Jamming and Spoofing for Counter-Drone Action

Second Lieutenant Younes Zidane

Thesis to obtain the Master of Science Degree in

Military Electrical Engineering

Supervisors: Prof. José Silvestre Serra da Silva
Prof. Gonçalo Nuno Gomes Tavares

Examination Committee

Chairperson: Prof. Pedro Mendonça dos Santos
Supervisor: Prof. Luís Filipe Soldado Granadeiro Rosado
Members of the Committee: Prof. José Silvestre Serra da Silva
Signals Lieutenant Colonel Pena Madeira

October 2024

Acknowledgments

First, I would like to express my deepest gratitude to my parents. Their constant support and education have shaped me into who I am today. Their encouragement has been a continuous source of strength at every stage of my life.

I would also like to express my sincere gratitude to my comrades, whom I am fortunate to call friends. Together, we have shared the highest and most challenging lows of this experience, enriching this journey with camaraderie and mutual support.

A special thanks goes to my girlfriend, whose presence has been invaluable. Her support, especially when I needed it most, has provided great comfort and motivation throughout this journey.

Finally, I am deeply grateful to my supervisor, Professor José Silvestre Serra da Silva, and my co-supervisor, Professor Gonçalo Nuno Gomes Tavares, for their constant availability, insightful guidance, and significant contributions to the successful completion of this Master's thesis. Their expertise and encouragement have been instrumental in this achievement.

Abstract

As Unmanned Aerial Vehicles (UAVs) are increasingly used for both commercial and military purposes, there has been much concern about the misuse of these devices in some restricted and security-sensitive areas.

This dissertation focuses on developing and evaluating interference mechanisms, known as jamming and signal spoofing techniques, with the ultimate goal of disrupting both communications and navigation systems. For this purpose, Software Defined Radio (SDR) technology was used to design a cost-effective, adaptable system capable of neutralizing drones by interrupting their control signals and geolocation services.

Experimental tests were conducted to assess the effectiveness of these implementations on commercial drones. The results showed that radio frequency jamming effectively disrupts control and image transmission. Spoofing also successfully emits false GNSS signals and indirectly interferes with the drone's behavior.

Keywords

UAV; Drone; Jamming; Spoofing; Software Defined Radio; Radio Frequency

Resumo

Com a crescente utilização de Veículos Aéreos Não Tripulados (VANTs), tanto para fins comerciais como militares, tem havido uma grande preocupação de que estes equipamentos sejam utilizados de forma incorrecta em algumas áreas restritas e zonas sensíveis em termos de segurança.

Esta dissertação centra-se no desenvolvimento e avaliação de mecanismos de interferência, conhecidos como técnicas de jamming e spoofing de sinal, com o objetivo final de perturbar os sistemas de comunicação e navegação. Para o efeito, foi utilizada a tecnologia Software Defined Radio (SDR) para conceber um sistema económico e adaptável capaz de neutralizar os drones, interrompendo os seus sinais de controlo e serviços de geolocalização.

Foram efectuados testes experimentais para avaliar a eficácia destas implementações em drones comerciais. Os resultados mostraram que a interferência de radiofrequência interrompe eficazmente o controlo e a transmissão de imagens. O spoofing também emite com sucesso sinais GNSS falsos e interfere indiretamente no comportamento do drone.

Palavras Chave

VANT; drone; jamming; spoofing; rádio definido por software; rádio frequência

Contents

1 Introduction **1**

1.1 Motivation . . . 3

1.2 Objectives and contributions . . . 3

1.3 Organization of the Document . . . 4

1.4 Publications . . . 5

2 Background **7**

2.1 UAVs Communication Standards . . . 9

2.2 UAVs Modulation and Protocols . . . 10

2.3 GNSS fundamentals . . . 12

2.4 Anti-Drone System Requirements . . . 14

2.5 Jammer Designs . . . 15

2.5.1 Circuit-Based Implementation . . . 15

2.5.2 SDR-Based Implementation . . . 15

2.6 UAVs Detection . . . 16

2.7 UAVs Neutralizing . . . 17

2.7.1 Radio Frequency Spoofing . . . 18

2.7.2 Radio Frequency Jamming . . . 19

2.8 Related Work . . . 20

3 System Design and Methodology **25**

3.1 Hardware and Software . . . 27

3.1.1 Hardware . . . 27

3.1.1.A ADALM-PLUTO . . . 27

3.1.1.B Amplifier . . . 29

3.1.1.C Antennas . . . 29

3.1.1.D Drones . . . 32

3.1.2 Software . . . 33

3.1.2.A GNU Radio . . . 33

3.1.2.B Visual Studio Code . . . 34
3.2 Methodology . . . 34
3.2.1 GNSS Implementation . . . 34
3.2.1.A GNSS Barrage Jamming . . . 34
3.2.1.B GNSS BPSK Jamming . . . 36
3.2.1.C GNSS Spoofing . . . 38
3.2.2 Jamming Implementation . . . 38
3.2.2.A RC and Video Barrage Jamming . . . 38
3.2.2.B RC and Video Sweep Jamming . . . 40
4 Results and Discussion **45**
4.1 GNSS Jamming and Spoofing . . . 47
4.1.1 GNSS Barrage Jamming . . . 47
4.1.2 GNSS BPSK Jamming . . . 50
4.1.3 GNSS Spoofing . . . 52
4.2 RC and Video Jamming . . . 55
4.2.1 RC and Video Barrage Jamming . . . 57
4.2.2 RC and Video Sweep Jamming . . . 60
5 Conclusion and Future Work **61**
5.1 Conclusion . . . 63
5.2 Future Work . . . 64
Bibliography **65**
A GPS Spoofing Signal Generation Setup **73**
B Points generator Python Code **75**

List of Figures

2.1 Wireless connectivity mechanisms designed for a drone. 9
2.2 Spectrum of Coarse/Acquisition (C/A) code GPS. 13
2.3 UAVs neutralizing techniques. 18

3.1 Diagram of the system's hardware components. 27
3.2 Adalm-Pluto Device and Block Diagram. 28
3.3 Power Amplifier: WYDZ-PA-1G-3GHz-1W. 29
3.4 2.4 GHz Antenna Image. 30
3.5 Measured return loss (S11) of the 2.4 GHz Antenna. 30
3.6 Measured return loss (S11) of the 1.5 GHz Antenna Image. 31
3.7 S11 of 1.5 GHz Antenna. 32
3.8 GNSS Barrage Jamming Script using GNU Radio. 35
3.9 GPS BPSK Jamming Script using GNU Radio. 37
3.10 Sweep Jamming Script Script using GNU Radio. 41

4.1 Satellite image of the physical testing space. 47
4.2 GNSS Barrage Jamming signal spectrum. 48
4.3 GNSS BPSK Jamming signal spectrum. 50
4.4 Static Spoofing to Tokyo, Japan. 52
4.5 Spoofing into a No-Fly Zone (Controller Display). 53
4.6 Overview of the testing areas used for drone experiments. 56
4.7 Illustration of the testing structure used during experiments. 56
4.8 2.4 GHz band Barrage Jamming signal spectrum (Sequential sub-band scan and random sub-band selection). 57
4.9 Interference detection on the controller. 59
4.10 RC and Video full Jamming. 59
4.11 2.4 GHz band Sweep Jamming signal spectrum. 60

List of Tables

2.1 LTE, 4G, UMTS, GSM, and 5G Portugal Communication Bands 10
2.2 Used modulations for each frequency 12
2.3 Comparison of GNSS with global coverage 14

3.1 Used Drones and respective operating frequencies 33

4.1 Distances for GNSS barrage jamming 49
4.2 Distances for GNSS BPSK jamming 51
4.3 Results obtained for Dynamic Spoofing 55
4.4 Effectiveness of RC and video barrage jamming. 58

Listings

B.1 Points generator Python Code 75

Acronyms

ANACOM	Autoridade Nacional de Comunicações
AWGN	Additive White Gaussian Noise
BPSK	Binary Phase Shift Keying
C/A	Coarse/Acquisition
CBOC	Composite Binary Offset Carrier
DEMPs	Directional Electromagnetic Pulses
DQPSK	Differential Quadrature Phase Shift Keying
DSSS	Direct Sequence Spread Spectrum
ECEF	Earth-Centered Earth-Fixed
EIRP	Effective Isotropic Radiated Power
FHSS	Frequency-Hopping Spread Spectrum
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GS	Ground Station
GUI	Graphical User Interface
GSM	Global System for Mobile Communications
ISM	Industrial, Scientific, Medical
LTE	Long-Term Evolution
LoS	Line-of-Sight
LPF	Low Pass Filter
NFZ	No-Fly Zone
OFDM	Orthogonal Frequency-Division Multiplexing
PAV	Personal Air Vehicle

PN	Pseudo Noise
PNT	Positioning, Navigation, and Timing
PRN	Pseudo-Random Noise
QPSK	Quadrature Phase Shift Keying
RC	Radio Control
RF	Radio Frequency
RFIC	Radio Frequency Integrated Circuit
SDR	Software Defined Radio
SINR	Signal-to-Interference-plus-Noise Ratio
SNR	Signal-to-Noise Ratio
UAV	Unmanned Aerial Vehicle
UMTS	Universal Mobile Telecommunications System
VCO	Voltage-Controlled Oscillator
VS Code	Visual Studio Code
WLAN	Wireless Local Area Network
WiMAX	Worldwide Interoperability for Microwave Access
3GPP	3rd Generation Partnership Project
8PSK	8 Phase Shift Keying

1

Introduction

Contents

1.1 Motivation 3

1.2 Objectives and contributions 3

1.3 Organization of the Document 4

1.4 Publications 5

1.1 Motivation

Unmanned Aerial Vehicles (UAVs), commonly referred to as drones, have recently undergone phenomenal development and are being adopted in industries such as photography and filming, mapping and surveying, and product delivery, among others [1]. Despite existing drone legislation in Europe [2], many operators choose not to respect the EU regulation and there are a lot of unwanted incidents, whether deliberate or unintentional. Analyzing the potential dangers connected to their employment requires analyzing armed conflicts that took place within the last years – for instance, the one in Nagorno-Karabakh, or the Ukrainian-Russian war, as well as the current situation on the Poland-Belarus border [1].

As drones become more prevalent in civilian technology, concerns about their potential security risks have grown, leading to increased interest in counter-drone technologies. This increased interest is driving the development of new technologies for various aspects of drones, such as detecting them using radio signals and radar, sorting them into different categories based on size and altitude, and monitoring their sideways and up/down movements. These systems are designed to protect against drone-related accidents or potential threats such as terrorism. Advances in counter-drone technology are essential to effectively deal with the evolving capabilities of drones. Currently, many counter-drone systems rely on high-value, military-grade components to effectively counter unauthorized drones. However, challenges arise when integrating these sophisticated military systems into civilian environments due to various intricate technical, regulatory, and operational complexities. These challenges can include issues such as compatibility with civilian infrastructure, regulatory constraints, cost implications, and potential security concerns when operating in civilian populated areas [3] [4].

Given these challenges, there is a need to explore more practical, adaptable methods for countering drones, with a particular focus on Radio Frequency (RF) jamming techniques to disrupt unauthorized UAV operations.

1.2 Objectives and contributions

This research investigates the use of electronic countermeasures for force protection, focusing on disrupting the communication systems of intrusive drones in military airspace and locations critical to infrastructure, such as airports and power stations. The study's relevance extends beyond military applications, addressing civil security scenarios that include public events, government facilities, and densely populated areas. The goal is to improve security protocols and reduce risks associated with drone intrusions in both military and civilian environments.

The primary objective is to evaluate the effectiveness of jamming techniques in disabling UAV communication links, specifically targeting connections to command bases and geolocation systems.

By causing interference in radio frequency communication, the aim is to prevent the drone from communicating or receiving GPS data, thus limiting its operational capabilities.

This work is structured around two core goals: evaluating the impact of jamming techniques on UAV communications and designing a low-cost, adaptable jamming device. The device targets essential communication aspects, including geolocation, radio control, and video transmission, providing flexible protection for various environments.

The contributions of this research include a comprehensive analysis of jamming techniques alongside developing a practical and cost-effective countermeasure system. It highlights the challenges of advanced drones using alternative communication frequencies like 4G and outlines future directions for developing multi-frequency jamming strategies.

1.3 Organization of the Document

This thesis is organized as follows: Chapter 1, Background, discusses the motivation for the research, followed by the objectives and contributions of the study, and provides a brief overview of the document's organization.

Chapter 2 covers the essential topics related to UAV communication standards, modulation protocols, and Global Navigation Satellite System (GNSS) fundamentals, focusing on anti-drone system requirements and jamming techniques.

Section 2.8, Related Work, reviews existing jamming and spoofing strategies, highlighting key studies and comparing techniques used in counter-drone systems.

Chapter 3, System Design and Methodology, provides an in-depth explanation of the hardware and software setup used in this research, detailing the jamming and spoofing methodologies implemented, such as GNSS jamming, RF sweep and barrage jamming, and the integration of spoofing techniques.

Chapter 4, Results and Discussion, presents the results of the experiments conducted, evaluating the effectiveness of the proposed jamming techniques on UAV communications and analyzing the overall efficiency of these approaches.

The thesis concludes with Chapter 5, Conclusion and Future Work, summarizing the key findings and suggesting areas for further research to enhance the capabilities of counter-drone systems. Finally, the Appendices provide additional materials such as code listings, equipment specifications, and supplementary data for reference.

1.4 Publications

This subsection includes both completed presentations and future contributions that reflect the exploration of jamming techniques in drone communications.

1. **RECPAD 2024** *"Jamming Drone Communications"* presented at the 25th Portuguese Conference on Pattern Recognition (RECPAD 2024), Covilhã, Portugal, October 25, 2024.
2. **Encontro de Ciências Militares, Escola Naval** *"Jamming and Spoofing Strategies for UAV Neutralization"* to be presented at the Military Sciences Meeting at Escola Naval, November 26, 2024.
3. **Jornadas das Engenharias da Academia Militar** *"Disrupting UAV Communications: Jamming and Spoofing Strategies for Anti-Drone Applications"* to be presented at the Engineering Days of the Military Academy (AM), February 2025.
4. **Publication in an International Journal** "Jamming and Spoofing Techniques for Drone Neutralization: An Experimental Study", published in the MDPI journal Drones on December 10, 2024.

2

Background

Contents

2.1 UAVs Communication Standards 9
2.2 UAVs Modulation and Protocols 10
2.3 GNSS fundamentals 12
2.4 Anti-Drone System Requirements 14
2.5 Jammer Designs 15
2.6 UAVs Detection 16
2.7 UAVs Neutralizing 17
2.8 Related Work 20

2.1 UAVs Communication Standards

A typical consumer drone wireless communication system, as shown in Figure 2.1, comprises four links: the Navigation link, the Radio Control (RC) link, the Telemetry link, and the Video link. The Navigation link is used by an onboard GNSS receiver to provide the drone with position and velocity data. The RC link provides the drone with information about the pilot's intent to maneuver or configure the drone. This information is typically transmitted in small data packets at high speed to ensure a stable, low-latency connection. The telemetry link sends information about the drone's status, such as battery levels, speed, and position, to the controller. The video link streams the drone's onboard camera feed either to the controller, if it has an interface, or to a smartphone connected to the remote controller [5].

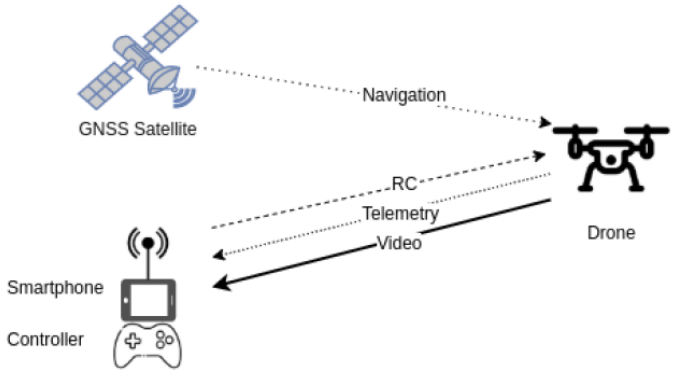


Figure 2.1: Wireless connectivity designed for a drone. Source: [5]

Many technologies can be used to establish communication between the ground station and the drone. Wi-Fi is a prominent one, as it is a widely used communication technology. The technology uses the IEEE 802.11 standards with 2.4 GHz Industrial, Scientific, Medical (ISM) band devices of 802.11 b/g/n and 5 GHz ISM band devices of 802.11 a/n/ac [6] [7].

IEEE 802.11ac refers to Wi-Fi 5 and covers the frequency range from 5180 MHz to 5825 MHz. Wi-Fi 6, known as IEEE 802.11ax, is an improved version of Wi-Fi 5 with features designed to work better in crowded places. Wi-Fi 6 covers frequencies in both the 2.4 GHz and 5 GHz bands [8]. Wi-Fi 6E operates in the 6 GHz band, specifically from 5.925 to 7.125 GHz. The Wi-Fi Alliance has allocated a 1200 MHz spectrum range within this band for Wi-Fi applications. This new band allows Wi-Fi 6E to operate with 14 80 MHz channels and 7 160 MHz channels. The absence of licensing requirements in ISM bands offers clear flexibility and convenience when deploying UAV-based communications systems.

The main challenges associated with Wi-Fi technologies include limited communication range and the need for a Line-of-Sight (LoS) connection. Conversely, UAVs connected via cellular networks using Long-Term Evolution (LTE) and 4G (LTE-A), as seen in Table 2.1, provides a solution to these Wi-Fi challenges by extending the communication range beyond LoS connections. In a UAV-based network,

interfaces are established for UAV communications [8] [9] [10].

In 2019, the Portuguese Autoridade Nacional de Comunicações (ANACOM) made a decision regarding 5G, approving the allocation of the 700 MHz band for electronic communications services. The decision also established limits on the number of frequency licenses to be issued for the 700 MHz, 900 MHz, 1800 MHz, 2.1 GHz, 2.6 GHz, and 3.6 GHz bands. Additionally, ANACOM detailed the procedures for the allocation of these frequencies [11]. The 5G auction took place in 2021 [12]. More detailed information can be found in Table 2.1.

We should also mention the 2G and 3G networks. The 2G network operates based on Global System for Mobile Communications (GSM) technologies, which primarily include GSM 900 and GSM 1800 frequency bands. A detailed breakdown of these frequency bands is presented in Table 2.1. The 3G network predominantly uses Universal Mobile Telecommunications System (UMTS) technology. The UMTS network operates across specific frequency bands, which are further detailed in Table 2.1 [13] [14].

