



INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Anti-UAV Mobile System with Jamming and Spoofing Capabilities
to Intercepting and Controlling Target-Drones

Renato Branco Ferreira

PhD in Information Science and Technology

Supervisor:

Doctor Pedro Joaquim Amaro Sebastião, Assistant Professor,
ISCTE – Instituto Universitário de Lisboa

Co-supervisor:

Doctor Nuno Manuel Branco Souto, Associate Professor (with Habilitation),
ISCTE – Instituto Universitário de Lisboa

December, 2022

[This page is deliberately left blank.]



TECNOLOGIAS
E ARQUITETURA

Department of Information Science and Technology

Anti-UAV Mobile System with Jamming and Spoofing Capabilities
to Intercepting and Controlling Target-Drones

Renato Branco Ferreira

PhD in Information Science and Technology

Jury:

Doctor Octavian Adrian Postolache, Associate Professor (with Habilitation), ISCTE – Instituto Universitário de Lisboa (President)

Doctor António Manuel de Jesus Pereira, Full Professor, Instituto Politécnico de Leiria

Doctor José Eduardo Charters Ribeiro da Cunha Sanguino, Assistant Professor, Instituto Superior Técnico

Doctor Francisco António Bucho Cercas, Full Professor, ISCTE - Instituto Universitário de Lisboa

Doctor Pedro Joaquim Amaro Sebastião, Assistant Professor, ISCTE – Instituto Universitário de Lisboa

December, 2022

[This page is deliberately left blank.]

Acknowledgment

First of all, I would like to acknowledge Prof. Dr. Pedro Sebastião, for all the help given in academic, professional and personal matters. This journey of thought of doing a PhD and now reaching this goal was not possible without him, without his inspiration, help, knowledge, dedication, and friendship.

To Prof. Dr. Nuno Souto, for being my co-supervisor, who throughout these years helped me to evaluate the work I developed and lead me in the right direction when necessary.

I also want to acknowledge my family for all the support given over the years. I want to thank Amanda Bueno Almeida, my partner in life, was also the person who had to deal with reading through initial drafts and listening to all my doubts or half-baked ideas. Her help was invaluable.

Thanks to my partner, friend and PhD colleague João Gaspar who allowed and helped to reconcile this journey with my professional obligations.

Finally, I would like to thank ISCTE-IUL and the Telecommunications Institute for the research support and equipment made available.

[This page is deliberately left blank.]

Resumo

Devido à difícil monitorização de Veículos Aéreos não Tripulados (VAT) e à ocorrência constante de incidentes, especialmente com voos em áreas próximas de aeroportos, áreas militares, áreas restritas, ou áreas perigosas, algumas soluções anti-VAT começaram a surgir. Tem havido forças policiais a treinar falcões para caçar VATs. O problema desta solução são as horas de treino necessárias destes animais e a possibilidade de o animal ser ferido pelas hélices do VAT. Outras soluções, tais como armas de fogo ou jammers são também utilizadas. As limitações destas soluções são enormes, uma vez que podem não garantir a segurança de vidas humanas. O VAT pode aterrar ou ser abatido de forma descontrolada, podendo ferir alguém com os estilhaços ou com a queda. O nosso projeto leva ao desenvolvimento de um sistema móvel que utiliza tecnologia jamming e spoofing. Avaliamos a utilização de plataformas de Software-Defined Radio de baixo custo (SDR) para a implementação de um jammer capaz de gerar um sinal interferente eficaz destinado ao sistema de navegação GPS. Utilizando uma plataforma programável BladeRF x40 da Nuand e o kit de ferramentas de desenvolvimento de software GNU Radio, são estudadas e avaliadas várias técnicas de interferência, considerando a eficiência espectral, eficiência energética e complexidade. Abordamos a utilização de plataformas SDR programáveis de baixo custo para a simulação de um Sistema Global de Navegação por Satélite (GNSS), mais especificamente sinais do Sistema Global de Posicionamento (GPS), a fim de transmitir sinais falsos e induzir um erro de localização no recetor GPS visado. Usando esta abordagem, foi implementado um sistema defensivo que pode desviar, ou mesmo assumir o controlo de VATs não autorizados cujo trajeto de voo depende da informação obtida pelo sistema GPS.

Primeiramente utilizamos sinais de interferência com antenas diretivas, para que apenas o VAT alvo seja afetado e não consiga obter os sinais de comunicação, parando a sua rota de voo. Após o VAT parar o seu percurso e pairar sobre a área, começamos a usar sinais de spoofing também com antenas diretivas, de modo que apenas o VAT alvo recebe os sinais “falsos”. O sistema pode redirecionar ou mesmo ganhar o controlo do veículo que sobrevoa as áreas protegidas. O sistema integra plataformas SDR de baixo custo, software de simulação de sinais GPS e utiliza um conjunto de sensores para determinar a localização não autorizada do VAT.

Podemos dividir os principais desafios desta tese em três grandes tópicos. Realizar um estudo para eleger a melhor técnica de interferência; estimar a localização do drone invasor através de um conjunto de sensores; e desviar o drone invasor para uma zona segura

previamente definida pelo utilizador. Outros objetivos são a construção de um protótipo funcional que seja móvel e adaptado a qualquer área do planeta; não depender de sistemas terceiros para o seu completo funcionamento; não depender da deteção de protocolos de comunicação específicos e poder funcionar com qualquer tipo de drone.

Para alcançar os objetivos propostos, foram realizadas diferentes fases de teste e desenvolvimento. A transferência de tecnologia começou por ser testada e desenvolvida num ambiente de laboratório sem a influência de sinais GNSS reais. Numa segunda fase, o sistema proposto foi testado num cenário controlado com a influência de sinais GNSS reais e com recetores estáticos. Finalmente, e como prova de conceito, o sistema foi testado num cenário real com UAVs em diferentes modos de voo.

Abstract

Due to the difficult monitoring of unmanned aerial vehicles (UAVs) and the constant occurrence of incidents, especially with flights in areas close to airports, military areas, restricted areas, or dangerous areas, several anti-UAV solutions have started to emerge. For example, there have been police forces training falcons to hunt UAVs. The problem with this solution is the hours of training required for these animals and the possibility of the animal being injured by the UAV's propellers. Other solutions such as firearms or jammers have also been proposed. The limitations of these solutions are huge as they may not guarantee the safety of human lives. In fact, the UAV may land or be shot down in an uncontrolled manner and may injure someone with the shrapnel from the fall. The approach proposed in this thesis relies on a mobile system that can use jamming and spoofing technology. With this aim, we evaluate the use of low-cost Software Defined Radio (SDR) platforms for the implementation of a jammer able to generate an effective interfering signal targeted at the GPS navigation system. Using this type of platforms, several interference techniques were studied and evaluated, considering the spectral efficiency, energy efficiency and complexity. Furthermore, we addressed the use of low-cost programmable SDR platforms for simulating a Global Navigation Satellite System (GNSS), more specifically Global Positioning System (GPS) signals, in order to transmit false signals and induce a location error on the targeted GPS receiver. Using this approach, a defensive system was implemented which can divert, or even take control of unauthorized UAVs whose flight path depends on the information obtained by the GPS system.

When the anti-UAV system is triggered, it starts to transmit jamming signals with directive antennas so that only the target UAV becomes unable to receive its original signals and stops its flying route. After the UAV stops flying and hovers over the area, the system estimates the location of the target drone and then uses spoofing signals also with directive antennas so that only the target UAV receives the false signals. This allows the system to redirect or even gain control of the vehicle flying over protected areas. The system integrates low-cost SDR platforms, a software GPS signal simulator and uses a set of sensors to determine the unauthorized UAV location.

We can divide the major challenges of this thesis into three major topics. Conducting the study for the best jamming technique; Estimating the location of the invading drone through a set of sensors; and diverting the invading drone to a safe zone previously defined by the user. Other objectives that were defined for this work are the construction of a functional prototype

that is mobile and can be adapted to any area of the planet; design the system so as not to depend on third party systems for its complete operation; make the system not dependent on the detection of specific communication protocols thus allowing it to work with any type of drone.

