field, dependence on this type of technology has also grown over the years, both in the command and control of units and in the conduct of maneuvers.

The GPS signal, due to its characteristics, is an easy target within the electromagnetic spectrum for what is known in the field of Electronic Warfare (EW) as electronic attack (EA). The disabling of this technology could be crucial for military operations, so in this project, a countermeasure system is developed that acts against the GPS frequency band by using Software Defined Radio (SDR).

Countermeasure is understood as any action designed to mitigate or cancel another action. The countermeasure system developed in this project aims to nullify the GPS signal of enemy systems by jamming and deception actions. Therefore, it is important to clarify that the countermeasure system has a purely offensive character, that is, it is not designed to protect own systems from attacks against their GPS signal.

For the implementation of this system the use of SDR has been chosen for two main reasons. The first one, due to the existence of SDR means in the Spanish Army EW units and the second one, due to its ease of use because these means are configurable via software.

In this project, a system capable of performing jamming and spoofing actions on the GPS signal has been developed whose capabilities have been tested in different practices against different types of GPS receivers. Therefore, results have been obtained in accordance with the proposed objectives. In addition, possible solutions to its limitations have been proposed, for example, the assembly of amplifiers and bandpass filters to the system to increase its effective range or the possibility of increasing the portability of the system using computers with a reduced motherboard.

KEYWORDS

GNSS, GPS, Software Defined Radio (SDR), countermeasures, Electronic Warfare (EW).

ÍNDICE DE CONTENIDO

Agradecimientos *2*

RESUMEN *3*

ABSTRACT *4*

ÍNDICE DE CONTENIDO *5*

ÍNDICE DE FIGURAS *7*

ÍNDICE DE TABLAS *9*

ABREVIATURAS, SIGLAS Y ACRONIMOS *10*

1. INTRODUCCIÓN *12*

1.1. MOTIVOS Y RAZONES DEL TRABAJO **12**

1.2. ÁMBITO DE APLICACIÓN **13**

1.3. ANTECEDENTES, ACTUALIDAD Y FUTURO **13**

1.4. CONCEPTOS CLAVE **16**

1.4.1. Los Sistemas GNSS 16

1.4.2. Software Defined Radio (SDR) 18

1.5. ESTRUCTURA DEL TRABAJO **19**

2. OBJETIVOS Y METODOLOGÍA *20*

2.1. OBJETIVOS Y ALCANCE **20**

2.2. METODOLOGÍA **21**

3. ANTECEDENTES Y MARCO TEÓRICO (ESTADO DEL ARTE) *22*

4. DESARROLLO: ANÁLISIS Y RESULTADOS *22*

4.1. ELEMENTO HARDWARE DEL SISTEMA SDR **22**

4.2. JAMMING **26**

4.2.1. Técnicas de Jamming 26

4.2.2. Puesta en práctica con SDR 28

4.3. SPOOFING **30**

4.3.1. Teléfono móvil 31
4.3.2. Radioteléfono ligero PR4G v3 33

4.4. SISTEMA FINAL 36
4.4.1. Validación del sistema desarrollado 37

4.5. MEJORAS SOBRE EL SISTEMA FINAL 40
4.5.1. Ganancia 40
4.5.2. Portabilidad 46

5. CONCLUSIONES 48

6. REFERENCIAS BIBLIOGRÁFICAS 49

Anexo I: Estación Mercurio 2000 53

Anexo II: Grupo de discusión 55

Anexo III: Información REW 31 57

Anexo IV: Instalación GNURadio 59

Anexo V: Instalación HackRF One en ordenador personal 60

Anexo VI: Introducción a GNURadio 64

Anexo VII: Proceso Spoofing 68

Anexo VIII: Radioteléfono ligero PR4G v3 (RT-9210 V3) 72

Anexo IX: Resultados práctica Sistema final 75

ÍNDICE DE FIGURAS

Figura 1: Espectro del código C/A de la señal GPS 17
Figura 2: HackRF One propiedad del REW31 23
Figura 3: Antena GPS banda L1 propiedad del REW31 23
Figura 4: Diagrama del sistema SDR 24
Figura 5: Modelado del HackRF en GNURadio 26
Figura 6: Espectro teórico de las diferentes técnicas analizadas 28
Figura 7: Diagrama Rx/Tx Jamming 28
Figura 8: Diseño en GNURadio de una barredora 29
Figura 9: Función sweeper (barredora) escrita en lenguaje Python sobre el editor Geany 29
Figura 10: Modelado P-AJ en GNURadio 30
Figura 11: Espectro protocol-aware jamming en GNURadio 30
Figura 12: App Google Maps mostrando la ubicación del ataque por spoofing 32
Figura 13: App GPS status buscando señal GPS 32
Figura 14: App GPS status con coordenadas del ataque por spoofing 32
Figura 15: Diagrama Rx/Tx spoofing a PR4G 33
Figura 16: Vista completa de ambas antenas 34
Figura 17: Base de antena Mercurio y antena del sistema SDR 34
Figura 18: PR4G v3 tras ataque spoofing 35
Figura 19: PR4G v3 con coordenadas de El Pardo (Madrid) 35
Figura 20: Sistema final 36
Figura 21: Prueba del Sistema final 37
Figura 22: Antena GPS USB modelo G-MOUSE 38
Figura 23: Ordenador personal mostrando ubicación simulada 38
Figura 24: Teléfono móvil mostrando coordenadas simuladas 39
Figura 25: Realización práctica con Sistema Final 2 40
Figura 26: Realización práctica con Sistema Final 1 40
Figura 27: Caso analizado en la práctica sobre el sistema final 41
Figura 28: Amp lna 41
Figura 29: Practica final con amp lna ensamblado en el sistema 42
Figura 30: Sistema final + amp lna 42
Figura 31: Sistema con amp ensamblado 43
Figura 32: Prueba del amplificador 43
Figura 33: Receptor para la prueba con amplificador 44
Figura 34: RTL-SDR recibiendo ruido 44
Figura 35: U-center 2 mostrando coordenadas originales de la práctica 45
Figura 36: U-center 2 tras la pérdida de las coordenadas originales 45
Figura 37: Filtro paso banda 46
Figura 38: Sistema final + amp lna + filtro 46
Figura 39: Raspberry Pi 3 modelo B+ 47
Figura 40: Sistema final con Raspberry Pi 47

Referente a los anexos:

Figura A. 1: Estación Mercurio 2000 sobre vehículo vamtac 53
Figura A. 2: Escudo de armas del REW 31, imagen obtenida de: 58
Figura A. 3: Vista aérea del acuartelamiento, imagen obtenida de: 58
Figura A. 4: Interfaz de trabajo de GNURadio 59
Figura A. 5: Interfaz Zadig 2.6 60
Figura A. 6: Instalación drivers en Zadig 61
Figura A. 7: Notificación de instalación 61
Figura A. 8: Interfaz SDR Console V3 62
Figura A. 9: Radio Definitions de SDR Console V3 62
Figura A. 10: Configuración ancho de banda en SDR Console V3 63
Figura A. 11: Programación receptor en GNURadio 64
Figura A. 12: Diagrama de bloques HackRF como RECEPTOR 64
Figura A. 13: HackRF en Rx 65
Figura A. 14: Detección de la emisión en el display de GNURadio 65

Figura A. 15: Walkie emitiendo 65
Figura A. 16: Display receptor GNURadio 65
Figura A. 17: Diagrama HackRF como emisor 66
Figura A. 18: Display GNURadio 66
Figura A. 19: Walkie en Rx 66
Figura A. 20: Programación TRANSMISOR en GNURadio 66
Figura A. 21: HackRF en Tx 67
Figura A. 22: Efemérides a descargar, imagen obtenida de 68
Figura A. 23: Captura de pantalla cmd (uso del comando cd) 68
Figura A. 24: Coordenadas elegidas (Portiragnes, Francia) 69
Figura A. 25: Explicación comandos gps-sdr-sim 69
Figura A. 26: Archivo generado por GPS-SDR-SIM 70
Figura A. 27: Resultados simulación de la constelación en cmd 70
Figura A. 28: Explicación comandos hackrf_transfer 70
Figura A. 29: Recepción con amplificador IF del HackRF a 10 dB 71
Figura A. 30: Recepción con amplificador IF del HackRF a 0 dB 71
Figura A. 31: HackRF conectado por cable coaxial a RTL-SDR 71
Figura A. 32: PR4G v3 en configuración portátil, sin GPS conectado 72
Figura A. 33: Elementos y accesorios PR4Gv3 (1) 74
Figura A. 34: Elementos y accesorios PR4Gv3 (2) 74

ÍNDICE DE TABLAS

Tabla 1: Códigos de las portadoras GPS 17
Tabla 2: Datos portadoras GPS 17
Tabla 3: Potencia de Tx HackRF 25
Tabla 4: Resultados en función de la variación de la ganancia (campo x) 32
Tabla 5: Resultados pruebas spoofing a PR4G v3 34
Tabla 6: Resultados práctica Sistema final 75

ABREVIATURAS, SIGLAS Y ACRONIMOS

AGT	Agrupación Táctica
amp	amplifier – amplificador
BB	base band – banda base
BEW I/31	Batallón de Guerra Electrónica I/31
BW	Ancho de banda
CAC	Caballero Alférez Cadete
Cap.	Capitán
CCAL	Centro de control de apoyo logístico
CE	Cuerpo de Ejército
cmd	Consola de comandos de Windows
CTPC	Centro de Transmisiones del Puesto de Mando
CTPCTAC	Centro de Transmisiones del Puesto de Mando Táctico
CUD	Centro Univesitario de la Defensa
DGPS	Differential GPS
DoD	Departamento de Defensa de los EEUU
EA	Ataque Electrónico
ECM	Contramedidas electrónicas
ED	Defensa Electrónica
EEUU	Estados Unidos de América
EPM	Electronic protection measures - Medidas de protección electrónica
EPM	Medidas de protección electrónica
ES	Vigilancia Electrónica
ESA	Agencia Espacial Europea
ESM	Medidas de apoyo electrónico
ESPFUN	Especialidad Fundamental
ET	Ejécito de Tierra
EW	Electronic Warfare - Guerra Electrónica
EWL	Guerra Electrónica Ligera
FUTER	Fuerza Terrestre
GLONASS	Global'naya Navigatsionnaya Sputnikovaya Sistema
GNSS	Global Navigation Satellite System – Sistema Global de Navegación por Satélite
GT	Grupo Táctico
GU	Gran Unidad
HF	High Frequency
HS	High Speed
IAI	Israel Aeroespace Industries
IEEE	Institute of Electrical and Electronics Engineers
IF	intermediate frequency – frecuencia intermedia
INTA	Instituto Nacional de Técnica Aroespacial
lna	low noise amplifier – amplificador de bajo ruido
MAM	Mando de Apoyo a la Maniobra
MATRANS	Mando de Transmisiones
Msps	Million simples per second – Millón de muestras por segundo
NASA	National Aeronautics and Space Administration

NAVSTAR-GPS	NAVigation System and Ranging - Global Position System
OAE	Órgano de Alta Especialización
P-AJ	Protocol-Aware Jamming
PC	Centro de Mando
PLMM	Plana mayor de mando
RETAC 21	Regimiento de Transmisiones Táctica nº 21
REW 31	Regimiento de Guerra Electrónica 31
RF	radiofrequency – radiofrecuencia
RT32	Regimiento de Transmisiones 32
Rx	Recepción
SBAS	Satellite-based augmentation system
SDR	Radio definida por Sofware, del inglés: Software Defined Radio
SIMACET	Sistema de Mando y control del Ejército de Tierra
SMA	SubMiniature version A
TRS	Transmisiones
TRS	Transmisiones
Tte.	Teniente
Tx	Transmisión
UAV	Vehículo Aéreo no tripulado, del inglés: Unmanned Aerial Vehicle
UAV	Unmanned Aerial Vehicle – Vehículo aéreo no tripulado
UEW II/31	Unidad de Guerra Electrónica II/31
UHF	Ultra High Frequency
URSS	Unión de Repúblicas Socialistas Soviéticas
vga	variable gain amplifier – amplificador de ganancia variable
VHF	Very High Frequency

1. INTRODUCCIÓN

El objetivo de este trabajo es el desarrollo de un sistema de contramedidas de señal GPS basado en Software Defined Radio (SDR). La palabra contramedida se define como cualquier medida que se toma para paliar o anular otra; especialmente, conjunto de sistemas destinado a neutralizar los dispositivos del enemigo. En este caso, el objetivo es cualquier sistema enemigo que dependa o utilice tecnología GNSS, como puede ser: navegación, posicionamiento/geolocalización de unidades, pilotaje remoto, etc. Se aclara así la finalidad ofensiva del sistema de contramedidas basado en SDR que en este trabajo se desarrolla, excluyéndose otras finalidades distintas de estas como, por ejemplo, detección o defensa contra este tipo ataques.

La introducción del trabajo se organiza en los subcapítulos que se detallan a continuación: (1) Motivos y razones del trabajo: en la que se explican las razones que justifican la realización del trabajo; (2) Ámbito de aplicación: explicando el usuario final destinado a explotar el sistema de contramedidas, además en este subcapítulo también se añaden algunos detalles importante sobre la unidad en la que se han realizado las práctica externas; (3) Antecedentes, actualidad y futuro: análisis de la línea temporal de la tecnologías de las que hace uso el sistema; (4) Conceptos clave: donde se desarrollan los términos esenciales base del sistema y del trabajo realizado, y finalmente, en el subcapítulo (5) Estructura del trabajo: se expone una vista general sobre todo el documento.

1.1. MOTIVOS Y RAZONES DEL TRABAJO

En primer lugar, es importante tener en cuenta que la creación de un sistema de contramedidas como el desarrollado en este trabajo supondría una mejora en las capacidades tácticas de cualquier unidad de EW (Electronic Warfare) como el Regimiento de Guerra Electrónica 31 (REW 31), lugar dónde se ha llevado a cabo el desarrollo del sistema. Esta unidad, única en el Ejército de Tierra (ET) por sus posibilidades de empleo táctico, no dispone de un sistema similar, encontrando en esta carencia la principal razón para justificar el trabajo realizado.

Otra importante razón que justifica el trabajo es la importancia e incluso dependencia en el ámbito militar, pero también en el civil, de los sistemas GNSS (Global Navigation Satellite System – Sistema Global de Navegación por Satélite). Conseguir perturbar, interferir o incluso engañar a las unidades enemigas podría llevar a la resolución de un conflicto, esto es debido a que los sistemas GNSS son ampliamente utilizados en los ejércitos actuales además de tener otras importantes aplicaciones en el ámbito civil[1], diferenciándose así tres ámbitos de aplicación que se pueden encontrar en la introducción del trabajo, más concretamente en el subcapítulo *1.4.1. Los Sistemas GNSS*.

En resumen, la carencia de un sistema similar junto con las importantes aplicaciones de los sistemas GNSS tanto civiles como militares son las dos principales razones que justifican el desarrollo de este trabajo.

[1] La tendencia en la actualidad es la transferencia de tecnología civil al ámbito militar, por ello no se deben perder de vista las aplicaciones civiles.

1.2. ÁMBITO DE APLICACIÓN

En lo que respecta al ámbito de aplicación del sistema de contramedidas, este se acotaría a la explotación y uso de este por parte del REW 31, dado que actualmente es la única unidad táctica de EW en el ámbito del ET. Asimismo, habida cuenta de la gran capacidad de despliegue de la unidad, una de las características principales del sistema de contramedidas objeto de este TFG debe ser la portabilidad.

Las capacidades de EW se llevaban desarrollando desde la primera publicación referente a la EW en el ET, la cual está fechada en julio de 1972, esto llevó, más adelante, a la creación en el 1988 del Regimiento de Transmisiones Táctica nº 21 (RETAC 21). Más adelante, en el 2005, se crearía el REW 31, Unidad donde se ha realizado este trabajo además de las prácticas externas. Se puede encontrar más información sobre la unidad en el Anexo III: Información REW 31.

La guerra electrónica puede tener efectos de gran valor en las operaciones, en comparación con los recursos empleados y llegar a ser fundamental para desequilibrar al enemigo.

En la clasificación de las actividades de EW se emplean dos terminologías distintas, pero complementarias:

- Atendiendo a los efectos operativos que persiguen, se denominan acciones de EW y pueden ser de tres tipos: vigilancia electrónica (ES), ataque electrónico (EA) y defensa electrónica (ED).
- Según la propia naturaleza electrónica de las actividades y el efecto que buscan provocar en los equipos objetivo u obtener de ellos, ya sean enemigos (atacándolos) o propios (protegiéndolos), reciben la denominación de medidas de EW y pueden ser: medidas de apoyo electrónico (ESM), contramedidas electrónicas (ECM) y medidas de protección electrónica (EPM). La ejecución de las ESM y de las ECM corresponde a las unidades de EW, mientras que las EPM deben ser adoptadas por todo tipo de unidades.

La correspondencia básica entre acciones y medidas es fácilmente intuitiva: la vigilancia electrónica se lleva a cabo mediante ESM; el ataque electrónico, mediante ECM y la defensa electrónica, con EPM. No obstante, hay que puntualizar que las ESM también proporcionan información indispensable del adversario para poder desarrollar las acciones EA y ED, y que, por otro lado, con las ECM se llevan a cabo contrataques que realiza la defensa electrónica ante las actividades de guerra electrónica del adversario.

Por lo tanto, el sistema desarrollado en este trabajo realiza acciones de EA, atendiendo al efecto que estas persiguen y de ECM según su naturaleza y efectos que persigue. (Ministerio de Defensa, 2017)

1.3. ANTECEDENTES, ACTUALIDAD Y FUTURO

En primer lugar, se procede a analizar los antecedentes de una tecnología tan importante y actual como es la geolocalización. Tiene su origen en el sistema *Transit* desarrollado por los Estados Unidos de América (EEUU), el primer lanzamiento de un satélite de esta constelación (que sólo contaba con seis satélites) se realizó en los años 60. Las características de este sistema de posicionamiento poco tienen que ver con las prestaciones actuales, la cobertura era parcialmente global ya que los seis satélites no podían cubrir en su plenitud el globo terráqueo haciendo así que el posicionamiento fuese intermitente. A esto había que sumarle que un receptor necesitaba de una media de quince minutos para posicionarse (Tispain, 2011). El desarrollo de un sistema como este fue uno de los múltiples campos de batalla de la Guerra Fría (1947-1991) que contribuyeron al desarrollo de la tecnología militar para su posterior aplicación al mundo civil. De hecho, el rival de los EEUU en este largo "enfrentamiento" (la Unión de Repúblicas Socialistas Soviéticas (URSS)), también desarrolló un sistema similar bautizado como *Tsikada*, produciéndose el primer lanzamiento de un satélite en 1974. Posteriormente, el departamento de defensa americano ha seguido desarrollando el sistema en tres etapas de lanzamiento (bloques I, II y III). Actualmente se cuenta con una constelación de 24 satélites, ofreciéndose así una cobertura global.

En la actualidad, la geolocalización juega un papel muy importante en el día a día tanto civil como militar, prueba de ello es el esfuerzo de otros países, diferentes de EEUU, en desarrollar sus propios sistemas de posicionamiento global: GLONASS (Global'naya Navigatsionnaya Sputnikovaya Sistema) desarrollado por el Ministerio de Defensa de Rusia; GALILEO Positioning System, desarrollado por la Unión Europea y operado por la Agencia Espacial Europea (ESA) y BeiDou Navigation Satellite System, desarrollado por el Gobierno chino. (véase 1.4.1. Los Sistemas GNSS para más información acerca del término sistemas GNSS).

En cuanto a la altísima dependencia de los medios GPS en la actualidad, en el ámbito militar: el Departamento de Defensa de los EEUU (DoD) reconoce que el ochenta por ciento de sus operaciones no podrían llevarse a cabo sin el uso del GPS (Chicharro Sánchez-Agustino, 2019). Mientras en el ámbito civil, por poner un ejemplo, el comercio marítimo representa el ochenta por ciento del comercio internacional. Siendo el GPS, en la actualidad, la base de la navegación y seguridad marítima. La geolocalización por GPS es una herramienta estratégica en términos militares además de tener un gran impacto comercial en el ámbito civil. Por otro lado, en lo que respecta a la defensa nacional, la dependencia de los sistemas GNSS es tal que el propio Ministerio de Defensa advierte de este problema en el Entorno Operativo 2035[2], (Ministerio de Defensa, 2019, p. 40):

> Además, una dependencia excesiva de la tecnología tiene efectos indeseados, especialmente en entornos y ambiente degradados […] por lo que será preciso contrarrestar esta vulnerabilidad con tecnologías aptas para su uso en entornos degradados, capaces de eliminar la dependencia de tecnologías «habilitadoras» (sistema de posicionamiento global –GPS–, bandas espectrales, etc.) […] Asimismo, será necesario el adiestramiento adecuado basado en los «viejos» procedimientos.

Como consecuencia del empleo masivo de estos sistemas GNSS de posicionamiento se han desarrollado tecnologías de perturbación (jamming) y decepción (spoofing) que tienen como objetivo las señales radioeléctricas GNSS (véase 4.2. Jamming y 4.3. Spoofing). Los titulares enumerados a continuación, son una prueba más

[2] El proyecto plantea las líneas a seguir para la mejora del Ejército de cara al futuro, el cumplimiento de estos objetivos se debería de producirse en torno al año 2035.

la gran cantidad de ataques contra las señales GNSS que se han producido en la historia reciente:

1. El conflicto enconado entre turcos y kurdos sirve como ejemplo de ataques jamming. Turquía cuenta con una unidad especial, armada con un fusil de radiofrecuencia, que cuenta con la capacidad de derribar drones en vuelo mediante está técnica (Pastor, 2018). Aunque a priori, se desconoce la frecuencia de trabajo de estos rifles usados por los "Drone Jammers", es muy probable que su finalidad sea la de atacar a las bandas GPS de los drones enemigos, imposibilitando así su pilotaje remoto.
2. Durante unas maniobras conjuntas de los EEUU y Corea del Sur se detectó una inhibición de la señal GPS en varios de los buques militares del ejercicio. La autoría del ataque se atribuye a Corea del Norte (Israel Defense, 2011).
3. A finales de 2011 Irán anunciaba públicamente que había sido capaz de hacerse con un UAV estadounidense mediante un ataque de spoofing. (Rawnsley, 2011)
4. En verano de 2017 la armada estadounidense notificó un supuesto ataque de spoofing en el Mar Muerto cuya autoría podía pertenecer a Rusia. (Goward, 2017)
5. Algunas informaciones (O'Dwyer, 2018) han señalado que la fragata noruega *Helge Instad*[3], previamente a su choque en uno de los fiordos noruegos, había sufrido un error en los equipos de navegación, coincidiendo con ataques rusos a los GPS durante el ejercicio TRIDENT JUNCTURE 2018 de la Alianza Atlántica. (Chicharro Sánchez-Agustino, 2019)

Se observa que, los ataques de inhibición y decepción de GPS y otras radiofrecuencias pueden tener gran repercusión sobre los medios utilizados por las unidades militares. El desarrollo de un sistema con estas capacidades supone una herramienta de vital importancia para unidades de guerra electrónica moderna. Dentro del ámbito nacional actual, se han desarrollado sistemas destinados a la defensa de este tipo de ataque como el sistema de protección de infraestructuras críticas contra el ataque de drones presentado en 2017 por el INTA, que cuenta con funcionalidad jamming (Navarro García, 2017).