Table 2.1: LTE, 4G, UMTS, GSM, and 5G Portugal Communication Bands. Sources: [15] [16] [17] [18] [19] [20]

Interface	Name	Uplink (MHz)	Downlink (MHz)	Channel Bandwidths (MHz)
LTE & 4G (LTE-A)	B3 (1800 +)	1710-1785	1805-1880	1.4, 3, 5, 10, 15, 20
	B1 (2100)	1920-1980	2110-2170	5, 10, 15, 20
	B7 (2600)	2500-2570	2620-2690	
	B20 (800 DD)	832-862	791-821	
UMTS	B1 (2100)	1920-1970	2110-2170	
	B8 (900)	880-915	925-960	
GSM	900 (E-GSM)	890-915	935-960	
	1800 (DCS)	1710-1880	1805-1880	
5G	APT 700	703-733	758-788	5, 10, 15, 20
	900	880-915	925-960	
	1800	1710-1785	1805-1880	
	2100	1920-1980	2110-2170	
	2600	2500-2570	2620-2690	
	TD 3500	3300-3800		10, 15, 20, 30, 30, 50, 60, 70, 90, 100

2.2 UAVs Modulation and Protocols

The RC is an integral part of the ground control system, along with the telemetry and video links. These elements use a variety of RF channels, including but not limited to Wi-Fi, LTE and ISM bands [21]. Regarding video transmission, Orthogonal Frequency-Division Multiplexing (OFDM) is the leading technology in wireless links [5]. In the field of remote control systems, it has been found that a large number of systems operate mainly in the 2.4 GHz band. In addition to using 2.4 GHz

bands, particularly those manufactured by DJI, can operate in both 2.4 and 5.8 GHz bands. These drones are designed to select the least crowded frequency band for operation. In RC, both bands use spread spectrum technologies due to their superior resilience, allowing them to better cope with potential interference [22] [23] [24] [25].

Spread-spectrum signals involve an additional form of modulation that significantly increases the signal's bandwidth beyond the underlying channel code and modulation demand. These communication systems serve various purposes: they help reduce interference, create challenges in detecting and processing secure communications, adapt to fading and multi-path channels, and enable multiple users to access the system simultaneously. Moreover, spread-spectrum signals create minimal disruption to other systems operating within the same frequency band [26] [27].

An examination of conventional drone technologies reveals that, in addition to OFDM, the most commonly used digital modulation techniques include Frequency-Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) [23] [24] [28].

The main characteristics of each modulation are as follows:

- **OFDM**: OFDM is a key modulation technique in UAV communication signals. It is the fundamental modulation method in several prominent systems, including 802.11Wireless Local Area Network (WLAN), which specifies protocols for computer communication [29]; 802.16 Worldwide Interoperability for Microwave Access (WiMAX), which provides options for wireless broadband communication and enables high-speed internet access over large distances [30]; and 3rd Generation Partnership Project (3GPP) LTE, which develops protocols for mobile telecommunications [31].

  Unlike traditional modulation, OFDM is a digital modulation technique that uses multiple subcarriers within a single channel instead of using a single carrier in traditional methods. Using multiple subcarriers, OFDM achieves the same data rates as conventional single-carrier modulation within a given frequency band. This is due to the parallel transmission of data across the multiple subcarriers, which enables improved spectral efficiency and robustness against various channel impairments commonly encountered in wireless communication environments [32].

- **DSSS**: DSSS is a communication technique that extends the signal by using a special wideband code called a Pseudo Noise (PN) code. This technique spreads the signal's frequencies over a wide spectrum, matching the bandwidth of the PN code. By doing so, it ensures that the transmitted signal is less susceptible to interference. In DSSS, modulation techniques such as Binary Phase Shift Keying (BPSK) or Quadrature Phase Shift Keying (QPSK) are used to encode the data onto the carrier wave by altering its phase.

  - In BPSK, each data bit (0 or 1) is represented by a phase shift of either 0° or 180°.
  - In QPSK, data bits are grouped into pairs, with each pair represented by a phase shift of 0°, 90°, 180°, or 270°.

The PN code not only spreads the signal but also serves as a key to decode it. DSSS is designed to operate at a level below the noise floor, making it difficult for an adversary to intercept or disrupt the communication without knowing the PN code. However, DSSS systems are still susceptible to jamming if the power of the jamming signal is significantly higher than that of the original signal [27] [32].

- **FHSS**: Frequency hopping refers to the regular switching of the carrier frequency in a transmitted signal. This dynamic feature provides significant resistance to interference in a communications system. Unlike direct sequence systems, which use spectral spreading, despreading, and filtering to mitigate interference, the primary method used in a frequency hopping system to suppress interference is avoidance [26]. Frequency hopping involves the signal moving or 'hopping' between different channels based on a sequence agreed between the controller and the drone. When the communication link is set, both devices synchronize their hopping sequence. The carrier frequencies are spread evenly throughout the frequency band, such as the 2.4 GHz band (from 2.4 GHz to 2.5 GHz) or the 5.8 GHz band (from 5.725 GHz to 5.875 GHz). There are typically 30 to 60 channels, and each is separated between 1.5 and less than 2 MHz [5] [33]. Table 2.2 lists the most common modulations by frequency band and functional link.

Table 2.2: Used modulations for each frequency. Source [24]

Link/Frequency	2.4 GHz	5 GHz
Control	DSSS+FHSS/DSSS/OFDM	DSSS+FHSS/DSSS/OFDM
Video	OFDM	OFDM
Telemetry	OFDM, DSSS	OFDM

2.3 GNSS fundamentals

The navigation link component uses GNSS technology. GNSS refers to any satellite constellation providing three services: global Positioning, Navigation, and Timing (PNT). GNSS currently consists of several systems: Global Positioning System (GPS); GLONASS; Galileo; and BeiDou [34].

GNSS satellites continuously transmit navigation signals in the L-band across two or more frequencies. These signals carry essential components like ranging codes and navigation data,

enabling users to calculate the time taken for the signal to travel from the satellite to the receiver and to determine the satellite's position at any time.

The key elements of these signals are outlined below [35] [36]:

- **Carrier:** This is the radio frequency sinusoidal wave transmitted at a designated frequency.
- **Ranging code:** These sequences of 0s and 1s, which are known as Pseudo-Random Noise (PRN) sequences or PRN codes, allow the receiver to calculate the time taken for the signal to travel from the satellite to the receiver. This principle is used in both the GPS Coarse/Acquisition (C/A) and P codes.
- **Navigation data:** This binary coded message conveys essential information, including the satellite's ephemeris (which describes the satellite's position and velocity using Keplerian elements), clock bias parameters, almanac data (which offers a less precise set of ephemeris data), satellite health status, and other pertinent details.

These concepts are relevant since many commercial drones have a 'return to home' function, designed to be activated when the drone loses signal from its remote control, relying on GNSS. From the systems mentioned above, GPS and Galileo are inter-operation systems in the European Union.

Regarding GPS, it operates on three bands: L1, L2, and L5. The L1 band has a bandwidth of 30 MHz, with a carrier frequency of 1575.42 MHz. The L2 band also has a bandwidth of 30 MHz, but its carrier frequency is 1227.60 MHz. Finally, the L5 band has a relatively smaller bandwidth of 26 MHz, with a carrier frequency of 1176.45 MHz [37] [38] [39]. The modulation used for the GPS C/A code is BPSK [40], and its spectrum is represented in Figure 2.2.

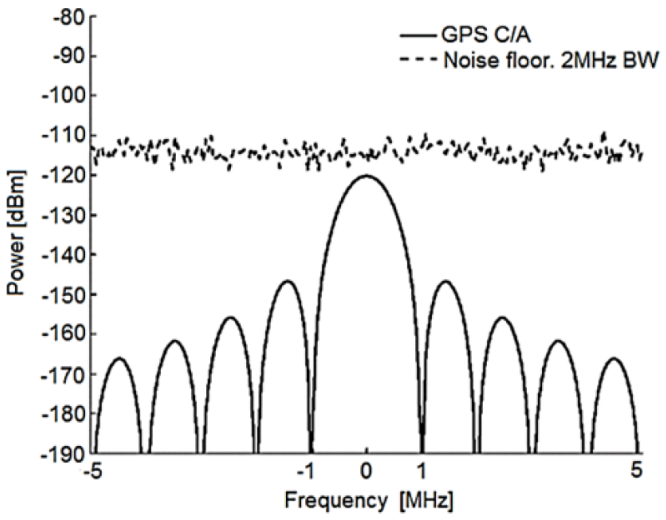


Figure 2.2: Spectrum of C/A code GPS. Source: [41]

Galileo operates on three primary frequency bands: E1, E5, and E6. The E1 band features a bandwidth of 24.552 MHz and a carrier frequency of 1575.42 MHz. The E5 band is split into two sub-bands, E5a and E5b. The E5a band has a bandwidth of 20.460 MHz and a carrier frequency of 1176.45 MHz, while the E5b band also has a bandwidth of 20.460 MHz, operating at a carrier frequency of 1207.14 MHz. Lastly, the E6 band has a bandwidth of 40.920 MHz and operates at a carrier frequency of 1278.75 MHz [42]. For Galileo, the C/A code equivalent is included in the E1 Open Service signal, which utilizes Composite Binary Offset Carrier (CBOC) modulation. This CBOC modulation is a more sophisticated version of BPSK, aimed at enhancing signal performance and ensuring compatibility with existing GPS signals [43].

Table 2.3 compiles all the data regarding the frequencies used for each of the technologies.

Table 2.3: Comparison of GNSS with global coverage. Source: [5] [44]

System	GPS	GLONASS	Galileo	BeiDou
Owner	USA	Russia	EU	China
Frequency	1.164–1.189 GHz (L5) 1.215–1.2396 GHz (L2) 1.563–1.587 GHz (L1)	1.189–1.214 GHz (L3) 1.237–1.254 GHz (L2) 1.593–1.610 GHz (L1)	1.164–1.215 GHz (E5a/b) 1.260–1.300 GHz (E6) 1.559–1.592 GHz (E1)	1.20714 GHz (L2) 1.26852 GHz (E6) 1.561098 GHz (L1) 1.589742 GHz (L1-2)

2.4 Anti-Drone System Requirements

To design an effective anti-drone combat system, several key properties must be considered. The following are the fundamental pillars [4]:

- **Drone Detection**: Traditional perimeter security systems typically use tools such as radar or cameras to detect drones. However, these systems often struggle to effectively identify different types of drone activity due to their limited capabilities. To create an anti-drone system using existing surveillance equipment, it's essential to rethink the entire structure to improve the detection of different types of drones from a significant distance, thereby increasing the readiness of defense mechanisms;

- **Defense capability against multiple drones**: Past unauthorized drone incidents have highlighted the risk of potential drone fleet attacks. After all, there will be many legitimate flying objects, including Personal Air Vehicles (PAVs), in the vicinity. This scenario requires the ability to detect and manage multiple drone threats simultaneously.

- **Collaboration with security forces**: The primary method of safely protecting an area from unauthorized or illegal drones is to intercept these drone threats. In addition to proactive

investigations, it's important to explore legal restrictions and potential cooperation with national or public security systems such as the police or military.

- **System Portability**: Protecting an area from unauthorized or illegal drones can vary depending on location and time. Rapid counter-drone operations can be implemented using mobile detection, identification, and neutralization components. This requires lightweight equipment and reliable wireless networks for effective deployment.

2.5 Jammer Designs

In this section, we analyze two methodologies for a jammer design: Software Defined Radio (SDR) and circuit-based implementations. Each has its advantages, disadvantages, and challenges in achieving signal jamming, while accommodating different levels of technical expertise and operational paradigms.

2.5.1 Circuit-Based Implementation

A circuit-based jammer is a hardware solution designed to disrupt drone control signals [45] and works by emitting powerful radio waves that interfere with the radio signals used by drones to communicate with their operators [46].

At the heart of the jammer's circuit lies the Voltage-Controlled Oscillator (VCO), a pivotal component where alterations in input voltage induce proportional changes in output frequencies. This component serves as the core of the drone jammer system [47].

The jamming mechanism works by transmitting electromagnetic signals at the same frequency of the drone's communication systems, effectively overriding them. This action commonly triggers the activation of the drone's Return to Home function, often aiding in the identification of the drone pilot [46].

This strategy embodies an electro-motive force defensive technique against signals, rendering UAVs incapable of communicating with the operator. Consequently, it shields the secured area against unauthorized drone intrusions [47].

2.5.2 SDR-Based Implementation

A SDR system represents a radio communication system in which functions typically realized by analog hardware are instead executed by software on a personal computer or embedded system. It is a sophisticated device designed to perform many complex operations simultaneously to ensure the seamless transmission and reception of data. This allows for rapid reconfiguration to handle different signalling technologies and standards [48] [49].

GNU Radio is an open-source software development toolkit that allows users to create and modify signal processing algorithms for SDRs. It provides a variety of signal processing blocks for tasks like demodulation and decoding, enabling experimentation with advanced SDR concepts and the development of digital signal processing applications [49]. Although SDRs and GNU Radio are often used together to design and customize signal processing systems, they can also operate independently [50] [51].

SDR and GNU Radio have important applications in drone jamming. Drone jamming involves using SDR platforms to generate a jamming signal aimed at the drone's GPS communication systems. This can neutralize the drone's ability to operate autonomously. The flexibility of SDR and GNU Radio allows the implementation of different jamming techniques, taking into account spectral efficiency, power efficiency, and complexity [50].

2.6 UAVs Detection

According to [1], [27], four methods can be used to detect the existence of UAVs:

- **Audio Surveillance**: Acoustic sensors rely on microphones to detect the unique sound emitted by drones, particularly the distinct noise their propellers produce. While proficient in detecting drones nearby, the efficacy of acoustic sensors decreases as the drone moves farther away.
- **RF sensors and direction finders**: In this approach, interception occurs by capturing the RF waves emitted by the UAV. Typically, a manually operated UAV establishes communication with a Ground Station (GS) and a GNSS for its functioning. However, these components might be absent if an autonomous UAV relies solely on onboard sensors. Communication between the GS and the UAV often involves methods like FHSS. For many commercial UAVs, the implementation of an AI-driven classification algorithm is feasible. This algorithm uses SDR to scrutinize the spectrum. Moreover, tracking and localizing UAVs are achievable based on the signal strength obtained from these RF waves.
- **Radar Systems**: Radar systems use radio waves to identify and track drones, providing long-range detection capabilities. These systems can effectively monitor drone movements from a distance. Various radar types, such as pulsed radar, continuous-wave radar, and frequency-modulated continuous-wave radar, offer distinct advantages and drawbacks.
- **Video Surveillance**: Strategically positioned cameras in an area facilitate video surveillance, enabling the implementation of deep learning models specialized in detecting and monitoring UAVs. These models focus on identifying UAV appearances or their movements. Employing multiple cameras with varying field views enhances the speed and probability of detection. In

low-light conditions, where conventional systems struggle with insufficient contrast and features, thermal and infrared imaging emerge as viable detection solutions.

2.7 UAVs Neutralizing

A UAV neutralization system operates in four steps: detection, identification, location, and neutralization [5]. First, the system detects the presence of a UAV using sensors like radar or cameras. It then identifies the type of drone to determine if it poses a threat. Afterward, the system locates the UAV´s precise position, including its coordinates and trajectory. The stages of identification and location within the drone neutralization process are intricately linked to the various techniques defined in 2.6. Two different forms of neutralisation can be used: hard and soft kill.

Hard-kill systems adopt a destructive methodology aimed at eliminating the drone. These mechanisms use kinetic projectiles, nets, lasers, birds, or even specialized drones to destroy the target. Hard-kill systems pose the risk of causing unintended collateral damage [5]. Below is a description of the most relevant examples [52]:

- **Nets:** Nets Capture involves a physical technique aimed at neutralizing UAVs. Defenders use firearms or specialized weaponry to launch nets that ensnare the UAV. Upon being shot, the net expands and, upon contact with the drone, closes to restrict its mobility and render it inoperable.
- **Directional Electromagnetic Pulses:** Directional Electromagnetic Pulses (DEMPs) are primarily used to counter unauthorized electronic devices within vehicles. These pulses aim to disrupt or deactivate control systems that could otherwise restart or interfere with the proper operation of the vehicle.

Soft-kill systems rely on electronic countermeasures to disrupt drone communications, either by jamming or spoofing signals. This jamming can either divert control of the drone or simulate control of the drone's communications to initiate a controlled landing or deter its presence. Soft-kill systems offer a rapid response time and are less destructive than hard-kill systems. However, soft-kill systems are much more complex to implement than hard-kill systems [5].

Fixed packet protocols govern the RF radio communication between the GS and the UAV. If intercepted and decoded, these packets can reveal their architecture, potentially leading to the execution of a spoofing attack. Additionally, RF jammers, emitting high-energy signals directed at the UAV, can disrupt communication. Consequently, such interference may trigger the UAVs fail-safe measures, resulting in actions like initiating a safe landing in its current position, returning to a predetermined base, or experiencing erratic flight leading to a crash. In the case of an autonomous UAV, there's a risk of tampering with sensor values. Specifically, GNSS signals are vulnerable to both jamming and

spoofing attacks. Furthermore, there exist other potential physical attacks within this context. All the possible techniques are mentioned in the Figure 2.3 [27].

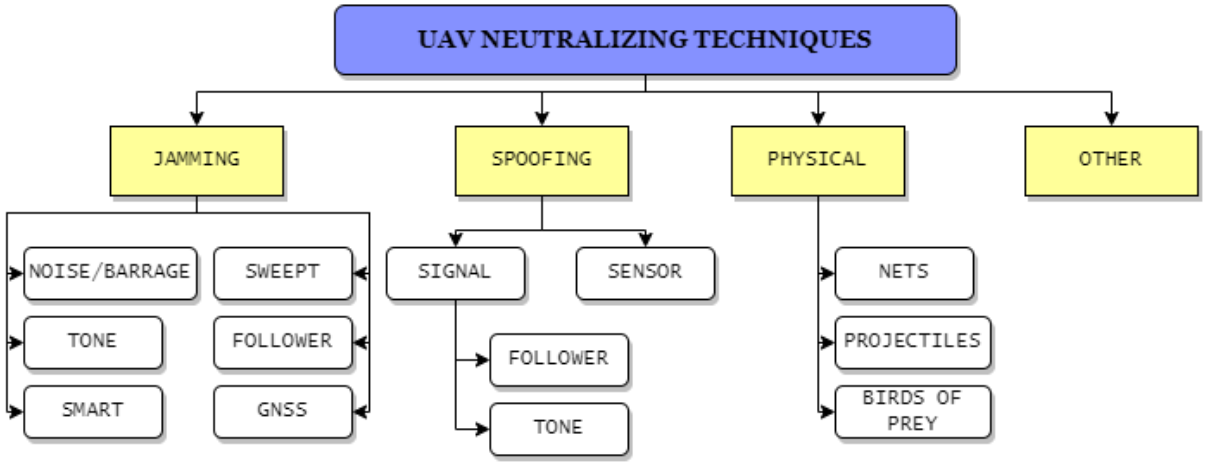


Figure 2.3: UAVs neutralizing techniques. Adapted from: [27].

2.7.1 Radio Frequency Spoofing

Spoofing involves sending fraudulent or misleading communications that appear to come from a known source to deceive the recipient. To execute spoofing effectively, understanding the communication protocol stacks beyond the physical layer is critical for accurate replication. However, if these stacks are unknown, determining them becomes an initial challenge. Spoofing is a complex method and is not always successful. Theoretically, the use of spoofing techniques could allow a malicious drone to be hijacked and redirected away from a protected area. Moreover, spoofing is particularly prevalent in the context of civil GPS signals, which lack encryption or authentication. The lack of security measures in civil GPS signals allows the creation of false signals that mimic legitimate satellite sources. By simulating GPS signals, a malicious actor can trick GPS receivers into accepting false location data, thereby compromising the integrity and reliability of location-based information [53] [54].

While on the subject of spoofing, there is another important aspect of airspace security, the concept of No-Fly Zone (NFZ). A NFZ, also known as an air exclusion zone, is an area over which certain aircraft types are prohibited from flying. These zones are usually created by decisions of military or governmental bodies to protect certain areas or occasions from airborne threats. They can be secured by surveillance, preventive action, or counter-action against an offending aircraft. The use of NFZs has been observed in various conflict areas and high-profile events as it increases the overall security against unwanted air incidents [55] [56]. As flying in these zones is illegal, spoofing into one of them could automatically force the drone to land or, if it hasn't already taken off, prevent it from taking off at all [57].