To achieve the proposed objectives, different phases of testing and development were carried out. The technology transfer started by being tested and developed in a laboratory environment without the influence of real GNSS signals. In a second phase, the proposed system was tested in a controlled scenario, with the influence of real GNSS signals and with static receivers. Finally, and as proof of concept, the system was tested in a real scenario with UAVs in different flight modes.

Contents

1. Introduction	1
1.1. Introduction to Thesis	2
1.2. Problem Statement	3
1.3. Objectives	5
1.4. Thesis Structure	11
1.5. Contribution of Research	11
2. State of Art	15
2.1. Introduction to State of Art	16
2.2. Unmanned Aerial Vehicle	17
2.3. Global Navigation Satellite Systems	19
2.3.1. GPS History	20
2.3.2. GPS Operation	23
2.3.3. Relevant Aspects of GPS	28
2.4. Jamming	29
2.4.1. Modulation	29
2.4.2. Main Components of a Jammer	31
2.5. Antennas	32
3. System Functionalities	35
3.1. Introduction to System Functionalities	36
3.2. System Overview	37
3.3. Radio Frequency Interference	40
3.3.1. Barrage Jamming	41
3.3.2. Tone Jamming	44
3.3.3. Sweep Jamming	45
3.3.4. Successive Pulses Jamming	47

3.3.5.	Protocol-Aware Jamming	49
3.4.	Mobile Spoofing System	52
3.4.1.	UAV Location Determination	52
3.4.2.	Deviation of UAV	53
4.	Prototype System	57
4.1.	Introduction to Prototype System	58
4.2.	Prototype Overview	59
4.3.	Yagi Antenna Sizing	60
4.4.	Battery Sizing	63
4.5.	Authentication Security	64
4.6.	SPG Vanguard System	67
5.	Experimental Results	73
5.1.	Introduction to Experimental Results	74
5.2.	Controlled Environment Tests	75
5.3.	Real Environment Tests	80
5.4.	Proof of Concept	84
5.5.	Prototype's Tests	87
5.5.1.	Coverage Test Plan	88
5.5.2.	Static Flight Test Plan	95
5.5.3.	Dynamic Flight Test Plan	99
5.5.4.	Altitude Variation Test Plan	102
6.	Conclusions	105
6.1.	Introduction to Conclusions	106
6.2.	Main Conclusions	107
6.3.	Future Work	109
	References	111
	Appendix A - Sistema móvel para imobilizar e desviar drones não autorizados	119

Resumo	120
Descrição	121
Domínio técnico da invenção	121
A técnica anterior	121
Descrição das figuras	122
Descrição pormenorizada da invenção	124
Reivindicações	128
Appendix A – translated version	135
Abstract	136
Description	137
Technical field of invention	137
The previous technique	137
Figures’ Description	138
Detailed description of the invention	140
Claims	144
Appendix B - A portable equipment for transporting countermeasure devices	151
Description	152
Field of the invention	152
Prior art	152
Summary of the invention	153
Description of figures	154
Detailed description	154
Claims	159
Abstract	163
Appendix C - Method and system for intercepting and controlling target-drones	165
Description	166
Field of the invention	166

Prior art	166
Summary of the invention	168
Description of figures	168
Detailed description	169
Claims	174
Abstract	178

List of Figures

Figure 2.1. UX SPYRO developed by UAVision	18
Figure 2.2. AR5 developed by Tekever	18
Figure 2.3. Autonomous Flight Control System components	18
Figure 2.4. Uniform Rectilinear Motion	23
Figure 2.5. Possible locations using only 1 satellite	24
Figure 2.6. Contribution of each satellite in the trilateration	25
Figure 2.7. Satellite and receiver clocks	26
Figure 2.8. Spectrum of GPS signal and thermal noise power	28
Figure 2.9. Binary PSK modulator	30
Figure 2.10. Baseband BPSK signal and Transmitted BPSK signal	30
Figure 2.11. GPS jammer for use in cars	32
Figure 2.12. Yagi-Uda antenna	34
Figure 3.1. System architecture	38
Figure 3.2. System flowchart	39
Figure 3.3. Different theoretical spectrum of jamming	41
Figure 3.4. Barrage jamming programmed in GNU radio	43
Figure 3.5. Spectrum resulting from barrage jamming	43
Figure 3.6. Tone jamming programmed in GNU radio	44
Figure 3.7. Spectrum resulting from successive pulses jamming	45
Figure 3.8. Sweep jamming programmed in GNU radio	46
Figure 3.9. Spectrum resulting from sweep jamming	47
Figure 3.10. Waterfall analysis of sweep jamming	47
Figure 3.11. Successive pulses jamming programmed in GNU radio	48
Figure 3.12. Impulses in time with low duty cycle	49
Figure 3.13. Spectrum resulting from successive pulses jamming	49
Figure 3.14. Protocol-Aware jamming programmed in GNU radio	50
Figure 3.15. Received protocol-aware jamming signal in time	51
Figure 3.16. Spectrum resulting from protocol-aware jamming	51
Figure 3.17. Spectrum resulting from protocol-aware jamming 2	52
Figure 3.18. UAV localization method	53
Figure 4.1. System Anti-UAVs version 1	59

Figure 4.2. Results of a VK5DJ's Yagi Calculator	60
Figure 4.3. Handmade Yagi Antenna	61
Figure 4.4. Radiation diagrams of the handmade Yagi antenna	61
Figure 4.5. Power amplifier SPF5189Z	63
Figure 4.6. Biometric process	65
Figure 4.7. Flowchart of the general functioning of the security system	66
Figure 4.8. Spoofing Portable Gun	68
Figure 4.9. Control Station Spoofing Systems	68
Figure 4.10. C3S Interface	69
Figure 4.11. How SPG Vanguard System work	71
Figure 5.1. Emitter block diagram	75
Figure 5.2. Block diagram reference setup	77
Figure 5.3. Ublox receiver	77
Figure 5.4. Test in real environment	81
Figure 5.5. Power of GPS satellite signals with sweep jamming	82
Figure 5.6. Power of GPS satellite signals with protocol-aware jamming	83
Figure 5.7. Unauthorized drone protection system	83
Figure 5.8. Real test scenario with selected forced landing site.	84
Figure 5.9. DJI Phantom 3 Standard	85
Figure 5.10. Real test scenario using jamming signals	86
Figure 5.11. Anti-UAV mobile system operator	86
Figure 5.12. Real test scenario using spoofing signals	87
Figure 5.13. Urban environment with LoS between SPG ↔ C3S	88
Figure 5.14. Urban environment with NLoS between SPG ↔ C3S	88
Figure 5.15. Suburban environment with LoS between SPG ↔ C3S	89
Figure 5.16. Jammer 2,4GHz spectrum analyser	90
Figure 5.17. Jammer GNSS spectrum analyser	91
Figure 5.18. Spoofing GPS spectrum analyser	92

List of Tables

Table 1.1 - Schedule of activities	9
Table 2.1 - Types of drones according to wing types	17
Table 2.2 - Types of antennas according to the physical structure	33
Table 4.1 - Spectral power density of different jammers	62
Table 4.2 - Hardware current consumption	64
Table 4.3 - Interpretation of the C3S interface	70
Table 4.4 - Technology Readiness Level	71
Table 5.1 - Spectral power density of different jammers	76
Table 5.2 - Maximum range of various jammers in a controlled environment	79
Table 5.3 - Coverage Test Plan	93
Table 5.4 - Static Flight Test Plan	97
Table 5.5 - Dynamic Flight Test Plan	100
Table 5.6 - Altitude Variation Test Plan	103

[This page is deliberately left blank.]

List of Acronyms

ADC: Analog to Digital Converter.

AFCS: Autonomous Flight Control System.

AGL: Above Ground Level.

AWGN: Additive White Gaussian Noise.

BB: Base Band.

BPSK: Binary Phase-Shift Keying.

C3S: Control Station Spoofing Systems.

COTS: Commercial-Of-The-Shelf.

C-UAS: Counter-Unmanned Aerial System.

dB: Decibel.

DC: Direct Current.

DCS: Digital Cellular System.

DJI: Da-Jiang Innovations.

DOA: Direction of Arrival.

ECEF: Earth-centered, Earth-fixed.