En este trabajo nos vamos a centrar en los sistemas basados en SDR (véase 1.4.2. Software Defined Radio). Debido al reducido coste y portabilidad de estos sistemas se ha optado por basar el sistema de contramedidas en esta tecnología. En la actualidad, la relación SDR y GNSS está aún en desarrollo tanto en perturbación (Ferreira, et al., 2020) como de decepción (Gaspar, et al., 2020).

Finalmente, y con vistas al futuro, se puede intuir que se seguirán desarrollando sistemas similares al de este trabajo ya que la gran dependencia de los medios GPS se mantendrá o aumentará con el paso de los años. Además, estos sistemas jugarán un papel muy importante en la guerra contra los drones, esta conclusión se extrae de los estragos causados por los drones turcos en el reciente conflicto de Nagorno-Karabag (Meta-Dèfense.fr, 2021).

[3] La fragata de la clase *Fridtjof Nansen* de la Armada Real de Noruega se hundió en un fiordo al norte de Bergen tras un accidente ocurrido el 8 de noviembre de 2018 cuando regresaba de su participación en el ejercicio TRIDENT JUNCTURE 2018.

1.4. CONCEPTOS CLAVE

En este capítulo, estructurado en (1) Los Sistemas GNSS y (2) Software Defined Radio (SDR), se expone la información necesaria sobre los conceptos clave del trabajo. Los subcapítulos aquí desarrollados son esenciales para entender el funcionamiento y el sentido del sistema de contramedidas que en este trabajo se desarrolla.

1.4.1. Los Sistemas GNSS

En primer lugar, el concepto GNSS se define como una constelación de satélites caracterizados por transmitir señales en una frecuencia determinada que es recibida por un receptor y que se utiliza para la localización y posicionamiento de un elemento en la superficie terrestre (García Martín, et al., 2021).

También es importante tener en cuenta que un sistema GNSS consta de partes diferentes conocidas como segmentos: (Álvarez Pérez, 2021)

- Segmento espacial o constelación de satélites: conjunto de satélites en órbita que proporcionan las señales de pseudodistancia y los mensajes de datos al equipo del usuario.
- Segmento de control o red de tierra de control y monitorización: tareas de mantenimiento de la órbita de los satélites, corrección de la deriva de los relojes atómicos de estos además de seguimiento.
- Segmento usuario o equipo de usuario: receptores terrestres.

La geolocalización se produce en base a los dos siguientes pasos:

- Los satélites emiten señales de radiofrecuencia, que contienen la siguiente información:
    - El identificador del satélite que emite la señal.
    - La posición exacta del satélite en el momento de emisión de la señal.
    - La hora exacta (hora, minuto, segundo y milisegundo) en el que fue transmitida la señal por el satélite.
- Estas señales son recibidas por los receptores que calculan en función de la hora a la que han recibido la señal en comparación con la hora a la que han sido emitidas por los satélites obteniendo una distancia esférica a estos. Finalmente, por el método de trilateración y con un mínimo de señales recibidas de cuatro satélites el receptor es capaz de ubicarse.

Existen a nivel mundial diferentes sistemas GNSS (véase 1.3. Antecedentes, Actualidad y Futuro), pero debido a su popularidad y a ser el más utilizado globalmente, sólo se analizará el NAVSTAR-GPS (NAVigation System and Ranging - Global Position System), desarrollado por el Departamento de Defensa de los EEUU. También se podrá observar que las pruebas realizadas en este trabajo están relacionadas con las señales características de este sistema.

Los satélites de la constelación GPS trabajan en una frecuencia fundamental de 10,23 MHz, esta se multiplica por dos constantes 154 y 120 (Ferreira, et al., 2020), generando, respectivamente, dos portadoras: L1 y L2. Reciben este nombre debido a que

ambas están en la banda UHF (Ultra High Frequency) definida por el IEEE (Institute of Electrical and Electronics Engineers) como L. Los datos relativos a cada portadora se pueden observar en la tabla mostrada a continuación:

Banda	Frecuencia fundamental [MHz]	Constante por la que se multiplica	Frecuencia [MHz]	Longitud de onda [cm]	Ancho de banda [MHz]
L1	10,23	154	1575,42	19	15,345
L2		120	1227,6	24	11

Tabla 2: Datos portadoras GPS

Cada una de estas portadoras, contiene información en diferentes códigos. Los receptores GPS únicamente pueden decodificar aquel código para el que están configurados. Se diferencian los siguientes códigos, la información correspondiente se presenta a continuación en forma de tabla:

Banda	Código	Significado	Observación
L1	C/A	Coarse Acquisition	código civil
	P	Precision	código militar
	M	Military	código militar
	L1C	L1 civilian	código civil mejorado
L2	P	Precision	código civil
	M	Military	código militar
	L2C	L2 civilian	nuevo código civil

Tabla 1: Códigos de las portadoras GPS

En la imagen expuesta a continuación se puede observar el espectro del código C/A de la señal GPS:

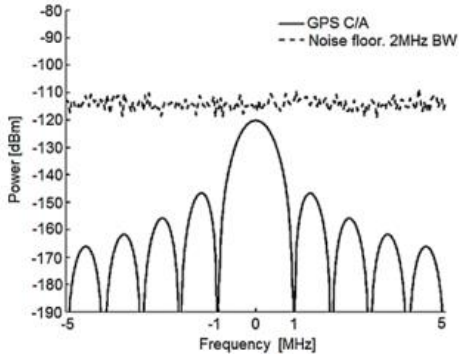


Figura 1: Espectro del código C/A de la señal GPS (Rahman, et al., 2021)

En relación con la precisión de los receptores, los receptores civiles sin capacidad de utilizar los códigos militares ofrecen una precisión máxima de 2 m, mientras que los receptores militares con capacidad de utilizar los códigos militares ofrecen una precisión máxima por debajo de 1 m.

Continuando con el desarrollo de este subcapítulo, se procede a explicar los tres procesos de corrección de precisión más utilizados por los receptores GNSS:

- Sistemas de aumentación basados en satélites (SBAS: Satellite-based aumentation system). El segmento de control emite correcciones que son

enviadas a los satélites y estos las reflejan sobre la superficie terretre, aumentando de esta manera la precisión y fiabilidad de los receptores ubicados en la superficie de la Tierra.

- Corrección diferencial (DGPS: Differential GPS). En la superficie terrestre existen antenas fijas de la cuales se conoce su ubicación exacta por medios diferentes a los ofrecidos por los sistemas GNSS. Dichas antenas también proporcionan a los receptores información sobre la ubicación facilitando así la corrección de errores en este.
- Tecnología A-GPS. Utilizado principalmente por dispositivos como smartphones y tablets. Los receptores que cuentan con esta tecnología tienen la capacidad no sólo de guardar la última ubicación guardada, además son capaces de estimar su ubicación en función de su posición en la red celular de telefonía móvil. A esto hay que sumarle que, debido a la capacidad de acceder a internet, son capaces de recibir datos de los servidores de asistencia. Dichos servidores poseen información muy precisa acerca de la posición de los distintos satélites en cada momento y lugar. De esta manera se consigue una mayor precisión y fiabilidad en ubicación de los receptores.

Para finalizar, se procede a los usos principales de estos sistemas, se diferencian principalmente tres ámbitos de aplicación

- Uso militar: es importante recordar que la navegación por satélite tiene su origen en el ámbito militar (creación del sistema *GPS Transit* en 1960). En la actualidad las principales aplicaciones son:
  - Gestión y navegación de unidades terrestres, aéreas y marítimas, por lo que un ataque a las frecuencias utilizadas por los receptores de vehículos, aeronaves o barcos podría resultar fatal en la maniobra enemiga.
  - Guiado de precisión de proyectiles, pudiendo llegar a repeler un ataque enemigo de este tipo con un sistema de contramedidas adecuado.
- Navegación aérea (tanto civil como militar): estos sistemas son el pilar fundamental del control del tráfico aéreo y la navegación aérea automática, destacando el control sobre drones y UAVs (Unmanned Aerial Vehicle – Vehículo aéreo no tripulado).
- Uso civil: por citar algún uso, cabe mencionar las ayudas a la navegación personal, pero este campo es muy amplio: ingeniería civil; construcciones e infraestructuras, control de flotas, etc.

1.4.2. Software Defined Radio (SDR)

En primer lugar, un SDR se define como un sistema de radiocomunicaciones donde gran parte de los componentes son implementados usando software en lugar de usar una implementación hardware, usando para ello un dispositivo embebido[4] que trata la información y la transmite a un computador. (Rodríguez de Haro, 2017).

[4] Se trata de un sistema que se ha creado para una función o varias funciones en concreto. También se puede encontrar referencias a este término como dispositivo empotrado.

Es importante destacar que, los SDR carecen de un microprocesador interno, ya que utilizan el del propio ordenador al que se conectan, esto repercute en gran medida en el precio de los periféricos haciendo que no sean excesivamente costosos. De hecho, el coste representa una de las principales ventajas de implementar un sistema SDR, además esto llama la atención de una gran cantidad de usuarios que pueden explotar sus capacidades generándose así gran cantidad de contenido divulgativo en internet sobre el uso de estos aparatos. Por normal general, el bajo coste de los SDR se ve reflejada en su bajo rendimiento (Bažec, et al., 2016).

En cuanto a las partes que lo componen, en todos los SDR se diferencian dos elementos principales:

- Un dispositivo hardware, por lo general se puede encontrar referencias a este como periférico, encargado de recibir las señales. Ejemplo: HackRF One, RTL-SDR, BladeRF, etc.
- Un software que será utilizando para configurar diferentes parámetros del dispositivo hardware. Ejemplo: GNURadio, hackrf_transfer, SDR#, SDR Console, etc.

Por lo tanto, un SDR no es un único dispositivo en sí, si no que se trata de la conjunción de un periférico conectado a un computador.

1.5. ESTRUCTURA DEL TRABAJO

Concluyendo con la introducción del trabajo, se procede a explicar brevemente la estructura de este. Tras este primer punto se puede encontrar los objetivos y metodología, esta parte se aprovecha para explicar las características principales que debe tener el sistema con base en los objetivos generales y específicos del trabajo además de la metodología utilizada para lograr dichos objetivos. Posteriormente se encuentra el cuerpo del trabajo, dónde se detalla el sistema de contramedidas basado en SDR desarrollado, así como las pruebas realizadas sobre el mismo. Finalmente, se exponen las conclusiones extraídas del desarrollo de dicho sistema.

2. OBJETIVOS Y METODOLOGÍA

Este segundo punto del trabajo se divide en los siguientes capítulos: (1) Objetivos y Alcance: dónde se desarrollan los objetivos tanto generales como específicos del trabajo que se verán reflejados en el sistema de contramedidas y (2) Metodología: en el cual se desarrolla la metodología empleada para conseguir dichos objetivos.

2.1. OBJETIVOS Y ALCANCE

En primer lugar, se presenta el objetivo general del trabajo, este es crear un sistema de contramedidas basado en SDR (Software Defined Radio) capaz de ejecutar acciones eficaces de jamming (perturbación) y spoofing (decepción) contra receptores GNSS. Se aborda de esta manera el problema hallado en la necesidad de las unidades de guerra electrónica de hacer frente a la amenaza relacionada con los sistemas de navegación y posicionamiento del enemigo, así como en la falta de un sistema en dotación que lleve a cabo contramedidas que neutralice la señal GPS de los medios enemigos. Asimismo, el problema se agrava dada la dificultad y el coste que los procesos de adquisición y desarrollo de proyectos tecnológicos militares suponen. Por esta razón el sistema desarrollado es este trabajo está basado en SDR, ya que la unidad dónde se han realizado las prácticas externas cuenta con estos medios en dotación.

En segundo lugar, se presentan los objetivos específicos de este trabajo, que coinciden a su vez con las características que debe cumplir el sistema de contramedidas:

- Desarrollar un interfaz de explotación user-friendly.
- Conseguir un sistema de bajo coste, tratando de aprovechar el material en dotación de las unidades.
- Valorar la posible implementación en el sistema de amplificadores de señal y antenas adaptadas, consiguiendo un mayor alcance de señal.

En lo que respecta al alcance, es importante diferenciar el alcance del producto del alcance del proyecto. El primero de ellos está relacionado con las características que se esperan del producto de este trabajo, es decir, las características del sistema de contramedidas. En este primer caso el alcance se extrae de los objetivos, esto es, que sea eficaz en decepción y perturbación, de fácil explotación, de bajo coste, que utilice medios en dotación de la unidad y que sea mejorable mediante la implementación de amplificadores y antenas directivas. El segundo de ellos, el alcance del proyecto es el trabajo requerido en el proyecto. De esta manera se introducen las fases del proyecto y la metodología analizada en el siguiente capítulo.

En cuanto a las fases del proyecto, para el desarrollo del sistema se ha seguido la siguiente organización iterativa:

- 1ª Fase: estudio y selección de los componentes del sistema a desarrollar.
- 2ª Fase: generación de una aplicación informática de explotación del sistema, una vez seleccionados y ensamblados los componentes elegidos.
- 3ª Fase: puesta en operación del sistema y realización de pruebas de campo.

- 4ª Fase: obtención de conclusiones fruto del análisis de los resultados obtenidos, estudiando la posibilidad de retornar a fases anteriores (cambiar componentes, modificar la aplicación, variar las condiciones de las pruebas, etc.) con la finalidad de mejorar el sistema.

Para finalizar este capítulo y en cuanto a las restricciones del proyecto, se advierte que estarán relacionadas con los medios SDR disponibles en la unidad.

2.2. METODOLOGÍA

Los objetivos del trabajo, descritos en el capítulo anterior, se intentarán alcanzar haciendo uso de la siguiente metodología:

- Lectura de bibliografía especializada: extrayendo la información necesaria que conformará la base teórica del sistema.
- Creación de un grupo de discusión de personal de la unidad: parte de las conclusiones extraídas de las prácticas aquí realizadas en este trabajo han sido consultadas con un grupo de expertos (véase Anexo II: Grupo de discusión) elegidos dentro de la unidad debido a sus conocimientos y experiencia sobre los temas aquí tratados.
- Programación en lenguaje Python.
- Realización de pruebas de campo con el objetivo de testear el sistema creado (véase 4. Desarrollo: Análisis y Resultados).
- Análisis de los resultados obtenidos mediante técnicas de scoring.

3. ANTECEDENTES Y MARCO TEÓRICO (ESTADO DEL ARTE)

En este tercer punto del trabajo, partiendo de la base de los antecedentes ya analizados en la introducción (véase 1.3. Antecedentes, Actualidad y Futuro), se presenta el estado del arte.

En cuanto a la existencia de sistemas similares, es muy difícil o prácticamente imposible encontrar información sobre sistemas militares de perturbación o decepción de GPS, la principal razón es la relación de estos con el ámbito de la guerra electrónica impidiendo la publicación de información relacionada con estos temas por el bien de la seguridad nacional. Por lo tanto, será difícil de encontrar información relacionada con la industria (civil y militar) que desarrolle estos tipos de sistemas de EA. Pero esto no significa que no existan, de hecho, las terribles repercusiones que puede tener un ataque de este tipo (véase 1.3. Antecedentes, Actualidad y Futuro), ha llevado a empresas como IAI (Israel Aeroespace Industries) a desarrollar un sistema con la finalidad de proteger aeronaves ante ataques GPS jamming, conocido como ADA. El sistema ADA ha sido probado satisfactoriamente en la operación *Guardian of the Walls* [5], además ha surgido recientemente un derivado a este sistema, el ADA-O destinado a la protección contra jamming en embarcaciones marítimas (UASweekly.com, 2021). A modo de conclusión, el desarrollo de sistemas de ED que protejan de ataques relacionados con el GPS es la principal prueba que justifica la existencia de sistemas de EA en dicha banda de frecuencias.

En cuanto al desarrollo del sistema basado en SDR, por las características de este tipo de tecnología (véase 1.4.2. Software Defined Radio (SDR)) como del sistema de este trabajo (véase 2.1. Objetivos y Alcance), se prevé que esta tecnología sea la predominante en las radiocomunicaciones, debido a que las innovaciones en esta tecnología son constantes y tienen un amplio campo de aplicación. (Ferreira, et al., 2020) (Gaspar, et al., 2020)

4. DESARROLLO: ANÁLISIS Y RESULTADOS

La información que se detalla en el cuerpo de este trabajo, se estructura en los siguientes subcapítulos: (1) Elemento hardware del sistema SDR: incluye la información sobre este elemento del SDR, para este trabajo se ha optado por un HackRF One, (2) Jamming; (3) Spoofing: siendo esta, junto con la técnica anterior, los dos tipos de ataque que el sistema de contramedidas lleva a cabo; (4) Sistema final: se presenta el sistema de contramedidas justificando sus componentes con base en las pruebas realizadas, además de realizar una práctica con este, y finalmente, (5) Mejoras sobre el sistema final: en el que se valoran ciertas implementaciones para mejorar la distancia a la que es efectivo el sistema y su portabilidad.

4.1. ELEMENTO HARDWARE DEL SISTEMA SDR

[5] Operación israelí surgida en mayo de 2021 para frenar los enfrentamientos producidos en la franja de Gaza.

En primer lugar, se analiza el dispositivo utilizado, este ha sido prestado por el REW 31. Dicho periférico es la pieza fundamental del sistema de contramedidas, se trata de un HackRF One (Transpondedor 1MHz - 6 GHz). El transceptor constituye la parte hardware del SDR (véase 1.4.2. Software Defined Radio (SDR)), siendo su función fundamental la emisión de señales GPS.

En las imágenes mostradas a continuación, se puede observar el dispositivo además de una antena GPS (también prestada por el REW 31) válida para la banda L1.

Figura 2: HackRF One propiedad del REW31

Figura 3: Antena GPS banda L1 propiedad del REW31

Figura 3: Reverso Antena GPS banda L1 propiedad del REW31

De esta manera el diagrama de emisión y recepción para del sistema del sistema de contramedidas se puede observar en la figura de a continuación:

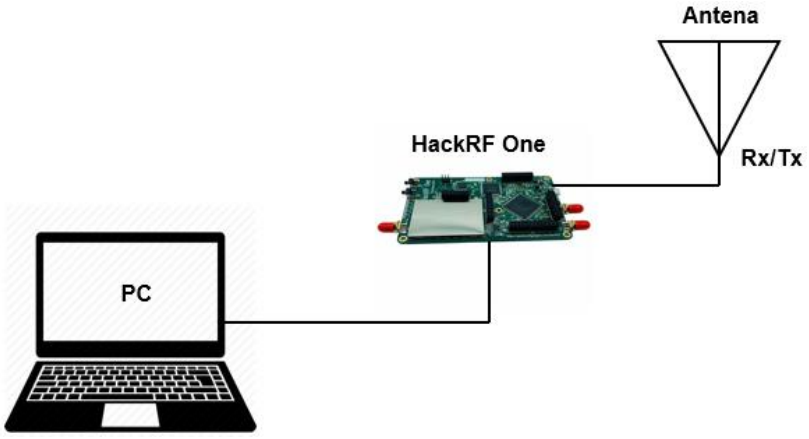


Figura 4: Diagrama del sistema SDR

El periférico SDR HackRF One es desarrollado por la empresa británica *Great Scott Gadgets*, los datos más importantes del dispositivo se detallan a continuación:

- El dispositivo es capaz de recibir y transmitir. A lo largo del trabajo se pueden observar referencias a este como transceptor del tipo half-duplex[6].
- Puede trabajar en un rango de frecuencias relativamente amplio: 1MHz a 6GHz. Siendo altamente polivalente y válido para diferentes campos: comunicaciones de radioaficionados (HF, VHF…), ataques replay [7], etc. En este trabajo se explotará principalmente su capacidad de trabajar en las diferentes bandas de los sistemas GNSS.
- El precio del dispositivo es relativamente bajo, alrededor de unos 300€, estando al alcance de una gran cantidad de usuarios. Prueba de su popularidad es el amplio número de proveedores que se puede encontrar por internet, incluso en páginas muy conocidas, por ejemplo, HackRF One original. Esto explica por qué se encuentra este dispositivo en dotación dentro del REW 31. De hecho, desde su aparición en el mercado en el 2014 han surgido numerosas copias, que permiten obtener el dispositivo por un precio aún más razonable, ejemplo de ello son los siguientes productos: Copia 1 o Copia 2.

Es importante destacar, que el dispositivo prestado por el REW 31 no es desarrollado por *Great Scott Gadgets*, pero ello no impide la correcta realización de las diferentes pruebas, puesto que ambos tienen la misma placa base.

Otras características más técnicas del dispositivo son (Ossmann, 2018):

- Velocidades de muestreo soportadas: 2-20 Msps (Million simples per second – Millón de muestras por segundo)
- Resolución de muestreo: 8 bits en cuadratura.
- Interfaz y alimentación del periférico: USB de alta velocidad (con conector USB Micro-B)

[6] En castellano: semidúplex. Capacidad de emisión y recepción, pero no de manera simultánea.
[7] Un ataque replay consiste en grabar una señal para posteriormente transmitirla.

- Alimentación del puerto de antena (controlable vía software): máx. 50 mA a 3,3 V.
- Conector de antena (impedancia de 50 ohmios): SMA hembra.
- Entrada y salida de reloj (para sincronización): SMA hembra. Pudiendo conectar asó otros dispositivos como este y trabajar con ellos conjuntamente, de esta manera, (mínimo 2 periféricos) se podría obtener la capacidad de operar en full-duplex[8].
- Alta portabilidad.
- Open-source[9], comúnmente conocido en castellano como código abierto.

Como se ha comentado en los objetivos de este trabajo (véase 2.1. Objetivos y Alcance), tras finalizar el diseño del sistema se valorará aumentar su alcance efectivo mediante un amplificador. A la hora de trabajar con amplificadores es importante tener en cuenta la potencia máxima a las que pueden trabajar este tipo de periféricos, ya que superarla puede causar daños en el dispositivo, llegándolo incluso a dejar inservible. Por esta razón, a continuación, se analiza la potencia en cuanto a:

- Rx (Recepción):

Máximo de -5 dBm, exceder dicha potencia máxima de Rx puede causar daños altamente perjudiciales al dispositivo. Con el amplificador interno desactivado se podría alcanzar los 10 dBm, pero el mismo fabricante no recomienda esta práctica.

- Tx (Transmisión): según la siguiente tabla:

Rango de frecuencias [MHz]	Potencia [dBm]	Observaciones
10 - 2150	5 - 15	Generalmente aumenta la potencia si la frecuencia disminuye.
2150 - 2750	13 - 15	Aumenta la potencia si la frecuencia disminuye.
2750 - 4000	0 - 5	
4000 - 6000	-10 - 0	Generalmente aumenta la potencia si la frecuencia disminuye.

Tabla 3: Potencia de Tx HackRF

Continuando con el análisis de los datos relacionados con la ganancia del dispositivo, se debe tener en cuenta que este cuenta con amplificadores configurables vía software, que pueden adoptar los siguientes valores predeterminados (Ossmann, 2021):

Para Rx, cuenta con 3 etapas:

- RF (radiofrequency – radiofrecuencia): “amp” (amplifier – amplificador), 0 o 14 dB.
- IF (intermediate frequency – frecuencia intermedia): “lna” (low noise amplifier – amplificador de bajo ruido), de 0 a 40 dB en múltiplos de 8 dB.
- BB (base band – banda base): “vga” (variable gain amplifier – amplificador de ganancia variable), de 0 a 62 dB en múltiplos de 2 dB.