2.7.2 Radio Frequency Jamming

RF jamming techniques are used to disrupt, degrade, or completely stop communication between a drone and the GS. This is done by creating a disruptive signal that drops the Signal-to-Interference-plus-Noise Ratio (SINR) picked up by the drone's receiver. This makes it difficult, if not impossible, for the drone to effectively receive instructions from the remote control. In addition, it is possible to jam the remote's signals, thereby interfering with any feedback data transmitted by the drone. Jamming GNSS signals is not a separate method from RF jamming, but focuses on specifically jamming GNSS signals. This distinction is crucial because the neutralization of GNSS signals is important due to their susceptibility to jamming. Signals received from satellites are low power, making them highly susceptible to interference from spurious signals. Therefore, the use of this technique can be particularly effective in this scenario [54].

Some drones have safety mechanisms that activate when they lose connection to their controller. These safety features can cause the drone to either slowly descend to the ground or return to its initial takeoff point by using GPS signals. However, jamming can result in drone malfunctions and potential crashes. Employing GPS jammers can interfere with the crucial GPS signals relied upon by autonomous and return-to-home drones. This method is considered the optimal and most effective approach as it ensures the drone will crash, preventing its return to the owner [58]. Nevertheless, jamming signals may also interfere with other devices operating within the same frequency range in the vicinity.

The most relevant jamming techniques are defined below [5] [27] [32]:

- **Noise/Barrage Jamming**: This type of jamming, considered the most basic form, involves introducing a noise signal into either a fraction or the entire spectrum of a wideband modulated signal. Such jamming directly impacts and diminishes the system's channel capacity by reducing the Signal-to-Noise Ratio (SNR) at the receiver. Consequently, it elevates the information error rate while decreasing the channel capacity. Specifically, in FHSS and DSSS systems, noise jamming disrupts crucial processes like clock synchronization and tracking necessary between the sender and receiver during transmissions, by introducing wideband background interference.

- **Sweep Jamming**: This method involves transmitting a signal with a narrow bandwidth that moves across an entire band in a sweeping motion. The speed at which this signal moves is termed the sweeping rate. One advantage of the sweep jammer is its practical feasibility compared to the barrage jammer. With a high enough sweeping rate, the sweep jammer can effectively resemble the barrage jammer.

- **Tone Jamming**: This method involves dividing the noise signal into separate tones and transmitting them simultaneously or through a sweeping motion, termed a chirp jammer. This

type of jammer has the advantage of potentially causing less interference with other radio communications. However, it is only suited for specific types of signals, particularly FHSS signals.

- **Follower Jamming**: A follower jammer monitors the frequency shifts in an FHSS system to identify and disrupt the newly used frequencies. It detects the target FHSS system frequency by assessing energy fluctuations within the spectrum: energy gains signify a new signal entering the band, while energy losses indicate a signal exiting. However, precise identification of whether a particular energy variation aligns with the target signal requires additional analysis and validation.

- **Smart Jamming**: This jamming method is suitable when the characteristics of the target signal are known beforehand, obtained from sources like Radio Frequency Integrated Circuit (RFIC) specifications. Smart jamming selectively disrupts essential signals to hinder successful communication, ensuring efficiency and effectiveness. Achieving this involves analyzing transmitted data to pinpoint critical areas for disruption. Protocol-aware jamming, facilitated by Software Defined Radios, entails crafting a jamming signal akin to the target signal in aspects such as hopping patterns (for FHSS systems), PN code data rate (for DSSS systems), and modulation techniques. This technique demonstrates superior effectiveness in jamming both for DSSS and for FHSS systems; however, its success relies on a thorough analysis of the target signal.

- **Response jamming**: Response jamming, often termed as spoofing, differs from noise jamming as it doesn't target specific parts of the spectrum to obstruct transmission. Instead, its objective is to generate and transmit a signal resembling the original one. This replicated signal, emitted with higher power than the authentic transmitter, aims to deceive the receiver, such as a UAV. The consequences of this tactic can range from confusing GPS systems to seizing control of the drone. Notably, constructing such a jammer is more intricate than developing a noise jammer. Response jamming or spoofing necessitates intercepting the original signal, altering it, and transmitting a false signal with sufficient power. This process tricks the UAVs system into perceiving the falsified signal as a legitimate control command.

2.8 Related Work

This section reviews the key studies that investigate different approaches to drone countermeasures using SDR platforms and other technologies. The works discussed here focus on the effectiveness of jamming methods such as barrage, sweep, and protocol-aware jamming, as well as spoofing techniques, with the goal of identifying optimal solutions for disrupting or controlling drones.

Aflah AL-Hajri and Selvarani Murugesan [59] explored the development of a cost-effective drone jammer using a SDR, specifically the HackRF One platform. They tested two jamming techniques:

barrage jamming and sweep jamming. The results showed that analog barrage jamming became more efficient as the signal amplitude increased, with optimal performance achieved at a sampling rate 20 MHz. In digital barrage jamming, QPSK and Differential Quadrature Phase Shift Keying (DQPSK) modulation outperformed BPSK and 8 Phase Shift Keying (8PSK). In contrast, sweep jamming proved less effective overall. The optimal jammer configuration identified in the study used analog barrage jamming with a fast noise signal, an amplitude of 15, a sampling rate 20 MHz, and a bandwidth of 20 MHz. This setup successfully jammed drones positioned 1 meter from the jammer and 16 meters from the remote control. The study concluded that analog barrage jamming is the most effective technique for countering unauthorized drone operations, offering a secure solution to prevent malicious drone activities.

Alexandre Heuchamps [33] implemented a jammer using GNU Radio on a SDR. He first considered the brute force jammer, performing theoretical calculations to determine the necessary power. Later he extended it to the sweep jammer and reactive jammer. When using Lime SDR [60], he could not cover the entire area of interest, because the maximum bandwidth allowed by Lime SDR is 61.44 MHz, and the band of interest was 83.5 MHz-wide. Analyzing the results obtained, the barrage jammer was ineffective because the Additive White Gaussian Noise (AWGN) was emitted over the entire bandwidth of the Lime SDR. He then implemented the sweep jammer, which guaranteed a significant improvement. It allowed periodic sweeping of the signal in a given bandwidth. Later, he concluded that it was still insufficient and needed something more complex. Finally, he applied a reactive jammer. This proved to be more complicated, but there was no precise answer about its effectiveness.

Rahman, Ghani, Khamis, and Sidek [41], carried out a field test in which they performed GPS jamming of a UAV using SDR and GNU radio software. The paper focussed essentially on blocking jamming of the GPS. The jamming technique used was Barrage jamming (broad-band jamming). The jamming signal was constructed using GNU Radio software, which included a Noise Source block combined with AWGN. The Noise Source block generates random noise, while AWGN simulates the effect of natural random noise by adding a constant power spectral density and a Gaussian amplitude distribution to the signal. The constructed signal was processed and transmitted by an SDR, using a DJI Phantom 4 Pro drone as a target. The outcomes were positive. Assessments were conducted across different angles and distances. Optimal performance occurred at an angular elevation of 0 degrees, achieving a maximum distance of 150 meters. At an absolute distance of 111.8 meters, jamming succeeded at an angle of 26.6 degrees but failed at 63.4 degrees.

Ferreira et al. [53] proposed an Anti-UAV system with features that enable jamming and spoofing. The proposed solution revolves around a portable system utilizing SDR platforms. Its primary function is to detect and counter unauthorized drones by employing electromagnetic waves, rendering the drone inoperable and potentially gaining control over it. Protocol-aware jamming demonstrated the most

effective outcomes when disrupting the GPS signal. On the other hand, barrage jamming emerged as the most proficient method for disrupting remote control frequencies, when the communication protocol is unknown. The authors assert that their developed system can disrupt communications for remotely controlled SDRs (commonly using radio frequencies at 2.4 GHz or 5.8 GHz) and autonomous flights using GNSS signals. Given the difficulty in determining the operational mode of the drone, the system emits jamming signals tailored to address both modes. Ultimately, by employing spoofing signals, they seized control of the drone, maneuvering it to a predetermined location.

Rozenbeek [5] conducted extensive research that focused on jamming and spoofing. When addressing the issue of jamming for drones using 802.11x WiFi, he used various techniques such as full-band barrage jamming, single-channel barrage, de-authentication and CSMA/CA attack. In addition, when dealing with drones using FHSS, he extended his approach to include sweep and protocol-aware jammers. Regarding the technical equipment used, Rozenbeek incorporated multiple SDRss in addition to conventional personal computers and Power over Ethernet. The software used for the experiments was GNU Radio. The results in jamming WiFi and FHSS drones were consistently positive. Full-band barrage jamming demonstrated superior performance among the techniques employed, particularly in the Identification Requirement parameter.

Slimeni and Dalleji [21] innovatively engineered a cost-effective SDR board designed for RF-based detection, identification, and interference capabilities, with a specific focus on disrupting either uplink drone command signals or downlink data streams like video transmission or telemetry. Their solution aimed to interfere with the drone-to-ground wireless connection prevalent in the 2.4 GHz frequency band. Their system comprised three core modules: Mini-UAV RF Detection, UAV RF Identification, and UAV RF Neutralization. Detection employed the Energy Detection technique via the SDR platform, while identification relied on machine learning algorithms. The neutralization phase involved deliberate jamming of the 2.4 GHz band, effectively obstructing or halting wireless connections within this frequency range. The jamming process was detailed through steps involving the generation of a continuous long training sequence, activation of the Modular Radio Platform's front end in Tx mode, and configuration of the hopping pattern for the chosen front end. Subsequent verification confirmed the successful jamming, resulting in restricted command link ranges for the affected drones.

Liaquat et al. [61] presented an advanced framework aimed at preventing unauthorized drone intrusions by integrating radar detection with GPS spoofing techniques. Their system employs an L-band radar combined with digital beamforming to accurately detect and track drones, providing comprehensive information including range, velocity, azimuth, and elevation angles. The radar's phased array system enhances detection accuracy, even for drones with smaller radar cross-sections operating at lower altitudes. Upon detection, the system uses GPS spoofing to transmit falsified GPS coordinates to the drone, effectively redirecting it from restricted areas. This process exploits the vulnerability of

civilian GPS systems, which lack encryption and are thus susceptible to spoofing. The framework was thoroughly validated through simulations and real-world experiments using SDR, confirming its efficacy in both detection and spoofing. The results demonstrated a high level of precision in altering drone paths and blocking access to sensitive airspace, underscoring the potential of this dual approach for securing critical locations from malicious drone activities.

Novák et al. [62] investigated vulnerabilities in GNSS signals used by UAVs, focusing on spoofing and jamming techniques using a HackRF One SDR. It generated signals that mimic authentic GPS transmissions to test spoofing on UAV models such as the DJI Inspire and 3DR IRIS+ with GPS broadcast ephemeris files. The HackRF One, equipped with a Temperature Compensated Crystal Oscillator, broadcasted GPS signals at 1575.42 MHz, enabling precise spoofing of the UAV' detection capabilities. The study found that jamming at certain power levels caused complete GPS signal disruption. Spoofing resulted in significant positional deviations, with a Root Mean Square Deviation in 2D space (RMS2D) positional error up to 57 times higher than normal, leading to navigation errors. Further analysis calculated the effective interference range, providing practical data on jamming and spoofing signals. Results indicated that while newer UAV models with anti-jamming capabilities showed some resilience, their vulnerability to spoofing remained high.

3

System Design and Methodology

Contents

3.1 Hardware and Software 27

3.2 Methodology 34

3.1 Hardware and Software

3.1.1 Hardware

This master's thesis relies on four key pieces of equipment. Figure 3.1 shows a diagram of the system's hardware components. The laptop acts as the control centre, where all signal generation and processing scripts are developed and executed. The ADALM-PLUTO SDR modulates and transmits these signals. Due to the low output power of the SDR, a power amplifier is required to boost the signal to a level sufficient for effective transmission. Frequency specific antennas ensure the best signal to send and receive. Each component is critical to the successful implementation and testing of the system.

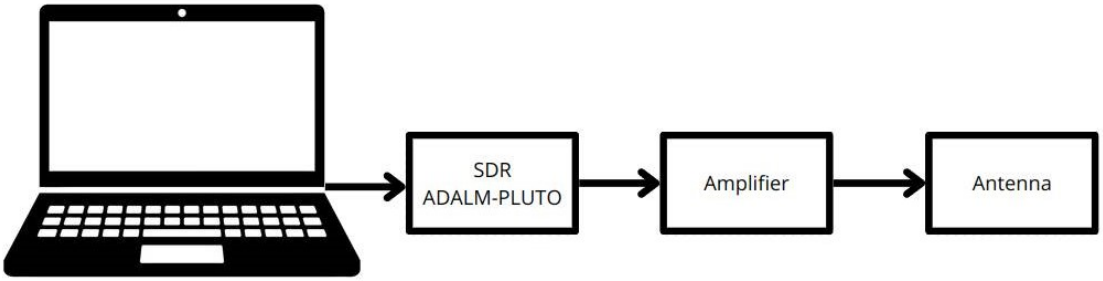


Figure 3.1: Diagram of the system's hardware components.

3.1.1.A ADALM-PLUTO

The ADALM-PLUTO, or PlutoSDR, is a RF learning module developed by Analog Devices Inc (ADI). It can be used for learning SDR, RF and wireless communications. This SDR is an easy-to-use tool suitable for both instructor-led and self-directed learning environments [63] [64].

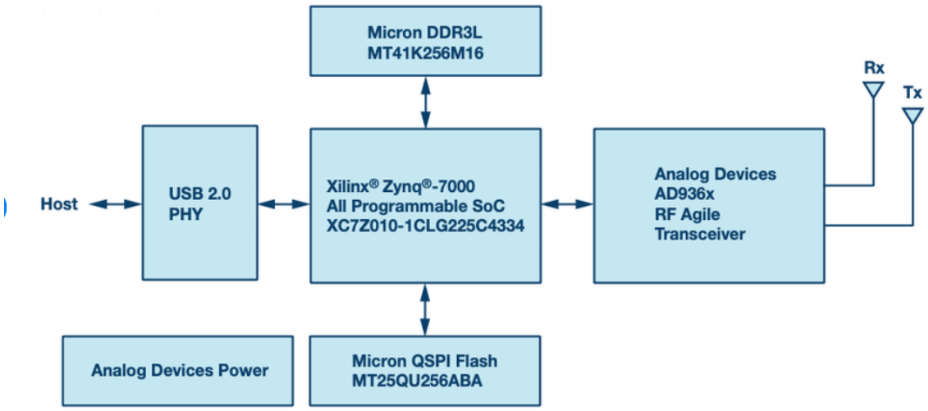
The ADALM-PLUTO, shown in Figure 3.2, uses the Analog Devices AD9363 RF Agile Transceiver and integrates the Xilinx Zynq Z-7010 FPGA [64]. The AD9363 is a high-performance, highly integrated, full duplex RF transceiver. It has transmit and receive channels that can operate at separate tuning frequencies. It has a tuning range of 325 MHz to 3.8 GHz with a 2.4 Hz LO step size and supports a tunable channel bandwidth of 200 kHz to 20 MHz. The device includes integrated 12-bit DACs (Tx) and ADCs (Rx) with variable output data rates from 61.44 kSPS to 65.1 MSPS [64] [65].

However, there is a method of extending the frequency range of the ADALM-PLUTO up to 6 GHz. This method involves modifying a device string on the PlutoSDR via a USB serial connection. This modification applies to both RX and TX. The AD9363 chip 3.2(b), which is limited to a frequency range of 325 - 3800 MHz and a bandwidth of 20 MHz, can be made to operate like the higher-end AD9364 chip. The AD9364 chip supports a frequency range of 70 MHz to 6000 MHz and a bandwidth of 56 MHz.

The Xilinx Zynq Z-7010 FPGA, which is part of the Zynq-7000 All Programmable SoC family, features

a single-core ARM® Cortex™-A9 MPCore™ running at 667 MHz. It contains 28k logic cells, 2.1 Mb Block RAM, and no DSP slices [64].

(a) Adalm-Pluto Image.



(b) Adalm-Pluto Block Diagram.

Figure 3.2: Adalm-Pluto Device and Block Diagram.

The PlutoSDR is powered via a USB 2.0 interface with a Micro-USB 2.0 connector. It has a high-quality plastic casing and is compact enough to fit in a shirt pocket or rucksack. The unit is fully USB-powered. The ADALM-PLUTO supports several software packages, including MATLAB, Simulink, GNU Radio, and libiio-a C, C++, C#, and Python API. These software packages offer an innovative Graphical User Interface (GUI) that provides an intuitive experience and reduces the learning curve. This allows students to learn faster, work smarter, and explore further [64] [63].

In sum, the ADALM-PLUTO is an excellent tool for learning and experimenting with SDR, RF, and wireless communications.

3.1.1.B Amplifier

The power output of the SDR used proved to be too low for the intended purpose. Laboratory results showed that the maximum output power achieved was around 2 dBm, a value verified at low frequencies. For the target frequencies of 1.5 GHz and 2.4 GHz, the output power varies between -4 dBm and 0 dBm [66] [67]. This value may fluctuate, but it would never be sufficient for our purposes. It was therefore necessary to include a power amplifier. The power amplifier chosen for this purpose is the WYDZ-PA-1G-3GHz-1W.

This broadband power amplifier operates in the frequency range from 1 to 3 GHz and provides a gain of 40 dB. Gain refers to the amplifier's ability to increase the power of a signal from its input to its output [68] [69]. The amplifier is powered via a type C cable and requires a current of 2A, with a 5V/2A power supply recommended. It has an SMA female output interface and both input and output impedances are 50 ohms. The P1dB, or output power at 1 dB compression point, is 30 dBm at 2 GHz, which is equivalent to 1 W [68].

Figure 3.3: Power Amplifier: WYDZ-PA-1G-3GHz-1W.

3.1.1.C Antennas

- **2.4 GHz Antenna**

  The WIFI YAGI ABAKS 18 dBi, figure 3.4 is a high-performance directional antenna designed for outdoor use. This Yagi-type antenna features 18 precisely engineered elements, allowing it to maintain consistent performance in any weather condition. It is ideal for highly directional point-to-point connections that can cover several kilometers and features 18 dBi gain. Operating in the 2.4 GHz to 2.5 GHz frequency range, it is well suited to the 2.4 GHz band. The antenna supports both horizontal and vertical polarisation with a 35º aperture. It also has an impedance of 50 ohms and weighs just under 1 kg [70].

Figure 3.4: 2.4 GHz Antenna Image.

To get more reliable and detailed information about the antenna, we measured the return loss (S11), which shows how well the antenna is matched to its transmission line and how much power is reflected back to the source. Using a Vector network analyzer, we collected the data shown in Figure 3.5.