EMFA: Estado Maior das Forças Armadas.

FCC: Federal Communications Commission.

GCS: Ground Control Station.

GNSS: Global Navigation Satellite System.

GPRS: General Packet Radio Service.

GPS: Global Positioning System.

GSM: Global System for Mobile.

GSM: Global System for Mobile.

GUI: Graphical User Interface.

IEEE: Institute of Electrical and Electronics Engineers.

IMU: Inertial Measurement Unit.

ISCTE: Instituto Superior de Ciências do Trabalho e da Empresa.

LNA: Low Noise Amplifier.

LoS: Line-of-Sight.

MAC: Medium Access Control.

NLoS: Non-Line-of-Sight.

NRZ: Non-Return-to-Zero.

PA: Power Amplifier.

PCS: Personal Communications Service.

PLC: Programmable Logic Controllers.

RF: Radio Frequency.

Rx: Receive.

SDR: Software Defined Radio.

SIM: Subscriber Identity Module.

SimCom: Simultaneous Communication.

SNR: Signal-to-Noise Ratio.

SoC: System on Chip.

SPG: Spoofing Portable Gun.

Tx: Transmit.

UAV: Unmanned Aerial Vehicle.

URSI: União Rádio Científica Internacional.

US: United States.

USB: Universal Serial Bus.

USRP: Universal Software Radio Peripheral.

UT: Universal Time.

UTC: Universal Time Coordinated.

VCO: Voltage Controlled Oscillator.

VGA: Variable Gain Amplifier.

Wi-Fi: Wireless Fidelity.

WPMC: Wireless Personal Multimedia Communications.

List of Symbols

k_B	Boltzmann constant in Joules per Kelvin [J/K]
T	Absolute resistance temperature in Kelvins [K]
Δf	Bandwidth in Hertz over which noise is measured [Hz]
λ	Wavelength [m]
c	Speed of light [m/s]
f	Signal frequency [Hz]
f_c	Carrier frequency [Hz]
d	Distance [m]
V_m	speed [m/s]
S	distance [m]
ρ	pseudorange
τ^s	clock of the satellite
τ	clock of the receiver
B	bandwidth
P_{Rx}	reception power
P_{Tx}	transmission power
G_{Rx}	reception gain
G_{Tx}	transmission gain
L_{fs}	free space path loss

[This page is deliberately left blank.]

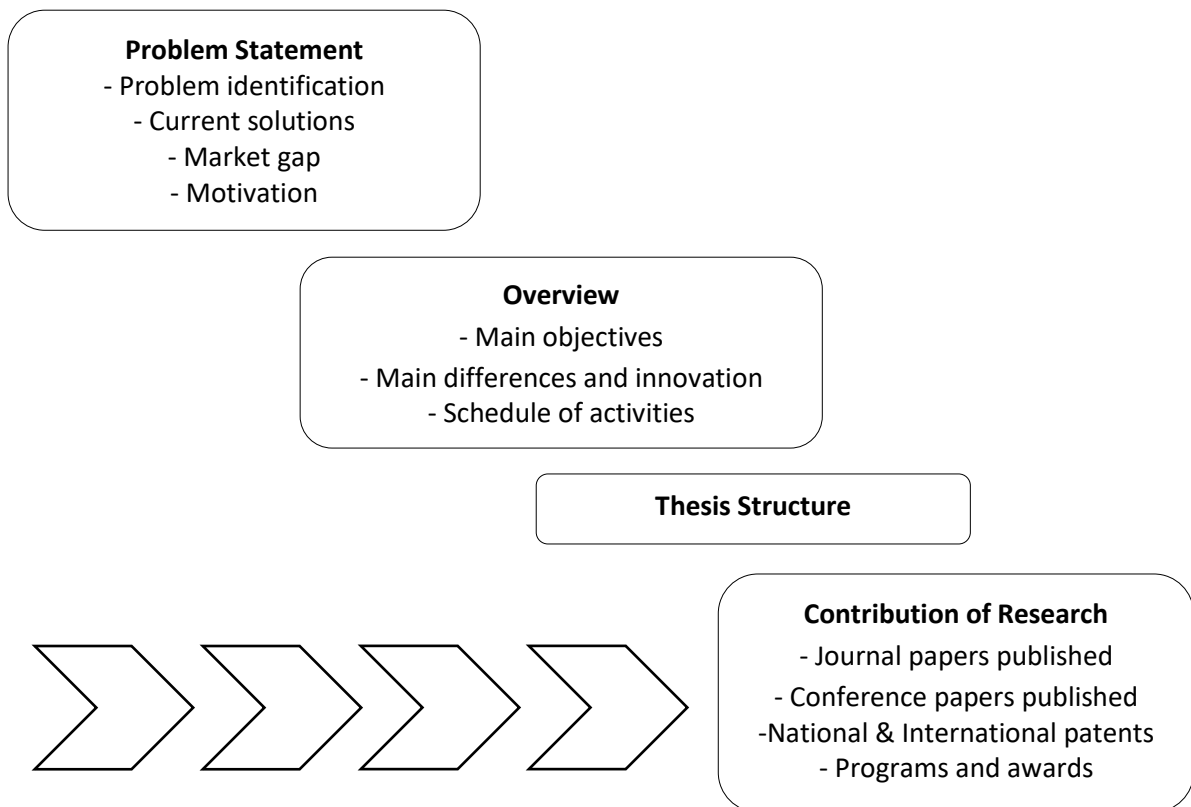
CHAPTER

1. Introduction

In this introductory section we provide an overview of the problem addressed in this thesis, as well as the thesis structure and scientific publications produced. Other research contributions are also presented.

1.1. Introduction to Thesis

The chart schematizes, in a more perceptible way, the subject discussed in Chapter 1. The Problem Statement section identifies the problem, current solutions, the market gap and explains the motivation that led to carry out this R&D. The Overview section describes the system's main objectives and differences comparing to those that currently exist. The Thesis Structure section explains individually which themes are covered in each chapter. The Contribution of Research section presents the articles published, submitted, and approved patents, program participations, awards and recognitions.



1.2. Problem Statement

Although drone legislation [1] exists, many unmanned aerial vehicle (UAV) operators choose not to comply with it, generating various types of incidents, either voluntarily or involuntarily.

Several solutions have been presented to try to solve this problem, such as birds of prey, capture nets, or even jammers as is the case below. For example, the Dutch police have trained some eagles and hawks, so that they can chase and hunt UAVs whenever necessary [2]. In Russia, a non-destructive solution was presented, the Rex-1, which comprises an emitter of an interference signal against the Global Navigation Satellite System (GNSS) signal [3].

Several studies on detection and jamming of these devices have also been carried out to combat this problem. The paper [4] emphasizes the guidelines for drone detection and for jamming. In [5], the authors present commercial-of-the-shelf (COTS) applications' components for various military purposes. Solutions aimed at military applications based on software defined radio (SDR) systems are considered, as well as a multifunctional system development base for detection and identification of unauthorized drones. Also, it is described the implementation of RF surveillance based on COTS components, which resorts to ADALMPLUTO and universal software radio peripheral (USRP) platforms. An SDR is a radio communication system that contains various reconfigurable software-based components for processing and converting digital signals. Unlike traditional radio communication systems, these radio devices are highly flexible, versatile, and configurable. In this thesis, the SDR used was the BladeRF x40 from the manufacturer Nuand. In past studies, the present authors have also studied techniques to solve the problem with unauthorized drones. In [6], we evaluated the use of low cost SDR's platforms for the implementation of a jammer able to generate an effective interfering signal aimed at the GPS navigation system. Using a programmable BladeRF x40 platform from Nuand and the GNU radio software development toolkit, several interference techniques were studied and evaluated considering the spectral efficiency, energy efficiency and complexity.