Para Tx, cuenta con 2 etapas:

- RF: 0 o 14 dB
- IF: 0 a 47 dB en múltiplos de 1 dB

[8] Capacidad de emitir y transmitir simultáneamente.
[9] Basado en el desarrollo mediante colaboración abierta (su código fuente es público), no confundir con software libre, este último se utiliza para hacer referencia a que este es gratuito.

La configuración de estos valores se puede observar en software específico de SDR como es GNURadio (este programa se utiliza en la puesta en *4.2.2. Puesta en práctica con SDR*):

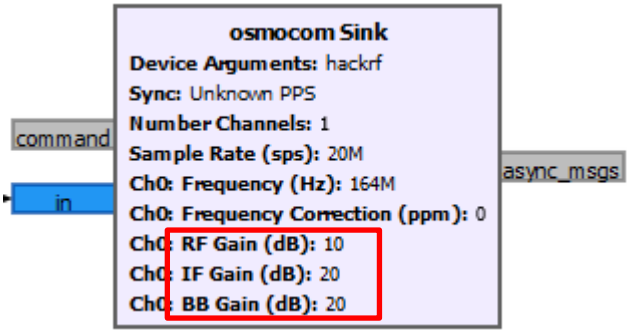


Figura 5: Modelado del HackRF en GNURadio

La instalación del periférico, por ser un proceso notablemente distinto de una instalación usual en el ámbito de la informática, se detalla en el Anexo V: Instalación HackRF One en ordenador personal.

4.2. JAMMING

En primer lugar, el jamming o perturbación no es un ataque específico a sistemas GNSS, sino que se puede dar en otros medios de telecomunicación: telefonía móvil, Wi-Fi, etc. Este tipo de ataque puede tener aplicación en casi cualquier medio inalámbrico con tecnología de radiofrecuencia. Consiste en interferir en la recepción de señales por medio de diferentes técnicas que se analizarán más adelante. Se conoce como jammer al dispositivo utilizado para esta función.

Así, la idea principal de este punto es la creación de un sistema efectivo basado en SDR capaz de perturbar la señal de GPS con un alcance adecuado a los medios disponibles. Posteriormente, se valorará la posibilidad de adaptar el sistema para aumentar su alcance.

4.2.1. Técnicas de Jamming

Las diferentes técnicas junto a sus respectivas ventajas y desventajas se resumen a continuación: (Ferreira, et al., 2020)

- Barrage Jamming

La palabra inglesa barrage hace referencia en términos civiles a una presa o dique, mientras que en el ámbito militar es comúnmente utilizada por la artillería con el significado de cortina de fuego o como el verbo bombardear.

Esta técnica consiste en emitir ruido en la porción del espectro en concreto que se quiere perturbar. Para incapacitar la recepción por el aumento de ruido.

Su principal ventaja es ser capaz de abarcar todo el ancho de banda de la señal (15,345 Mhz para la banda L1 de GPS).

- Tone Jamming

Consiste en transmitir un único pulso a la portadora de la señal a perturbar, de esta manera se concentra toda la energía en la frecuencia central.

Lo más destacable de esta técnica es la simplicidad de la señal, pero juega su contra que es una de las menos efectivas contra GPS.

- Sweep Jamming

También conocido como barrido de frecuencia consiste en una emisión dinámica que comienza en $Frecuencia\ central - BW/2$ y termina en $Frecuencia\ central + BW/2$. Esta técnica, más eficiente que barrage jamming, emite una señal conocida como Chirp (del inglés pío) signal.

Es una de las más efectivas para perturbar la señal de GPS debido a que con un menor ancho de banda, en comparación con Barrage Jamming, aplica una mayor potencia de densidad espectral. Pudiendo cubrir la totalidad de la banda L1 gracias a su barrido de frecuencias. Aunque tiene una desventaja importante, ya que para hacer el cambio en la emisión de una frecuencia a otra lo suficientemente rápido sin que el receptor recupere la señal original se puede llegar a requerir de hardware externo. (Ferreira, et al., 2020)

- Successive Pulses Jamming

Esta técnica se basa en emitir una cantidad de pulsos sucesivos en todo el espectro de la señal en cuestión. Esto quiere decir, que aparte de atacar a la señal portadora (como sucede en Tone Jamming) también se cubre el resto de las frecuencias del espectro, siendo, por lo tanto, más efectiva que la segunda técnica analizada.

Esta técnica, al igual que Sweep Jamming, aplica una mayor densidad espectral de potencia que Barrage Jamming y también es capaz de cubrir el espectro de la banda L1 al completo. En detrimento, debido al espacio entre frecuencias que emite el jammer, el receptor puede llegar a recuperar la señal original.

- Protocol-Aware Jamming

A diferencia del resto de técnicas analizadas anteriormente, esta va más allá de emitir ruido en determinadas frecuencias. Tiene su base en la congestión del protocolo inalámbrico, de hecho, en los estándares Wi-Fi, es decir IEEE 802.11, se habla de los protocol-aware jammers (Hussain, et al., 2014). La señal emitida por el jammer tendrá las siguientes características:

  - Modulación binaria en fase (BPSK)
  - Muestreo a 1.023 MHz
  - Ancho de banda de 15.345 MHz

Para finalizar, esta técnica también se presenta como una de las más efectivas. Presentando una ventaja fundamental: su dificultad de detección por parte del receptor. Su comportamiento, aunque muy similar a Barrage Jamming, cambia la emisión de ruido por la de bits aleatorios con modulación BPSK. De esta manera, el espectro de este tipo de jammers emiten una réplica fiel de la señal de GPS original.

Dados los resultados del estudio de los científicos portugueses (Ferreira, et al., 2020), únicamente se realizarán prueba de jamming con las técnicas que han resultado ser más efectivas: Sweep Jamming (Barrido de frecuencias) y Protocol-Aware Jamming (P-AJ) siendo está aún más efectiva que la anterior.

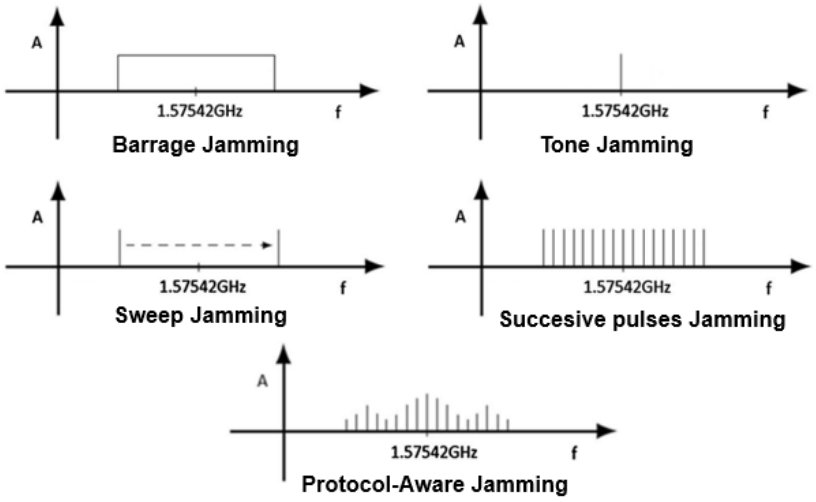


Figura 6: Espectro teórico de las diferentes técnicas analizadas (Ferreira, et al., 2020)

4.2.2. Puesta en práctica con SDR

Para modelar las señales se utilizará el programa GNU Radio. Consiste en un entorno gráfico basado en diagrama de bloques sobre Python como lenguaje de programación desarrollado para sistema Linux, aunque en este trabajo el modelado se ha desarrollado sobre la versión Beta para Windows. La instalación del software se hace a partir de PothosSDR, el proceso completo, por su complejidad, se detalla en el Anexo IV: Instalación de GNURadio.

El diagrama de Rx/Tx para las pruebas de este proceso es el siguiente:

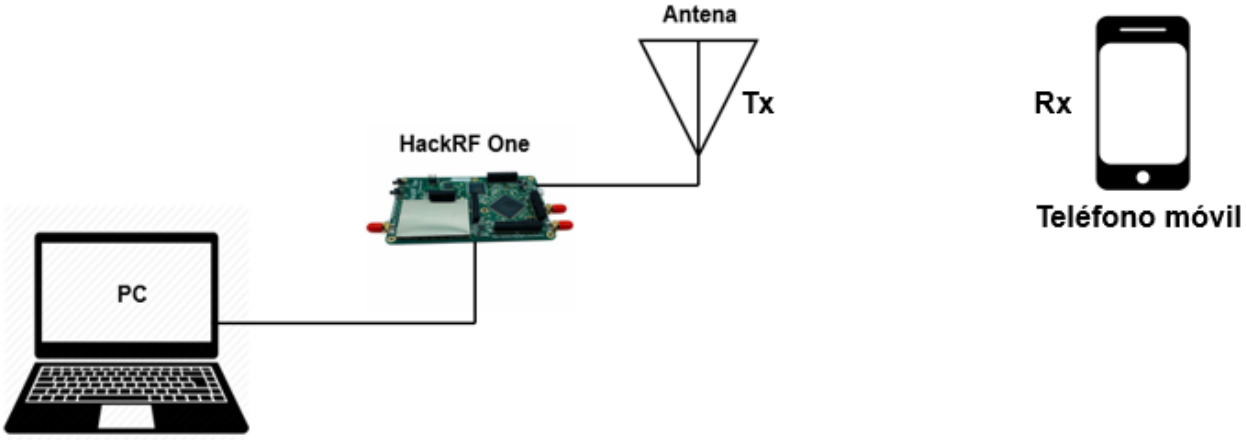


Figura 7: Diagrama Rx/Tx Jamming

En primer lugar, se ha creado un proyecto en GNURadio según la técnica de Sweep Jamming. La barredora, en lo que el espectro de la frecuencia respecta, consiste en la generación de un pulso que actúe de la siguiente manera: inicio en $F\ central\ (L1) - BW_{gps}/2$ [10]que avanza saltando de 10kHz en 10KHz hasta alcanzar $F\ central\ (L1) + BW_{gps}/2$, momento en el que el pulso volvería a la frecuencia de partida. Para conseguir

[10] $F\ central\ (L1)$: frecuencia central de la banda L1 de GPS, $BWgps$: Ancho de banda de la señal GPS en banda L1. Ambos valores aparecen en 1.4.1. Los Sistema GNSS.

este comportamiento se ha creado un diagrama de bloques y una función de Python. Esta función se puede escribir de la siguiente forma:

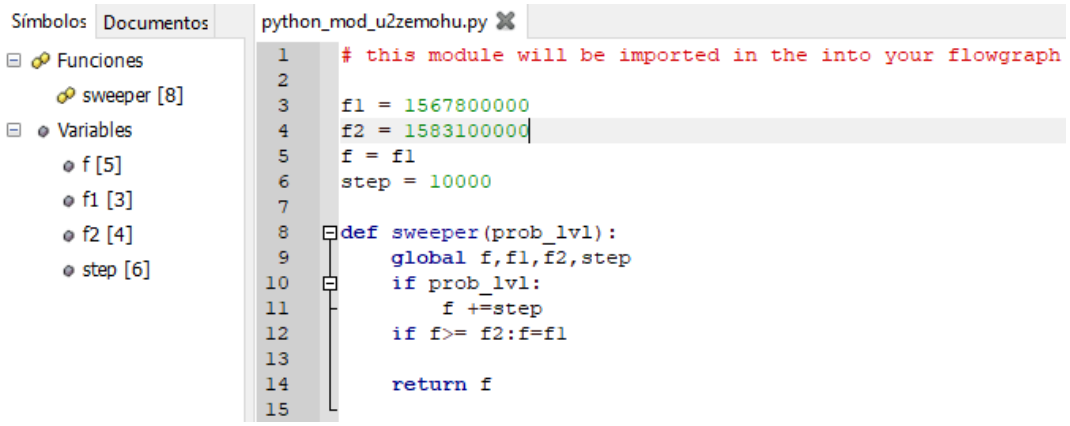


Figura 8: Función sweeper (barredora) escrita en lenguaje Python sobre el editor Geany

Por otro lado, está función se incluye en el diagrama de bloques de GNURadio en (a), esto se puede observar en la imagen de a continuación.

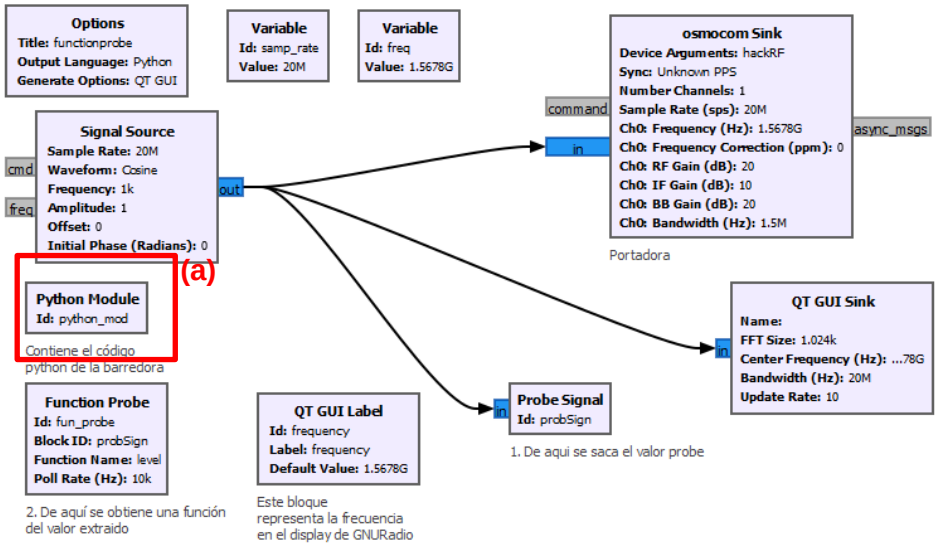


Figura 9: Diseño en GNURadio de una barredora (elaboración propia)

Este diseño sobrecarga de manera desmedida el procesador del ordenador personal, no pudiéndose ejecutar el diseño de GNURadio, como se había explicado previamente en el análisis de Sweep Jamming, para ello se requeriría de hardware externo.

Debido a esta desventaja, se pasa al diseño de un diagrama para la técnica de Protocol-Aware Jamming, mediante GNURadio:

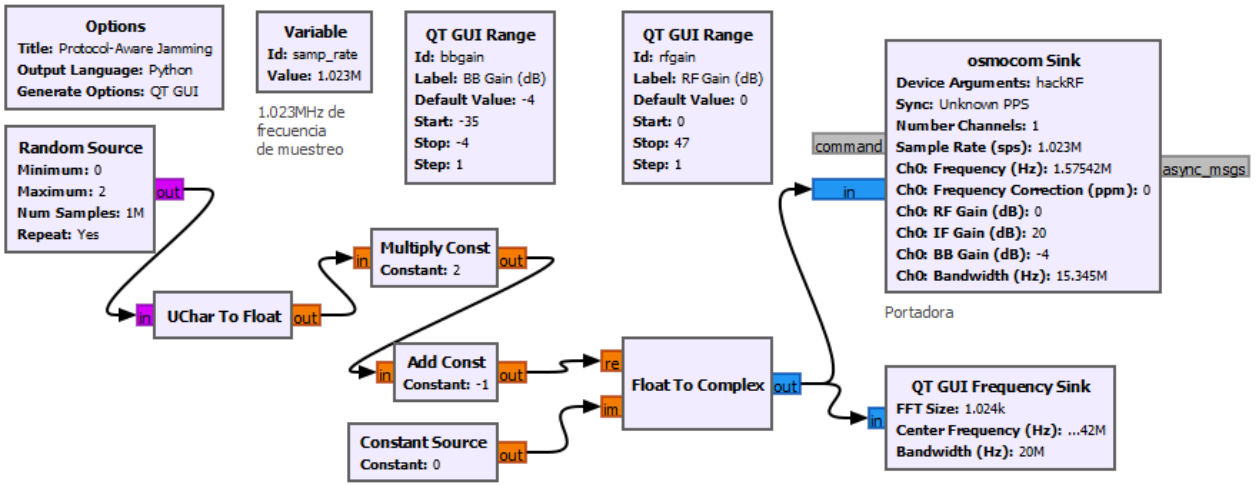


Figura 9: Modelado P-AJ en GNURadio (Ferreira, et al., 2020)

El espectro generado por la técnica P-AJ se muestra en la siguiente figura:

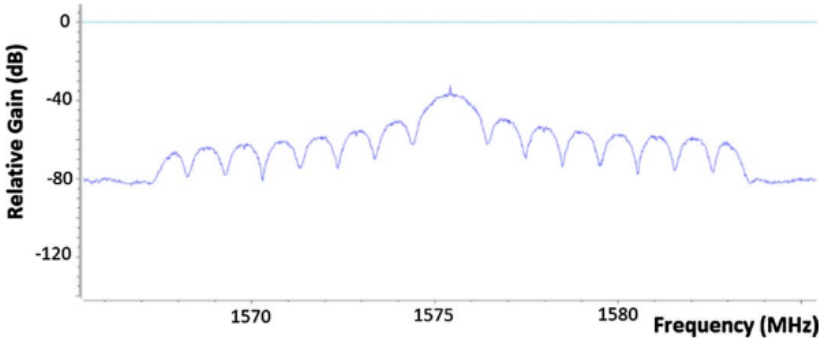


Figura 10: Espectro protocol-aware jamming en GNURadio (Ferreira, et al., 2020)

Se puede encontrar una gran fidelidad en el espectro entre protocol-aware jamming y la señal original C/A de GPS: espectro código C/A de la señal GPS.

Como alternativa a esta última técnica, se ha comprobado que se obtienen los mismos resultados de perturbación emitiendo cualquier señal GPS desde gps-sdr-sim (Ferreira, et al., 2020). Este método está detallado en detalle en el apartado de spoofing. Por esta razón, en las diferentes pruebas que se realizan en el capítulo 4.3. Spoofing, en las cuales se utiliza el software gps-sdr-sim, se pueden observar algunos casos en los que no se consigue engañar al receptor (que este se ubique en unas coordenadas ficticias) pero sí se consigue perturbar la señal.

4.3. SPOOFING

En primer lugar, esta técnica de ataque a los receptores GNSS consiste en el engaño o decepción. El receptor recibe unos datos falsos que le hacen reflejar una ubicación diferente a la que en realidad tiene.

Por otro lado, un ataque como este puede llevar a la confusión en rutas de convoyes que utilicen sistemas GNSS para la navegación. Pero no sólo puede afectar a vehículos

terrestres, también puede ser utilizada contra vehículos aéreos como por ejemplo drones (Rawnsley, 2011).

Así, la idea principal de este punto es elaborar un sistema basado en SDR que sea relativamente efectivo acorde a los medios del trabajo y pueda llevar a cabo con éxito un ataque de spoofing a pequeña escala, para posteriormente valorar si es posible aumentar su alcance.

Este capítulo se divide en función de las pruebas de spoofing realizas: (1) Teléfono móvil: en el que se ha utilizado un smartphone como receptor del ataque y (2) Radioteléfono ligero PR4G v3: siendo la radio de dotación del ET el objetivo del ataque de spoofing.

Los pasos detallados para llevar a cabo este tipo de ataque en el sistema se pueden encontrar desarrollados en el Anexo VII: Proceso Spoofing.

4.3.1. Teléfono móvil

En primer lugar, se ha desarrollado una prueba del sistema de contramedidas sobre un smartphone Xiaomi Mi 9t (sistema operativo Android) en modo avión para evitar la acción de procesos de corrección de error en la posición (analizado anteriormente en: técnicas corrección de error). Dicha práctica se ha realizado en una atmósfera de pruebas controlada que consiste en una habitación cerrada (de 4m x 4m) en la que el propio terminal no es capaz de posicionarse con el modo avión activado. En todo momento la antena estaba ubicada a 1,5m del dispositivo.

Los resultados de la práctica se han medido en función de la geolocalización del teléfono en base a dos aplicaciones:

1. GPS status: esta aplicación ha sido configurada para recibir las efemérides únicamente por GPS, es decir, obviando procesos de corrección (véase técnicas corrección de error). Dicha aplicación muestra la constelación de satélites de los que recibe efemérides además de las coordenadas del dispositivo en formato latitud longitud.
2. Google Maps: esta aplicación muestra la posición del teléfono móvil sobre un mapa terrestre.

La emisión de la señal simulada de GPS la realiza el HackRF, dicha emisión se configura vía software por consola de comando, utilizando el siguiente:

hackrf_transfer -t gpssim.bin -f 1575420000 -s 2000000 -a 1 -x 0

El proceso para llevar a cabo este ataque aparece ampliamente detallado[11] (osqzss, 2021) en el Anexo VII: Proceso Spoofing. El campo *-a 1* indica que el amplificador de Tx del propio HackRF está activado, pero con una ganancia nula (*-x 0*), mientras que el campo *-x* del comando anterior hace referencia la configuración de la ganancia (en dB) del amplificador de la etapa IF de Tx del HackRF. Este último campo se encuentra reflejado en la tabla de resultados de esta prueba, la cual se puede encontrar a continuación:

[11] osqzss es un colaborador japonés anónimo de GitHub, creador del proceso. Su proyecto de spoofing aparece citado por otros autores en artículos de divulgación científica sobre el tema. (Gaspar, et al., 2020)

Valor campo -x	Cantidad de satélites conectados (GPS status)	Resultado	Observaciones
0	0	Desfavorable	No se recibe ningún tipo de información por parte del terminal.
47	30	Desfavorable	Se recibe demasiada cantidad de información, no es posible la ubicación.
37	27-28	Desfavorable	Se recibe demasiada cantidad de información, no es posible la ubicación.
30	20-22	Desfavorable	Se recibe demasiada cantidad de información, no es posible la ubicación.
20	8-11	Favorable	Se recibe la información necesaria para la ubicación.

Tabla 4: Resultados en función de la variación de la ganancia (campo x)

.

Además, también se adjuntan las capturas de pantalla del teléfono móvil mostrando los resultados del único caso favorable del ataque (campo -x a 20 dB):

Figura 11: App GPS status buscando señal GPS

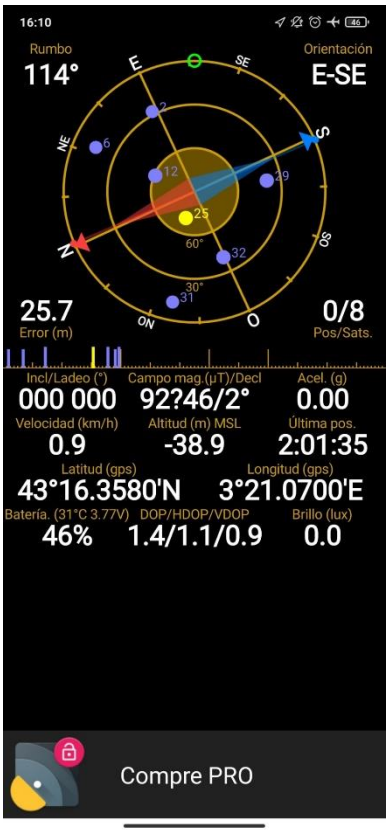


Figura 12: App GPS status con coordenadas del ataque por spoofing

Figura 13: App Google Maps mostrando la ubicación del ataque por spoofing

En las imágenes anteriores se puede observar (de izquierda a derecha): la aplicación GPS status buscando señal de GPS, la aplicación GPS status mostrando una constelación simulada de 8 satélites, las coordenadas del punto arbitrario elegido en la costa mediterránea francesa (véase Anexo VII: Proceso Spoofing) y la aplicación Google Maps mostrando la ubicación en dicho punto.