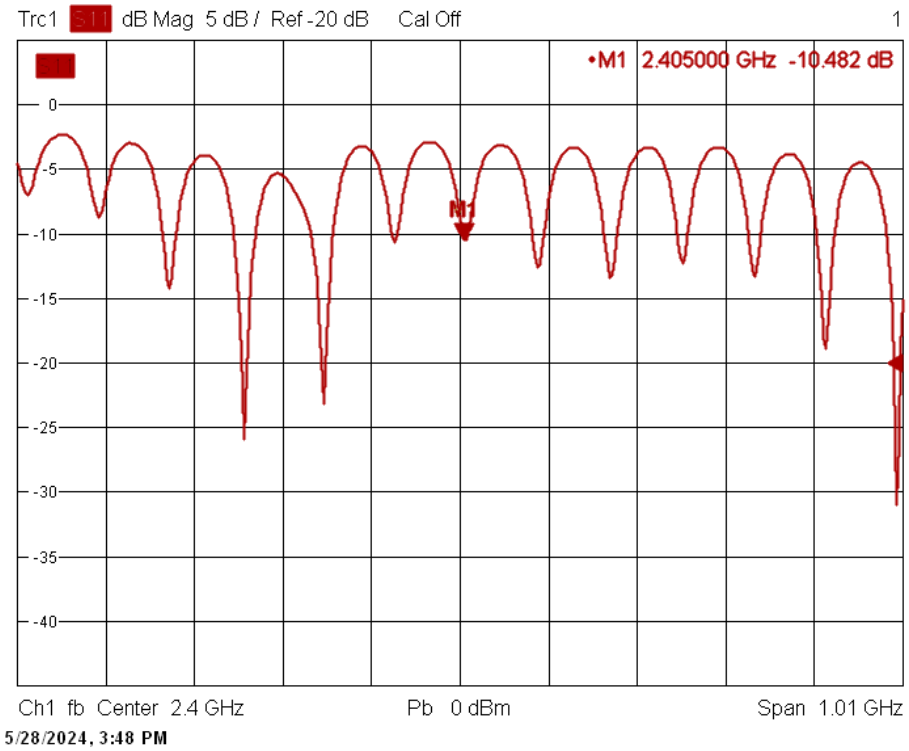


Figure 3.5: Measured return loss (S11) of the 2.4 GHz Antenna.

The S11 parameter is the reflection coefficient or the return loss of the antenna, which measures how much of the input signal is echoed back to the source. A lower S11 value is favorable, in other

words, a more negative S11 in dB, means that the matching in impedance is improved. The plot also reveals several valleys in the S11 values which suggest the frequencies at which the antenna and the transmission line are highly matched, usually where S11 is below -10 dB. The lowest descents are observed at about 2.05 GHz, 2.4 GHz (centered at M1, 2.405 GHz), 2.55 GHz, and 2.7 GHz. These points denote the operating frequency at which the antenna is most effective in radiating or receiving the electromagnetic power.

As for the bandwidth, one has to determine the range of frequencies over which the return loss is less than 10 dB. As can be seen from the plot below, the antenna seems to have multiple bandwidths centered around its resonant frequencies including the 2.4 GHz frequency.

The provided S11 plot reveals that the antenna is designed to operate efficiently around 2.4 GHz, with good impedance matching indicated by the return loss of -10.482 dB at 2.405 GHz. This characteristic makes it suitable for applications in the 2.4 GHz ISM band, including Wi-Fi and Bluetooth communications.

The plot spans a frequency range from approximately 1.895 GHz to 2.905 GHz, with each horizontal division representing 101 MHz. To determine the bandwidth, we look at the frequencies around M1 where the return loss crosses -5 dB, from roughly 2.34 GHz to 2.52 GHz, giving a bandwidth of 180 MHz. This ensures the antenna efficiently covers the 2.4 GHz ISM band (2.400 to 2.483 GHz).

- **1.5 GHz Antenna** The 1.5 GHz antenna, shown in Figure 3.6, operates within a frequency range of 1.560 GHz to 1.580 GHz, making it ideal for GNSS applications such as GPS. This antenna boasts a gain of 12 dBi, which makes it a suitable option for this master thesis. Additionally, it features a 30º aperture [71].

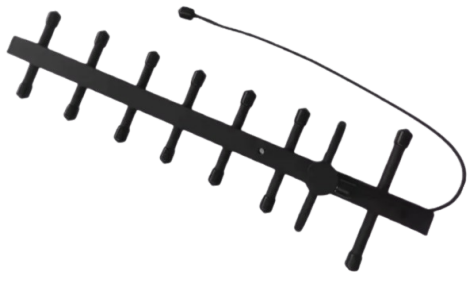


Figure 3.6: Measured return loss (S11) of the 1.5 GHz Antenna Image.

Due to the limited information available about this antenna, S11 was obtained using a Vector network analyzer, as shown in Figure 3.7.

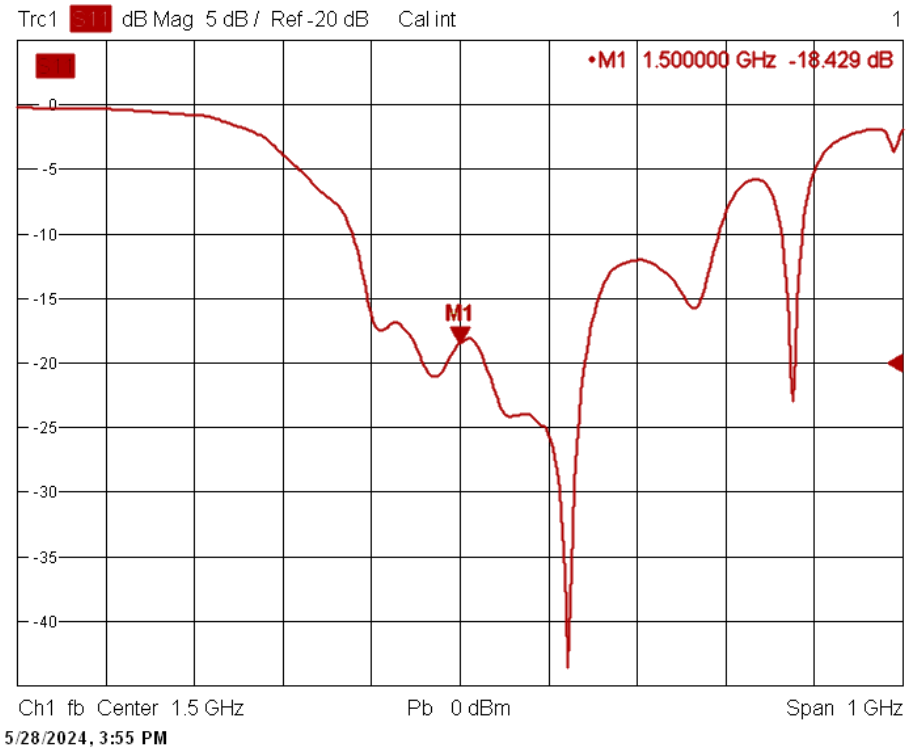


Figure 3.7: S11 of 1.5 GHz Antenna.

As is seen, the frequency range is from 1 GHz to 2 GHz, with a center frequency of 1.5 GHz. In this plot, the regions where the S11 value dips below -10 dB are considered frequencies where the antenna has good performance. Summarizing the analysis, we can identify the main frequencies with good performance: 1.1-1.2 GHz, around 1.3 GHz, 1.5 GHz, 1.6-1.7 GHz, and around 1.8 GHz.

It is worth nothing that this antenna is very well watched at 1.5 GHz, with S11 $<$ -15 dB over a with bandwidth.

3.1.1.D Drones

To test the efficiency and effectiveness of the methods developed, it is necessary to have what can be called a target or objective. In this way, the different methodologies implemented were tested on a set of drones, to obtain a more robust set of results that allow us to determine the versatility of the techniques implemented. Table 3.1 presents the specifications for the RC and video links of the drones used:

Table 3.1: Used Drones and respective operating frequencies

		Frequency (RC and Video Link)				
		2.400-2.4835GHz	2.405-2.475GHz	5.725-5.850GHz	5.150-5.250GHz	4G
Drone	DJI Mini 3 [72] [73]	X		X		
	DJI Mini 3 Pro [74] [75]	X		X		
	Autel Evo Nano+ [76] [77]	X		X	X	
	Husban Zino Mini Pro [78] [79]		X			X
	ZLL SG 108 [80] [81]	X				

As shown in Table 3.1, most drones primarily operate on two frequency bands: 2.5 GHz and 5.8 GHz. However, some drones come with unique features. For instance, the Autel Evo Nano+ can use an additional band, 5.150-5.250 GHz, which enhances its resilience compared to other drones. Conversely, the Husban Zini Mini Pro, an advanced version, can switch to 4G if the 2.4 GHz band is blocked, providing it with increased robustness and protection against interference.

3.1.2 Software

To develop the methods implemented in this Master's thesis, various software programs were used. The main concern was to ensure that all software was compatible with the LINUX operating system, specifically Ubuntu 24.04.1 LTS. This was important because some programs run better on LINUX, and working within a single operating system was preferable. Consequently, all software used was selected for its compatibility with LINUX.

3.1.2.A GNU Radio

Signal processing tasks are essential to implementing software radios. For this, we used GNU Radio, an open-source software available for free. Specifically, version GNU Radio 3.10.1.1 was employed in this work. GNU Radio works with easily accessible, low-cost external RF hardware to create software-defined radios. It can also function without hardware, operating in a simulation-like environment [82].

In GNU Radio, applications are commonly referred to as "flowgraphs". These are essentially sequences of signal processing blocks that are linked together to define a data flow. A major advantage of software-defined radio systems is their reconfigurability; instead of needing different radios designed for specific and different tasks, a single, versatile radio can serve as the radio front-end. The signal

processing software, in this case, GNU Radio, manages the specific processing required for different radio applications. This processing can be programmed in either C++ or Python. The core infrastructure of GNU Radio is written entirely in C++, while many of the user tools, including the GNU Radio Companion, are written in Python [83].

3.1.2.B Visual Studio Code

The previous software, GNU Radio, generates an executable written in Python, where the mentioned ”flowgraphs” are coded. However, to improve the capabilities of the generated scripts, it became necessary to implement some changes directly through the Python code. For this task, we used Visual Studio Code (VS Code). VS Code runs on various desktop platforms including Windows, macOS, and Linux. It has a rich ecosystem of extensions for other languages and runtimes, including Python [84].

3.2 Methodology

In this section, we focus on defining and outlining the tests and experiments to be implemented in our study. The implementations will be divided into two main groups based on their respective frequency bands. The first group focuses on the GNSS bands, with a particular emphasis on GPS. The second group pertains to the 2.4 GHz band, directly related to the RC and Video Transmission components.

3.2.1 GNSS Implementation

To interfere with the UAVs, various GNSS interference techniques were implemented. These methods, including jamming and spoofing, simulate real-world scenarios to analyze their effects on GNSS receivers.

3.2.1.A GNSS Barrage Jamming

To achieve a jamming solution, GNU Radio was used to develop the necessary scripts, as shown in Figure 3.8. The first script tested was for barrage jamming. Barrage jamming allows the jamming of GNSS signals by overwhelming the receiver with high power noise over a wide frequency spectrum. Since the GNSS signals are typically weak, they become vulnerable to jamming. In barrage jamming, the jammer transmits a continuous stream of noise over the frequencies used by the GNSS satellites. This noise raises the noise floor, drowning out legitimate satellite signals. As a result, the UAV GNSS receiver struggles to lock on to the satellite signals, resulting in degraded positional accuracy or even a complete loss of GNSS functionality.

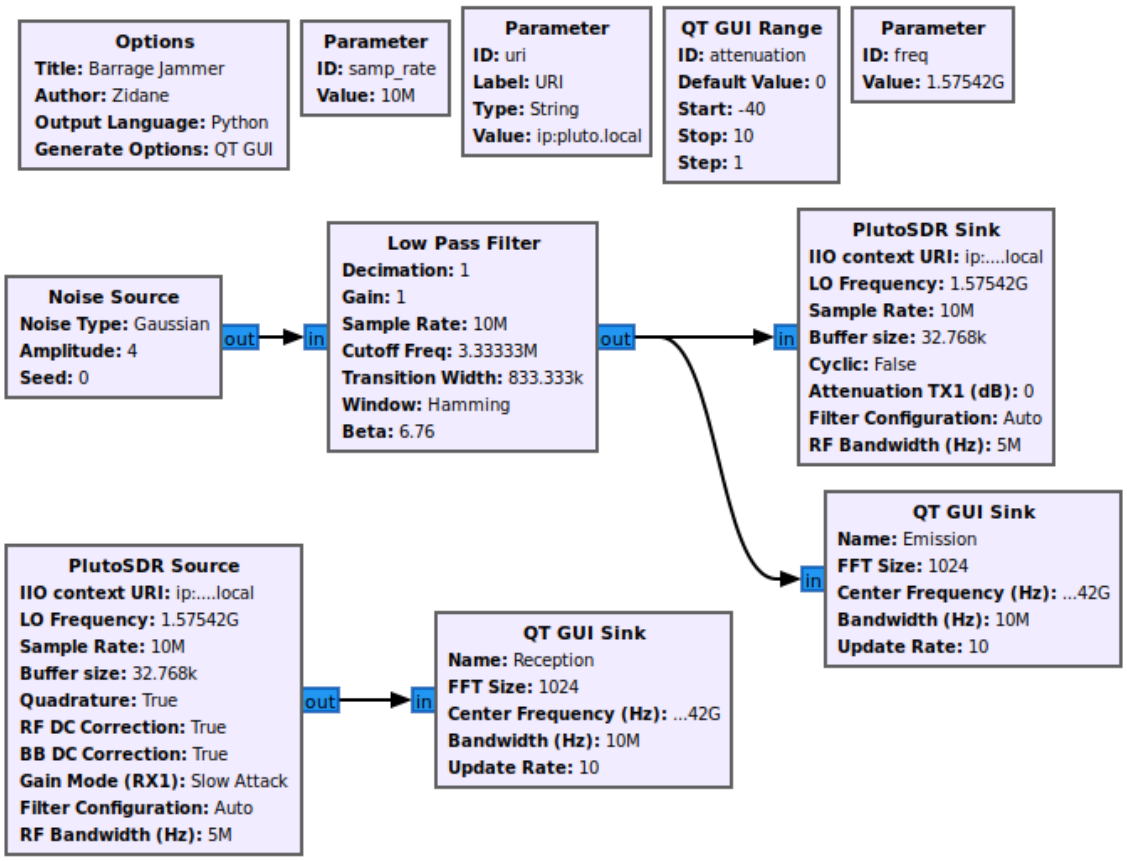


Figure 3.8: GNSS Barrage Jamming Script using GNU Radio.

The first block is a Noise Source that generates Gaussian noise. White noise is ideal for creating wideband interference due to its uniform power distribution across the bandwidth. An amplitude of 4 (unitless) ensures a sufficiently strong noise signal, and above this value, the PlutoSDR saturates. The seed value of 0 allows the random number generator to produce noise in a potentially non-deterministic manner. If a specific and repeatable noise pattern is desired for consistent results across different runs, a fixed seed value other than 0 should be used.

The Low Pass Filter (LPF) in the barrage jammer system is crucial for filtering the noise signal before transmission, ensuring that only the desired frequency range is transmitted for effective and targeted jamming. The LPF limits the bandwidth of the Gaussian noise to a cutoff frequency of approximately 3.(3) MHz, with a transition width of 833.(3) kHz. The LPF uses a Hamming window to reduce spectral leakage, where signal energy spreads to neighboring frequencies. This configuration ensures the noise signal occupies a well-defined frequency range, explicitly targeting the GPS L1 band centered at 1.57542 GHz. The filter parameters, including a sample rate (SR) of 10 MHz and a gain of 1, are chosen to maintain signal integrity and synchronization with the system, optimizing overall jamming performance. The cutoff frequency, set to one-third of the sample rate, balances the need for effective

jamming with practical filter design considerations, ensuring the jammer's effectiveness.

The PlutoSDR Source block configures the SDR to receive signals centered at 1.57542 GHz with a sample rate of 10 MHz, incorporating DC offset correction and automatic gain control. The PlutoSDR Sink block transmits the filtered noise signal at the GPS L1 frequency of 1.57542 GHz with the same sample rate, ensuring effective jamming.

The QT GUI Sink Blocks offer real-time visualization of the transmitted and received signals, displaying their frequency domain representations with an FFT size of 1024 and a bandwidth of 10 MHz.

3.2.1.B GNSS BPSK Jamming

Protocol-aware jamming is a more sophisticated technique that can effectively disrupt signals by mimicking and overlaying the original signal. This method optimizes the power-bandwidth relationship, which is essential for efficient signal processing. In signal processing, the power-bandwidth relationship refers to the balance between the power of the signal and the bandwidth over which that power is distributed. By optimizing this relationship, protocol-aware jamming ensures that the jammer's power is used most effectively within the specified bandwidth. This means that rather than just increasing the total power, the jammer strategically uses the available power to cover the target signal's bandwidth efficiently. Leveraging SDR capabilities enhances this process, allowing for precise control and adjustment of the jamming signal. SDRs enables the adaptation of the jamming signal to the characteristics of the target signal, thereby improving the jammer's overall effectiveness.

In GPS applications, which utilize BPSK modulation, signal integrity and accuracy are fundamental. BPSK alternates the phase of the carrier signal to encode data bits, which is vital for transmitting navigation messages and maintaining satellite clock synchronization across the designated L1 and L2 frequency bands.

When applying protocol-aware jamming to GPS with BPSK modulation, an interfering signal is generated. This signal not only overlays the original GPS signal but also mimics its modulation characteristics. This method deceives the GPS receiver into interpreting the interfering signal as genuine, compromising the accuracy of positioning information. This demonstrates the effectiveness of protocol-aware jamming when it is precisely synchronized with BPSK modulation in GPS systems.

The corresponding GNU Radio script is shown in Figure 3.9.

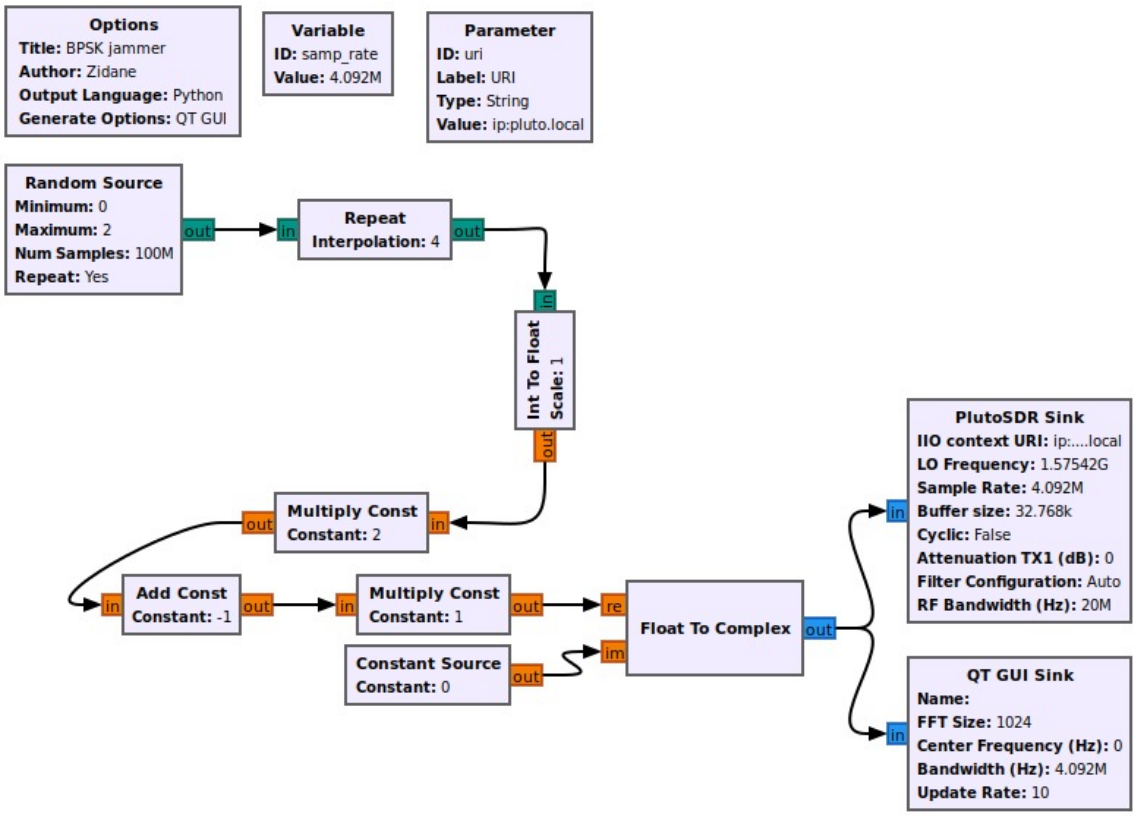


Figure 3.9: GPS BPSK Jamming Script using GNU Radio.