The different types of UAVs, the regulatory laws for UAV activities, their use cases, recreational and military UAV incidents have already been discussed in [7]. Various techniques for monitoring and preventing UAV attacks were studied and described along with case studies in [8-12]. In [13], the authors conducted an extensive market research of 581 counter-unmanned aerial systems (C-UAS) from 282 manufacturers in 39 countries around the world based on the literature and practice, making it a four-way statistical analysis. Based on this, they classified and summarized the most advanced weapon systems according to different technologies. In

[14], the authors presented the results from the field test of UAV GPS jamming by using software defined radio (SDR) and GNU radio software. The field test was carried out to study the performance of the jamming signal produced and the effect of elevation angle on the jamming range. The test subject used in this field test was a DJI Phantom 4 Pro, a commercial consumer grade drone.

A different approach to jamming consists in gaining control of the UAV by spoofing the control commands, which normally rely on radio waves. However, different UAVs may operate with different communication protocols, depending on the UAV brands or models.

Furthermore, since some UAVs may communicate under a dedicated communication protocol, this command-and-control spoofing solution may not work. It becomes simpler to perform satellite navigation signal spoofing, since global positioning system (GPS) signals are widely used by most UAVs, especially for autonomous operations [15].

Studies have already been carried out with the subject of spoofing the GNSS signals against systems that depend on these, namely UAVs and smart grid devices. It was demonstrated that a civil UAV could be “steered” by a spoofer by moving its perceived location in the opposite direction of the desired motion. Furthermore, short-term control of the UAV was demonstrated in all directions (east, north, and up) during the tests [16].

There have been a few other studies and investigations in the area of GPS spoofing against UAVs. In [15] [17], the authors studied and exploited the vulnerabilities of GPS systems in drones in order to hijack or gain control over the aircrafts. Another example of exploiting GPS vulnerability is that the one from the UnicornTeam, a group of security researchers focusing on systems based on radio technologies. They proved, in [18], through several approaches, that it is possible to spoof a GPS receiver, which the present authors have also demonstrated in [19].

Some more robust systems have already been developed in order to solve the problem of unauthorized drones. For example, the system presented in [20] is based on the identification of communication protocols for later disruption and/or replication and is designed for implementation in a distributed system. While it may be very effective against a few specific UAVs, the implementation complexity can be very high and the portability may be limited. The systems proposed in [21] [22] also constitute anti-UAV approaches but it includes only the blocking solution, i.e., they do not have the ability to gain control over the invading drone and to force it to land in a safe zone [23-32].

It is important to note that there are several other approaches’ types. Such is the case of the system presented in [33], which uses a more basic technique, i.e., resorting to a net to capture the invading drone. The icon concluded uses non-destructive methods, using radio frequency.

Motivated by the work above, in this thesis, we study a system capable of neutralizing unauthorized UAV flights using low cost SDR platforms. The implemented system is capable of stop the target UAV while transmits false GPS signals and jamming the communications, even gain control of the vehicle flying over protected areas.

1.3. Objectives

This thesis is related to technology transfer. The result is the development of a prototype for a new solution to the problem of unauthorized drones. The goal of this thesis is to design and implement a complete mobile system that can, in a controlled way, land the invading UAV in a geographical point determined by the user, thus, neutralizing the potential threat. The development of a prototype is to demonstrate that the result of R&D can be implemented in practice and that the system can work in various environments. A prototype of the system will be developed throughout the initial phase of the PhD, so that it will be possible study the techniques used, but also practical studies and theoretical-practical comparisons between the two areas. This prototype will have to be built in some light but strong materials. It comprises electronic components, microprocessor, selectors for transmission, powered by batteries making them mobile and easy to carry anywhere, coupled with SDRs to process the signals and transmit them. The hardware part will also be developed, namely specific antennas for each navigation and communication system. The main objectives can be summarized as follows:

- We propose and describe a low-cost portable system relying on SDR platforms, which can be manipulated simply by a user, and which can detect and neutralizing unauthorized drones using electromagnetic waves. With drones having two modes of operation, manual piloting mode (controlling the drone with the remote control) and autonomous mode (plotting a route in advance using geographical location coordinates), the system must have the functionality of emitting efficient signals to jamming these two types of communication with the device;
- Jamming should be done efficiently and on a directional target so as not to interfere with third party systems. Specific Yagi-Uda antennas for each navigation and communication systems are designed and produced to have the most directional emission possible;

- The system is characterized by the processing module being additionally programmed to control the transmission power of the signal emitted by the transmission module, based on the distance between the system and the target drone;
- The system must have a capacity to estimate the geolocation of the invading drone. The set of sensors and the GPS receiver is to be incorporated into the prototype;
- We propose and describe the implementation of a spoofing scheme incorporated into the anti-UAV system that consists of first jamming the GPS signal, followed by the transmission of false signals that allow the acquisition and indirect control of the unauthorized drone, enabling the user to land it in a pre-defined location. It does not depend on the detection of specific communication protocols and work with any type of drone;
- The system must have a security module configured to send a periodic message via mobile network, with information on the system's location to a supervising entity; and send a message via mobile network with the user's name, whenever the user initializes the system;
- The system must be mobile and adapted to any area of the planet and not depend on third party systems for its complete operation.

For evaluating the behavior of the system's operation, several types of jamming techniques were implemented, and different types of GPS receivers were tested as targets for the spoofed signal in different scenarios. Based on our previous work regarding jamming [34] and spoofing [35] and considering, in addition, the problem of determining the location of the target UAV. Differently from other approaches, the system presented in this thesis adopts a simpler philosophy being directed to a compact and localized/independent implementation. The main differences between the proposed system and other existing solutions can be summarized as follows:

- The system presented in this thesis does not depend on third-party systems to determine the location of the UAV;
- The system presented in this thesis does not depend on the detection of specific communication protocols and does not need to carry out any identification of the protocol type used between the UAV and the controller (no sniffing of packages). The system offers a more generalized applicability, since it works for UAVs that use conventional communication schemes and protocols, as well as variations of these;
- The proposed scheme does not replicate remote control commands to take over the UAV control. The system acquires indirect control of the UAV by deceiving the radionavigation system and not through signals transmitted by the remote control.

A timetable was drawn up to accomplish all the proposed objectives. The Table 1.1 shows the activities carried out and their duration. The activities are constituted by different tasks. The R&D had a duration of four years. The schedule also provides for the duration of an additional fifth year which focus on the management and promotion of the system.

[This page is deliberately left blank.]

Table 1.1 - Schedule of activities

Nº	Activities	Nº	Tasks	Duration of Activity (months)	Duration of the Task (months)	Gantt chart									
						Y1S1	Y1S2	Y2S1	Y2S2	Y3S1	Y3S2	Y4S1	Y4S2	Y5S1	Y5S2
1	R&D of anti-UAV algorithms	1.1	R&D of UAV communications jamming	42	12										
		1.2	R&D of UAV control		30										
		1.3	Integration and technology transfer		30										
2	Development of real-time system monitoring	2.1	Development of the application's graphic interface	12	6										
		2.2	Monitoring data collection and processing		6										
		2.3	Communications protocol for data transmission		12										
3	Development and construction of the system	3.1	Enquiry of requirements and specifications	60	48										
		3.2	Building the functional prototype		24										
		3.3	Production of pilot products		12										
4	Tests and results	4.1	Laboratory tests	36	36										
		4.2	Test in a controlled environment		12										
		4.3	Real-life scenario testing		12										
5	Management and promotion of the system	5.1	Project management and coordination	60	48										
		5.2	Participation in international defence fairs		12										
		5.3	Demonstration and pilots action		12										

[This page is deliberately left blank.]

1.4. Thesis Structure

In this introductory section we provide an overview of the problem addressed in this thesis, as well as the thesis structure and scientific publications produced over the past four years. Other research contributions are also presented.

In Chapter 2, there is an overview of GNSS systems with focus on GPS, a brief review of various types of jammers and the impact they have on the GNSS receiver. The SDR technology and the software used for testing are also reported.

Chapter 3, called System Functionalities, explains how the system works. The chapter is divided into two parts, the first part discusses the jamming of GNSS signal communications, covering five different techniques and choosing which one is best considering spectrum analysis. The second part describes how the system determines the location and gains control of the UAV.