Como se ha comentado anteriormente, el ataque se ha realizado en un radio relativamente pequeño (1,5 m) y libre de la recepción por parte del terminal de otras

señales GPS. Sería conveniente ponerlo en práctica con el uso de un amplificador externo, debido a que 1,5 m no es una distancia al enemigo lo suficientemente segura para realizar un ataque de spoofing por parte de fuerzas propias. Para fuerzas ligeras una distancia aceptable sería 800 m – 1 km, mientras que para otro tipo de fuerzas que dispongan de menor movilidad esta sería de unos 8 a 10 km. Este tipo de mejora sobre el sistema final aparece desarrollado en 4.5.1. Ganancia.

4.3.2. Radioteléfono ligero PR4G v3

De manera similar al ataque anterior, se ha probado el sistema contra un receptor GNSS más robusto, el radioteléfono ligero PR4G.

El ataque se ha realizado contra una PR4G v3[12] (por ser este modelo el que tiene funcionalidad GPS) montada sobre una estación Mercurio. Para más información sobre la radio en cuestión véase el Anexo VIII: Radioteléfono ligero PR4G v3 (RT-9210 V3), de igual manera para obtener más información sobre la estación Mercurio véase el Anexo I: Estación Mercurio 2000.

El funcionamiento de Rx GNSS por parte de la radio es el que se detalla a continuación. El radioteléfono, en su forma portátil, no tiene ninguna antena con funcionalidad GNSS, pero si dispone de un conector SMA en el cual se podría conectar, por ejemplo, una antena como la utilizada en el caso anterior (ataque a teléfono móvil). Otra opción sería conectar la radio a una estación vehicular, como es el caso del Mercurio. De esta manera, la antena de la propia estación cuenta en su base con una antena GPS. Se ha optado por la segunda opción, siendo un objetivo por engañar (spoofing) más robusto. En concreto, la antena con la que cuenta dicha estación es la: ANT 3088 LP/GPS, antena del tipo monopolo vertical de bajo perfil para su montaje en blindados y que requiere un plano de tierra mayor que la del tipo dipolo. Dispone de una antena GPS integrada que evita tener que disponer de una ubicación específica de dicha antena, que trabaja en L1, 1575,42 ± 10 MHz. (Ministerio de Defensa, 2012).

El sistema de contramedidas también varía con respecto al caso anterior, esta vez se ha conectado al HackRF una base de antena seguida de una antena de varilla simple, capaz de operar desde los 40 MHz hasta los 6 GHz, el diagrama de Tx/Rx se muestra en la siguiente imagen:

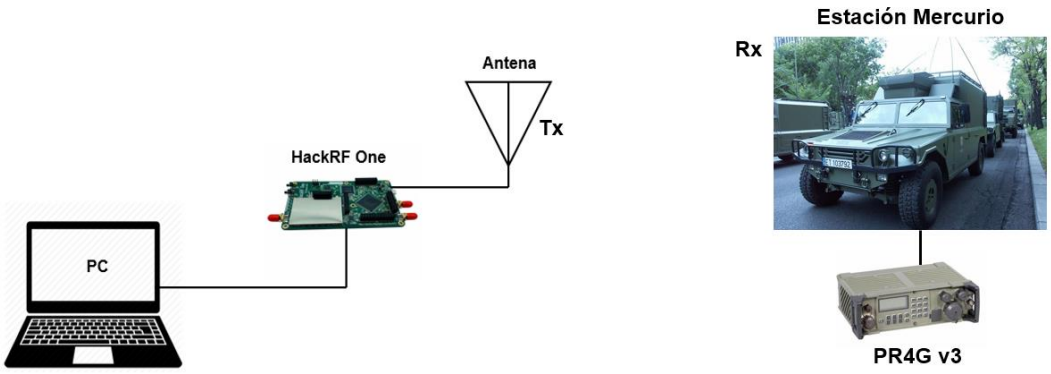


Figura 14: diagrama Rx/Tx spoofing a PR4G

Como se puede observar en las imágenes de a continuación, la base de la antena verde se corresponde la de la estación Mercurio, mientras que la antena de color metálico es la del sistema SDR. También se puede observar que la práctica se realiza en un

[12] También se puede encontrar referencias a esta radio como RT-9210 V3

entorno abierto (patio de armas del REW31) donde la radio es capaz de geolocalizarse en menos de 10 s.

Figura 15: Base de antena Mercurio y antena del sistema SDR

Figura 16: Vista completa de ambas antenas

Los resultados de las pruebas se detallan en la siguiente tabla:

Valor campo -x	Resultado de la decepción	Observaciones	
		Tiempo en perder las coordenadas reales (s)	Se mantiene la señal GPS original
47	Desfavorable	5	No
30	Desfavorable	12	No
25	Desfavorable	19	No
20	Desfavorable	25	No
10	Desfavorable	No afecta	Sí
0	Desfavorable	No afecta	Sí

Tabla 5: Resultados pruebas spoofing a PR4G v3

En base a los resultados obtenidos, se puede observar que en ningún caso se consigue realizar exitosamente el ataque de spoofing sobre la PR4G, obteniéndose únicamente una perturbación en valores del campo -x mayores a 20, es decir, en este caso no se consigue un ataque de decepción, pero sí de perturbación (jamming). En las siguientes imágenes se puede observar (de izquierda a derecha): PR4G mostrando coordenadas de El Pardo (Madrid) y la misma radio perdiendo las coordenadas anteriores cuando el HackRF comenzaba a emitir la señal simulada.

Figura 18: PR4G v3 con coordenadas de El Pardo (Madrid)

Figura 17: PR4G v3 tras ataque spoofing

Se afirma de esta manera, que en ningún momento se llega a engañar al receptor, pero para valores de -x mayores o iguales a 20 dB se produce un efectivo ataque de jamming. Anteriormente, se llegó a la conclusión de que la técnica de jamming más efectiva (Protocol-Aware Jamming) producía un espectro muy similar al que emitiría el HackRF al transmitir una coordenadas arbitrarias o falsas con gps-sdr-sim (Ferreira, et al., 2020). Se afirma de esta manera, que la técnica más eficaz de jamming es, por lo tanto, un ataque de spoofing.

Tras consultar los resultados de esta práctica con el grupo de discusión (véase Anexo II: Grupo de discusión), se ha llegado a las siguientes conclusiones: el ataque debería de ser más eficaz con unas coordenadas simuladas más cercanas a la ubicación real del dispositivo[13], debido a que de esta manera podría bajar la capacidad del receptor de discriminar entre unas efemérides reales y unas falsas. Las señales de GPS son muy débiles a su llegada al receptor, por ello la sensibilidad de este tipo de receptores suele estar entre -160 y -130 dBm (Domínguez Sánchez, 1999), esto podría ser otra razón para

[13] Para esta prueba se utilizaron unas coordenadas simuladas de Colombia.

explicar los fallos de spoofing de esta prueba, la sensibilidad de la antena, esta podría recibir una señal con una potencia relativamente superior a la que normalmente captaría y desecharla por ser falsa. Las señales son débiles debido a que la atenuación del radioenlace es mucho menor entre la antena del HackRF y la antena de la estación, que entre el satélite y la antena de la estación. La atenuación del radioenlace se puede calcular según la siguiente fórmula (Izquierdo, 2021):

$L\,(atenuación) = \left(\frac{4\pi f l}{c}\right)^2$, con l = longitud del radioenlace y c = velocidad de la luz en el vacío = 299.792.458 m/s. Se observa que a misma frecuencia (f) la atenuación es mayor cuanto mayor sea la longitud del radioenlace.

4.4. SISTEMA FINAL

En función de las técnicas analizadas anteriormente y de sus ventajas y desventajas, así como de los resultados extraídos de las pruebas realizadas, se propone el siguiente sistema final de contramedidas basado en SDR:

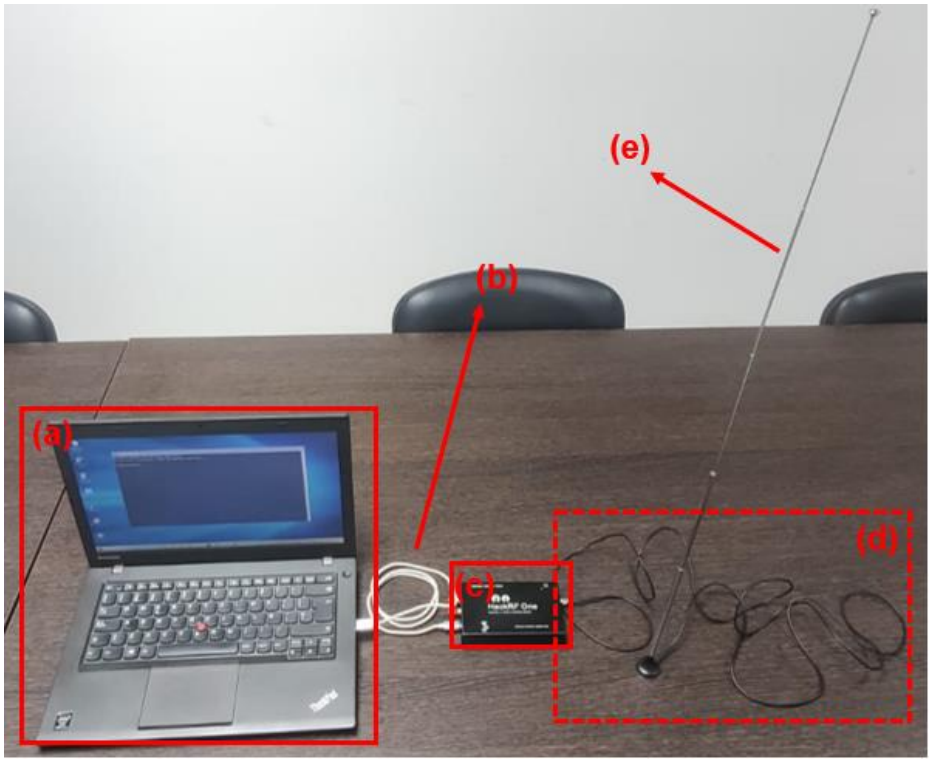


Figura 19: Sistema final

El sistema propuesto se ha de componer de los siguientes elementos:

a) Ordenador personal.

b) Cable de USB a micro USB.

c) HackRF One.

d) Base de antena.

e) Antena de varilla plegable apta para el siguiente rango de frecuencias: 40 MHz a 6 GHz.

A la vista está que un ataque de spoofing, si no es capaz de engañar al receptor GNSS, puede ser capaz de perturbarlo (Ferreira, et al., 2020). Por ello, el sistema propuesto tendrá únicamente la finalidad de realizar un ataque de spoofing con unas coordenadas simuladas cercanas al receptor al que se quiere atacar (radio de menos de 40 km). Esto presenta las siguientes ventajas en cuanto al desarrollo del sistema:

- Llevar a cabo un ataque de spoofing (según los pasos descritos en este trabajo, véase Anexo VII: Proceso Spoofing) presenta una dificultad menor que realizar un ataque de jamming, llegando la segunda técnica a usar diagramas de bloques (GNURadio) incluso implicando utilizar la programación (función barredora desarrollada en Python), mientras que un ataque de spoofing requiere únicamente seguir unos sencillos comandos.
- Realizar un ataque de spoofing requiere de unos requerimientos del sistema menores que los necesarios para un ataque de jamming. En cuanto a memoria (sólo es necesario instalar PothosSDR y utilizar la consola de comandos, mientras que para jamming se necesita: GNURadio, Geany, Python para Windows, librería matplotlib, etc.) y también en cuanto a rendimiento, la ejecución de la técnica de Sweep Jamming no se podía llegar a ejecutar por la ingente cantidad de recursos de los que requería por parte del ordenador personal.

De esta manera, en el caso de que no se consiga realizar un ataque de spoofing, se producirá un ataque jamming, siempre y cuando la distancia al receptor no sea excesiva.

4.4.1. Validación del sistema desarrollado

A continuación, se describe la prueba realiza para testear el sistema desarrollado. Seguidamente se puede encontrar una figura que representa dicha prueba de manera esquemática:

Figura 20: Prueba del Sistema final

Como se observa en la imagen anterior, las señales transmitidas desde el HackRF tienen como objeto atacar a dos receptores diferentes. El primero, consiste en un teléfono Xiaomi Mi 9t en modo avión, con la aplicación GPSstatus. El segundo consiste en un ordenador personal que adquiere la capacidad de recepción GPS gracias una antena conectada al puerto USB (dicha antena se muestra en la siguiente imagen). Los datos de

dicha antena son interpretados por el software U-Center 2, desarrollado por una conocida empresa de receptores GNSS llamada U-Blox.

Figura 21: Antena GPS USB modelo G-MOUSE

La prueba tiene lugar en un entorno abierto (patio exterior) donde ambos receptores son capaces de geolocalizarse en aproximadamente menos de 10 s. Es decir, en este caso, los receptores no solo van a recibir las señales de las coordenadas simuladas, sino también las originales. Se ha optado por emitir unas coordenadas de un lugar no relativamente lejano a los receptores (la prueba tuvo lugar en Alcalá de Henares (Madrid)), eligiéndose así un punto de la periferia de la ciudad de Guadalajara, concretamente: 40.635898, -3.181815, 20.

En las siguientes imágenes se puede observar unos de los resultados favorables obtenidos sobre ambos receptores, mostrando las coordenadas de la ubicación simulada de Guadalajara, tanto en el ordenador como en el teléfono móvil:

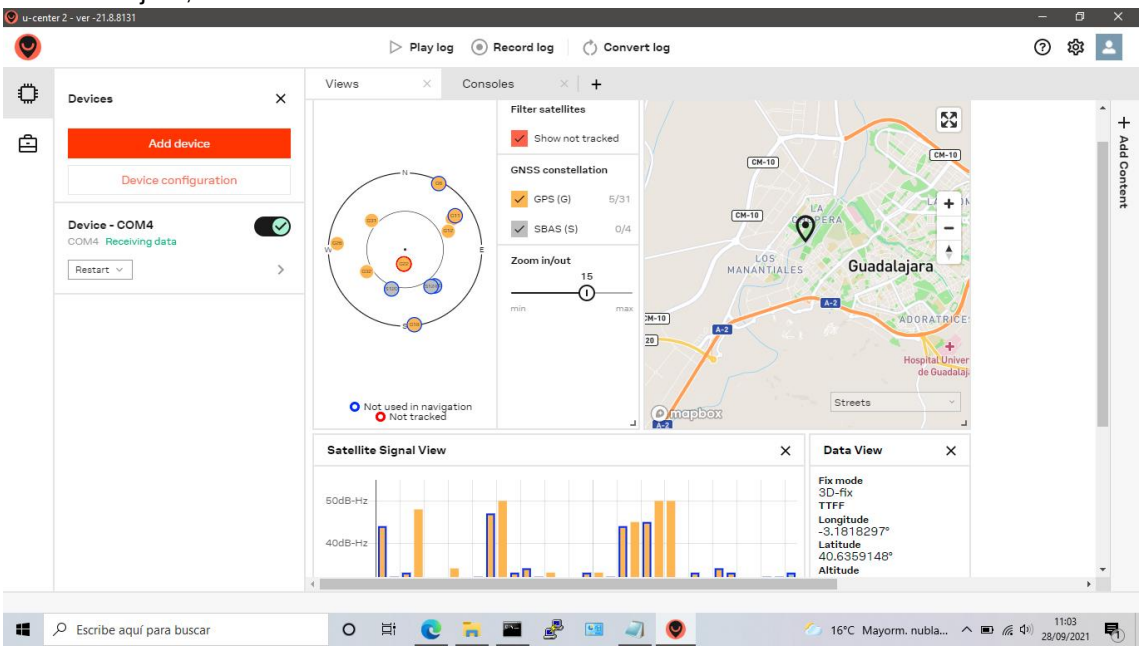


Figura 22: Ordenador personal mostrando ubicación simulada

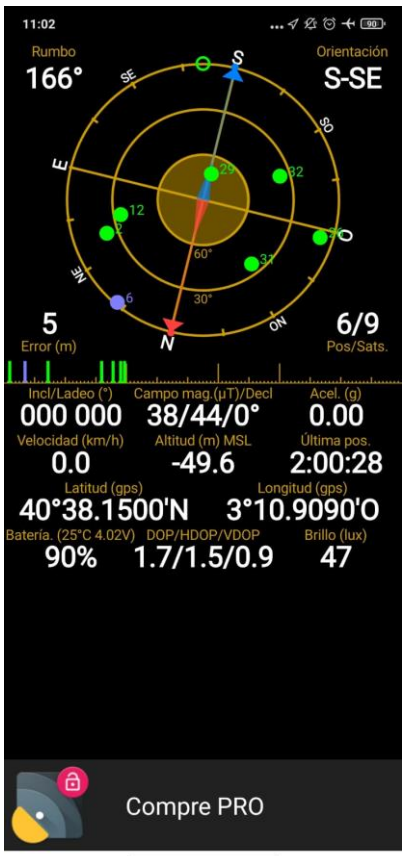


Figura 23: Teléfono móvil mostrando coordenadas simuladas

Los resultados de la práctica pueden observarse en el Anexo IX: Resultado práctica Sistema final. De los cuales, se extraen las siguientes conclusiones:

- Las distancias de los casos favorables no son lo suficientemente prudenciales como para realizar un ataque a una unidad enemiga, por ello se debe valorar el uso de un amplificador externo.
    - El ataque jamming contra el teléfono móvil deja de ser efectivo a partir de los 3,6 m.
    - El ataque spoofing contra el teléfono móvil a 1,2 m con una ganancia en el amplificador interno de IF de 20 dB.
    - Ambos ataques, jamming y spoofing, dejan de ser efectivos a partir de los 6 m.
- El receptor del teléfono móvil es más difícil de perturbar y de engañar que el ordenador personal equipado con la antena de GPS, pero esto no tiene porqué significar que el receptor GPS del teléfono es menos robusto que la antena GPS USB, sino que, por el contrario, la antena sea más sensible que el la integrada en el teléfono.

Finalmente, y con motivo ilustrativo de incluye unas fotografías tomadas durante la realización de esta práctica.

Figura 25: Realización práctica con Sistema Final 1

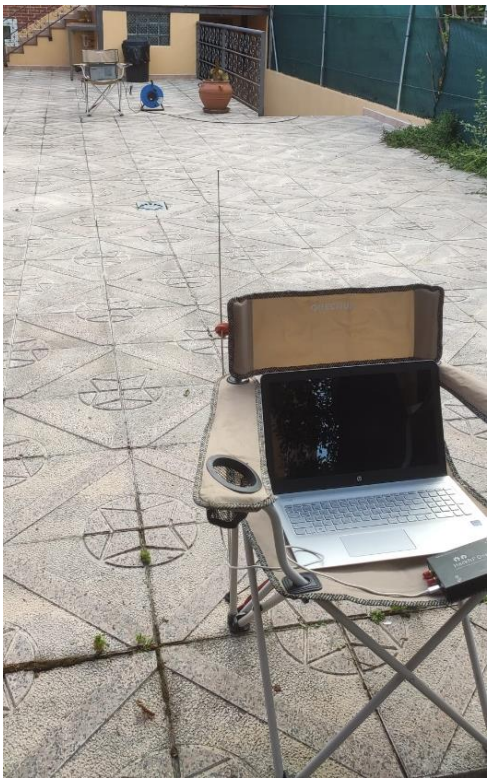


Figura 24: Realización práctica con Sistema Final 2

4.5. MEJORAS SOBRE EL SISTEMA FINAL

En este subcapítulo se diferencian dos formas de mejorar el sistema propuesto en el punto anterior: (1) Alcance eficaz; mediante el uso de amplificadores se propone aumentar la distancia efectiva de las contramedidas y (2) Portabilidad; se busca aumentar la movilidad del sistema.

4.5.1. Ganancia

En base a los resultados de la práctica realizada sobre el sistema final, los cuales se pueden encontrar en Anexo IX: Resultados práctica Sistema final. Considerando el caso en el cual se emitía con una ganancia del amplificador de IF de 30 dB a una distancia entre emisor y receptor de 2,4 m obteniéndose un resultado favorable, ya que se conseguía realizar jamming sobre un receptor (teléfono móvil) y spoofing sobre otro (ordenador portátil), dicha situación se recrea en la siguiente figura:

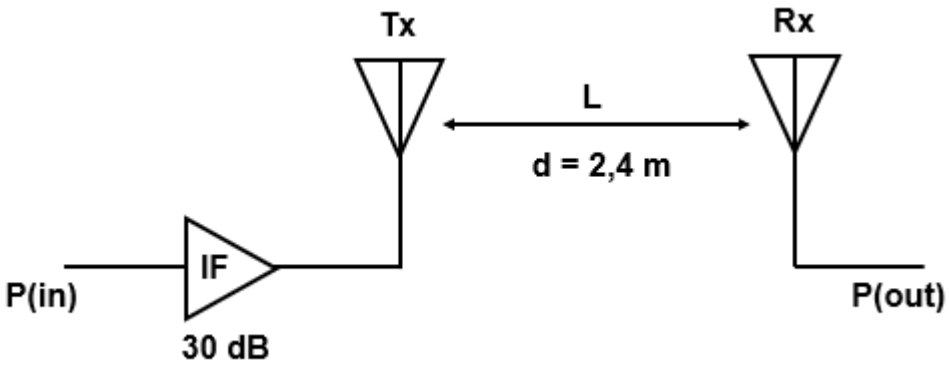


Figura 26: caso analizado en la práctica sobre el sistema final

Sabiendo que P(in) representa la potencia de transmisión del HackRF, P(out) significada la potencia de recepción que llega a los receptores situados a 2,4 m del emisor y que L es la atenuación causada por el aire en el radioenlace en cuestión, se va a obtener los valores de cada uno de estos parámetros:

- P(in): la potencia de emisión del HackRF a 10 MHz es 15 dBm y a 2150 MHz es 5 dBm (Ossmann, 2018), para hallar la potencia en la frecuencia de emisión (L1 GPS: 1575,42 MHz) se procede a realizar una interpolación lineal entre dichos valores, obteniendo como resultado: 7,685 dBm. Aplicando la fórmula: $P[dBW] = P[dBm] - 30\ dB$, se obtiene un valor final de -22,315 dB.
- L: se aplica la siguiente fórmula: $L = 20\log(d[km]) + 20\log(f[GHz]) + 92{,}45$ (Izquierdo, 2021). Obteniendo un valor de 44 dB.
- P(out): finalmente, se calcula este último parámetro $P(out) = P(in) + 30\ dB + L$, obteniéndose -46,32 dB o lo que es lo mismo -16,32 dBm.