The script starts with a Random Source block, which generates a continuous sequence of random bits. It has a 100 M sample period to ensure sufficient data flow for jamming effectiveness. The choice of an interpolation factor of 4 matches the 4.092 MHz sampling rate of the PlutoSDR sink. This upsampling is required to match the data rate required for transmission.

The Int to Float block converts the integer values from the random source to floating point values while preserving their scale. The Multiply Const block then multiplies the float values by a factor of 2, which is used to prepare the signal for modulation and transmission. The Add Const block centers the data around 0 by subtracting 1 from each sample, which is required for proper BPSK modulation (mapping 0 to -1 and 1 to +1). The Float to Complex block then converts these values into complex numbers necessary for In-phase (I) and Quadrature-phase (Q) transmission in SDR systems. The Constant Source block generates a continuous stream of zeros for the imaginary component, maintaining the real signal.

Finally, the PlutoSDR Sink block transmits the processed signal via the PlutoSDR device. Configured for the GPS L1 center frequency, it operates with a 4.092 MHz sampling rate and a 20 MHz RF bandwidth. Additional parameters include a buffer size of 32.768 ksamples, non-cyclic transmission, and a TX1 attenuation of 0 dB.

This setup effectively implements a BPSK jammer, generating a random signal, modulating it using BPSK, and transmitting it on the GPS L1 frequency using a PlutoSDR device.

3.2.1.C GNSS Spoofing

A spoofing attack was conducted using a software-defined GPS signal simulator to manipulate the position and timing of a target receiver. The GPS-SDR-SIM [85] was selected for this purpose, as it generates realistic GPS baseband signal streams that can be converted into RF signals using SDRs. This simulator enables controlled manipulation and spoofing of GPS signals, making it ideal for experimental purposes.

The GPS-SDR-SIM supports user-defined motion trajectories, allowing for both static and dynamic motion models. These trajectories can be specified using various input sources, such as CSV files containing Earth-Centered Earth-Fixed (ECEF) user positions, NMEA GGA streams (data format commonly used to carry GPS fix information), or latitude, longitude, and altitude coordinates in supported units. This research used the ADALM-Pluto to broadcast the simulated GPS signals. To accurately simulate motion, the user motion sampling rate was set to 10 Hz, meaning the system updates the position 10 times per second. This rate is sufficient to track most dynamic movements without overwhelming the hardware's processing capabilities, making it particularly valuable for precise motion tracking in dynamic simulations [86].

To generate the GPS signal, the simulator requires GPS broadcast ephemeris files, which contain the data required to calculate pseudoranges and Doppler shifts for each visible satellite. These calculations are essential for producing the digitized in-phase (I) and quadrature-phase (Q) samples that form the core of every simulated GPS signal. This approach creates a realistic spoofed GPS signal, enabling controlled GPS spoofing vulnerability tests to be carried out.

The process of generating a spoofed GPS signal was conducted using the GPS-SDR-SIM software on an Ubuntu system. For details on the installation and execution of the simulator, refer to Appendix A.

3.2.2 Jamming Implementation

To implement jamming in the 2.4 GHz band, two techniques were used: barrage jamming and sweep jamming.

3.2.2.A RC and Video Barrage Jamming

This script adopts the same logic as described in Section 3.2.1.A, with specific adjustments for RC and video barrage jamming. In this case, we set the sample rate to 20 MHz to cover the maximum 2.4 GHz band, under the limitations of the SDR. Additionally, we set the noise amplitude to 2 to achieve

a stronger jamming signal without causing saturation. The Adalm-Pluto has a maximum bandwidth of 20 MHz, and setting a sample rate above twice this value would be ineffective. In addition to modifying the sample rate, the frequency must also be changed to the center frequency of the 2.4 GHz band, which is 2.44 GHz.

These modifications proved insufficient since the 2.4 GHz band is considerably wide, approximately 80 MHz. The Python code generated from GNU Radio needed further adjustments to cover the entire band. For this effect, it was necessary to modify the generated Python code using the ADALM-PLUTO API.

Sequential Frequency Increment Jamming Script: Both the original and modified scripts are available in the GitHub repository at the following link: `https://github.com/Younes619/UAV-Jamming-Scrips`. The files are named Fixed Frequency Barrage Jamming and Sequential Frequency Increment Barrage Jamming. The changes made between these versions are detailed and explained below:

1. **Initialization Method Modification:**
   - Add a frequency parameter to the `__init__` method.
   - Store the frequency as a class attribute.
   - Update the frequency setting for `iio_pluto_sink_0` to use the passed parameter during initialization.
2. **Frequency Control in the Main Method:**
   - Define new variables:
     - `start_frequency` with a value of 2.405 GHz.
     - `stop_frequency` with a value of 2.475 GHz.
     - `step` with a value of 15 MHz.
     - `bandwidth` with a value of 20 MHz to size the window of the plot.
3. **Creating the Update Function:**
   - Implement a function named `update_frequency`.
   - This function updates the frequency at regular intervals by incrementing the start frequency by the step value.
   - The function resets the frequency to the start frequency once the stop frequency is reached.

4. **Setting Up a Timer:**

    - Configure a timer to call the `update_frequency` function at regular intervals, set to 5 seconds based on empirical observations for optimal performance.

5. **Signal Handling:**

    - Add a signal handler to cleanly stop the top block and exit the application when a termination signal is received.

By incorporating these modifications, the script substantially improves covering the 2.4 GHz band effectively. The new functionality allows for dynamic frequency updates at regular intervals, enhancing the script's overall performance and adaptability.

Random Frequency Selection Jamming Script: Since the 2.4 GHz band employs FHSS technology, drones utilize a technique where their operating frequency changes randomly. This needs a new approach to jamming strategies. In the previous section, several modifications were made to scan the entire 2.4 GHz spectrum sequentially. Building on the changes introduced in Sequential Frequency Increment Barrage Jamming, additional adjustments were implemented to cover the entire band, but with random frequency hops, leading to the development of Random Frequency Selecting Barrage Jamming.

Firstly, a list of center frequencies,[2.41, 2.425, 2.44, 2.455, 2.47] GHz, was introduced in the 'main' function instead of defining start, step, and stop frequencies. This list represents potential frequencies at which the drone may operate.

The '$update\_frequency$' function was also modified to incorporate the 'random' module. Instead of incrementing frequencies sequentially, this function now selects a random value from the list of center frequencies. This adjustment enables the jamming system to adapt to the unpredictable frequency changes of the drone.

These changes aim to enhance the effectiveness of the jamming strategy against drones employing FHSS technology by dynamically adjusting the jamming signal to match the varying frequencies used by the drone.

3.2.2.B RC and Video Sweep Jamming

Another measure that was implemented during the jamming operation was sweep jamming. This technique focuses the jamming signal on a narrow frequency band at a time, in contrast to spreading the interference over a wide range as in barrage jamming. Concentrating the signal in smaller bandwidth channels focuses the available power into a narrower frequency band, effectively increasing the signal's strength within that specific band. This approach aims to maximize the power delivered to the targeted

frequencies, allowing for more substantial interference that can penetrate over greater distances. In essence, sweep jamming sacrifices bandwidth to concentrate power, enhancing its potential to disrupt communications over a more extended range. For this purpose, the script shown in Figure 3.10 was developed.

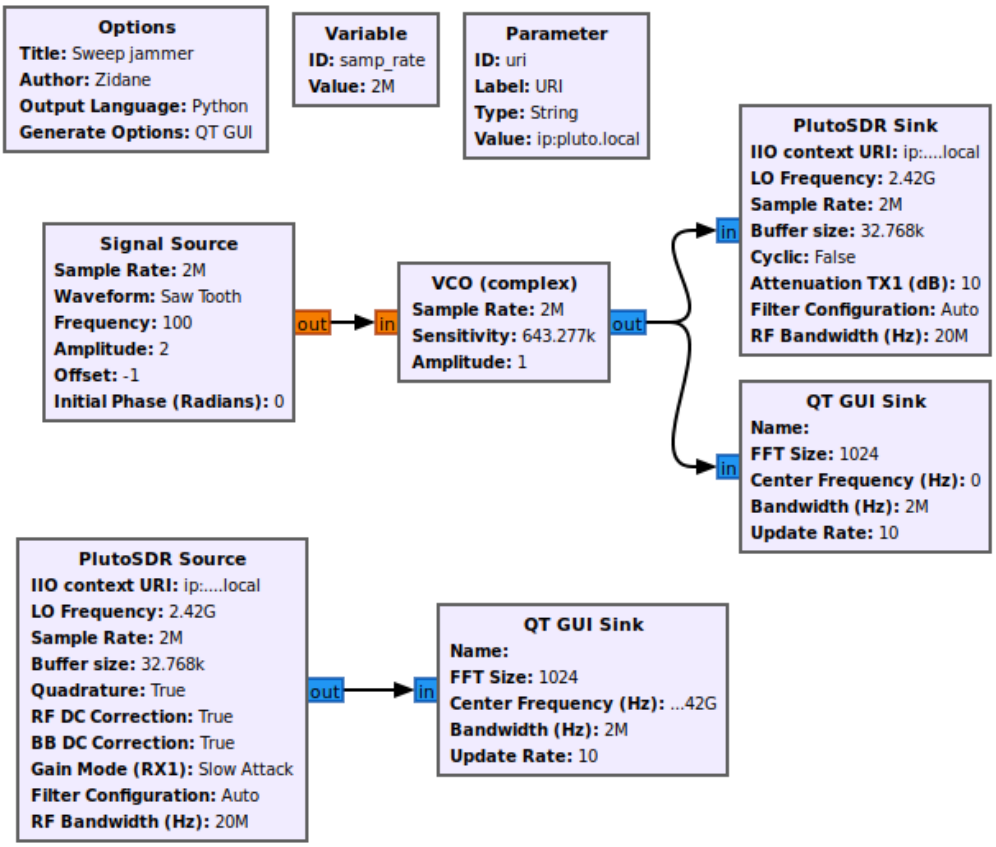


Figure 3.10: Sweep Jamming Script Script using GNU Radio.

The Signal Source block generates a sawtooth wave with a frequency of 100 Hz, an amplitude of 2, and an offset of -1. This amplitude ensures that the modulation signal can fully drive the VCO across its desired frequency range, maximizing the sweep's effectiveness. The offset of -1 centers the waveform around zero, allowing the VCO to sweep symmetrically above and below its center frequency, thus providing a balanced modulation and covering the full target frequency range.

The VCO block generates a sinusoidal signal whose frequency is controlled by the input signal (the sawtooth wave). The sensitivity parameter, set to Δ = 643.277 kHz, controls how much the input signal shifts the output frequency, enabling a broad sweep across the frequency range and ensuring a frequency deviation. The amplitude of the VCO output is set to 1.

Finally, the transmission and reception blocks manage the signal's transmission and reception. The modulated signal is sent to the PlutoSDR Sink block, which transmits it over the air at a center frequency of 2.42 GHz. The PlutoSDR Source block receives signals within the specified bandwidth, allowing for observation and analysis.

Similar to the approach used for barrage jamming, the generated script does not guarantee full coverage of the 2.4 GHz band. Therefore, starting with the generated Python code (Fixed Frequency Sweep Jamming), modifications were necessary to ensure the entire band was covered, as was done with the barrage jamming technique. A frequency sweep feature, which was absent in the original version, was introduced. This feature is implemented using a timer that periodically updates the transmitted signal's frequency. The most significant changes applied are as follows:

1. **Adapting sample rate:**
    - The sample rate was reduced from 2 MHz to 1 MHz. Reducing the sample rate to half of its previous value decreases the maximum possible bandwidth of the signal by half. Specifically, the bandwidth is reduced from 1 MHz to 500 kHz.
2. **Frequency Control in the Main Method:**
    - New variables were defined for frequency control:
        - `start_freq` with a value of 2.405 GHz.
        - `stop_freq` with a value of 2.475 GHz.
        - `step_freq` with a value of 2 MHz.
        - `bandwidth` with a value of 20 MHz.
3. **Creating the Update Function:**
    - A function named `update_frequency` was implemented.
    - This function updates the frequency at regular intervals by incrementing the current frequency by the step value.
    - The function resets the frequency to the start frequency once the stop frequency is reached.
4. **Setting Up a Timer:**
    - A timer was configured to call the `update_frequency` function at regular intervals. The interval is set to 1 second for frequent updates.
5. **Signal Handling:**
    - A signal handler was added to cleanly stop the top block and exit the application when a termination signal (SIGINT or SIGTERM) is received.

The new script, 2.4 GHz band Sweep Jamming, adds functionality to sweep the frequency of the transmitted signal over a specified range, which is a major enhancement. This feature is implemented using additional variables and a timer-based mechanism that periodically updates the frequency. The rest of the code remains similar, with minor adjustments to parameters such as the sample rate. The new features make the script more versatile for jamming applications that require frequency flexibility.

4

Results and Discussion

Contents

4.1 GNSS Jamming and Spoofing 47

4.2 RC and Video Jamming 55

This section examines the performance and effectiveness of the developed system and discusses the results. The analysis includes a detailed examination of frequency coverage, signal quality, and limitations encountered during testing. By thoroughly evaluating these results, we aim to provide a comprehensive understanding of the neutralization techniques and identify areas for potential improvement.

4.1 GNSS Jamming and Spoofing

The practical tests for this implementation were carried out at Campo Militar de Santa Margarida, during the ARTEX24 exercise [87]. Figure 4.1 shows the physical space where these tests took place. Concerning the image description, the red marker represents where the operator and the jammer were. These two elements remained static throughout the test. The tests were carried out by increasing the drone distance from the jammer, thus moving it along the green-shaded corridor in the image. In terms of the scale of the image, each division represents a distance of 25 meters.

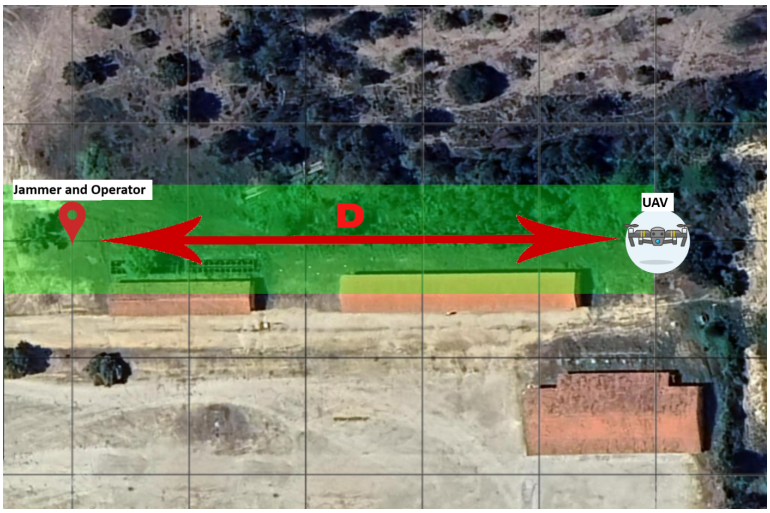


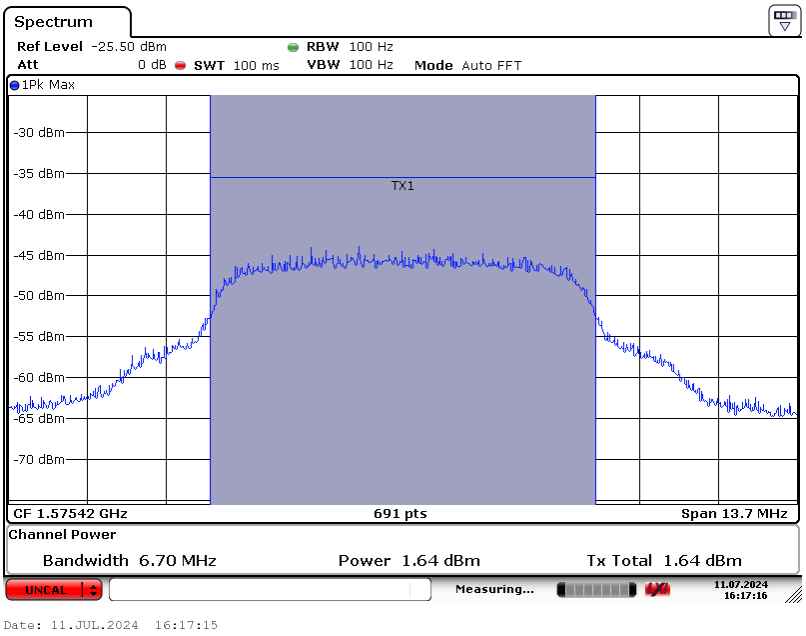
Figure 4.1: Satellite image of the physical testing space.

We used a Rohde & Schwarz FSV30 10 Hz - 30 GHz Signal / Spectrum Analyzer to assess the output signals and ensure they met expectations accurately. Additionally, the amplifier output power was measured to gauge the potential effectiveness of the attack. A 30 dB attenuator was used to protect the equipment during these measurements.

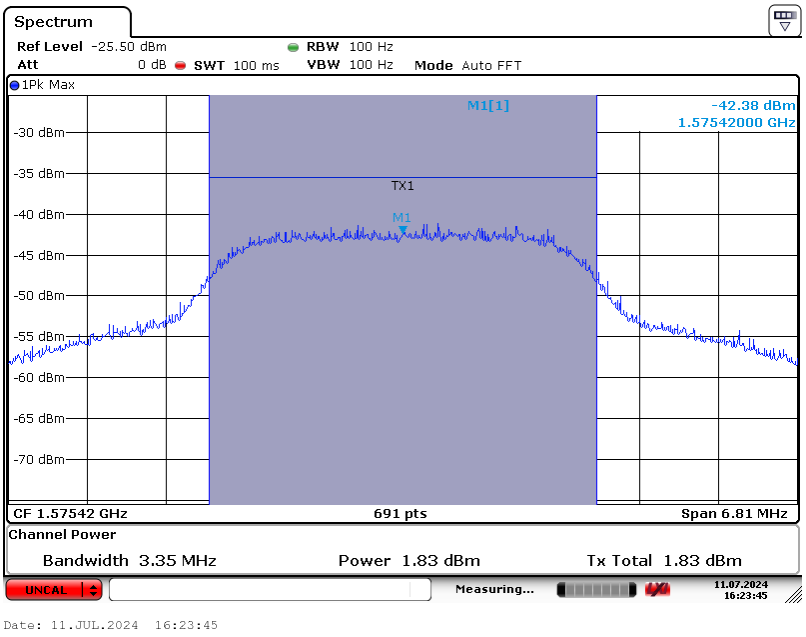
4.1.1 GNSS Barrage Jamming

For the GNSS barrage jamming tests, we explored multiple approaches by modifying the filter's cutoff frequency while keeping the rest of the script unchanged. The results of these tests are illustrated in

Figure 4.2. Specifically, in Figure 4.2(a), the cutoff frequency is set to one-third of the sample rate (SR/3), and in Figure 4.2(b), it is set to one-sixth of the sample rate (SR/6).