In Chapter 4, we applied our learning system methodology to create a prototype which should be portable and easily manageable by an operator. For that, the chapter begins with the study to produce the Yagi-Uda antenna for the GPS frequency. It was necessary to develop part of the hardware to build the prototype. Since it is a mobile system, it was necessary to calculate the battery for the system. The battery was dimensioned for the system considering the consumption of each component. Technology is a double-edged sword, and we must always see both sides of the coin. Along with the benefits of each step forward comes the possibility that it may be used for malignant purposes. For this reason, it was felt the need to restrict the use of the system developed for safety.

In Chapter 5, the developed system was integrated and tested in different environments. Several tests were accomplished to evaluate the performance of the complete anti-UAV mobile system under the influence of real GNSS signals.

In Chapter 6, we conclude the thesis and discuss future directions of research.

1.5. Contribution of Research

During our research and development, several journal papers were published:

- Ferreira, R.; Gaspar, J.; Sebastião, P.; Souto, N. A Software Defined Radio Based Anti-UAV Mobile System with Jamming and Spoofing Capabilities. *Sensors* 2022, 22, 1487.

- Pavia, J.P.; Velez, V.; Ferreira, R.; Souto, N.; Ribeiro, M.; Silva, J.; Dinis, R. Low Complexity Hybrid Precoding Designs for Multiuser mmWave/THz Ultra Massive MIMO Systems. *Sensors* 2021, 21, 6054.
- Gaspar, J., Ferreira, R., Sebastião, P. et al. Capture of UAVs Through GPS Spoofing Using Low-Cost SDR Platforms. *Wireless Pers Commun* 115, 2729–2754 (2020).
- Ferreira, R., Gaspar, J., Sebastião, P. et al. Effective GPS Jamming Techniques for UAVs Using Low-Cost SDR Platforms. *Wireless Pers Commun* 115, 2705–2727 (2020).

Conference papers were also published and presented:

- Ferreira, R.; Gaspar, J.; Souto, N.; Sebastião, P. “Effective GPS Jamming Techniques for UAVs Using Low-Cost SDR Platforms”. In *Proceedings of the 2018 Global Wireless Summit (GWS)*, Chiang Rai, Thailand, 25–28 November 2018; pp. 27–32.
- J. Gaspar, R. Ferreira, P. Sebastião and N. Souto, "Capture of UAVs Through GPS Spoofing," In *Proceedings of the 2018 Global Wireless Summit (GWS)*, Chiang Rai, Thailand, 25–28 November 2018; pp. 21–26.
- Ferreira, R.; Gaspar, J.; Souto, N.; Sebastião, P. “GPS Jamming for unauthorized UAVs using SDR platforms”, 12º Congresso do Comité Português da União Rádio Científica Internacional (URSI), "Inteligência artificial e as ciências rádio", 14-Dezember 2018, Portuguese Communications Foundation, Lisbon.
- Two participations in the “Noite Europeia dos Investigadores – Ciência na Cidade”, 2018 and 2019, at the National Museum of Natural History and Science of the University of Lisbon.
- Participation in Conftele 2019, Workshop on Communications, Public Safety and Innovative Applications with Aerial Drones, speaker: A new way of protecting areas for unauthorized drones, 26-June 2019, at the headquarters of the Order of Engineers in Lisbon, Portugal.

- Ferreira, R.; Gaspar, J.; Souto, N.; Sebastião, P; Postolache, O. “Anti-UAV Mobile System with RTLS integration and User Authentication”, International Symposium on Sensors and Instrumentation in IoT Era, 29-30 August 2019, ISCTE-IUL Lisbon, Portugal.

Result of this study resulted in the creation of a startup and consequent patents:

- Portuguese national patent conceived: SISTEMA MÓVEL PARA IMOBILIZAR E DESVIAR DRONES NÃO AUTORIZADOS. Order date: 2019.07.19; Order publication date: 2021.01.19; Concession Date: 2021.07.26; Date of Publication of the Concession: 2021.07.29.
- International patent request: A PORTABLE EQUIPMENT FOR TRANSPORTING COUNTERMEASURE DEVICES. Recession date: 2021.08.31.
- International patent request: METHOD AND SYSTEM FOR INTERCEPTING AND CONTROLLING TARGET-DRONES. Recession date: 2021.08.05.

Participation in programmes, awards and recognition:

- Participation in the 2nd edition of the StartUp Voucher Programme, with application number 752, with the project Mobile UAV Protection System, from November 2018 to October 2019.
- Silver Medal (world's top 100) China International College Students' "Internet +" Innovation & Entrepreneurship Competition, December 2020.
- Participation in the intensive week on digital skills: “How to live and learn in a digital world held” from October 10 to October 14, 2022 (34 hrs.), at the University of Economics in Katowice, Poland.

[This page is deliberately left blank.]

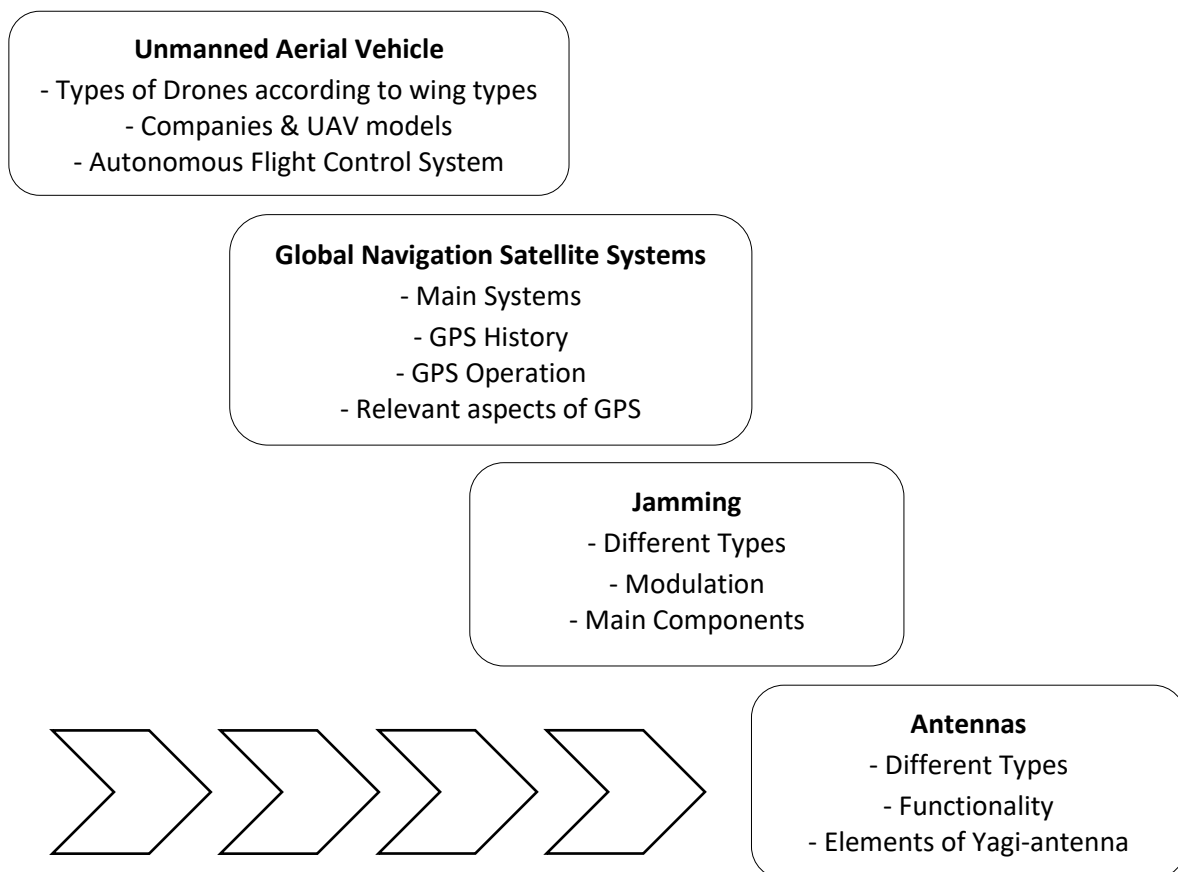
CHAPTER

2. State of the Art

In this chapter there is an overview of GNSS systems with focus on GPS, a brief review of various types of jammers and the impact they have on the GNSS receiver. The SDR technology and the software used for testing is also reported.