De estos cálculos se extrae la siguiente conclusión, el sistema final actúa de manera óptima sobre los receptores cuando esto reciben a -46,32 dB. Para poder realizar el mismo efecto a una distancia mayor se necesita aumentar considerablemente la ganancia de nuestro sistema, por ello en este punto se valora el ensamblaje de un amplificador al sistema desarrollado. Con la finalidad de no disminuir la portabilidad del sistema se ha optado por una amplificador lna de tamaño considerablemente reducido (50x70x22mm), otras características importantes para tener en cuenta, como la alimentación (12V 70mA), se pueden observar en la fotografía:

Figura 27: Amp lna

Según especificaciones del fabricante de este amplificador (el cual aparece referenciado en las figuras como LNA) para una frecuencia de 1,59 GHz, muy aproximada a L1 GPS, se obtiene una ganancia de 48,18 dB. Si a esta ganancia le sumamos el máximo valor configurable vía software de la etapa IF del HackRF (47 dB – este valor se configuraba en el campo "-x" del comando del *hackrf_tranfer*) obtenemos un valor total de 95,18 dB. Se plantea entonces la siguiente situación:

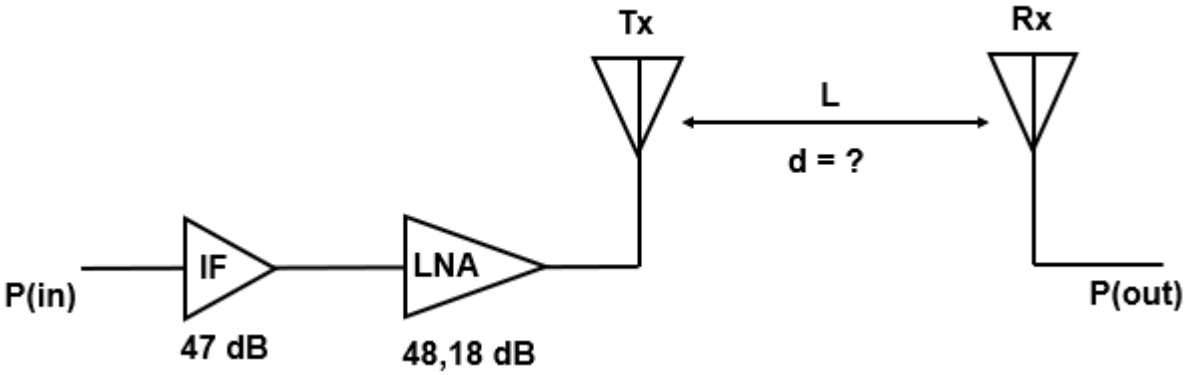


Figura 28: practica final con amp lna ensamblado en el sistema

Se utilizan los datos de P(in) y P(out) anteriormente calculados. La atenuación en el radioenlace se calcula en base a la siguiente ecuación: $P(out) = L + 48{,}18\ dB + 47\ dB + P(in)$, se obtiene un valor para L de -119,185 dB. Finalmente, teniendo en cuenta que $L = 20\log(d[km]) + 20\log(f[GHz]) + 92{,}45$, se extrae un valor concreto de la distancia: 13,78 km.

Finalmente se puede afirmar numéricamente que con el amplificador IF del HackRF a 47 dB y usando el amplificador LNA se podrían obtener resultados aparentemente favorables hasta una distancia aproximada de 13,78 km.

Con la finalidad de probar las características del sistema mejorado, se plantea una práctica análoga a la realizada sobre el sistema final (Práctica Sistema Final) con la diferencia de que la primera prueba se realizará a 4 m.

Para la alimentación del amplificador se utilizará una pila alcalina cilíndrica modelo A23 de 12V por medio de un adaptador, el amplificador lna se ensambla entre HackRF y antena, para ello se ha utilizado una transición SMA. El diagrama del sistema se muestra en la siguiente imagen:

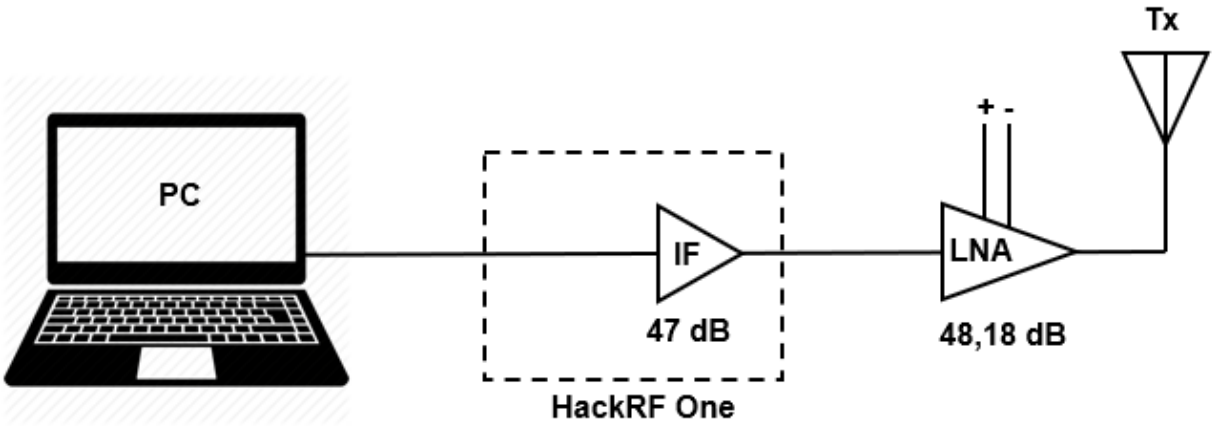


Figura 29: Sistema final + amp lna

Por otro lado, el sistema de contramedidas físico con el amplificador ensamblado gracias a la transición, y con su respectiva alimentación, adopta la forma que se observa a continuación:

Figura 30: Sistema con amp ensamblado

Antes de comenzar la práctica y con la finalidad de confirmar el estado de operatividad del amplificador con el que se está trabajando, este se ha conectado un osciloscopio digital. Desde el osciloscopio se ha generado una señal de pulso centrada en 1,59 GHz, esta entra al amplificador por el puerto SMA RF_in (el de la izquierda de la imagen mostrada a continuación) y debería de salir amplificada 48,18 dB por el puerto SMA RF_out (el de la derecha de la imagen mostrada a continuación). Pero en el osciloscopio no se recibió señal alguna, esto podría ser debido a que el amplificador en cuestión se encuentre inoperativo.

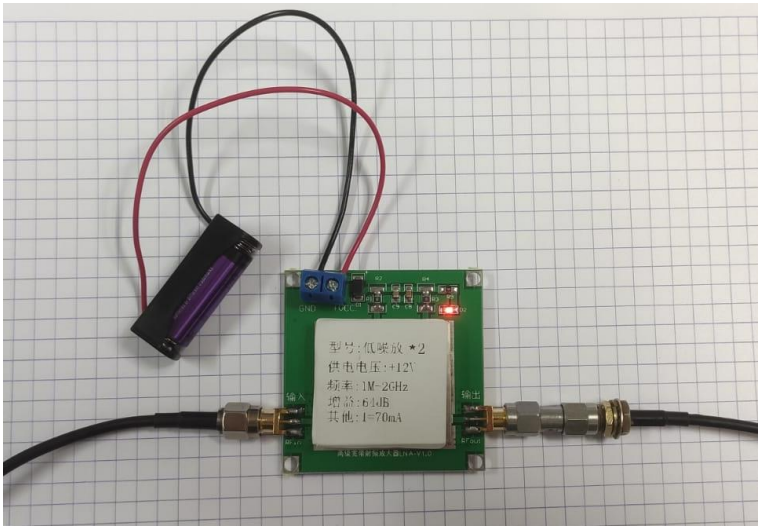


Figura 31: prueba del amplificador

Con la finalidad de acotar el problema y comprobar que efectivamente este tiene que ver con el amplificador: se descarta el estado de inoperatividad de la pila debido que se ha comprobado su tensión entre bornes del adaptador utilizado mediante un multímetro (obteniéndose 12,1 V aproximadamente en las diferentes medidas). También se

descartan problemas en el cable SMA utilizado, así como en la transición, debido a que se ha comprobado su correcto funcionamiento en el osciloscopio.

Aún con las comprobaciones pertinentes, se ha procedido a realizar una prueba sobre el sistema con el amplificador. En esta prueba el receptor también ha variado, se puede observar en la siguiente imagen:

Figura 32: receptor para la prueba con amplificador

Para esta ocasión, únicamente un ordenador personal (con la misma antena receptora de GPS y software que en la práctica final) actuará como receptor eliminando de la escena al teléfono móvil. En su lugar se añade un periférico SDR (RTL-SDR) utilizando el software SDR Console v3 (se puede observar la instalación de este programa en el Anexo V: Instalación HackRF One en ordenador personal) con la finalidad de poder observar el espectro electromagnético, en la imagen de a continuación muestra que de esta forma no se recibe ningún tipo de señal en la banda L1 de GPS:

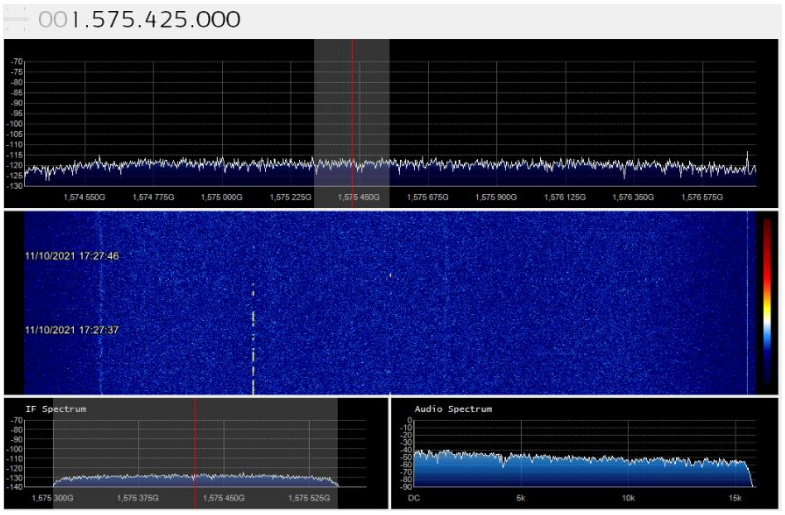


Figura 33: RTL-SDR recibiendo ruido

Se concluye finalmente que el amplificador no funciona, debido a que a 4 m no se recibe nada más que ruido, además tampoco se obtienen efectos de jamming, como se observa en la siguiente imagen, que muestra las coordenadas original del lugar de la práctica captadas por el ordenador personal:

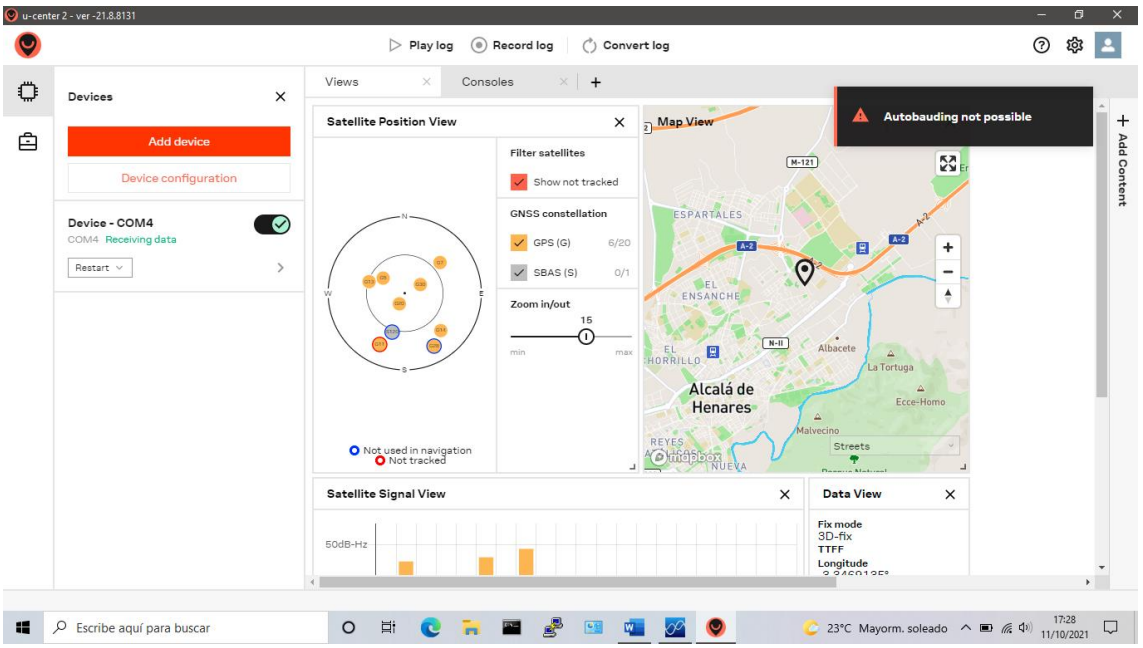


Figura 34: U-center 2 mostrando coordenadas originales de la práctica

Mientras que, a la misma distancia, sin uso del amplificador, sí que se produce un favorable ataque de jamming sobre el receptor, esto se observa en la imagen de a continuación:

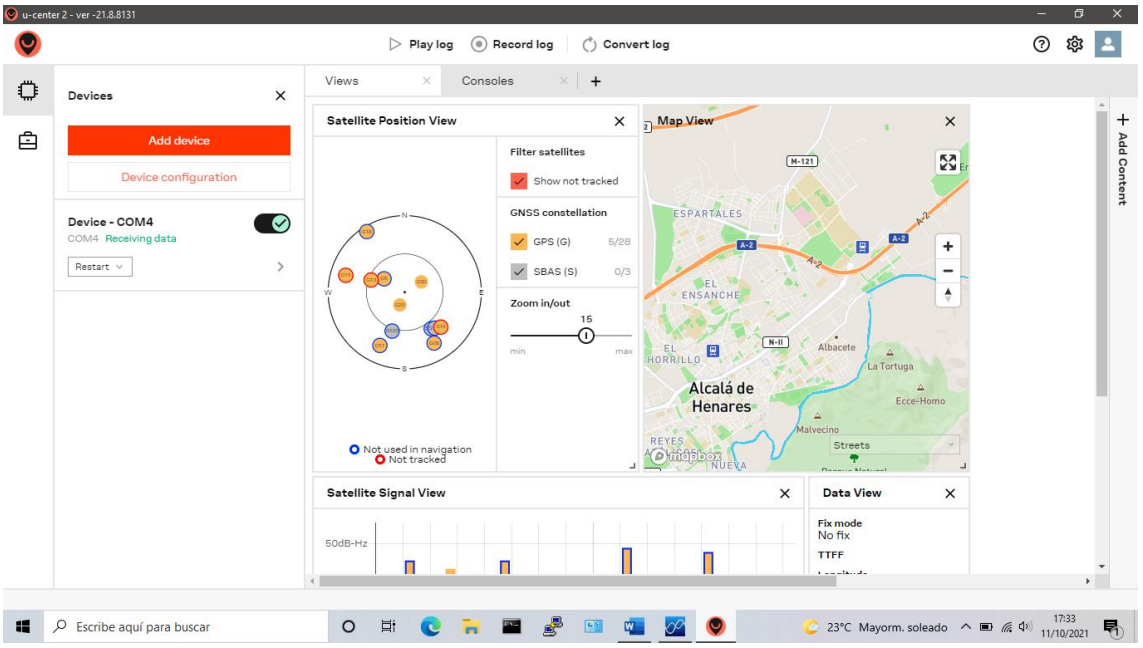


Figura 35: U-center 2 tras la pérdida de las coordenadas originales

Finalmente, la principal conclusión extraída de esta práctica es que teóricamente el sistema de contramedidas podría ser efectivo en un radio de 13,78 km con un amplificador de 48,18 dB de ganancia conectado en serie al HackRF.

El uso de un amplificador externo generaría armónicos en la señal, sería conveniente utilizar un filtro paso banda, este se colocaría entre el amplificador y la antena. El filtro

ideal para el sistema debería de ser capaz de aislar la señal GPS banda L1, es decir, de $Frecuencia\ central - BW/2$ hasta $Frecuencia\ centra + BW/2$, según los datos expuestos en la introducción (datos señales en Los Sistemas GNSS), estas frecuencias serían 1567,7475 MHz y 1583,0925 MHz respectivamente. Por esto se propone utilizar un filtro de similar circuitería al expuesto siguiente imagen:

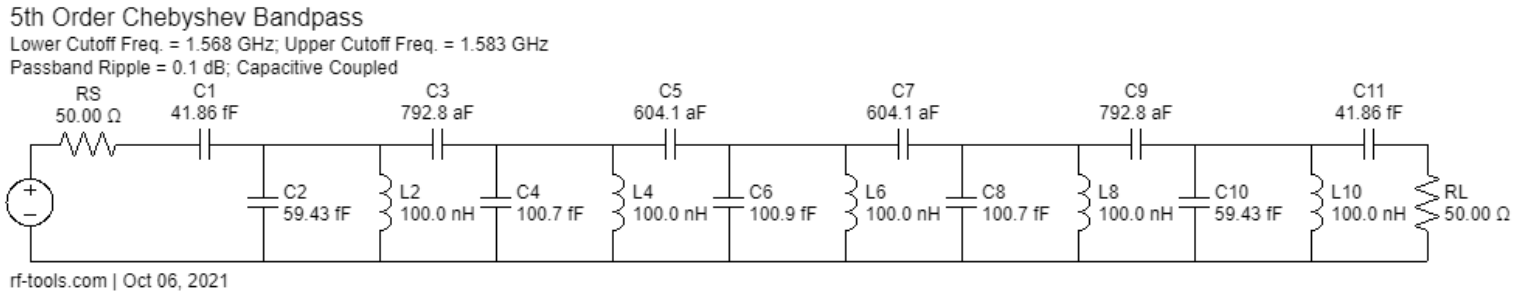


Figura 36: Filtro paso banda, obtenido de: https://rf-tools.com/lc-filter/

Debido a esta modificación, el diagrama de bloques del sistema quedaría de la siguiente forma:

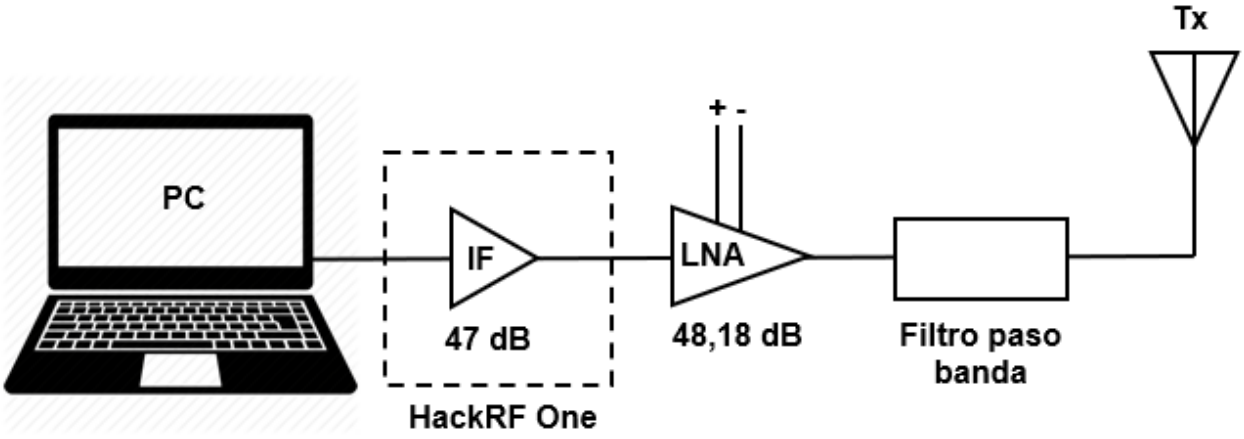


Figura 37: Sistema final + amp lna + filtro

4.5.2. Portabilidad

Con la única finalidad de aumentar la portabilidad del sistema se propone cambiar el ordenador personal del sistema final por una Raspberry Pi. Esto conseguiría reducir considerablemente el tamaño del sistema además del peso del conjunto, facilitando así su transporte y aumentando así el abanico de posibilidades de efectuar las medidas de EA para las que está diseñado. Esta variación, junto con la sencillez de la interfaz, podría llevar al uso del sistema de contramedidas aquí desarrollado por unidades ligeras del ET.

Raspberry Pi es una serie de ordenadores de placa reducida. Tiene unas dimensiones de 85 x 53 mm, muy similares a las de una tarjeta de crédito. El precio de esta placa de desarrollo ronda los 100€, es decir, no supone una gran variación en el coste siendo este precio inferior al de un ordenador personal. Además, este tipo de ordenador reducido también se encuentra en dotación en el Regimiento dónde se han realizado las prácticas externas. En cuanto a sus componentes hardware, suele contar

con 1 GB de memoria RAM (Raspberry Pi 3 modelo B+) y diferentes puertos de expansión, entre ellos:

- USB para conectar al HackRF One.
- Alimentación por micro USB, dónde se conectará una batería externa.
- Slot de microSD, en la cual se instalará el sistema operativo a utilizar.

En las imágenes de a continuación se puede observar la placa del micro ordenador en cuestión con los puertos a utilizar señalados:

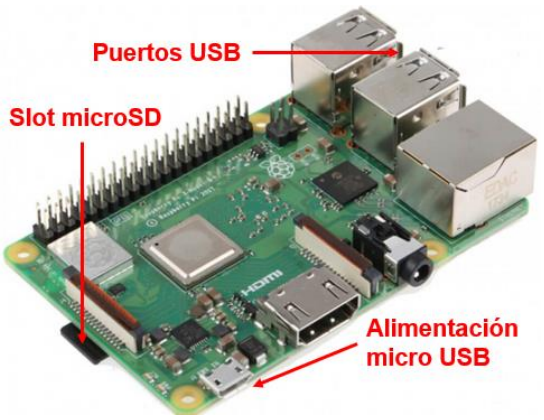


Figura 38: Raspberry Pi 3 modelo B+

De esta manera el sistema, contando con las mejoras propuesta en el punto anterior (véase 4.5.1. Ganancia) se correspondería con el diagrama de la imagen de continuación.

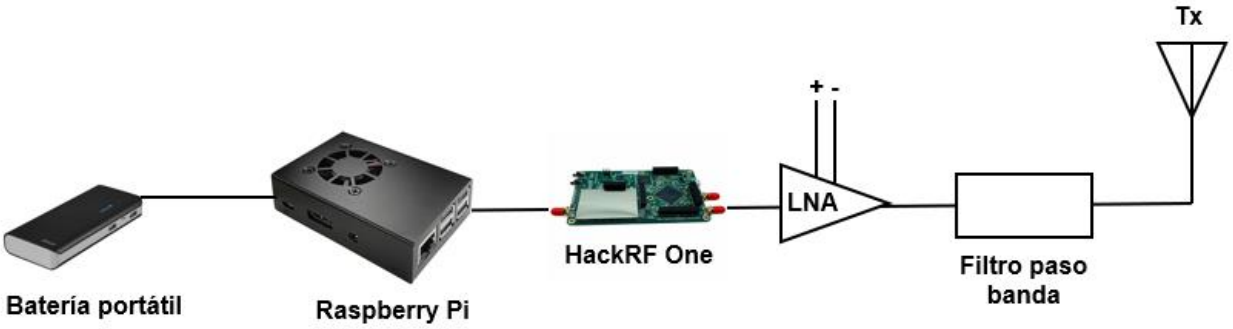


Figura 39: Sistema final con Raspberry Pi

5. CONCLUSIONES

En este último punto del trabajo se presentan las diferentes conclusiones extraídas a partir de los objetivos ya analizados (véase 2.1. Objetivos y Alcance). Además, se proponen diferentes soluciones a las limitaciones encontradas.