(a) Barrage Jamming (fc=SR/3).



(b) Barrage Jamming (fc=SR/6).

Figure 4.2: GNSS Barrage Jamming signal spectrum.

Despite the different cutoff frequencies, the implementations show minimal differences in the calculated signal output power, which is determined from the area under the blue-shaded region of the spectrum. Although the bandwidth is lower in the implementation with a cutoff frequency of SR/6, the signal output power at M1 is approximately -43 dBm, 3 dB higher than the -46 dBm observed in the SR/3 case. This shows that while the bandwidth is reduced, the power level can still be greater due to the concentration of energy within a narrower frequency range. Thus, the spectral power density differs between the two implementations, reflecting how power distribution across the signal spectrum can vary with bandwidth changes.

To estimate the true output power of the amplifier, it is necessary to add back the 30 dB attenuation. After making these adjustments, the calculated output power is 31.6 dBm.

The amplifier was also connected to a Yagi antenna with a gain of 12 dBi. To calculate the Effective Isotropic Radiated Power (EIRP) [1], we added the antenna gain to the output power. This calculation gave a EIRP of 42.6 dBm.

The interference results presented in Table 4.1 were promising. The distance (D) refers to the space between the jammer and the drone, as the tests were conducted with the jammer in a fixed position while the drone was moved away to determine the effective range of jamming. A green checkmark shows that the GNSS jammer was 100% effective, successfully preventing the drone from connecting to any satellites. Conversely, a red cross signifies that the jamming was ineffective, meaning the GNSS connection could not be inhibited.

Table 4.1: Effectiveness of GNSS barrage jamming at varying distances between the jammer and the drone. (✗) shows that jamming was ineffective. (✓) shows successful jamming

Drone/Distance (D)	80 m	100 m	120 m	130 m	140 m
DJI Mini 3	✓	✓	✓	✗	✗
DJI Mini 3 Pro	✓	✓	✓	✗	✗
Autel Evo Nano+	✓	✓	✓	✓	✗
Husban Zino Mini Pro	✓	✓	✓	✓	✓
ZLL SG 108	✓	✓	✓	✓	✓

In this experiment, we assessed the impact of GNSS jamming on different drones. We set up a jammer at varying distances from the drone and measured its ability to maintain a satellite connection. The effectiveness of the jamming was evaluated by observing whether the drone could connect to satellites despite the interference.

The primary consequence of GNSS jamming for all drones is the failure of the return-to-home function. When GNSS jamming occurs, the drone loses its ability to determine its location. Without the return-to-home function, the drone can be lost. Operators usually control the drone from a considerable

[1] EIRP is the power required by an ideal isotropic antenna to achieve the same intensity (or power density) as the actual antenna at the same far location in the direction of its main lobe.

distance and often without direct visual contact, so losing the ability to know its location can be crucial for neutralizing it.

Different models of UAVs behave differently when jammed. The DJI and Husban models both experienced a loss of connection, but all the drones remained in the state commanded by the last signal without making any further corrections. However, regarding safety, the Autel and ZLL models reacted better to the loss of connection by immediately performing a landing procedure. This safety feature causes the drone to immediately land and return to the ground in the event of a loss of communication with the controller, thus avoiding scenarios in which the drone goes into uncontrolled flight.

4.1.2 GNSS BPSK Jamming

The spectrum of the transmitted signal for the BPSK jamming implementation is illustrated in figure 4.3.

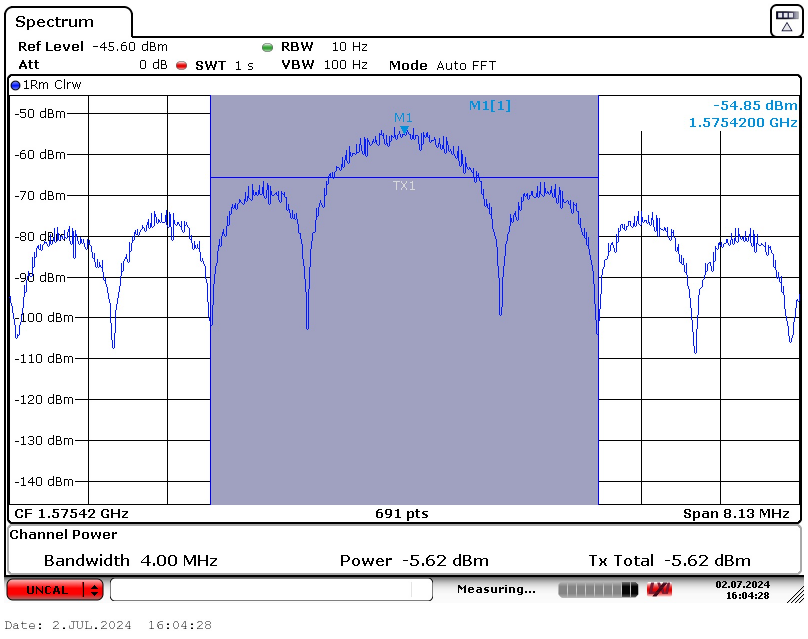


Figure 4.3: GNSS BPSK Jamming signal spectrum.

Analyzing the image, we see that the signal is as theoretically predicted, exhibiting the expected characteristics. The output power measured from the spectrum analyzer is approximately -5.6 dBm. However, to determine the total EIRP, we must take into account the amplifier gain (30 dB) and the antenna gain (12 dBi). Applying the amplifier gain, offset correction, and antenna gain, we arrive at a final EIRP of approximately 36.4 dBm.

Table 4.2 presents the results obtained from jamming using BPSK modulation. Like the barrage jamming tests, the distance (D) represents the space between the jammer and the UAV, determining the distance at which jamming is no longer effective. A green checkmark shows that jamming was

successful at that distance, while a red ”X” signifies the point at which jamming ceases to be effective.

Table 4.2: Effectiveness of BPSK barrage jamming at varying distances between the jammer and the drone. (✗) shows that jamming was ineffective. (✓) shows successful jamming

Drone/Distance (D)	80 m	100 m	120 m	130 m	140 m
DJI Mini 3	✓	✓	✓	✓	✗
DJI Mini 3 Pro	✓	✓	✓	✓	✗
Autel Evo Nano+	✓	✓	✓	✓	✗
Husban Zino Mini Pro	✓	✓	✓	✓	✓
ZLL SG 108	✓	✓	✓	✓	✓

BPSK modulation proves to be slightly more efficient than barrage jamming, for GNSS jamming, particularly over longer distances and with lower power. The superior effectiveness of BPSK jamming can be attributed to several key factors: power density, processing gain, and modulation similarity with the GNSS signal.

BPSK signals concentrate their energy within a narrow frequency band, typically matching the frequency band used by GNSS systems like GPS. This results is a higher power density, meaning more power is directed to the targeted frequency range. Power density is crucial in jamming because it determines how much power is available to interfere with a signal within a specific bandwidth. Since BPSK jamming confines its energy to the same frequency band as the GNSS signal (L1 at 1.57542 GHz), it becomes more effective in disrupting the GNSS receiver. At longer distances, where signal power naturally diminishes due to path loss, having a higher power density allows the BPSK signal to maintain its effectiveness.

Another factor is the concept of processing gain, which is intrinsic to GNSS systems. GNSS systems, including GPS, use spread spectrum techniques to distribute their signal energy over a broader bandwidth. This technique provides resilience against interference and noise, and it enhances the receiver's ability to detect weak signals through processing gain. BPSK modulation, by operating within the same frequency band and using similar signal characteristics as GNSS, effectively reduces the processing gain of the GNSS receiver.

The modulation similarity between the jamming signal and the GNSS signal is another factor that explains the better performance of BPSK jamming. GNSS signals, like those from GPS satellites, use BPSK modulation to encode data. When the jamming signal also uses BPSK modulation, it closely mimics the legitimate GNSS signal. This similarity creates significant problems for the receiver because it uses correlation techniques to detect and process the satellite signals. The receiver expects to see signals with specific modulation patterns, such as BPSK, and when a jamming signal uses the same modulation, the receiver cannot easily differentiate between the real satellite signal and the jammer signal.

4.1.3 GNSS Spoofing

All the implementations were tested using an Android device, which acted as the receiver for the spoofed GNSS signals. By programming the SDR to transmit false geospatial data, we were able to simulate a spoofing attack. The Android device, using the GPS Test app [88], received these spoofed signals, and we confirmed that the device displayed the false coordinates, thus validating the effectiveness of the spoofing function.

- **Static spoofing to a random position**

  The first approach was in its most basic form, spoofing to a location far from the real one. The choice of location was completely random, so the capital of Japan was chosen, as we can see in Figure 4.4. This implementation has no direct effect on the drone's behavior, but its main objective is to mislead the operator, using the principle of deception so that the operator believes that the drone is in a different location from the real one.

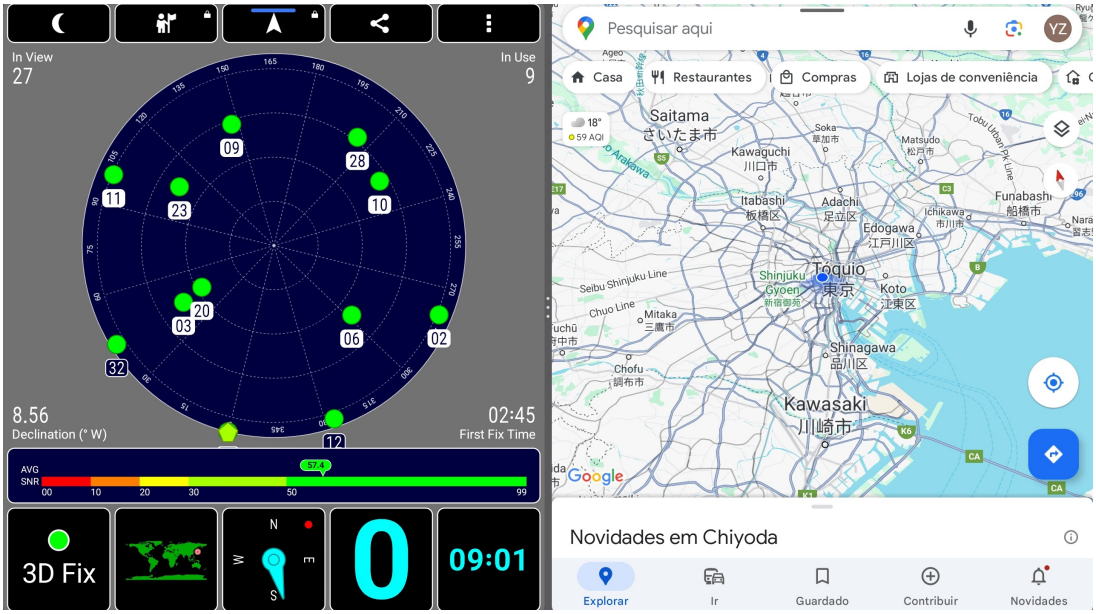


Figure 4.4: Static Spoofing to Tokyo, Japan.

- **Static spoofing to a NFZ**

  Since the previous approach does not directly cause changes in the drone's behavior, but rather serves as a method of deception, the idea of using the NFZ concept for this purpose emerged.

  As previously described, instead of spoofing to a random location, the coordinates were selected in a weighted manner by checking a location where overflight is not allowed. The chosen location was Francisco Sá Carneiro Airport in Porto, Portugal's second largest airport.

This method only has additional effects for DJI drones, as the others cannot distinguish a NFZ from an area that is allowed to fly over. DJI drones, when spoofed to an NFZ, will automatically initiate several actions, including: on-screen warnings, Figure 4.5, where the drone must land as ”you are not allowed to fly” there; and a 100 second countdown to an automatic forced landing. Once the drone has landed, either by the pilot or at the end of the countdown, it will never take off again and remain where it landed until it is collected.

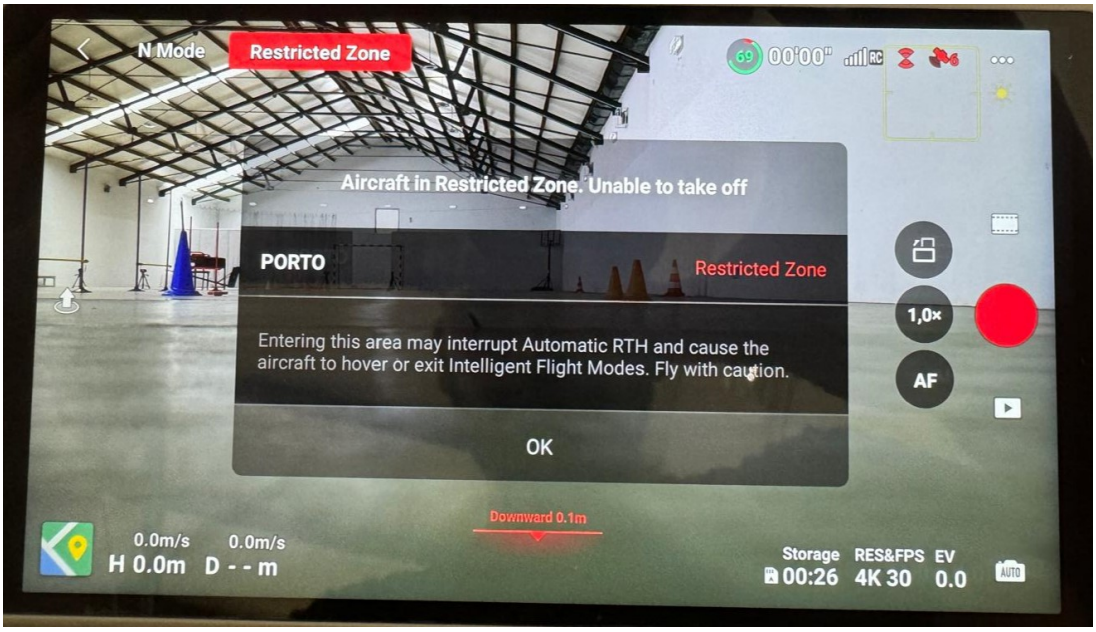


Figure 4.5: Spoofing into a No-Fly Zone (Controller Display). This image was captured during the test conducted in a gymnasium.

- **Dynamic spoofing with altitude variation**

The static aspect of spoofing turns out to be limited, as it does not directly affect the drone’s flight. This is where the concept of dynamic spoofing comes in. This method is more complex than the previous one, as it requires the creation of a CSV file.

The CSV file structure consisted of a set of 3000 points, each defined by latitude, longitude, and height. To generate the 3000 points, a Python code was developed, listed in Appedix B, so that the points were generated equidistantly around a central coordinate, within a radius of 100 meters.

Once the coordinates were obtained, the main modification was to introduce altitude variations into the CSV file. These height variations confuse the drone by giving it false heights so that it reacts to these variations, thus increasing the chances of hitting an obstacle or even losing control.

Regarding the results obtained, all the drones were susceptible to the dynamic spoofing attack,

though their responses varied in severity. DJI drones, known for their advanced GPS systems and stabilization technologies, demonstrated significantly more stability in handling altitude variations. Although they registered the false altitude data, their sophisticated flight control systems were better able to compensate for the inconsistent height information, resulting in fewer noticeable deviations in flight behaviour. In contrast, other drones exhibited more erratic behaviour, with some losing altitude control more easily, such as ZLL SG 108 and Autel Evo Nano+, reacting abruptly to the spoofed height changes. This increased the likelihood of collisions or loss of control, particularly in confined environments. Overall, the dynamic spoofing technique proved effective across all tested drones, though its impact was more pronounced on non-DJI models due to less robust control algorithms and GPS spoofing defenses.

- **Dynamic spoofing to an NFZ with altitude set to zero**

Building on the results of dynamic altitude variation spoofing, a new approach was tested where the drone's altitude was forced to zero throughout the spoofing technique. This method was designed to more drastically disrupt the drone's GNSS receiver by tricking it into continuously interpreting its altitude as zero, regardless of its actual position. By eliminating gradual altitude changes and fixing the altitude at zero, the drone's flight behaviour became more destabilized. This often led to premature landing attempts, incorrect altitude corrections, and an increased risk of collisions or loss of control. The simplified spoofing signal resulted in a more immediate and pronounced response from the drone, testing the limits of its navigation system under sustained and extreme spoofing conditions.

The GNSS system provides drones with accurate positioning and altitude data, which is particularly reliable in open areas where satellite signals are strong. However, this also makes spoofing more challenging, as real signals are often stronger. To overcome this, a two-step process was implemented: first, the legitimate GNSS signal was jammed to block satellite data, followed by spoofing to trick the drone into accepting the false signals as real. By forcing the drone to believe it was at ground level while airborne, the system induced significant instability, causing the drone to deviate from its route and struggle with altitude corrections, leading to a faster loss of control.

It should be noted that only DJI drones in the test group could detect NFZ. The spoofing tests were carried out by generating fake GNSS points centred on the runway of Francisco Sá Carneiro Airport, an NFZ, to evaluate the effectiveness of the attack.

In conclusion, this method successfully integrated various spoofing strategies into a cohesive approach that maximized disruption. The results of this dynamic spoofing technique, which severely impacted the stability and control of the drones, are presented in Table 4.3.

Table 4.3: Results obtained for Dynamic Spoofing

	Drone Behaviour (hovering)	Drone Behaviour (in motion)	Automatic landing
DJI Mini 3	Stable, but may wobble a little	Great instability, can lose control and go off course	Spoof an NFZ, start countdown to an automatic landing
DJI Mini 3 Pro	Stable, but may wobble a little	Great instability, can lose control and go off course	Spoof an NFZ, start countdown to an automatic landing
Autel Evo Nano+	Total instability, lost its way, climbed to a high, landed uncontrolled		Yes
Husban Zino Mini Pro	Practically stable, small fluctuations	Instability, losing control, and moving in transverse plane until hitting an obstacle	No
ZLL SG 108	Total instability, moving in a downward trajectory until landing		Yes

The results in Table 4.3 highlights the varying responses to dynamic spoofing across different models. The DJI Mini 3 and Mini 3 Pro were mostly stable while hovering, showing minor wobbling, but became significantly unstable during flight and often veered off course. They also initiated automatic landings when spoofed into an NFZ, showing robust NFZ detection. The Autel Evo Nano+ and ZLL SG 108 displayed severe instability, with the Autel drone ascending uncontrollably and landing erratically, while the ZLL drone descended rapidly before landing. The Husban Zino Mini Pro remained fairly stable while hovering but lost control during motion, drifting until it hit an obstacle. Unlike the DJI models, the Husban and ZLL drones did not initiate automatic landings, indicating weaker responses to spoofing attacks.