2.1. Introduction to State of the Art

The chart schematizes what is discussed in chapter 2 in a more perceptible way. The Unmanned Aerial Vehicle section reports on how the different drones are classified according to wing types, examples of Companies and UAV models in market and the components of Autonomous Flight Control System. The Global Navigation Satellite Systems section identifies the main geolocation systems, explains how the GPS came into existence, GPS operation and relevant aspects of GPS. The Jamming section identifies different types of jammers, modulation and main components of jammers. The Antennas section characterizes the different types of antennas according to the physical structure, their functionalities and activities, and the elements of which a Yagi-Uda antenna is composed.



2.2. Unmanned Aerial Vehicle

Unmanned Aerial Vehicle (UAV) or drone is any type of aircraft that can be controlled in the 3 axes and that does not need pilots on board to be guided. These types of aircraft are remotely controlled by electronic and computational means, under the supervision of humans, or even without their intervention, by means of programmable logic controllers (PLC).

There are different types of UAV according to wing types. Each one has its own way of taking off, landing, aerodynamics and usability. Table 2.1 elaborates on the advantages, disadvantages and usability of different types of UAV according to wing types [36].

Table 2.1 - Types of drones according to wing types

Drone Type	Advantage	Disadvantage	Use
Multi-rotor drones	- Easy to control and maneuver - VTOL and hover flight - Often lower price - Portability	- Limited flying time - Small payload capabilities - Less stability in the wind - Lower flight speeds	- Aerial photography - Aerial inspection - Landing surveying - Agriculture
Fixed-wing drones	- Longer flight time - Can carry a heavier payload - Greater stability in the wind - Higher flight speeds	- More training needed - No VTOL/hover - Expensive - Difficult to land, more places needed	- Aerial mapping - Utility inspection - Surveillance - Agriculture
Single-rotor helicopter drones	- VTOL and hover flight - Long endurance (with gas power) - Heavier payload capability	- More dangerous - Harder to fly, more training needed - Expensive	- Aerial LiDAR laser scanning
Fixed-wing hybrid VTOL drones	- VTOL and hover - Long-endurance flight - Fast speed - Heavier payload capability	- More training needed - Expensive	- Aerial mapping - Utility inspection - Surveillance - Agriculture - Search and rescue

Drones can be further classified by their size, payload capacity, range, power sources, abilities & equipment, or motors. The main group of commercial drones are multi-rotor drones, and the main group of military drones are fixed-wing drones.

Examples of Multi-rotor drones and Fixed-wing drones are presented, using two Portuguese Companies operating in the DefenseTech market. UAVision with Multi-rotor drone (UX SPYRO) illustrated in Figure 2.1 and Tekever with Fixed-wing drone (AR5) illustrated in Figure 2.2.



Figure 2.1. UX SPYRO developed by UAVision [37]



Figure 2.2. AR5 developed by Tekever [38]

Besides the aircraft, the UAV is also composed of a ground control station (GCS) through which it is possible to carry out the mission to be executed and monitor the entire flight remotely. The UAV also has a GPS receiver attached for real-time location, as well as an inertial navigation unit. The vehicle does not accept movement commands directly linked by GPS, resorting to an inertial measurement unit (IMU) ensuring a better precision of the position.

Inertial navigation is used by rockets, submarines and ships to determine coordinates. An inertial navigation unit is nothing more than a navigation system that integrates the accelerations in North/South, East/West through inertial sensors, determining the position. Listed below are some advantages of inertial navigation [39]:

- Does not require external information;
- Does not require signal emissions or receptions;
- Immune to interference.

The autopilot or Autonomous Flight Control System (AFCS) is an integrated package usually supplied by the manufacturer. The AFCS receives control from the GCS via the system control telemetry which acts autonomously. It generally consists of 5 components [39]:



Figure 2.3. Autonomous Flight Control System components

2.3. Global Navigation Satellite Systems

Global Navigation Satellite Systems (GNSS) can provide accurate location and timing information which are required for various applications such as in UAV autonomous operations. GPS is the most used system in the vast majority of applications, especially in UAVs, although there are other systems of positioning.

Main systems that make up GNSS:

- GPS - Global Positioning System - USA, operational since 1995;
- GLONASS - GLObal'naya NAVigatsionnaya Sputnikovaya System - Russia, started in 1982 and completed in 1995;
- GALILEO - ESA EU operational in 2013.

Space component - GPS

- 24 satellites (+5) of blocks II, IIA (Advanced) and IIR (Replacement) distributed over 6 orbits;
- Approximately circular orbits with a radius of 26 600 km, separated from each other by 60° in length;
- 12-h orbital period ($\approx 11\text{ h }58\text{ min }26\text{ s UTC}$) which causes the birth of the satellites to occur about 4 min earlier each day;
- Orbital inclination near 55°, relative to the terrestrial equatorial plane.

Space component - Glonass

- 24 Satellites (+3) distributed in 3 orbits;
- Approximately circular orbits with a radius of 25 510 km, separated from each other by 110° in length;
- Orbital period of 11:15 min sidereal which causes the birth of the satellites to be given about 50 min earlier each day;
- Orbital inclination close to 64,8°, relative to the terrestrial equatorial plane;
- Path repeats at the end of 8 sidereal days (the next satellite travels through the orbit of the previous satellite).

Space component- Galileo

- 30 satellites distributed by 3 orbits;
- Approximately circular orbits with a radius of 30 000 km, separated from each other by 120° in length;

- Orbital period of 14 h 21 min sidereal that causes the birth of the satellites to be given about 2 h and 24 min later in each day;
- Orbital slope close to 56° , relative to the terrestrial equatorial plane [40].

GNSS (Global Navigation Satellite Systems) are capable of providing accurate location and timing information that is found in a variety of applications. The use of GNSS is not limited to personal or automotive navigation. They can also be used for tracking goods and animals, tracking trains, navigating ships and for sports applications. In addition, new GNSS applications are currently under development or consolidation. For example, GPS boxes can be used by insurance companies to monitor a driver's behaviour and adjust the agreed insurance premium. GPS and GNSS in general enable applications that requires monitoring of user behaviour. This type of application inevitably introduces privacy issues, as GNSS are used to cluster information about users. This lack of privacy motivates the development and use of devices that can deny GNSS signal reception [41].

Of the GNSS systems most prominence is given to GPS because it is the most widely used by commercial drones and it is the system that we perform spoofing.

2.3.1. GPS History

Before, for most of human history, to find a location, you unfold a paper map. And if you are lucky, you can fold it back up again. But that all changes in October 1957. The Soviets shocked the world by launching the first-ever satellite, Sputnik, proving that a simple radio transmitter can work from space. In America, physicists William Guier and George Weiffenbach are messing around with some home-recording gear, listening to Sputnik's beeps, when they realize something extraordinary. By measuring the change in frequency of Sputnik's beeps as it passes overhead, they can pinpoint exactly where the satellite is. Their boss has an even bigger idea. *"What if they flipped this discovery on its head? Could tracking a beep from a satellite with a known trajectory allow them to pinpoint the location of a receiver anywhere on Earth below?"* Turns out, with a lot of maths, that it is possible. The discovery was gigantic news for the US military. To launch their missiles more effectively, the Navy wanted a targeting system that, unlike sonar, was invisible to the enemy, so they get to work on a satellite program named Transit. By the mid-'60s, they have got six satellites in orbit, but accuracy was initially off by more than a mile. Still, navigation by satellite worked. But it would need to work better. Over a steamy Labor Day weekend in 1973, inside the Pentagon, Colonel Brad Parkinson organised a top-secret meeting of engineers to work on satellite "global positioning system." The plan,

called Navstar, went like this. They needed 24 satellites. Each one would circle the planet twice a day in one of six fixed orbits to achieve 24-7 global coverage. On board, ultra-precise atomic clocks sent signals, giving their exact position and time, reaching the Earth at the speed of light. Below, a GPS receiver took signals from at least four available satellites and measured its distance from each one to calculate its exact location, giving the entire US military a navigational edge in the water, in the air and on land. In 1978, the first Navstar satellite reached orbit. Parkinson thought GPS would improve the target accuracy of weapons systems, making them more humane by reducing collateral damage. In the late '70s, F-4 jets tested this theory by using GPS to drop sand bombs in the desert at the proving test range near Yuma, Arizona. Skeptics were invited to take a seat, right beside the target, in the "doubters chair." Sure enough, the jets repeatedly hit the same target within just five to ten meters. The system required massive, power-hungry receivers on the ground, but still it was a huge moment. GPS worked.