En primer lugar, se puede afirmar que se ha conseguido satisfactoriamente el objetivo general. Se ha creado un sistema de contramedidas con la capacidad de efectuar acciones de jamming y spoofing contra receptores GPS, prueba de ello son las diferentes prácticas que se pueden encontrar en el cuerpo del trabajo. En las cuales, si el sistema no era capaz de engañar al receptor para que este mostrara unas coordenadas falsas si conseguía imposibilitar la geolocalización, todo esto a una distancia relativamente reducida del objetivo.

Por otro lado, y con el objetivo específico de ampliar la distancia de acción del sistema, se valoró la posibilidad de ensamblar un amplificador externo al sistema. Las pruebas realizadas no fueron satisfactorias debido a que el amplificador utilizado se encontraba inoperativo, pero se estimó la distancia efectiva que podría alcanzar el sistema con el uso de este, la cual se puede consultar en 4.5.1. Ganancia. Dentro de este mismo objetivo también se valoraba utilizar antenas más directivas (las utilizadas en las pruebas son omnidireccionales), pero esto no se pudo llevar a cabo por falta de medios.

El sistema desarrollado tiene las siguientes especificidades, las cuales se extraen de los objetivos específicos. Una interfaz del sistema user-friendly, así el sistema final únicamente necesita cuatro líneas introducidas por consola de comandos para efectuar las acciones de EA. Asimismo, los requisitos de hardware necesarios para ejecutar dichas acciones son muy reducidos, pudiendo usar así ordenadores de bajo rendimiento, coincidiendo estos con los que podemos encontrar en las diferentes unidades del ET. Además, para todas las partes del sistema se ha utilizado material en dotación, desarrollándose así el sistema sin ningún tipo de coste para el ET.

En resumen, además de haber cumplido con los objetivos del trabajo se ha conseguido que el sistema, aparte de ser sencillo de utilizar, sea extremadamente barato y portable, explotando más aún esta última capacidad en 4.5.2. Portabilidad (se sustituyen el ordenador personal por una Raspberry Pi). El único problema encontrado ha sido la distancia efectiva del sistema. Por ello se propone el ensamblaje a este de un amplificador operativo, de manera análoga a 4.5.1. Ganancia, además se podría utilizar una antena directiva capaz de trabajar en la banda L1 de GPS y de conectarse por SMA al sistema. Esta antena podría ser acompañada de un sistema de apuntado, que por lo general sería manual, es decir el propio operador apunta hacia sistema enemigo al que quiere dirigir el ataque. De este modo se aumentaría el alcance del sistema de contramedidas propuesto.

6. REFERENCIAS BIBLIOGRÁFICAS

Bažec, M., Luin, B. & Dimc, F., 2016. *Research Gate: GPS JAMMING DETECTION WITH SDR.* [En línea]
Available at: https://www.researchgate.net/publication/304777109
[Último acceso: 13 Octubre 2021].

Chicharro Sánchez-Agustino, J. A., 2019. *El GPS un atractivo blanco para el enemigo.* Primera ed. Madrid: Ministerio de Defensa.

Domínguez Sánchez, J. J., 1999. Sistemas de posicionamiento. GPS. *Anales de mecánica y electricidad,* LXXVI(2), pp. 28-42.

Fernández, F. J., 2021. Regimiento de Guerra Electrónica nº 31: 25 años dominando el espectro. *EJÉRCITO,* I(962), pp. 69-77.

Ferreira, R., Gaspar, J., Sebastiao, P. & Souto, N., 2020. *Efective GPS Jamming Techniques for UAVs Using Low-Cost SDR Platforms.* [En línea]
Available at: https://doi.org/10.1007/s11277-020-07212-6
[Último acceso: 2021 Septiembre 17].

Gaspar, J., Ferreira, R., Sebastiao, P. & Souto, N., 2020. *Capture of UAVs through GPS spoofing using low-cost SDR platforms.* [En línea]
Available at: https://dx.doi.org/10.1007/s11277-020-07211-7
[Último acceso: 14 Septiembre 2021].

Hussain, A. y otros, 2014. Protocol-aware radio frequency. *Journal of Communications and Networks,* 16(4), pp. 397-406.

Rahman, A. D. B. A., Ghani, K. A., Khamis, N. H. H. & Sidek, A. R. M., 2021. Unmanned Aerial Vehicle (UAV) GPS Jamming Test by using Software Defined Radio (SDR) platform. *Journal of Physics: Conference Series,* II(1793), p. ref. 012060.

Rodríguez de Haro, J., 2017. *Análisis software y hardware del SDR HackRF One.* Universidad de Granada: Trabajo Fin de Grado.

Referencias de manuales de Defensa:

Ministerio de Defensa, 2011. *MI4-503. MANUAL DE INSTRUCCIÓN MERCURIO 2000.* Primera ed. Granada: Ministerio de Defensa - Mando de Adiestramiento y Doctrina.

Ministerio de Defensa, 2012. *Manual de Operación y Mantenimiento Orgánico de 1º y 2º Escalón de las configuraciones dotadas con el RT-9210 V3.* Quinta ed. Granada: Ministerio de Defensa.
Ministerio de Defensa, 2016. *MI-500. RADIOTELÉFONO PR4G V3.* Primera ed. Granada: Ministerio de Defensa - Mando de Adiestramientro y Doctrina.

Ministerio de Defensa, 2017. *PD4-504. PUBLICACIÓN DOCTRINAL: Empleo de las Unidades desplegables de Guerra Electrónica.* Primera ed. Granada: Ministerio de Defensa - Mando de Adiestramientro y Doctrina.

Ministerio de Defensa, 2019. *Entorno Opertaivo 2035.* Primera ed. Madrid: Secretaría General Técnica del Ministerio de Defensa.

Referencias docentes:

Álvarez Pérez, J. L., 2021. *Apuntes de clase: Sistemas de Navegación Satelital,* Asignatura "Teoría de la Señal y Comunicaciones": Universidad de Alcalá de Henares: grado en Ingeniería Técnica en Sistemas de Telecomunicación.

García Martín, A., Lamelas, T. & Montealegre, A., 2021. *Apuntes de clase: Bloque II: Los Sistemas GNSS como fuente de información en los SIG,* Asignatura “Información geográfica digital y Teledetección": Centro Universitario de la Defensa: grado en ingeniería de organización industrial.

Izquierdo, D., 2021. *Apuntes de clase: Tema 3: El Canal de Transmisión,* Asignatura "Teoría de la Comunicación": Centro Universitario de la Defensa: grado en ingeniería de organización industrial.

Referencias webs:

defensa.com, 2017. *Protegiendo a las aeronaves contra perturbaciones de GPS.* [En línea]
Available at: https://www.defensa.com/industria/protegiendo-aeronaves-contra-perturbaciones-gps
[Último acceso: 23 Noviembre 2021].

Goward, D., 2017. *The Maritime Executive: Mass GPS Spoofing Attack in Black Sea?.* [En línea]
Available at: https://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea
[Último acceso: 13 Septiembre 2021].

Israel Defense, 2011. *Israel Defense: Future Fighting Without GPS?.* [En línea]
Available at: https://www.israeldefense.co.il/en/content/future-fighting-without-gps
[Último acceso: 16 Septiembre 2021].

Meta-Dèfense.fr, 2021. *Los drones de combate turco multiplican los éxitos comerciales.* [En línea]
Available at: https://es.meta-defense.fr/2021/06/14/Los-drones-de-combate-turcos-multiplican-los-%C3%A9xitos-comerciales/
[Último acceso: 1 Octubre 2021].

Navarro García, J. M., 2017. *Defensa.com: CENTUM demuestra su solución antidrones NoFlyZrone.* [En línea]
Available at: https://www.defensa.com/espana/centum-demuestra-solucion-antidrones-noflyzrone
[Último acceso: 16 Septiembre 2021].

O'Dwyer, G., 2018. *Defense News: Finland, Norway press Russia on suspected GPS jamming during NATO drill.* [En línea]
Available at: https://www.defensenews.com/global/europe/2018/11/16/finland-norway-press-russia-on-suspected-gps-jamming-during-nato-drill/
[Último acceso: 23 Octubre 2021].

osqzss, 2021. *GPS-SDR-SIM (GitHub).* [En línea]
Available at: https://github.com/osqzss/gps-sdr-sim
[Último acceso: 14 Septiembre 2021].

Ossmann, M., 2018. *GitHub: repositorio oficial del HackRF One.* [En línea]
Available at: https://www.robotshop.com/media/files/content/s/spa/pdf/hackrf-one-software-defined-radio-datasheet.pdf
[Último acceso: 27 Septiembre 2021].

Ossmann, M., 2021. *HackRF's documentation.* [En línea]
Available at: https://hackrf.readthedocs.io/_/downloads/en/latest/pdf/
[Último acceso: 27 Septiembre 2021].

Pastor, J., 2018. *Xataka: Así es como los 'Drone Jammers' usan sus rifles de radiofrecuencia para derribar drones en pleno vuelo.* [En línea]
Available at: https://www.xataka.com/drones/asi-como-drone-jammers-usan-sus-rifles-radiofrecuencia-para-derribar-drones-pleno-vuelo
[Último acceso: 2021 Septiembre 16].

Rawnsley, A., 2011. *Wired: Iran's Alleged Drone Hack: Tough, but Possible.* [En línea]
Available at: https://www.wired.com/2011/12/iran-drone-hack-gps/
[Último acceso: 13 Septiembre 2021].

Tispain, 2011. *El primer sistema de navegación basado en satélites.* [En línea]
Available at: https://www.tispain.com/2011/03/el-transit-primer-sistema-de-navegacion-gps-basado-en-satelites.html
[Último acceso: 1 Octubre 2021].

UASweekly.com, 2021. *ADA, an Anti-Jam GPS System, was successfully operated during Operation 'Guardian of the Walls'.* [En línea]
Available at: https://uasweekly.com/2021/10/20/ada-an-anti-jam-gps-system-was-successfully-operated-during-operation-guardian-of-the-walls/
[Último acceso: 23 Octubre 2021].

ANEXOS

Anexo I: Estación Mercurio 2000

En el presente anexo se relaciona la información esencial necesaria para entender el papel de la Estación Mercurio 2000 en la práctica de spoofing realizada en este trabajo. Seguidamente se puede encontrar una imagen que muestra la estación en cuestión.

Figura A. 1: Estación Mercurio 2000 sobre vehículo vamtac

Para satisfacer las necesidades de conocer y transmitir la información y las órdenes se necesita, de forma general, un sistema de telecomunicaciones. Un sistema inicial rápido en su establecimiento, con grandes distancias de cobertura y fiable en su permanencia es el proporcionado por los medios radio.

El mercurio 2000 es un vehículo de transmisiones radio que da servicio a los centros de transmisiones de los PC (Centro de mando) de GU (Gran Unidad) y los PC de PU (Pequeña Unidad), así como a los centros de transmisiones nodales de la red básica de área (RBA), y que, gracias a las medidas TRANSEC (salto de frecuencia) y COMSEC (cifrado) de las propias emisoras que monta, permite un enlace seguro en un entorno de protección electrónica (medidas EPM: Electronic protection measures - Medidas de protección electrónica).

Se trata de una estación radio equipada para dar servicio en los distintos centros de transmisiones de GU, o en los PC de PU, es decir:

- En CE (Cuerpo de Ejército) /División: CTPC (Centro de Transmisiones del Puesto de Mando), CTPCTAC (Centro de Transmisiones del Puesto de Mando Táctico) y CT nodales.
- En una brigada: CTPC.
- En AGT (Agrupación Táctica) /GT (Grupo Táctico) /batallón: asociado al PC.

En los CT Nodales y en los PC de PU nos encontraremos un solo Mercurio-2000. En el resto de CT dispondremos de Mercurios en número acorde a las redes de VHF y HF que se establezcan en cada situación.

Cada estación Mercurio-2000 nos proporciona capacidad de acceso e integración en dos redes de VHF (voz/datos) y una de HF (voz/datos). A continuación, sólo se desarrolla la información relevante de la red VHF por ser esta la utilizada en la práctica.

Para las dos redes de VHF, cada estación cuenta con dos RT-9500 V2/RT-9210 V3 de la familia PR4G, ambas con sus accesorios: microteléfono, altavoz y antena vehicular. Estas redes pueden explotarse desde el propio vehículo, parado o en movimiento, o desde el exterior mediante un mando a distancia TRC-9730, esto último con el vehículo detenido. Estas emisoras pueden trabajar en los modos de funcionamiento: SFR (salto de frecuencia), BCL (búsqueda de canal libre), MIX (mixto), FFD (frecuencia fija digital) y FFA (frecuencia fija analógica).

Por último, el Mercurio 2000 contiene el software de SIMACET (Sistema de Mando y control del Ejército de Tierra), lo que, junto al resto de elementos, le permite constituirse como un cliente aislado, un Nodo SIMACET PU o una pasarela SIMACET GU-PU. Y, por último, la impresora nos permite disponer de la mensajería en formato papel.

Referencia bibliográfica: (Ministerio de Defensa, 2011)

Anexo II: Grupo de discusión

A continuación, se puede encontrar una relación del personal militar destinado en el REW 31 que conforma el grupo de expertos. Todos ellos han ayudado a extraer parte de las conclusiones sobre las pruebas realizadas en este mismo trabajo. El grupo está conformado por cuatro suboficiales cuya amplia experiencia en el ámbito de las transmisiones y más concretamente en la EW ha sido de gran ayuda para el trabajo en general. Han demostrado así, aparte de sus grandes capacidades como militares, sus amplios conocimientos en la materia.

Brigada Jose Luis Abejaro Soto, especialidad fundamental de Transmisiones.

Comenzó su empleo de Sargento en el REW 31 como operador y supervisor de estaciones del antiguo sistema TELEOKA, se trata del primer sistema de EW que tuvo el Ejército de Tierra, posteriormente evolucionaría al sistema GESTA, el cual se sigue usando en la actualidad. Su carrera militar también ha estado relacionada con la docencia militar, ejerciendo el mando durante el empleo de Sargento 1º de una sección de alumnos en la Academia de Ingenieros del Ejército cuna de suboficiales y oficiales de la especialidad fundamental de Transmisiones, situada en Hoyo de Manzanares (Madrid). Posteriormente ejerció como Auxiliar del Jefe de la Cía de Telecomunicaciones del BEW I/31. En la actualidad, está destinado en la Plana Mayor de Mando del BEW I/31 como auxiliar de la célula de operaciones.

El Brigada Abejaro aportó información de gran valor sobre el ataque realizado contra el radioteléfono ligero militar. Debido a sus amplios conocimientos del RT-9210 V3 (PR4G v3) y de la EW, ayudó en gran manera a interpretar los resultados de esta práctica.

Sargento 1º Adoración Carrasco Alcaraz, especialidad fundamental de Transmisiones.

En el año 2008, comenzó el empleo de Sargento ejerciendo hasta el 2018 como Jefe de Equipos Satélites en la Sección de Satélites de la Cía. de Apoyo del Regimiento de Transmisiones 1 (Madrid). Durante esta etapa fue desplegada en tres ocasiones en zona de operaciones. La primera de ellas en el 2009 como Jefe de Centro de Comunicaciones en la misión LIBRE HIGALGO (El Líbano). Su segundo despliegue tuvo lugar en 2011 en Afganistán (misión ISAF-AFGANISTÁN) ocupando el puesto de Jefe de Equipos Satélites. Finalmente, en 2017 desplegó en Mali (misión EUTM MALI) también como Jefe de Centro de Comunicaciones. Posteriormente, desde el 2018 hasta la actualidad ha estado destinada en el BEW I/31 como Jefe de la sección de Mando e Interceptación de la Cía de Telecomunicaciones.

La Sargento 1º Carrasco, debido a su profunda experiencia en el campo de las comunicaciones satélite militar fue clave para interpretar los resultados de los diferentes ataques de Jamming y Spoofing, manifestó al resto del grupo de discusión la importancia de la potencia de emisión del sistema SDR, entre otros factores de vital importancia como la sensibilidad de las antenas receptoras de las prueba y la atenuación que sufría la señal al propagarse por el aire.

Sargento 1º Daniel Calomarde Lorente, especialista en Telecomunicaciones.

Durante el empleo de Sargento y Sargento primero ha ejercido como: Jefe de pelotón de mantenimiento de helicópteros en el Batallón de Helicopteros de Emergencia nº 2, ubicado en Bétera (Valencia), Jefe de pelotón de mantenimiento en Telecomunicaciones de la Red Básica de Área y del sistema SkyGuard (sistema de Artillería Antiaérea) en el Regimiento de Artillería Antiaérea nº 71 ubicado en Fuencarral (Madrid). También cuenta con experiencia en zona de operaciones ya que ejerció como jefe del mantenimiento especializado en Telecomunicaciones, telefonía y Red Básica de Área (Antiguo sistema de Radioenlace) del sistema Patriot (sistema de Artillería Antiaérea) en Turquía (misión AT/V Turquía). Durante su andadura en el REW 31 ha mandado de pelotón de mantenimiento de Red Básica de Área y del sistema GESTA. En la actualidad manda la sección de mantenimiento de material de telecomunicaciones en dicho regimiento.

El Sargento 1º Calomarde, debida a su amplia experiencia en el campo de las Telecomunicaciones y su capacidad de manejo de instrumentos típicos de un laboratorio de electrotecnia fue clave para interpretar los resultados de las pruebas en función de las potencias de emisión del HackRF, así como para comprobar el estado de operatividad de todos los componentes del sistema (cables, antenas y amplificador).

Sargento Pedro Manuel Ruiz García, especialidad fundamental de Transmisiones.

En el 2017 comenzó mandando el pelotón de estación sensoras (captación de información) para un año más tarde ejercer como jefe de pelotón estación de control (tratamiento e interpretación de información), ambos tipos de estaciones forman parte del sistema GESTA de EW operado por el BEW I/31. En este mismo año, 2018 fue Jefe medios de telecomunicaciones de la Cía de Telecomunicaciones. Desde el 2019 hasta la actualidad ejerce el mando del pelotón Sigilo del BEW I/31.

El Sargento Ruiz era el experto en el Regimiento sobre medios SDR, por ellos sus aportaciones fueron de vital importancia para la interpretación de los resultados obtenidos.

Anexo III: Información REW 31

El trabajo en general no tendría sentido sin comentar ciertos aspectos importantes sobre la unidad, lugar donde se han realizado las prácticas de mando a la vez que este trabajo y que ha prestado todos los medios específicos que se han utiliza para desarrollar el sistema.

Las capacidades de EW se llevaban desarrollando desde la primera publicación referente a la EW en el ET, la cual está fechada en julio de 1972, esto llevó, más adelante, a la creación en el 1988 del Regimiento de Transmisiones Táctica nº 21 (RETAC 21) en base Batallón de Guerra Electrónica Táctica. Más adelante, en junio del 1996, nace del seno de dicha unidad el Regimiento de Guerra Electrónica Táctica nº 31. El origen de este se encuentra en la necesidad del ET en renovar capacidades de EW. Posteriormente, en el año 2005, el apellido "Táctica" se suprimió del nombre de la unidad, mismo año en el que se crea dentro del regimiento una nueva unidad, la Unidad de Guerra Electrónica Táctica (Fernández, 2021).

En lo que respecta a la jerárquica interna del Ejército, el Regimiento depende directamente del Mando de Transmisiones del ET (MATRANS) cuyo Cuartel General se ubica en Bétera (Valencia), a su vez MATRANS depende del Mando de Apoyo a la Maniobra (MAM), el cuartel general de este se localiza en A Coruña y, finalmente, el MAM depende de la Fuerza Terrestre del ET (FUTER).

En cuanto a la orgánica actual del Regimiento, se diferencian tres elementos fundamentales:

- PLMM (Plana mayor de mando): que incluye un centro de control de apoyo logístico (CCAL) necesario para acelerar el proceso de adquisición de material del Regimiento, que tiene consideración de Órgano de Alta Especialización (OAE), facilitando la actualización de los medios empleados en un mundo en constante desarrollo como es la EW.
- BEW I/31 (Batallón de Guerra Electrónica I/31): que proporciona apoyo general de EW a unidades de entidad División y Cuerpo de ejército además de la capacidad de Ciberdefensa Militar táctica a las unidades de maniobra del ET.
- UEW II/31 (Unidad de Guerra Electrónica II/31): que proporciona apoyo directo de Guerra Electrónica Ligera (EWL) a las unidades de maniobra.

El Regimiento se ubica en el Acuartelamiento Zarco del Valle. Cabe destacar que se trata del cuartel en funcionamiento más antiguo de España, fue inaugurado en el 1817, en el Real sitio de El Pardo, manteniendo la misma ubicación en la actualidad. El cuartel recibió entonces el nombre del ilustre militar español D. Antonio Remón Zarco del Valle y Huet. En la siguiente figura se puede observar una vista aérea del lugar en la actualidad, junto con el escudo de armas del Regimiento.

Figura A. 3: Vista aérea del acuartelamiento, imagen obtenida de: https://ejercito.defensa.gob.es/unidades/Madrid/rew31/

Figura A. 2: Escudo de armas del REW 31, imagen obtenida de: https://ejercito.defensa.gob.es/unidades/Madrid/rew31/

Anexo IV: Instalación GNURadio

En primer lugar y teniendo en cuenta que PothosSDR ya se encuentra instalado sobre el ordenador personal, deberemos seguir los siguientes pasos:

- Instalar la última versión de Python disponible, descargando esta desde la página web oficial: Python, al instalar habilitar la opción “PATH” para añadir el plug-in de pip. Pip es un instalador de complementos para Python que se utilizará posteriormente.
- Desde la consola de comando de Windows comprobar que se ha instalado correctamente pip junto con Python. En la propia consola escribir pip, si esta la reconoce como un comando significa que la instalación tanto de Python como del plug-in pip ha sido satisfactoria.
- Instalar la librería de Python Mathplotlib, su función principal es representar gráficamente código Python y será necesaria para observar el espectro generado en GNURadio. En la consola de comandos escribir de forma sucesiva las siguientes líneas de código:

```
python -m pip install -U pip
python -m pip install -U matplotlib
```

- Con la finalidad de poder escribir código completando así las características de GNURadio se deberá de instalar un editor de Python. Se ha optado por Geany, debido a su fácil instalación y amigable interfaz. Se puede descargar la última versión disponible desde su página web oficial: Geany
- Ejecutar desde la ruta C:\Program Files\PothosSDR\bin el programa gnuradio-companion.exe y seguir los pasos relativos a la solución de errores de instalación que se apreciarán en el propio ejecutable. Repetir este paso hasta que al abrir gnuradio-companion.exe observemos la siguiente interfaz:

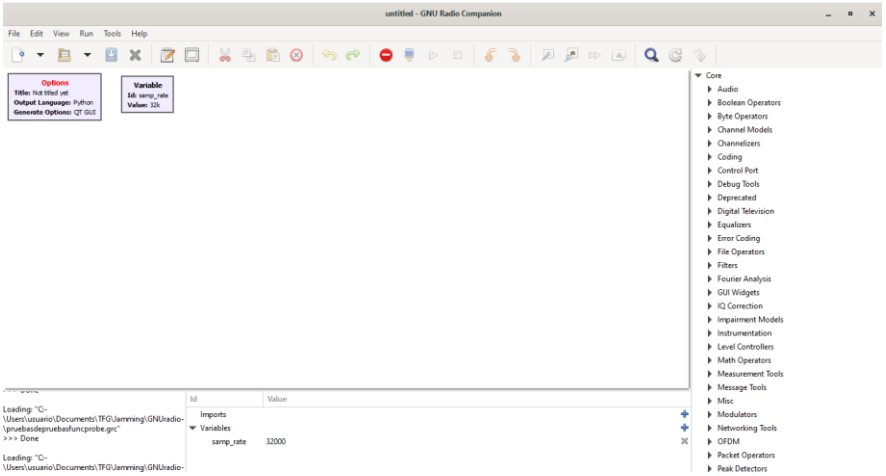


Figura A. 4: Interfaz de trabajo de GNURadio

Finalmente, GNURadio está listo para ser usado por el usuario.