4.2 RC and Video Jamming

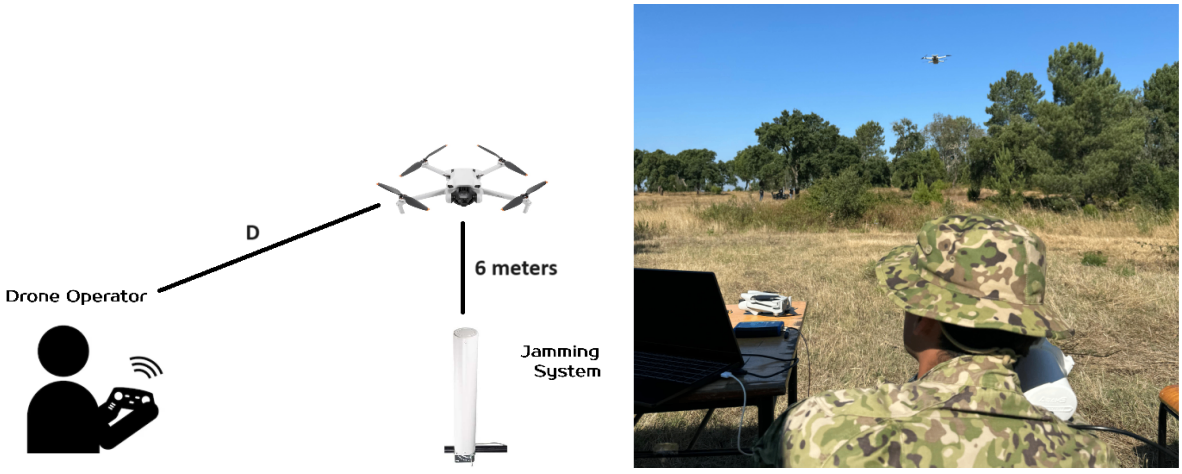
Implementations were tested to assess the effectiveness of jamming methods and identify the most suitable approach for RC and Video disruption. The tests were carried out at Campo Militar de Santa Margarida and Academia Militar de Amadora, ensuring cross-verification of results.

Figure 4.6 shows the terrain where the tests were conducted. Each division in the image corresponds to a distance of 25 meters.

(a) Test site in the Campo Militar de Sta. Margarida. **(b)** Test area at the Academia Militar Amadora.

Figure 4.6: Overview of the testing areas used for drone experiments.

To evaluate the effectiveness of the scripts used, the operator-drone distance needed to be significantly greater than the jammer-drone distance. This arrangement ensured that the jamming signals could effectively disrupt communication between the operator and the drone. The jammer was placed at 6 meters from the drone, as shown in Figure 4.7, to maintain a strong and consistent jamming signal. The choice of 6 meters was made to ensure the jammer was close enough to effectively interfere with the UAVs control systems, but not so close as to render the signal too overpowering and unrealistic for typical scenarios. By varying the operator-drone distance (denoted D), the experiment assessed how the jamming signal affected the drone's control under different conditions, with the operator distance being the key variable influencing the results.



(a) System testing set-up. **(b)** Field testing in real terrain conditions.

Figure 4.7: Illustration of the testing structure used during experiments.

4.2.1 RC and Video Barrage Jamming

The output obtained from the spectrum analysis, as illustrated in Figure 4.8, showcases the emission patterns for the two barrage jamming implementations conducted: a sequential scan of the 2.4 GHz sub-band and random sub-band selection. Both jamming modes effectively cover nearly the entire spectrum, ensuring that the jamming signals are comprehensive and efficient across the designated band.

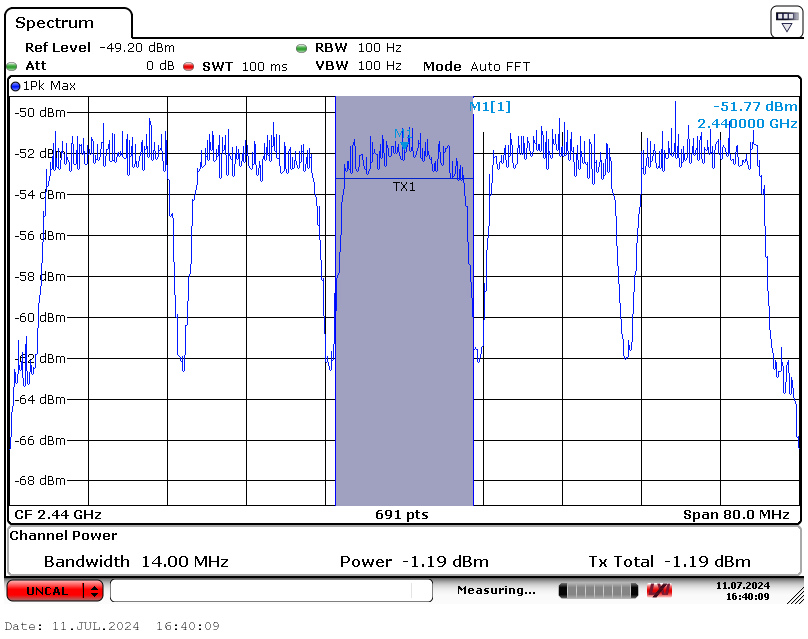


Figure 4.8: 2.4 GHz band Barrage Jamming signal spectrum (Sequential sub-band scan and random sub-band selection).

Given the characteristics of the signal, which has a bandwidth of approximately 14 MHz, it was necessary to divide the 2.4 GHz band into five distinct segments to achieve full coverage. This segmentation was required due to the limitations of the available equipment, as previously discussed. Each segment was targeted individually to ensure that the entire band was effectively jammed.

To estimate the signal strength at the output of the system architecture, specifically the antenna, we performed some calculations. The initial output signal at the amplifier was measured to be -1.2 dBm. We must consider several factors: firstly, the 30 dB attenuation introduced by the attenuator, and secondly, the gain of the Yagi antenna, which is 18 dBi. Combining these values, we obtain an EIRP of approximately 46.8 dBm. The EIRP calculation is based on the measured output at the amplifier, accounting for attenuation, offsets, and antenna gain, which is independent of the reference level used in the spectrum plot. The results are presented in Table 4.4.

The distances (D) are reference distances for which tests have been carried out, as represented in

Figure 4.7(a), the distance between the operator and the drone. The red ”X” shows that the jamming attempt was unsuccessful and did not disrupt communication between the operator and the drone. Despite possible interference, the control signals and the transmission of image or video remain fully functional. In contrast, the green checkmark signifies that jamming was completely successful, leading to a 100% disruption of communication. This means all connections between the operator and the drone, including control and video transmission, were entirely severed.

Table 4.4: Effectiveness of RC and video barrage jamming at varying distances between the operator and the drone. (✗) shows that jamming was ineffective. (✓) shows successful jamming

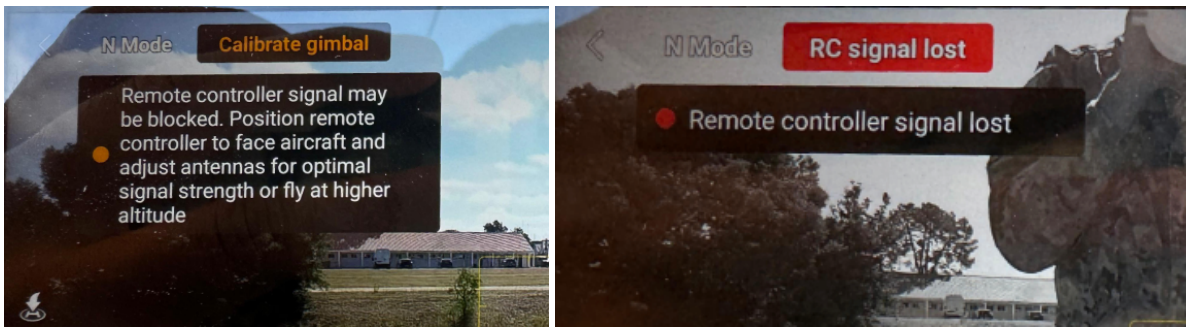
Drone/Distance (D)	30 m	50 m	80 m	100 m	120 m
DJI Mini 3	✗	✗	✗	✗	✓
DJI Mini 3 Pro	✗	✗	✗	✗	✓
Autel Evo Nano+	✗	✓	✓	✓	✓
Husban Zino Mini Pro	✗	✗	✗	✗	✗
ZLL SG 108	✓	✓	✓	✓	✓

Upon conducting a detailed analysis of each drone’s performance during the testing phases, it was observed that both DJI models exhibited similar behaviour. Therefore, the results will be described collectively for both.

During the tests, the DJI drones maintained stable operation up to a distance of approximately 40 meters from the operator, at this point, minor interference began to appear. However, this interference was negligible and did not compromise the control or functionality of the devices.

The interference gradually became more noticeable as the distance between the operator and the drone increased. At around 85 meters, this interference started to affect the connection, Figure 4.9(a), causing video transmission interruptions and introducing a slight delay in executing the manoeuvres commanded by the operator.

This interference intensified progressively until the connection was lost at approximately 120 meters. At this point, the drone stopped responding to the operator’s commands, and the video transmission froze, displaying the last frame in black and white on the remote control, along with the message ”Remote Controller signal lost”, as shown in Figure 4.9(b).



(a) Controller image with partial interference warning.

(b) Controller image with total interference warning.

Figure 4.9: Interference detection on the controller.

Another drone used in the tests was the Autel Evo Nano+. The results for this drone were even more significant, as it experienced successful jamming at much shorter distances. Effective jamming was observed starting from 50 meters, beyond which the drone stopped responding to the operator's commands, and the video feed froze on the last received frame.

Figure 4.10 shows a screenshot of the drone when it was subjected to the jamming attack.

Figure 4.10: RC and Video full Jamming.

Husban Zino Mini Pro was the only drone for which jamming did not interfere. Since the FCC ID showed that it only used the 2.4 GHz band, we didn't get any kind of reaction to the jamming. After some research, it was found that the drone in question was a "Refined" version, which was prepared to switch to 4G communication, and was possibly the only one in its weight class [79].

Finally, the ZLL SG 108 was a simple and rudimentary drone with no visual interface. For this drone, the tests were the most effective, and at 30 meters the drone became unfeasible, landing automatically.

4.2.2 RC and Video Sweep Jamming

For the sweep jamming tests, the output displayed in Figure 4.11 was obtained. In this scenario, the frequency hopping interval was reduced to 1 second. This adjustment was crucial because the bandwidth of each emitted signal is relatively narrow, measuring only 2 MHz. Given this limited bandwidth, it was necessary to sweep through the entire 2.4 GHz band at a sufficiently fast rate to ensure comprehensive coverage within a practical timeframe.

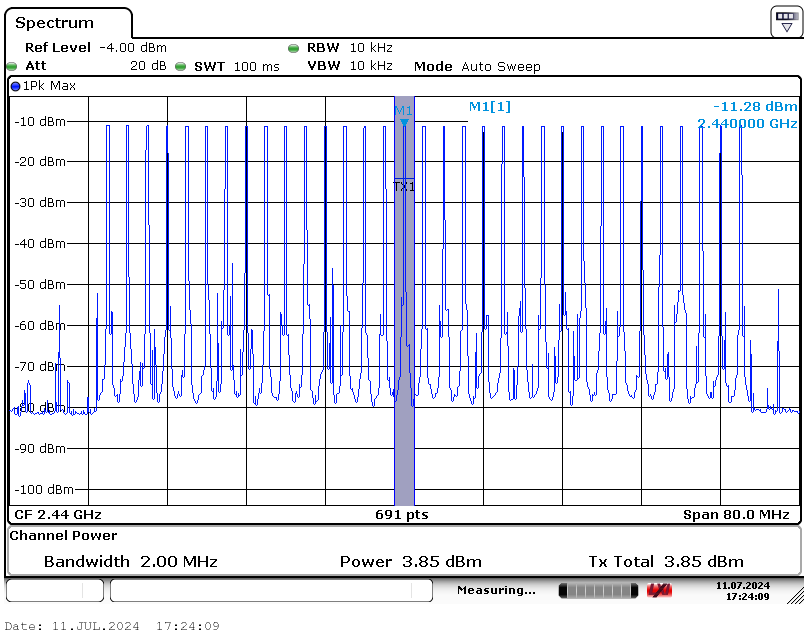


Figure 4.11: 2.4 GHz band Sweep Jamming signal spectrum.

This method effectively replicates the scanning logic in two dimensions: first, by sweeping across the entire frequency band, and second, by generating individual jamming signals at each frequency step. This dual-scanning approach allows for efficient and thorough jamming of the targeted band.

In this case, the signal was measured to be 3.85 dBm at the output of the amplifier with the attenuator in place. To calculate the EIRP at the antenna output, we accounted for the 30 dB attenuation by adding it back to the measured value. We also included the 18 dBi gain of the Yagi antenna. These adjustments yielded a final EIRP of approximately 51.9 dBm.

The results obtained from the sweep jamming tests indicate that the interference signal generated was inadequate for disrupting communications. Specifically, the signal bandwidth during sweep jamming is limited to just 2 MHz at any given moment. This bandwidth is relatively narrow compared to the extensive spectrum the UAV utilises for its communication systems. As a result, the jamming signal lacked the necessary characteristics to effectively interfere with the drone's operations across the entire frequency range it employs.

5

Conclusion and Future Work

Contents

5.1 Conclusion 63

5.2 Future Work 64

5.1 Conclusion

This thesis successfully explored and implemented jamming and spoofing techniques to interfere with drone control and communication systems, aiming to neutralize or limit UAV functionality in complex environments. By testing various drones and communication links, the study achieved comprehensive results across different environments, demonstrating the effectiveness of these counter-drone measures.

The jamming experiments focused on three core communication components: Navigation, RC, and Video links. A detailed analysis identified the frequencies and modulations used by common drones, which guided the development of the jamming system. For the navigation link, both barrage jamming and BPSK jamming were employed. BPSK jamming demonstrated achieving a slightly longer range and greater efficiency in disrupting GNSS signals compared to barrage jamming, making it a more effective method for interfering with UAV navigation systems without affecting other frequency bands.

In terms of RC and video links, barrage and sweep jamming were tested. Barrage jamming proved effective in most cases, successfully disrupting control signals and video feeds. However, the Husban Zino Mini Pro presented a notable exception, as it switched to a 4G frequency that was outside the scope of the jamming attempts. This exception highlighted the limitations of targeting only certain frequency bands and underscored the need for more comprehensive strategies, particularly for drones with multi-frequency capabilities.

The spoofing process evolved through several iterations to enhance its effectiveness. Initial static spoofing experiments successfully deceived the operator by sending false GNSS signals, tricking the drone into perceiving a false location. However, this method had little effect on the drone's real-time flight dynamics. To improve the impact on drone behavior, the NFZ concept was introduced. This method involved spoofing GNSS signals to simulate the drone entering restricted airspace, triggering automatic landings in DJI drones. While effective, this technique was limited to initiating landings without significantly influencing the drone's overall flight dynamics.

To overcome these limitations, dynamic spoofing techniques were developed. Tests such as dynamic altitude variation, spoofing into an NFZ, and combining dynamic spoofing with altitude manipulation were conducted. The most effective approach combined dynamic spoofing with the NFZ concept, setting the drone's altitude to zero. This method directly interfered with the UAV navigation system, leading to erratic flight behavior, forced landings, and collisions. Among the various techniques tested, this combination proved to be the most comprehensive and impactful.

Initial testing was conducted in a controlled environment, but further outdoor field tests introduced challenges in overpowering real GNSS signals. To address this issue, a two-step process was adopted: first, jamming the legitimate GNSS signals and next broadcasting spoofed signals. This sequence allowed the drone to accept the false location data as authentic, successfully disrupting its navigation and behavior.

The findings of this thesis demonstrate the effectiveness of SDR-based jamming and spoofing techniques in countering UAV threats. Both methods were successful in neutralizing drone control and navigation, with BPSK jamming, barrage jamming and dynamic spoofing yielding the most effective results. These outcomes provide practical insights for developing low-cost, adaptable anti-drone systems capable of protecting critical infrastructure and sensitive areas from unauthorized UAV activity.

In conclusion, this study has laid the foundation for further advancements in electronic countermeasures for drones. It offers a robust framework for defending against unauthorized UAVs in both civilian and military environments.

5.2 Future Work

Future research should focus on improving the reliability of jamming and spoofing in outdoor environments, particularly by enhancing the ability to consistently overpower real GNSS signals. This may involve stronger transmission power, advanced antennas, or more sophisticated signal modulation. Additionally, with drones increasingly operating on 4G/5G frequencies, developing multi-frequency jamming systems capable of disrupting communications beyond the traditional 2.4 GHz and 5.8 GHz bands will be essential.

A promising direction is the development of adaptive and cognitive jamming systems. Cognitive jamming, for example, involves the jammer analyzing the drone's signal to determine its modulation and parameters and then synthesizing a jamming signal that closely resembles the original in real-time. This could enable more precise countermeasures based on environmental factors and drone behavior. Integrating these jamming systems with physical interception technologies or advanced neutralization techniques could further enhance defenses against evolving UAV threats. Extensive real-world testing across diverse environments will be essential to validate these approaches.

Bibliography

[1] D. Zmyslowski, P. Skokowski, and J. Kelner, “Anti-drone Sensors, Effectors, and Systems-A Concise Overview.” *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, vol. 17, no. 2, p. 455–461, 2023.

[2] European Union Aviation Safety Agency. (2024) Easy Access Rules for Unmanned Aircraft Systems (Regulation (EU) 2019/947 and Regulation (EU) 2019/945). [Online]. Available: https://www.easa.europa.eu/document-library/easy-access-rules/easy-access-rules-unmanned-aircraft-systems-regulationeu

[3] G. Abro, S. Zulkifli, R. Masood, V. Asirvadam, and A. Laouiti, “Comprehensive Review of UAV Detection, Security, and Communication Advancements to Prevent Threats,” *Drones*, vol. 6, no. 10, p. 284, 2022.

[4] S. Park, H. T. Kim, S. Lee, H. Joo, and H. Kim, “Survey on Anti-Drone systems: Components, Designs, and Challenges,” *IEEE Access*, vol. 9, p. 42635–42659, 2021.

[5] D. J. Rozenbeek, “Evaluation of Drone Neutralization Methods using Radio Jamming and Spoofing Techniques,” Ph.D. dissertation, KTH Royal Institute of Technology, 2020. [Online]. Available: https://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-279557

[6] M. A. Jasim, H. Shakhatreh, N. Siasi, A. H. Sawalmeh, A. Aldalbahi, and A. Al-Fuqaha, “A Survey on Spectrum Management for Unmanned Aerial Vehicles (UAVs),” *IEEE Access*, vol. 10, p. 11443–11499, 2022.

[7] S. I. Han, “Survey on UAV Deployment and Trajectory in Wireless Communication Networks: Applications and Challenges,” *Information*, vol. 13, no. 8, p. 389, 2022.

[8] E. Danel, “An Introduction to Wi-Fi 6E Spectrum in the 6 GHz band – Wi-Fi’s First Unlicensed Spectrum Boost in 20 Years,” 2020, accessed: 2023-12-25. [Online]. Available: https://www.litepoint.com/blog/an-introduction-to-wi-fi-6e-spectrum/

[9] D. Lin, P. Zuo, T. Peng, R. Qian, and W. Wang, “Energy-Efficient UAV-Based IoT Communications With WiFi Suppression in 5 GHz ISM Bands,” *IEEE Transactions on Vehicular Technology*, vol. 72, no. 2, p. 2024–2039, 2023.