It soon became clear that GPS could be as useful in saving lives as in taking them. In September 1983, the Korean Air Line massacre, the attack by the Soviet Union against 269 innocent men, women and children aboard an unarmed Korean passenger plane. It was a very big diplomatic crisis. But it was believed that the pilots failed to notice the plane deviating from its replanned route into prohibited Soviet airspace. Access to GPS could have averted the tragedy. So, on September 16th, 1983, President Ronald Reagan made a historic move that transformed life for everyone. He signed an executive order allowing the first-ever civilian use of the Pentagon's GPS system for free, well, paid for by US taxpayers, so such a disaster will never happen again. What he did not say was that civilians would get a separate signal from the military, one that was not quite as good. That means worldwide navigation and aircraft control became safer thanks to GPS. Two years later, he opened up GPS even further by allowing private companies to produce GPS receivers for the public. It was a great start-up opportunity. As commercial receivers steadily improved, the US military realizes that GPS could be offering its enemies a strategic advantage. But the genie's out of the bottle, so they decided to make the nonmilitary signal even worse. They called it Selective Availability.

There have always been separate satellite signals, one for the military and one for civilians. On March the 25th, 1990, engineers flipped a switch, deliberately scrambling the civilian signal. Accuracy goes from around ten meters out to one hundred. Immediately, drivers with GPS systems started missing their turns. The military signal, however, remained extremely accurate, and early the following year, it was called into action. During the first Gulf War, America's military GPS system revolutionised the battlefield. It guided smart weapons in surgical strikes on Iraqi targets and gave lead US mobile units a powerful strategic advantage, letting them

navigate the desert at night, giving them the crucial element of surprise. But regular soldiers operating in the featureless desert wanted a navigational boost too, so they wrote home to their families, asking them to send commercial GPS devices. That was a problem for Commanders. You cannot coordinate a battlefield when not everyone is using the same signal. So, temporarily, the US switched off Selective Availability. Of course, after the Gulf War was over, the government flipped the switch back. But the public now knows what is possible.

By 1995, the US's GPS system had 24 satellites, offering complete global coverage for both military and civilian use. Consumer GPS devices were steadily dropping in size and price. In 1998, the StreetPilot became the first portable car-friendly satnav device. Though, at \$400 per unit, it was still out of reach for many, but the days of reading maps were numbered. GPS was doing a job that was once one of humanity's greatest talents. Historically, humans have navigated thousands of miles over water without technology by reading the sun, sea, and stars. Over land, we have big distances with natural navigation, plotting routes with landmarks or creating a mental map in our brains. GPS started to replace those human skills with technology, making navigation much easier with less effort required.

Through the 1990s, people grew more dependent on GPS. And other nations wanted their own GPS systems. Russia completed their military only GLONASS in 1993. In 2000, China launched their first BeiDou satellite with coverage limited only to China. But international competition is inevitable, and private enterprise is demanding a more accurate and consistent signal. On May the 2nd, 2000, President Clinton bows to corporate pressure and turns off Selective Availability for good. Overnight, the GPS system improved by a factor of five or better. Sales of GPS receivers took off, disrupting how we work and play. Emergency services and search rescue teams add GPS to their lifesaving operations. GPS helped to develop systems for commercial aircraft to make safer precision landings on hard-to-reach airstrips. And satnav sales increased, competing to offer new features. People soon realised GPS was not just good for finding your way but also for keeping an eye on others, from young children to teenagers with newfound freedom. But the GPS revolution really took off in 2008 with the release of the Internet-enabled iPhone 3G. GPS receivers in our pockets soon became mainstream and at no additional cost. Location-based apps in the mid-2010s connected was in new ways, transforming how we socialize. GPS even founds itself used in sports. With so many potential applications, it was no surprise the GPS economy just kept on growing. If it moves, GPS will find way to track it in creative and unexpected ways. Drones with GPS alert lifeguards to sharks approaching the shore. Helicopters use GPS to map the spread of forest fires for better use of firefighting resources. In London, pigeons wearing sensors and a GPS tracker have monitored

poor air quality. And in India, GPS snakebite apps speedily connect victims with antivenom, saving lives.

By the late 20-teens, GPS is deeply embedded in our lives through a new generation of apps that help connect us with people and resources. They make everything from sharing food, travel, photos, and information easier. By June 2020, China's BeiDou system had 35 satellites, more than the US GPS system, offering the world's most complete coverage. It now guides robotic taxis in the streets of Beijing, as driverless cars take another step towards reality. Self-driving vehicles, robotic tractors, delivery drones, and flying transports using GPS are all on the horizon [42].

2.3.2. GPS Operation

The GPS operating principle is quite simple. To understand it we use the concept of average speed. Figure 2.4 shows a Formula One car travelling along a straight line. The car starts from the point S_0 and moves for a certain period of time to the final position S .

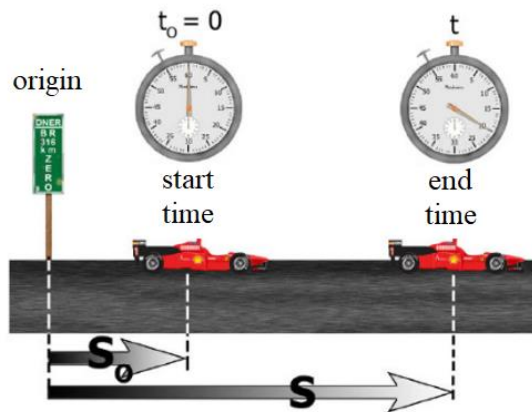


Figure 2.4. Uniform Rectilinear Motion [41]

To find out the speed of the car on the route you simply measure the distance it travelled and divide it by the time (equation 1).

$$V_m = \frac{\Delta S}{\Delta t} = \frac{S - S_0}{t - t_0} \quad (1)$$

You can also use the opposite procedure, i.e., knowing the speed with which an object moves, you measure the time of displacement and thus find the distance travelled (equation 2). In this case, it is enough to isolate ΔS in equation 1:

$$\Delta S = V_m \cdot \Delta t \quad (2)$$

In the case of GPS, the satellite sends a radio signal to the receiving device with the information of the time when the signal was sent. When it receives it, the receiver compares the time of sending with the time of receiving and calculates the time of displacement [43] [44].

Since the signal is sent by an electromagnetic wave, it is known that its speed is equal to the speed of light, i.e., approximately 3×10^8 m/s. In this way, it is enough to apply equation 2 to calculate the distance between the satellite and the receiver.

For example: the time calculated by the receiver was 80 ms (0.08s) and the speed of the signal is 3×10^8 m/s. So, it is enough to multiply these two values to find the distance between the satellite and the device. In this case: 24 000 km.

However, using only one satellite we will have only one distance, i.e., the device can be at any point in a 24 000 km radius circle, as shown in Figure 2.5.

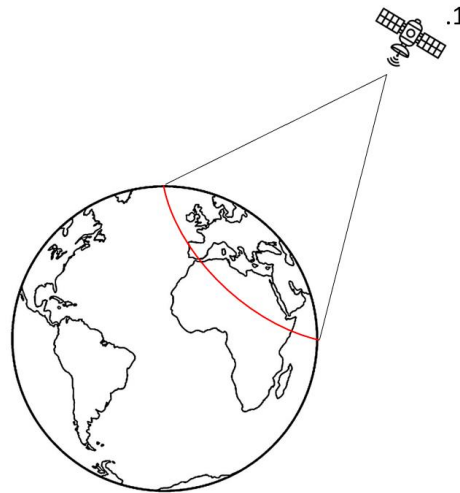


Figure 2.5. Possible locations using only 1 satellite

With the use of only one satellite the receiver can be located on the entire circumference represented in Figure 2.5. With the contribution of two satellites the circles intersect and the receiver can only be located at two points (point Q or point P). Three satellites are used to obtain the exact location. The receiver calculates the distance between itself and each of the three satellites and is able to know its exact location.