Anexo V: Instalación HackRF One en ordenador personal

Antes de nada, se advierte de la facilidad de este proceso que a continuación se expone. Siendo únicamente necesario dos programas libres para poner en funcionamiento el transpondedor.

En primer lugar, una vez conectado en periférico (también se pueden hacer referencia a este tipo de hardware como *dongle*) a un puerto USB del ordenador (se recomienda seguir el siguiente orden: conectar la antena al transpondedor y posteriormente este a un puerto USB) se debe ejecutar el programa Zadig. Este es bastante intuitivo y su función principal es la correcta instalación de los drivers. Para obtener el programa se debe descargar directamente de la página web oficial: https://zadig.akeo.ie/. A día 07/09/2021 la última versión del software es la 2.6. Al ejecutar el programa encontraremos el siguiente interfaz:

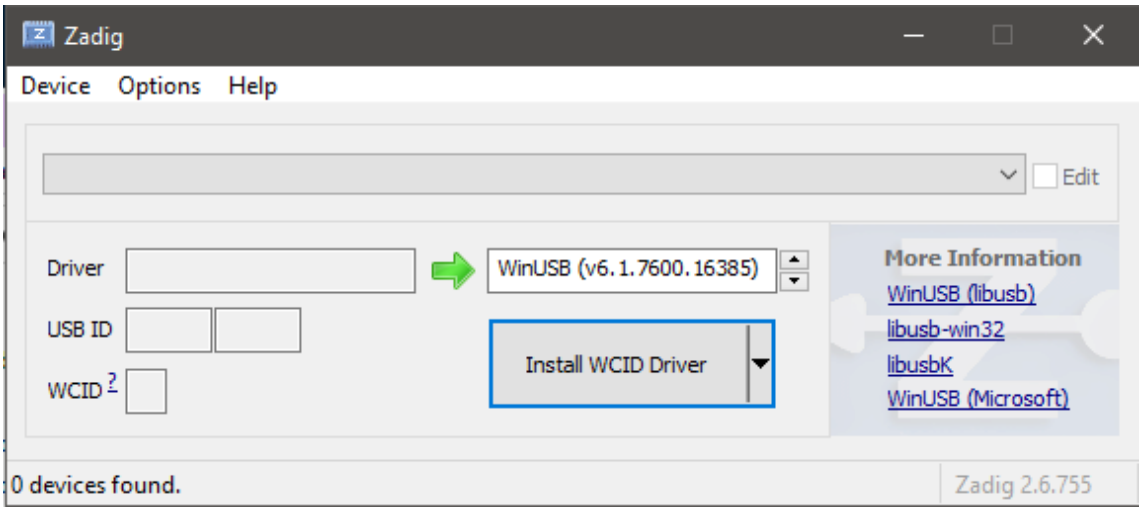


Figura A. 5: Interfaz Zadig 2.6

A continuación, se deben seguir estos pasos:

- Options > List All Devices
- En el desplegable elegir: HackRF One
- Clic en el siguiente recuadro señalado en rojo:

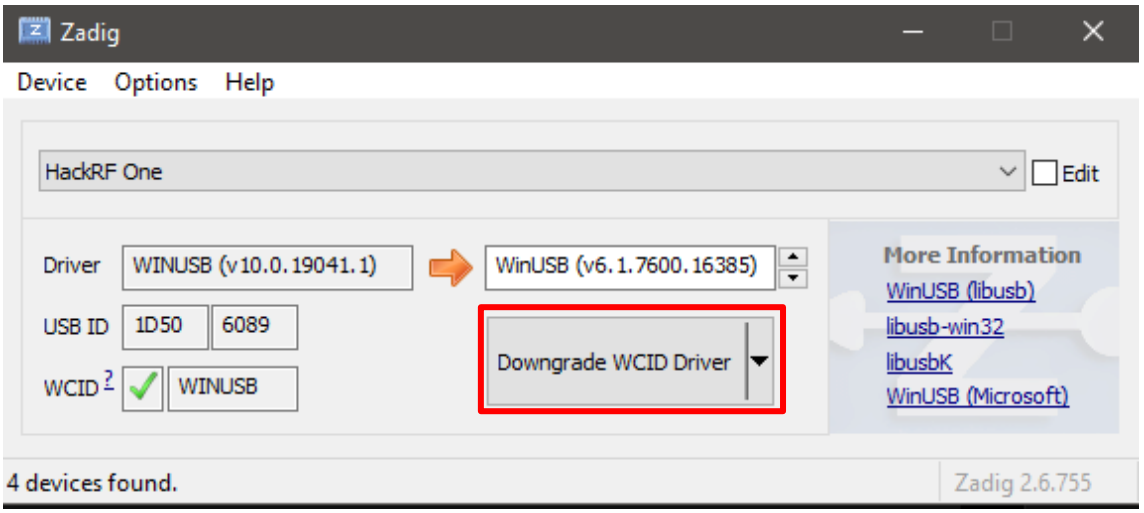


Figura A. 6: Instalación drivers en Zadig

Por lo general, deberá de aparecer “Downgrade WCID Driver” pero esto podría variar en función de la antigüedad de nuestro equipo y de otras actualizaciones de drivers realizadas anteriormente. Igualmente se hará clic en el rectángulo señalado independiente del texto que este contenga.

- Se recibirá una notificación de que el proceso se ha realizado correctamente tras aproximadamente un minuto de espera.

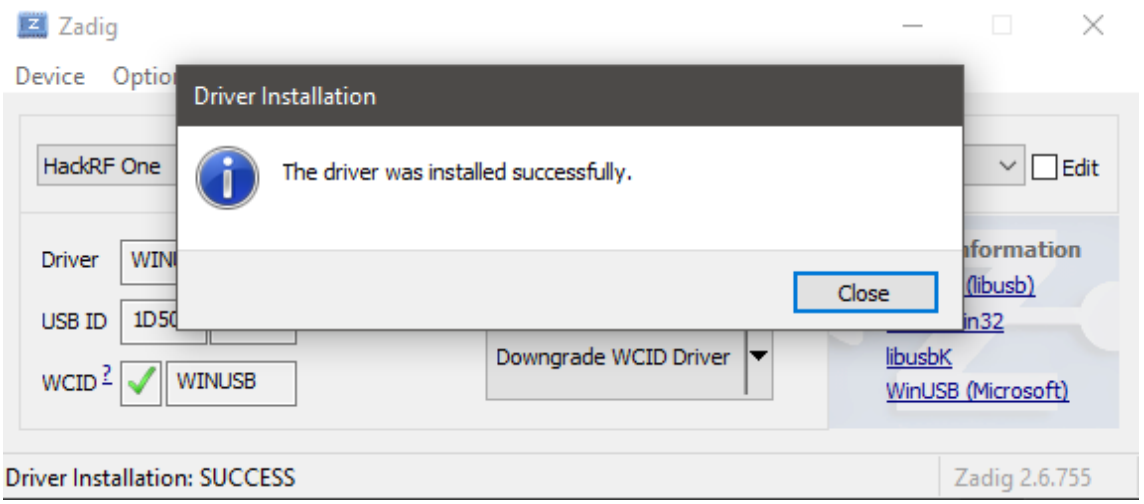


Figura A. 7: Notificación de instalación

- Desconectar el Dongle del puerto USB del ordenador.
- Reiniciar el equipo.

En segundo lugar, se procederá con la instalación del software a utilizar para explotar el HackRF. El programa en cuestión es SDR Console V3, se debe descargar la última

versión disponible de la página web oficial: https://www.sdr-radio.com/download. Una vez instalado el programa deberemos seguir estos pasos:

- Ejecutar el programa en el que encontraremos la siguiente interfaz:

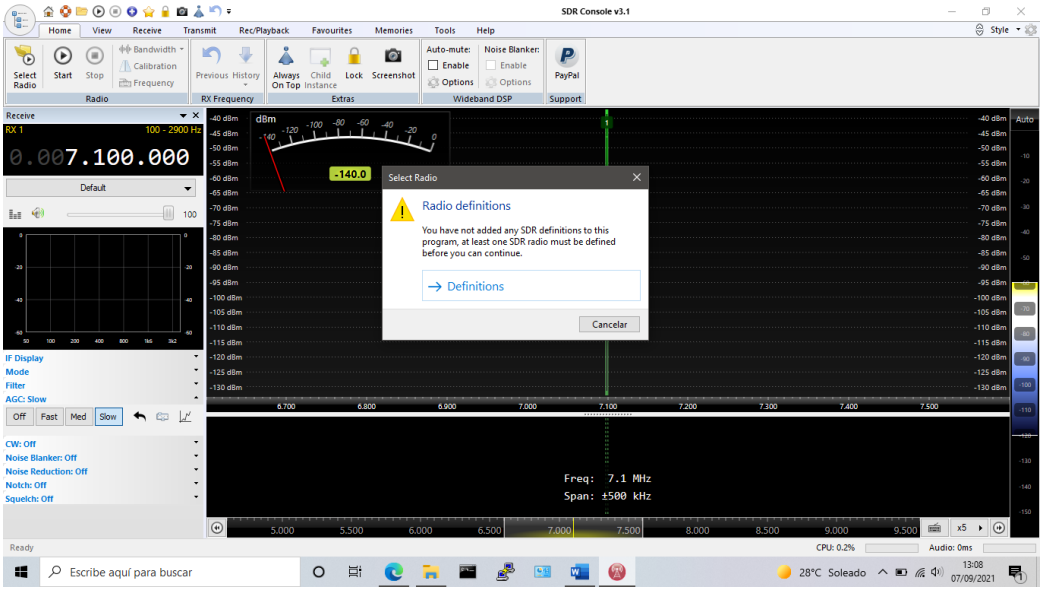


Figura A. 8: Interfaz SDR Console V3

- Clic en “Definitions”
- En la pestaña de la figura que se encuentra a continuación, clic en “Search” > Seleccionamos “HackRF” en el desplegable > “Add” > “Save”

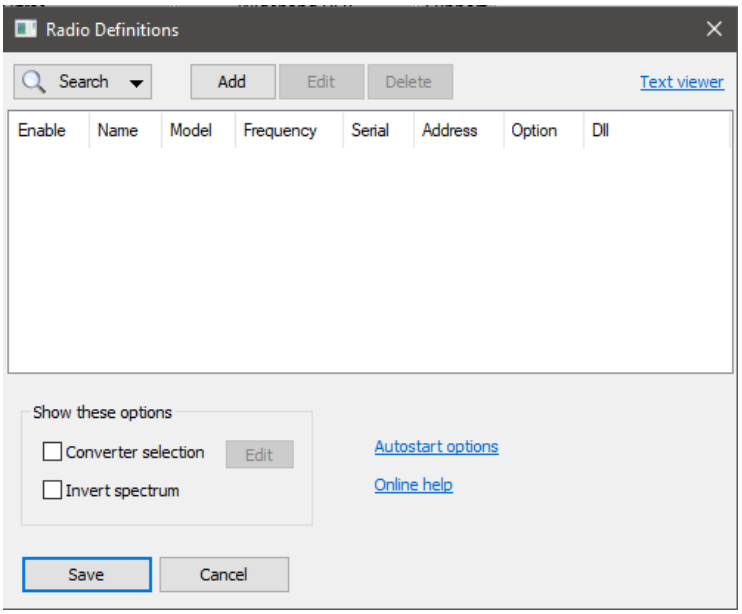


Figura A. 9: Radio Definitions de SDR Console V3

- Comprobar que el ancho de banda “Bandwidth” es de 20MHz y clic en “Start”, según la siguiente imagen:

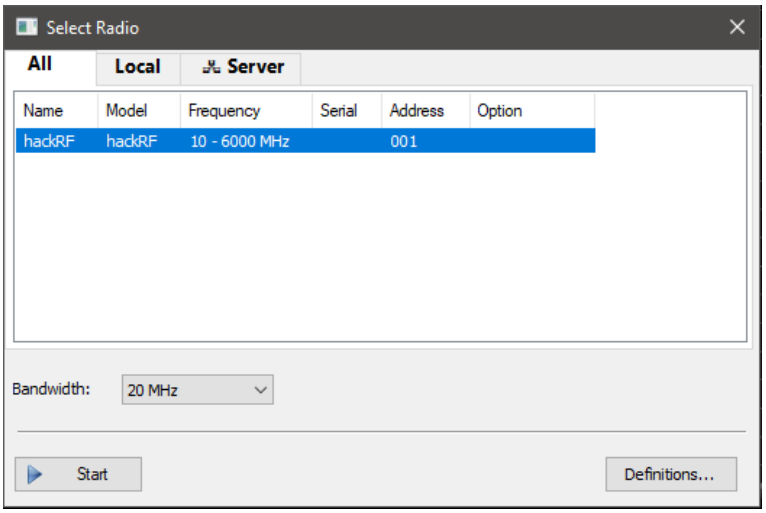


Figura A. 10: Configuración ancho de banda en SDR Console V3

Finalmente, se ha completado la instalación del dispositivo y está preparado para comenzar a explotarse. Para la instalación del periférico RTL-SDR se siguen exactamente los mismos pasos a diferencia de que para este caso se debe configurar un ancho de banda de 2,4 MHz.

Anexo VI: Introducción a GNURadio

En primer lugar, antes de comenzar a crear diagramas de bloques más complejos en GNURadio para Windows se propone la creación de un sencillo Receptor y Transmisor. Para comenzar, se creará un Receptor se comprobará su utilidad en base a:

- Al ejecutar el Receptor el HackRF entra en modo Rx
- El espectro de frecuencia que está captando el HackRF mostrado por la interfaz de GNU se modifica a la hora de emitir desde un walkie, en concreto un Baofeng UV9Rplus

Posteriormente, se creará un diagrama de bloques en función de Transmisor, su correcto funcionamiento se comprobará de la siguiente manera:

- Al ejecutar el Transmisor el HackRF entra en modo Tx
- El walkie detecta la emisión en dicha frecuencia

Los diagramas de bloques y los resultados son los siguientes:

- RECEPTOR

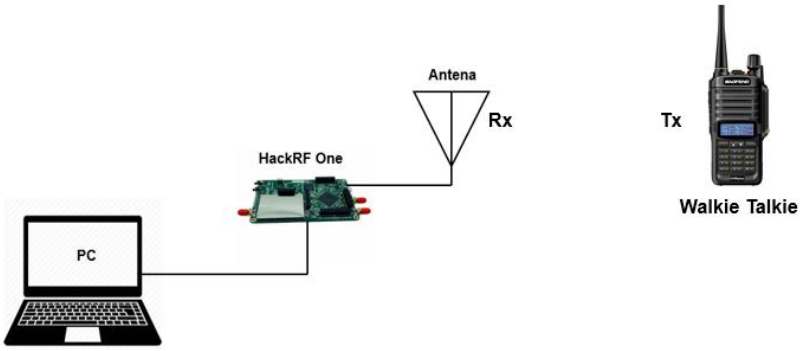


Figura A. 12: Diagrama de bloques HackRF como RECEPTOR

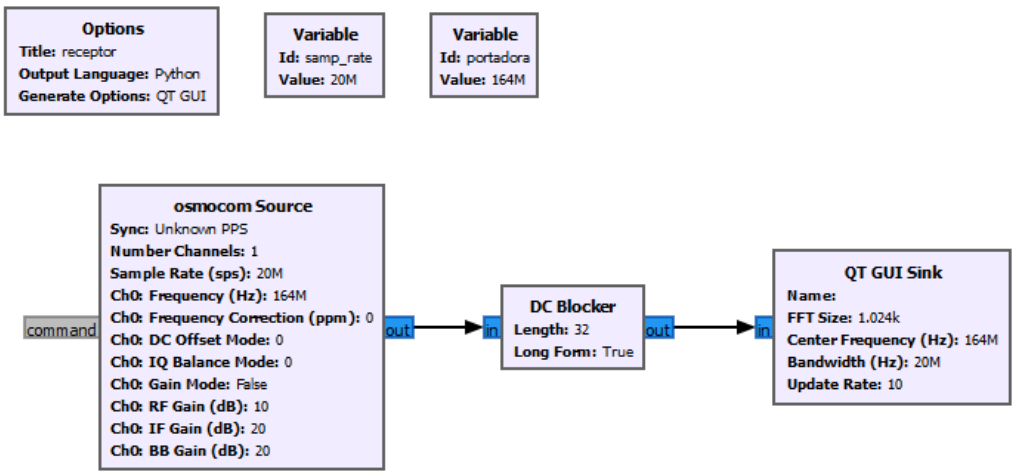


Figura A. 11: Programación receptor en GNURadio

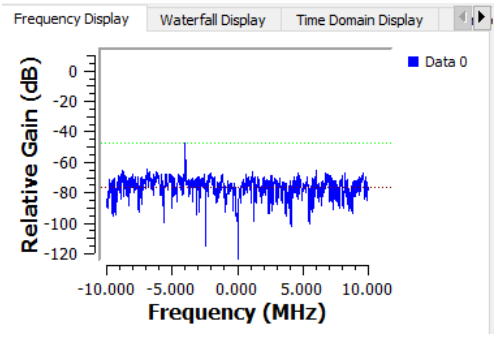


Figura A. 16: Display receptor GNURadio

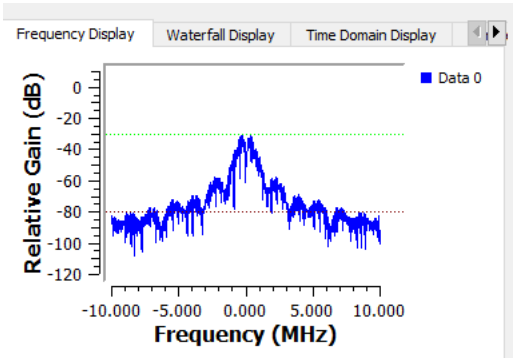


Figura A. 14: Detección de la emisión en el display de GNURadio

Figura A. 15: Walkie emitiendo

Figura A. 13: HackRF en Rx

El resultado es positivo ya que, como se puede comprobar: el Hackr RF entra en modo emisión, el diagrama de GNU es acorde a la frecuencia del walkie, el display de GNU Radio cambia al emitir desde el walkie.

- TRANSMISOR

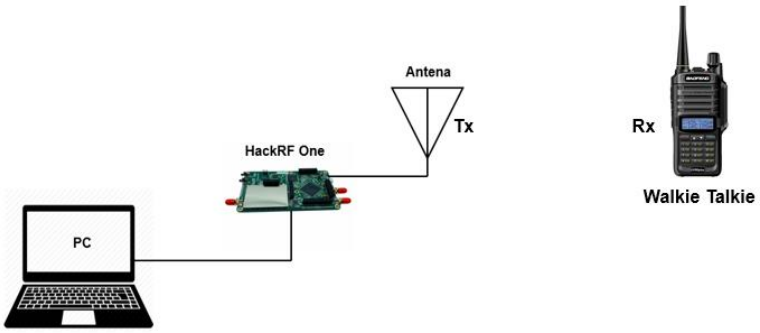


Figura A. 17: Diagrama HackRF como emisor

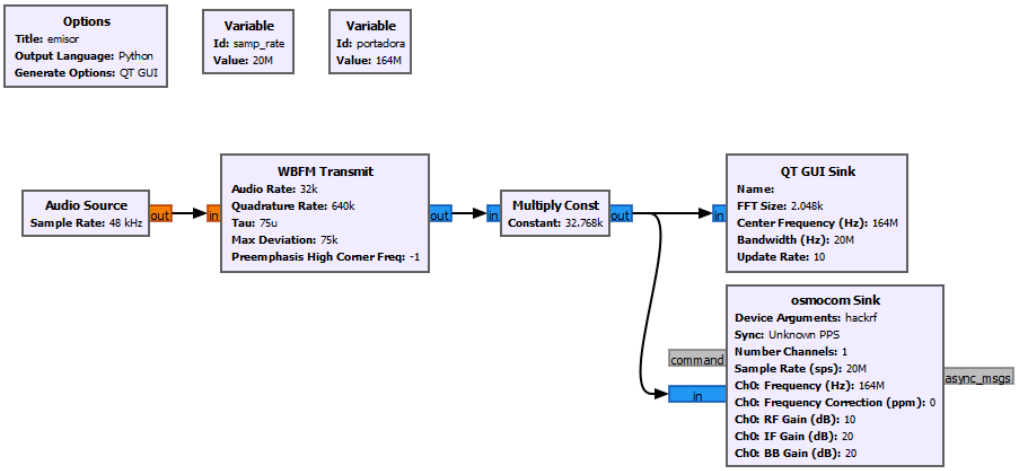


Figura A. 20: Programación TRANSMISOR en GNURadio

Figura A. 19: Walkie en Rx

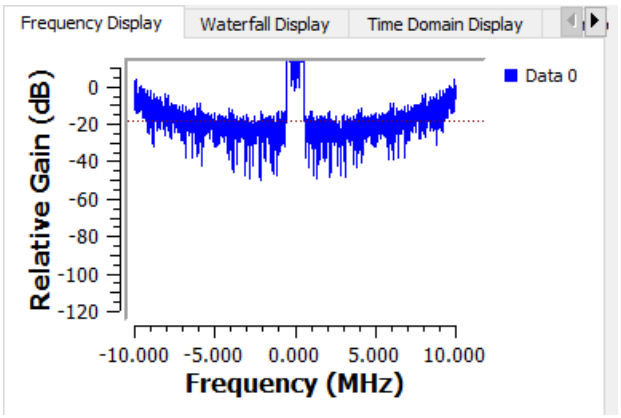


Figura A. 18: Display GNURadio

Figura A. 21: HackRF en Tx

El resultado es positivo ya que, como se puede comprobar: el Hackr RF entra en modo transmisión, el diagrama de GNU es acorde a la frecuencia del walkie, el walkie recibe ruido proveniente del HackRF (se ilumina una luz en verde y se escucha el ruido).

Anexo VII: Proceso Spoofing

En este anexo se detalla paso a paso el proceso llevado a cabo por nuestro sistema para realizar un ataque de decepción (spoofing).

Para este proceso, desarrollado en un sistema operativo Windows 10, necesitaremos:

- El software GPS-SDR-SIM. Se puede obtener del repositorio oficial de GitHub[14]: GPS-SDR-SIM. Es un programa cuya finalidad es la de simular señales GPS mediante SDR. Una vez descargado gps-sdr-sim.zip, será descomprimido.
- Una difusión broadcast de efemérides, lo más recientemente posibles. Se puede descargar de la siguiente página web de la NASA: CDDIS NASA. Es necesario registrarse en la web para acceder al contenido. Después, automáticamente se redireccionará a la página anterior, deslizar hasta el fondo de la web y descargar el último archivo (extensión .gz). Este fichero se guardará (descomprimido) en la misma carpeta donde se haya descomprimido el archivo gps-sdr-sim.zip.