[10] Y. M. Hyasat, D. Abualnadi, and Y. S. Faouri, “Two Elements Ultra Wideband MIMO Antenna for 5G Communications, WiFi-5 and WiFi-6 Applications,” in *2022 14th International Conference on Communications (COMM)*. IEEE, 2022.

[11] “ANACOM creates conditions for consistent and competitive development of 5G in Portugal,” 11 2019, accessed: 2023-12-25. [Online]. Available: https://www.anacom.pt/render.jsp?contentId=1493002

[12] “Divulgação de resultados das fases de licitação do leilão,” 10 2021, accessed: 2023-12-25. [Online]. Available: https://www.anacom.pt/render.jsp?contentId=1709327

[13] ANACOM, “Autoridade Nacional de Comunicações,” 2015, accessed: 2023-12-23. [Online]. Available: https://www.anacom.pt/render.jsp?categoryId=383094

[14] GSMArena, “Network coverage in Portugal - 2G/3G/4G/5G mobile networks,” 2023, accessed: 2023-12-23. [Online]. Available: https://www.gsmarena.com/network-bands.php3?sCountry=PORTUGAL

[15] FrequencyCheck, “Wireless Frequency Band Information by Country,” 2023, accessed: 2023-12-20. [Online]. Available: https://www.frequencycheck.com/countries/portugal

[16] H. Bastion, “LTE Frequency Bands - HB Radiofrequency,” 2023, accessed: 2023-12-20. [Online]. Available: https://halberdbastion.com/technology/cellular/4g-lte/lte-frequency-bands

[17] S. Tracker, “Frequency spectrum database,” 2023, accessed: 2023-12-23. [Online]. Available: https://www.spectrum-tracker.com/Portugal

[18] R. K. Mistri, S. K. Mahto, and R. Sinha, “Dual band 8×8 MIMO antenna system for DCS 1800 and 5G mobile applications,” *International Journal of Communication Systems*, vol. 36, no. 3, 2022.

[19] “EMF-Portal — Home,” https://www.emf-portal.org/en/emf-source/354, accessed: 2023-12-19.

[20] M. Kanagasabai, S. Shanmuganathan, M. G. N. Alsath, and J. Govindan, “Novel Low Profile Beam Switchable 5G Sub-6 GHz E-GSM Antenna for Vehicular Communication,” *International Journal of Electronics*, p. 1–18, 2023.

[21] F. Slimeni and T. Dalleji, “RF-based mini-Drone Detection, Identification Jamming in No Fly Zones using Software Defined Radio,” in *Proceedings of the XYZ Conference on Advanced Technologies*. Research Square Platform LLC, 2022.

[22] i. F. B. F. Ir. Gerton de Goeij (Strict), ir. Eildert H. van Dijken (Strict), “Research into the Radio Interference Risks of Drones,” 2016. [Online]. Available: https://www.rdi.nl/documenten/rapporten/2017/december/6/rapport-research-into-the-radio-interference-risks-of-drones

[23] D. Mototolea, “A Study On The Actual And Upcoming Drone Communication Systems,” in *2019 International Symposium on Signals, Circuits and Systems (ISSCS)*, 2019, pp. 1–4.

[24] A. Bello, “Radio Frequency Toolbox for Drone Detection and Classification,” 2019. [Online]. Available: https://digitalcommons.odu.edu/ece_etds/160/

[25] M. Tang, “Drone Detection and Classification with Machine Learning,” 2023.

[26] D. Torrieri, *Direct-Sequence Systems*. Springer International Publishing, 2021, p. 81–150.

[27] V. Chamola, P. Kotesh, A. Agarwal, Naren, N. Gupta, and M. Guizani, “A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques,” *Ad Hoc Networks*, vol. 111, p. 102324, 2021.

[28] M. M. Alam and Y. Le Moullec, “Jamming of spread spectrum communications used in UAV remote control systems.”

[29] “IEEE 802.11 - Wikipedia,” https://en.wikipedia.org/wiki/IEEE_802.11, 2024, accessed: 2024-09-10.

[30] “WiMAX - Wikipedia,” https://en.wikipedia.org/wiki/WiMAX, 2024, accessed: 2024-09-10.

[31] “3GPP - Wikipedia,” https://en.wikipedia.org/wiki/3GPP, 2024, accessed: 2024-09-10.

[32] O. Šimon and T. Götthans, “A Survey on the Use of Deep Learning Techniques for UAV Jamming and Deception,” *Electronics*, vol. 11, no. 19, p. 3025, 2022.

[33] A. Heuchamps, “Study and Design of UAS Jamming Systems,” Master’s thesis, Faculté des Sciences appliquées, 2022, master: ingénieur civil électricien, à finalité spécialisée en ”electronic systems and devices”. [Online]. Available: http://hdl.handle.net/2268.2/14454

[34] EU Agency for the Space Programme, “What is GNSS,” https://www.euspa.europa.eu/eu-space-programme/galileo/what-gnss, accessed: 2024-08-23.

[35] J. S. Subirana, J. J. Zornoza, and M. Hernandez-Pajares, “GNSS signal,” 2011, accessed: 2024-08-23. [Online]. Available: https://gssc.esa.int/navipedia/index.php/GNSS_signal

[36] V. Rivero Díez, “Spoofing y jamming sobre los GNSS,” *INCIBE-CERT Blog*, July 2020. [Online]. Available: https://www.incibe.es/incibe-cert/blog/spoofing-y-jamming-los-gnss

[37] MDPI, “GPS Signal Plan,” *Sensors*, vol. 24, no. 17, p. 5529, 2024. [Online]. Available: https://www.mdpi.com/1424-8220/24/17/5529

[38] Navipedia, “GPS Signal Plan,” https://gssc.esa.int/navipedia/index.php/GPS_Signal_Plan, accessed: 2024-08-24.

[39] E. RF, “What is the GPS L5 Band?” https://www.everythingrf.com/community/what-is-the-gps-l5-band, accessed: 2024-08-24.

[40] J. W. Betz, “Binary offset carrier modulations for radionavigation,” *Navigation*, vol. 48, no. 4, pp. 227–246, 2001.

[41] A. D. B. A. Rahman, K. A. Ghani, N. H. H. Khamis, and A. R. M. Sidek, “Unmanned Aerial Vehicle (UAV) GPS Jamming Test by using Software Defined Radio (SDR) platform,” *Journal of Physics: Conference Series*, vol. 1793, no. 1, p. 012060, 2021.

[42] Navipedia, “GALILEO Signal Plan - E1 Band,” https://gssc.esa.int/navipedia/index.php?title=GALILEO_Signal_Plan, accessed: 2024-08-24.

[43] E. S. Lohan, “Analytical performance of CBOC-modulated Galileo E1 signal using sine BOC(1,1) receiver for mass-market applications,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 46, no. 4, pp. 1965–1976, 2010.

[44] P.-Y. Kong, “A Survey of Cyberattack Countermeasures for Unmanned Aerial Vehicles, volume = 9,” *IEEE Access*, p. 148244–148263, 2021.

[45] Airsight, “Jammers and Spoofers,” https://www.airsight.com/knowledge-hub/counter-drone-technology/jammers-and-spoofers, accessed: 2024-01-04.

[46] P. Institute, “Drone Jammers,” https://pilotinstitute.com/drone-jammers/, accessed: 2024-01-04.

[47] F. S. S. AL-Ghafri and L. Vidhya, “Unmanned aerial vehicles (UAV) jammer,” in *Inventive Communication and Computational Technologies*, G. Ranganathan, X. Fernando, and F. Shi, Eds. Singapore: Springer Nature Singapore, 2022, pp. 439–453.

[48] T. Collins, R. Getz, A. Wyglinski, and D. Pu, *Software-Defined Radio for Engineers*. Artech, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/9100100

[49] K. Parlin, M. M. Alam, and Y. Le Moullec, “Jamming of UAV remote control systems using software defined radio,” in *2018 International Conference on Military Communications and Information Systems (ICMCIS)*. IEEE, 2018.

[50] R. Ferreira, J. Gaspar, P. Sebastião, and N. Souto, “Effective GPS Jamming Techniques for UAVs Using Low-Cost SDR Platforms,” *Wireless Personal Communications*, vol. 115, no. 4, pp. 2705–2727, 2020.

[51] O. Levent, “Dronesense: A limesdr based drone detector and jammer,” 2019. [Online]. Available: https://www.rtl-sdr.com/dronesense-a-limesdr-based-drone-detector-and-jammer/

[52] J. Wang, Y. Liu, and H. Song, “Counter-Unmanned Aircraft System(s) (C-UAS): State of the Art, Challenges, and Future Trends,” *IEEE Aerospace and Electronic Systems Magazine*, vol. 36, no. 3, p. 4–29, 2021.

[53] R. Ferreira, J. Gaspar, P. Sebastião, and N. Souto, “A Software Defined Radio Based Anti-UAV Mobile System with Jamming and Spoofing Capabilities,” *Sensors*, vol. 22, no. 4, p. 1487, 2022.

[54] V. U. Castrillo, A. Manco, D. Pascarella, and G. Gigante, “A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones,” *Drones*, vol. 6, no. 3, p. 65, 2022.

[55] Wikipedia contributors, “No-fly zone,” https://en.wikipedia.org/wiki/No-fly_zone, 2024, accessed: 2024-08-27.

[56] DJI, “DJI FlySafe,” https://fly-safe.dji.com/home, 2024, accessed: 2024-08-27.

[57] D. Drones, “FIX No Fly Zone, won’t takeoff, DJI Drones,” 2024, accessed: 2024-08-28. [Online]. Available: https://www.youtube.com/watch?v=nm5YdxXKV3E

[58] J. Radivojević, A. Lebl, M. Mileusnić, A. Vujić, T. Šević, and V. Joksimović, “Multichannel Radio-jammer Development Considerations for prevention of Illicit Drone Missions,” in *9th International Scientific Conference on Defensive Technologies OTEH*, 2020, pp. 15–16. [Online]. Available: https://www.mycity-military.com/uploads2/164168_930815299_Drone%20Jammer.pdf

[59] A. AL-Hajri and S. Murugesan, “Experimental Study of Radio Frequency Drone Jamming,” in *Proceedings of the First International Conference on Aeronautical Sciences, Engineering and Technology (ICASET 2023)*. Springer Nature Singapore Pte Ltd., 2023, pp. 119–128. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-99-7775-8_12

[60] “LimeSDR - Lime Microsystems,” https://limemicro.com/products/boards/limesdr/, accessed: 2024-01-05.

[61] S. Liaquat, M. Faizan, J. N. Chattha, F. A. Butt, N. M. Mahyuddin, and I. H. Naqvi, “A framework for preventing unauthorized drone intrusions through radar detection and GPS spoofing,” *Ain Shams Engineering Journal*, vol. 15, no. 5, p. 102707, 2024.

[62] A. Novák, K. Kováčiková, B. Kandera, and A. N. Sedláčková, “Global Navigation Satellite Systems Signal Vulnerabilities in Unmanned Aerial Vehicle Operations: Impact of Affordable Software-Defined Radio,” *Drones*, vol. 8, no. 3, 2024. [Online]. Available: https://www.mdpi.com/2504-446X/8/3/109

[63] A. U. Program, “PlutoSDR,” https://wiki.analog.com/university/tools/pluto, 2024, accessed: 2024-07-09.

[64] A. D. Inc., “ADALM-PLUTO Overview,” https://www.analog.com/en/design-center/evaluation-hardware-and-software/evaluation-boards-kits/adalm-pluto.html, 2024, accessed: 2024-07-09.

[65] ——, “AD9363: RF Agile Transceiver,” Analog Devices Inc., Tech. Rep., 2024, accessed: 2024-07-09. [Online]. Available: https://www.analog.com/media/en/technical-documentation/data-sheets/AD9363.pdf

[66] M. K., “ADALM Pluto TX Output Power,” 2021, accessed: 2024-08-22. [Online]. Available: https://www.dd1us.de/Downloads/ADALM%20Pluto%20TX%20output%20power%20rev1.pdf

[67] A. Devices, “ADALM-PLUTO Transmit,” 2019, accessed: 2024-08-22. [Online]. Available: https://wiki.analog.com/university/tools/pluto/users/transmit

[68] Alibaba, “40DB WYDZ-PA-1G-3GHz-1W SBB5089+SZA2044 One-Way Microwave Power Amplifier RF Power Amplifier Module,” https://www.alibaba.com, 2024, accessed: 2024-07-10.

[69] ThanksBuyer, “SBB5089+SZA2044 One-Way Microwave Power Amplifier RF Power Amplifier Module 40DB WYDZ-PA-1G-3GHz-1W,” https://www.thanksbuyer.com, 2024, accessed: 2024-07-10.

[70] Abaks, “Abaks Yagi 18dBi Antena WiFi Exterior 5 metros Pigtail RP SMA Largo alcance,” https://www.zoominformatica.com/Abaks-Yagi-18dBi-Antena-WiFi-Exterior-5-metros-Pigtail-RP-SMA-Largo-alcance.html, 2024, accessed: 2024-07-12.

[71] Aliexpress, “Antena direcional de alto ganho para roteador, Wi-Fi, GPS, Beidou, UAV, Drone, RF Ham Radio Amplifier, 12dB, 10DB, 1.5G, 2.4G, 5.8G,” 2024, accessed: 12-07-2024. [Online]. Available: https://pt.aliexpress.com/item/1005005937911579.html?gatewayAdapt=glo2bra

[72] DJI, “DJI Mini 3 - Especificações,” 2024, accessed: 2024-07-14. [Online]. Available: https://www.dji.com/pt/mini-3/specs

[73] FCC, “DJI Mini 3 FCC ID SS3-MT3PD22,” 2024, accessed: 2024-07-14. [Online]. Available: https://fccid.io/SS3-MT3PD22

[74] DJI, “DJI Mini 3 Pro - Specs - DJI,” 2024, accessed: 2024-07-15. [Online]. Available: https://www.dji.com/pt/mini-3-pro/specs

[75] SZ DJI technology CO., LTD, “FCC ID: SS3-MT3M3VD DJI Mini 3 Pro,” 2022, accessed: 2024-07-15. [Online]. Available: https://fccid.io/SS3-MT3M3VD

[76] Autel Robotics Co., Ltd, “FCC ID: 2AGNTMDA2409A EVO Nano, EVO Nano+,” 2024, accessed: 2024-07-15. [Online]. Available: https://fccid.io/2AGNTMDA2409A

[77] L. Autel Robotics Co., “Drones EVO Nano Plus - Autel Robotics Official Store,” 2024, accessed: 2024-07-15. [Online]. Available: https://shop.autelrobotics.com/products/drones-evo-nano-plus

[78] Shenzhen Husban technology CO., LTD, “FCC ID: 2AN75-HT018F-1TX HUBSAN HT018F Remote Control,” 2021, accessed: 2024-07-15. [Online]. Available: https://fccid.io/2AN75-HT018F-1TX?utm_content=cmp-true

[79] Wheelspin Models, “Hubsan Zino Mini Pro Refined Drone - Three Batteries,” 2024, accessed: 2024-07-15. [Online]. Available: https://wheelspinmodels.co.uk/i/357894/

[80] Amazon.fr, “Moteur Sans Brosse Drone avec 2 Caméras 40KM/h MAX Résistance au Vent Classe 4 5GHz WIFI FPV Drones avec Caméra HD Quadcopter RC pour Adultes Débutants 2 Batteries 30 Minutes de Vol idea16 UAV,” 2024, accessed: 2024-07-15. [Online]. Available: https://www.amazon.fr/Cam%C3%A9ra-portable-quadcopter-d%C3%A9butants-minutes/dp/B097JRGGL8

[81] CAFAGO, “ZLRC SG108 5G WiFi FPV GPS 4K Camera RC Drone - CAFAGO,” 2024, accessed: 2024-07-15. [Online]. Available: https://www.cafago.com/en/p-rm13031-1.html

[82] G. Radio, “About - GNU Radio,” 2024, accessed: 2024-07-12. [Online]. Available: https://www.gnuradio.org/about/

[83] GNU Radio, “GNU Radio — Wikipedia, The Free Encyclopedia,” 2023, accessed: 2024-07-12. [Online]. Available: https://en.wikipedia.org/wiki/GNU_Radio

[84] Visual Estudio Code, “Visual Estudio Code,” 2024, accessed: 2024-07-12. [Online]. Available: https://code.visualstudio.com/

[85] O. Takaoka, “GPS-SDR-SIM: Software-Defined GPS Signal Simulator,” https://github.com/osqzss/gps-sdr-sim, 2024.

[86] C. Michel, K. Kelevitz, N. Houlié, B. Edwards, P. Psimoulis, Z. Su, J. Clinton, and D. Giardini, “The Potential of High[U+2010]Rate GPS for Strong Ground Motion Assessment,” *Bulletin of the Seismological Society of America*, vol. 107, no. 4, pp. 1849–1859, 2017.

[87] IDD Portugal, “Exercício ARTEX 24: Soluções Tecnológicas para o Exército Português,” https://www.iddportugal.pt/exercicio-artex-24-solucoes-tecnologicas-para-o-exercito-portugues/, 2024, accessed: 2024-10-22.

[88] Chartcross Limited, “Gps test,” 2024, accessed: 2024-09-04. [Online]. Available: https://play.google.com/store/apps/details?id=com.chartcross.gpstest&hl=pt_PT&pli=1

GPS Spoofing Signal Generation Setup

This appendix outlines the installation and execution process for generating a simulated GPS signal using the GPS-SDR-SIM software on an Ubuntu system.

Steps for Installation and Execution:

1. Clone the GPS-SDR-SIM repository:

```
$ git clone https://github.com/osqzss/gps-sdr-sim.git
```

2. Navigate to the directory and compile the code:

```
$ cd gps-sdr-sim
$ gcc gpssim.c -lm -O3 -o gps-sdr-sim
```

3. Download the latest daily broadcast ephemeris file (BRDC):
    - This can be obtained from the NASA CDDIS website.
4. Generate the simulated GPS signal file:

```
$ ./gps-sdr-sim -e brdc3540.14n -l 35.68548,139.75333,100
```

    (Here, the example uses latitude, longitude, and altitude coordinates. File-based input can also be used.)
5. Copy the generated file to the player directory:

```
$ cp gpssim.bin player/
```

6. Navigate to the player directory and run the PlutoSDR player:

```
$ cd player/
$ ./plutoplayer -t gpssim.bin
```

B

Points generator Python Code

Listing B.1: Points generator Python Code

```
from geopy import Point
from geopy.distance import geodesic
import numpy as np
import csv

# Coordenadas do centro
centro = Point(41.242550904041174, -8.679871377904485)

# Raio em metros
raio = 50

# Numero de pontos
num_pontos = 3000
```

```
14
15 # Lista para armazenar os pontos
16 pontos = []
17
18 # Gerar pontos
19 for i in range(num_pontos):
20     # Calcular o angulo
21     angulo = i * (360.0 / num_pontos)
22
23     # Calcular o novo ponto
24     ponto = geodesic(meters=raio).destination(centro, angulo)
25
26     # Adicionar o ponto a lista
27     pontos.append((ponto.latitude, ponto.longitude))
28
29 # Escrever os pontos em um arquivo CSV
30 with open('pontos.csv', 'w', newline='') as f:
31     writer = csv.writer(f)
32     writer.writerow(['Latitude', 'Longitude'])  # cabecalho
33     for ponto in pontos:
34         writer.writerow(ponto)
```