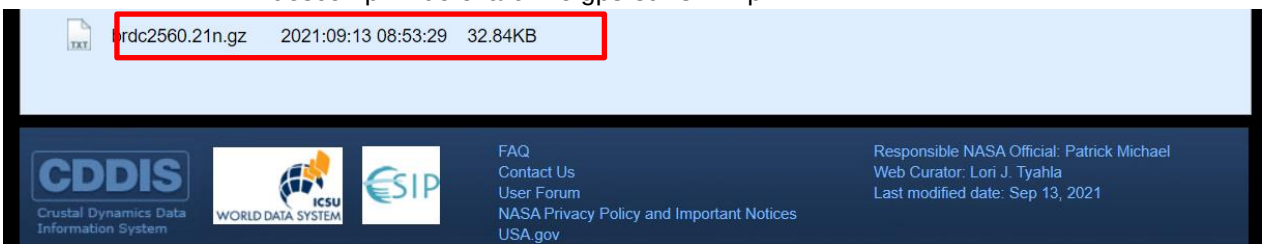


Figura A. 22: Efemérides a descargar, imagen obtenida de: https://cddis.nasa.gov/archive/gnss/data/daily/2021/brdc/

- Un programa para poder transmitir con el HackRF One, en concreto se utilizará el hackrf_transfer, se obtiene instalando PothosSDR de la siguiente web: PothosSDR. Es importante conocer la ruta en la que se encuentra el programa (posteriormente se utilizará), por defecto esta será: *C:\Program Files\PothosSDR\bin*.

Ambos programas anteriormente mencionados (*gps-sdr-sim* y *hackrf_tranfer*) se ejecutan desde la consola de comandos de Windows.

En primer lugar, se abre la consola y tras el comando *cd* se debe de escribir la ruta donde esté el archivo extraído "gps-sdr-sim.zip". En este paso, se está ordenando por comandos al ordenador que se dirija a la ruta[15] en cuestión.

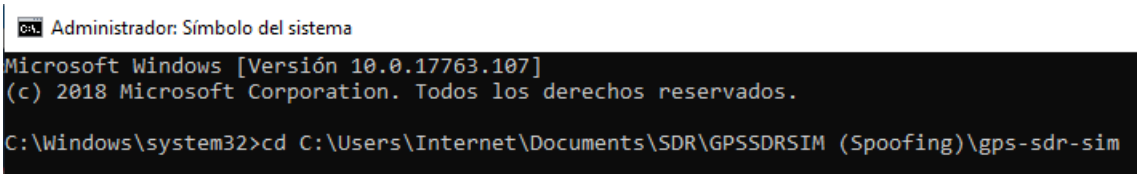


Figura A. 23: Captura de pantalla cmd (uso del comando cd)

[14] Principal plataforma de desarrollo colaborativo de software a nivel mundial, especializada en código fuente para Linux, se puede obtener más información de su página web oficial: https://github.com/.

[15] En lugar de escribir manualmente la ruta, esta se puede copiar directamente haciendo clic derecho sobre la consola.

Tras pulsar intro, la consola está ubicada en la carpeta deseada. A continuación, se deben obtener unas coordenadas en formato latitud y longitud, una forma sencilla es elegir un punto arbitrario con Google Maps. Se ha elegido un punto en la costa mediterránea francesa.

Figura A. 24: Coordenadas elegidas (Portiragnes, Francia), imagen obtenida de: Google Maps

Posteriormente y en la propia consola, se debe introducir el siguiente comando, este proceso consiste en modificar las efemérides broadcast anteriormente descargar para darle las coordenadas deseadas generando un archivo que posteriormente se transmitirá por el HackRF.

gps-sdr-sim -b 8 -e brdc2560.21n -l 43.272635,3.351212,20

A continuación, se encuentra la explicación del comando:

```
C:\Users\usuario>cd C:\Users\usuario\Documents\TFG\Spoofing\gps-sdr-sim

C:\Users\usuario\Documents\TFG\Spoofing\gps-sdr-sim>gps-sdr-sim
Usage: 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. 3967283.154,1022538.181,4872414.484
  -l <location>    Lat,Lon,Hgt (static mode) e.g. 35.681298,139.766247,10.0
  -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] (dynamic mode max: 300, 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
```

Figura A. 25: Explicación comandos gps-sdr-sim, obtenidos desde cmd

Tras una espera de 300 s, se ha generado un archivo “gpssim.bin”, de aproximadamente 1,5GB de peso, en la ruta sobre la que se está trabajando. Importante: b (iq_bits) debe tener un valor de 8 para que el archivo generado se corresponda con las características técnicas del HackRF analizadas anteriormente, por ello se observa *-b 8* en el comando.

```
Using static location mode.
Start time = 2021/09/13,00:00:00 (2175:86400)
Duration = 300.0 [sec]
02   63.9  14.4   24488335.5   3.7
10  251.4  11.4   24369859.4   3.9
11   66.4   8.3   24881604.8   4.2
13  148.0   5.4   25327988.7   4.5
15  159.7  30.1   23146392.2   2.6
18  190.6  19.5   23763208.1   3.3
23  218.7  19.9   23686419.8   3.3
24   73.1  46.6   21719772.9   2.0
25  344.6  29.5   22572752.2   2.7
29  255.1  79.2   20302022.4   1.5
32  314.9  23.2   23401371.0   3.0
Time into run = 300.0
Done!
```

Figura A. 27: Resultados simulación de la constelación en cmd

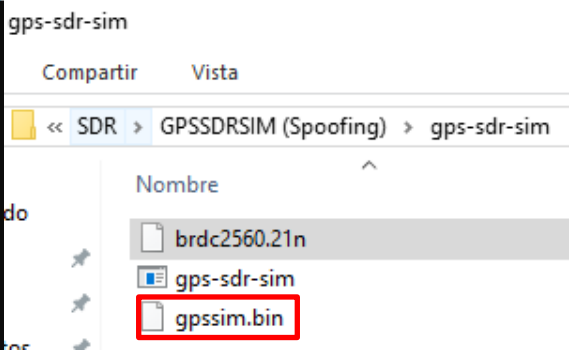


Figura A. 26: Archivo generado por GPS-SDR-SIM

Seguidamente, y tras cambiar la ubicación del archivo generado a la ruta del hackrf_transfer. Usando el comando cd se accede a la ruta de este (*C:\Program Files\PothosSDR\bin*). Una vez allí, se introduce el siguiente comando:

hackrf_transfer -t gpssim.bin -f 1575420000 -s 2000000 -a 1 -x 0

De esta manera, el HackRF comienza a emitir el archivo *gpssim.bin* (el diagrama de Rx/Tx es el mismo que en Jamming) generado anteriormente, por el gps-sdr-sim. En la siguiente figura se puede observar una explicación de los comandos de hackrf_transfer:

```
C:\Users\usuario\Documents\TFG\Spoofing\gps-sdr-sim>cd C:\Program Files\PothosSDR\bin

C:\Program Files\PothosSDR\bin>hackrf_transfer
specify one of: -t, -c, -r, -w
Usage:
        -h # this help
        [-d serial_number] # Serial number of desired HackRF.
        -r <filename> # Receive data into file (use '-' for stdout).
        -t <filename> # Transmit data from file (use '-' for stdin).
        -w # Receive data into file with WAV header and automatic name.
           # This is for SDR# compatibility and may not work with other software.
        [-f freq_hz] # Frequency in Hz [0MHz to 7250MHz].
        [-i if_freq_hz] # Intermediate Frequency (IF) in Hz [2150MHz to 2750MHz].
        [-o lo_freq_hz] # Front-end Local Oscillator (LO) frequency in Hz [84MHz to 5400MHz].
        [-m image_reject] # Image rejection filter selection, 0=bypass, 1=low pass, 2=high pass.
        [-a amp_enable] # RX/TX RF amplifier 1=Enable, 0=Disable.
        [-p antenna_enable] # Antenna port power, 1=Enable, 0=Disable.
        [-l gain_db] # RX LNA (IF) gain, 0-40dB, 8dB steps
        [-g gain_db] # RX VGA (baseband) gain, 0-62dB, 2dB steps
        [-x gain_db] # TX VGA (IF) gain, 0-47dB, 1dB steps
        [-s sample_rate_hz] # Sample rate in Hz (2-20MHz, default 10MHz).
        [-n num_samples] # Number of samples to transfer (default is unlimited).
        [-c amplitude] # CW signal source mode, amplitude 0-127 (DC value to DAC).
        [-R] # Repeat TX mode (default is off)
        [-b baseband_filter_bw_hz] # Set baseband filter bandwidth in Hz.
        Possible values: 1.75/2.5/3.5/5/5.5/6/7/8/9/10/12/14/15/20/24/28MHz, default <= 0.75 * sample_rate_hz.
        [-C ppm] # Set Internal crystal clock error in ppm.
        [-H hw_sync_enable] # Synchronise USB transfer using GPIO pins.
```

Figura A. 28: Explicación comandos hackrf_transfer, obtenido desde cmd

Observando el comando utilizado para transmitir la simulación de señal se puede ver que se está haciendo en una frecuencia de *1575420000,* es decir, 1,57542 GHz coincidiendo con la banda L1 de GPS y con la frecuencia de emisión de la antena utilizada.

Por otro lado, y para obtener información sobre la señal generada en este ataque de spoofing se ha procedido a analizar dicho pulso conectando directamente, es decir por cable SMA en vez de radiando a través de una antena, el HackRF a otro periférico SDR (RTL-SDR) utilizando el software SDR Console v3 (el cual se puede obtener información sobre su instalación en Anexo V: Instalación HackRF One en ordenador personal), en la imágenes añadidas a continuación se puede observar ambos periféricos conectados y el aspecto del pulso respectivamente:

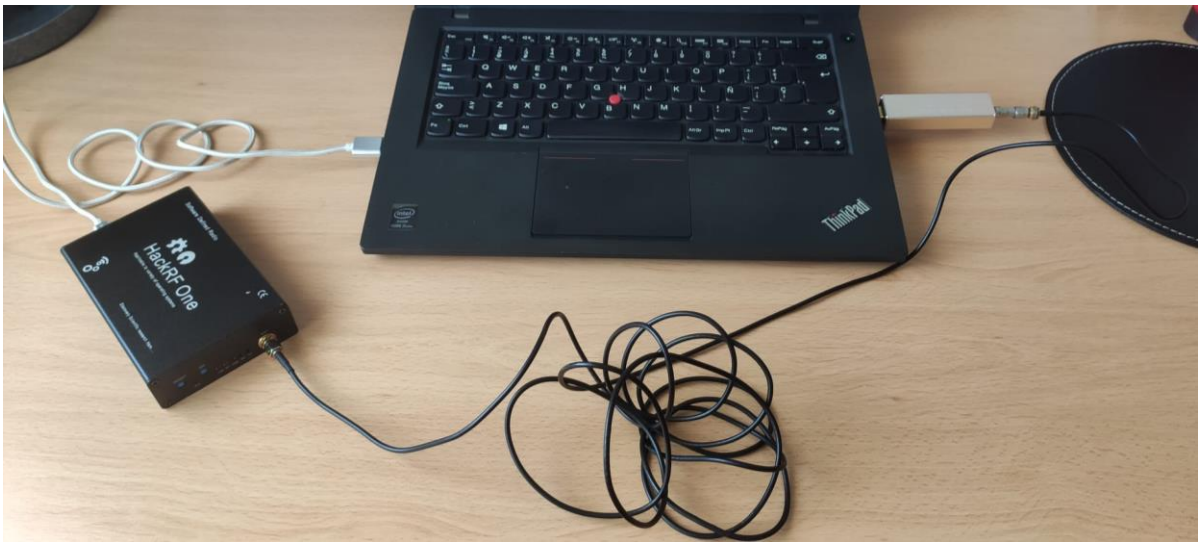


Figura A. 31: HackRF conectado por cable coaxial a RTL-SDR

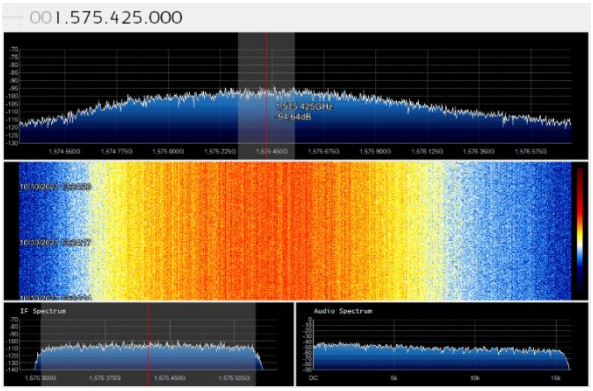


Figura A. 29: Recepción con amplificador IF del HackRF a 10 dB

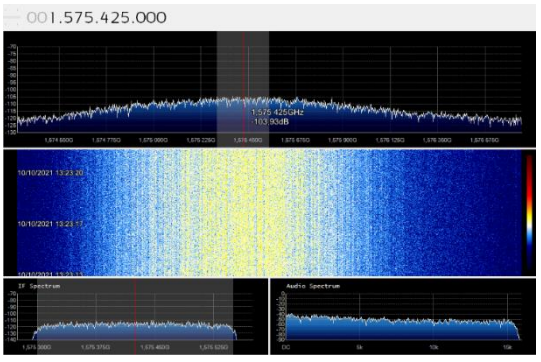


Figura A. 30: Recepción con amplificador IF del HackRF a 0 dB

USO OFICIAL

Anexo VIII: Radioteléfono ligero PR4G v3 (RT-9210 V3)

En el presente anexo se relaciona la información esencial necesaria para entender el papel de la PR4G v3 en la práctica de spoofing realizada en este trabajo. Seguidamente se puede encontrar una imagen de esta en su configuración portátil.

Figura A. 32: PR4G v3 en configuración portátil, sin GPS conectado

Para ejercer el mando de forma eficaz y permanente es preciso mantener el enlace con las unidades subordinadas, laterales y superior, por lo que será necesario un sistema de telecomunicaciones flexible y fiable, capaz de adaptarse a las diferentes y cambiantes situaciones y características de las operaciones.

Será habitual el empleo de medios de comunicaciones que permitan mantener el enlace durante el movimiento, sobre todo en el ámbito de las pequeñas unidades.

Uno de los medios más extendidos en la dotación de las unidades del Ejército de Tierra son los radioteléfonos PR4G, tanto en su configuración vehicular como portátil. Existen varias versiones, siendo la última la v3, que proporciona mejores prestaciones que las anteriores.

El radioteléfono PR4G es uno de los medios principales de comunicaciones en todos los escalones de mando y en todo tipo de unidades, siendo los operadores de estos equipos los responsables de establecer y mantener el enlace en las mallas correspondientes.

Ahondando más en este sistema radio, es importante saber que el radioteléfono descrito en este manual es un transceptor VHF/FM de la familia PR4G (radios portátiles de cuarta generación) de alto nivel de protección ECCM que permite efectuar

transmisiones seguras en un ambiente electromagnético hostil. Opera en la siguiente banda de frecuencias: 30 - 87,975 MHz

La denominación correcta de este transceptor es: PR4GE F@stnet. Pero también es válida la denominación PR4G v3, que es la más habitual y la que se empleará para referirse a la radio de modo genérico, independientemente de la configuración en que se presente.

La PR4G v3 puede ser empleada para transmisión de voz (fonía), de datos o como relé (analógico o digital), y además, a diferencia de anteriores versiones, incorpora una introducción a los nuevos modos de trabajo IP en modalidades SAP y MUX con capacidad para compatibilizar voz y datos en la misma transmisión/recepción en este último caso. Funciona en modo semidúplex con un cambio manual (PTT) entre las funciones de transmisión y recepción.

En modo fonía, el equipo dispone de un vocoder interno que mejora la calidad de la señal recibida en entornos muy interferidos. Incorpora los módulos TRANSEC (salto de frecuencia) y COMSEC (cifrado).

La voz o los datos son cifrados para evitar cualquier escucha o intrusión en la malla. La memorización de una clave COMSEC implica automáticamente el cifrado de las comunicaciones.

Cuenta con los siguientes modos de trabajo:

- Salto de frecuencia rápido (SFR, 300 saltos/s.).
- Búsqueda de canal libre (BCL).
- Modo MIX autoadaptativo (elección automática entre SFR y BCL).
- Frecuencia digital (FD). Con protección COMSEC.
- Frecuencia fija analógica (FFC y FFG). Sin protección COMSEC.
- Modos temporales ORTHO y BUSQUEDA.

Existen dos configuraciones posibles:

- La portátil tipo “man-pack” que tiene la denominación de RT-9210.
- La vehicular para instalaciones en vehículos que se denomina RT-9310.

Cada configuración consta del mismo radioteléfono más unos accesorios que diferencian una de otra. Por ser la configuración vehicular la utiliza en la práctica es la única que se desarrollará a continuación. Esta se compone de los siguientes elementos:

- Radioteléfono PR4G v3.
- Amplificador de potencia ALA-126AP. El ALA-126AP es un amplificador de potencia de 50 W para el uso vehicular de la PR4G v3. Su empleo permite aumentar el alcance efectivo de transmisión.
- Cable coaxial CHF-147. Para la transmisión de la señal de antena entre el transceptor y el amplificador.
- Cable CG-142-03. Cable de transmisión de la señal entre antena y amplificador. — Cable GPS SMA/SMA. Para la transmisión de la señal GPS entre antena y transceptor.
- Cable CX-222D-05. De alimentación a 24 V.

- Soporte vehicular MT-188. Para la sujeción del conjunto radio-amplificador en el interior del vehículo.
- Antenas vehiculares AT-3088 LP/GPS, AT-3088 VM/GPS. Se empleará una u otra en función del tipo de vehiculo.
- Microteléfono COT 207TA.

Seguidamente se pueden observar imágenes en las que se observan dichos elementos/accesorios.

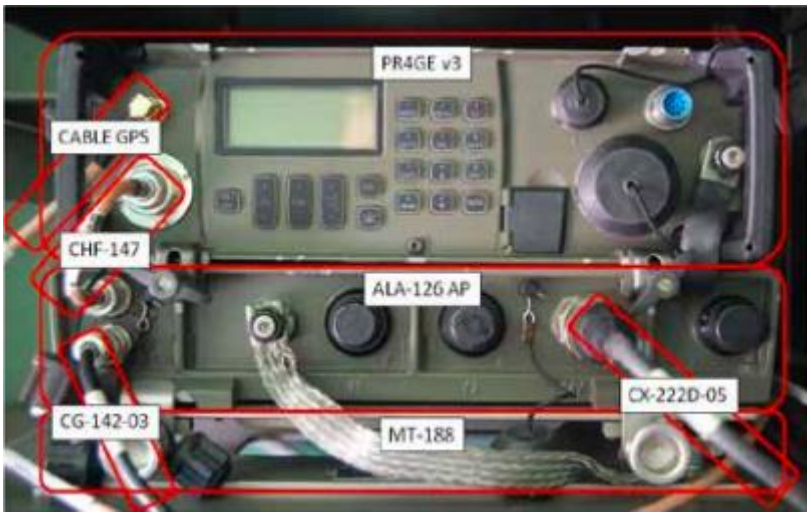
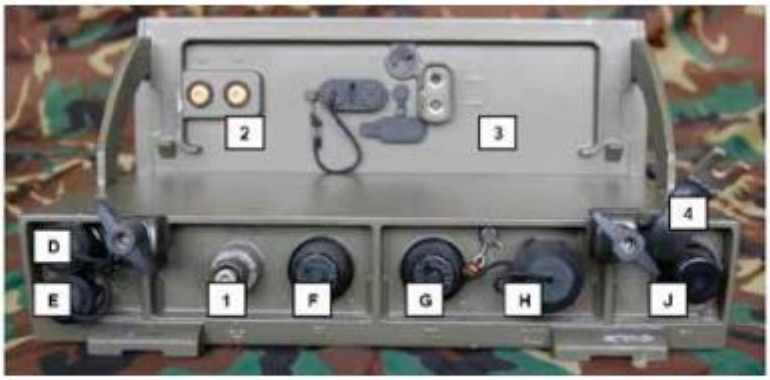


Figura A. 33: Elementos y accesorios PR4Gv3 (1)



D. Toma de antena superior (hacia RT).
E. Toma de antena inferior (hacia vehículo).
F. Fusible F1.
G. Fusible F2.
H. Toma de alimentación de 24 V.
J. Fusible F0.
1. Toma de tierra hacia vehículo.
2. Contactos de alimentación al RT.
3. Interfaz de infrarrojos.
4. Toma de tierra hacia RT.

Figura A. 34: Elementos y accesorios PR4Gv3 (2)

Fuente bibliográfica: (Ministerio de Defensa, 2016)

Anexo IX: Resultados práctica Sistema final

Según la siguiente tabla:

distancia (m)	campo -x (dB)	Teléfono móvil					PC + antena GPS				
		Jamming		Spoofing		Obs	Jamming		Spoofing		Obs
		Resultado	t	Resultado	t		Resultado	t	Resultado	t	
1,2	0	Desfavorable	25"	Desfavorable	25"	R adquiere coordenadas reales	Desfavorable	25"	Desfavorable	25"	R adquiere coordenadas reales
	47	Favorable		Desfavorable		R no adquiere coordenadas reales	Favorable		Desfavorable		R no adquiere coordenadas reales
	20	No procede		Favorable	1'30"	R adquiere coordenadas falsas	No procede		Favorable	10"	R adquiere coordenadas falsas
2,4	20	Favorable		Desfavorable		R no adquiere coordenadas reales	Favorable		Desfavorable		R no adquiere coordenadas reales
	30	Favorable		Desfavorable		R no adquiere coordenadas reales	No procede		Favorable	1'	R adquiere coordenadas falsas
3,6	30	Desfavorable	10"	Desfavorable	10"	R adquiere coordenadas reales	No procede		Favorable	1'	R adquiere coordenadas falsas
	47	Desfavorable	10"	Desfavorable	10"	R adquiere coordenadas reales	No procede		Favorable	30"	R adquiere coordenadas falsas
4,8	47	Desfavorable	10"	Desfavorable	10"	R adquiere coordenadas reales	No procede		Favorable	46"	R adquiere coordenadas falsas
6	47	Desfavorable	10"	Desfavorable	10"	R adquiere coordenadas reales	Desfavorable	1'	Desfavorable	1'	R adquiere coordenadas reales
7,2	47	Desfavorable	10"	Desfavorable	10"	R adquiere coordenadas reales	Desfavorable	25"	Desfavorable	25"	R adquiere coordenadas reales

Tabla 6: Resultados práctica Sistema final

Leyenda:

- Obs.: Observaciones.
- t: tiempo.
- Una casilla de tiempo vacía indica que tras 5’ de transmisión se pasó a la siguiente distancia/ganancia de la tabla. 5’ es el tiempo máximo que el programa “hackrf_transfer.exe” se mantiene emitiendo.
- Campo -x (dB): hace referencia al amplificador de Tx de IF.
- Los tiempos de la tabla se corresponde con el tiempo que tardó el receptor en adquirir unas coordenadas reales (casos desfavorables) /simuladas (casos favorables).