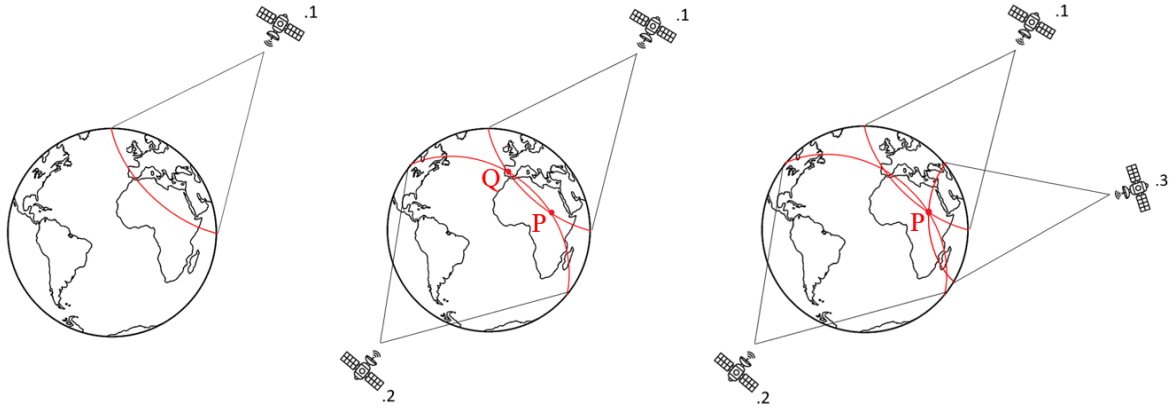


Figure 2.6. Contribution of each satellite in the trilateration

In this case it is known that the receiving device is located at point P in Figure 2.6. This process is called trilateration. To ensure that the receiver can communicate with the satellites from anywhere on Earth, the 24 satellites orbit the planet in 6 planes with 4 satellites each. This makes it so that there are always at least 4 satellites visible at any point on the planet [45].

A signal is transmitted by each satellite in the direction of planet Earth. This signal is encoded with the "Navigation Message", which can be read by GPS receivers. The "Navigation Message" includes orbit parameters (often called "transmission ephemeris"), from which the receiver can calculate satellite coordinates (X, Y, Z). These are Cartesian coordinates in a geocentric system, known as WGS-84, which has the origin at the Earth's centre of mass, Z axis pointing to the North Pole, X pointing to the Prime Meridian (which runs through Greenwich) and Y at right angles to X and Z. The algorithm that transforms the orbit parameters into WGS-84 coordinates is called the "Ephemeris Algorithm", which is defined in GPS Textbooks (e.g., Leick, 1991). The "Navigation Message" is discussed in more detail later. For now, we address pseudoranges.

The time at which the signal is transmitted from the satellite is encoded in the signal, using time according to an atomic clock on board the satellite. The time the signal is received is recorded by the receiver using an atomic clock as well. The receiver measures the difference in these times (equation 3):

$$\rho = (T - T^S) \cdot c \quad (3)$$

The pseudorange (ρ) can be calculated as the difference between known clock reading of the receiver when the signal is received (T) and the reading of the satellite clock when the signal was transmitted (T^S) multiplied by the speed of light (c).

Receivers record data at regular, specified intervals (typically every 30 seconds, as instructed by the receiver user). It is the receiver's clock time reading T , which is used to specify exactly the sampling of the measurement. Therefore, the value of T at a measurement epoch is known exactly and is recorded in the data file along with the observation. What is not known is the actual measurement time and for a clearer explanation the Figure 2.7 is illustrated [46].

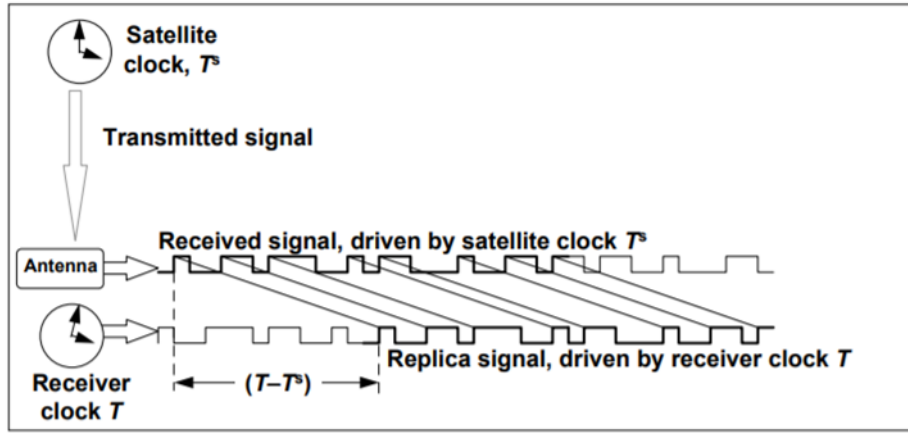


Figure 2.7. Satellite and receiver clocks [46]

The modelled observation can be developed by setting the clock time T equal to the actual reception time t plus a clock bias τ for both the receiver (equation 4) and satellite clocks (equation 5):

$$T = t + \tau \quad (4)$$

$$T^s = t^s + \tau^s \quad (5)$$

The substitution gives the pseudorange as a function of the actual time at which the signal was received (equation 6):

$$\begin{aligned} P^s(t) &= ((t + \tau) - (t^s + \tau^s)) \cdot c \\ &= (t - t^s)c + c\tau - c\tau^s \\ &= \rho^s(t, t^s) + c\tau - c\tau^s \end{aligned} \quad (6)$$

$\rho^s(t, t^s)$ represents the interval from the receiver (at receive time) to the satellite (at transmit time). This model is simplified; for example, it assumes that the speed of light in the atmosphere is c , and ignores the theory of relativity; but this simplified model is useful for obtaining information about the principles of GPS. Using the Pythagorean theorem, one can write:

$$\rho^S(t, t^S) = \sqrt{(x^S(t^S) - x(t))^2 + (y^S(t^S) - y(t))^2 + (z^S(t^S) - z(t))^2} \quad (7)$$

The Navigation Message calculates the satellite position (x^S, y^S, z^S) and the clock of the satellite τ^S . Therefore, we are left with 4 unknowns, the position of the receiver (x, y, z) and the clock of the receiver τ .

If the reception time were used, the error in the calculated interval could be tens of meters. Starting with the actual reception time, t , the transmission time can be calculated by an iterative algorithm known as "the light time equation", which can be written as follows:

$$t^S(0) = t = (T - \tau) \quad (8)$$

$$t^S(1) = t - \frac{\rho^S(t, t^S(0))}{c}$$

$$t^S(2) = t - \frac{\rho^S(t, t^S(1))}{c}$$

where the satellite position $\rho^S(t, t^S)$ is computed at each time step using the Kepler-type elements of the Navigation Message, and the algorithm is stopped when the computed interval converges (i.e., does not change by more than an insignificant value). Although more convergent methods have been implemented, the above method is probably the easiest to understand.

Looking at the system of simplified observation equations from 4 satellites in view of the receiver, one can write the pseudoranges for each satellite as (equation 9):

$$\rho^1 = ((x^1 - x)^2 + (y^1 - y)^2 + (z^1 - z)^2)^{1/2} + c\tau - c\tau^1 \quad (9)$$

$$\rho^2 = ((x^2 - x)^2 + (y^2 - y)^2 + (z^2 - z)^2)^{1/2} + c\tau - c\tau^2$$

$$\rho^3 = ((x^3 - x)^2 + (y^3 - y)^2 + (z^3 - z)^2)^{1/2} + c\tau - c\tau^3$$

$$\rho^4 = ((x^4 - x)^2 + (y^4 - y)^2 + (z^4 - z)^2)^{1/2} + c\tau - c\tau^4$$

Note: (The superscripts next to the satellite coordinates are intended to identify the satellite and should not be confused with exponents) [46].

2.3.3. Relevant Aspects of GPS

GPS satellites transmit simultaneously several ranging codes and navigation data using binary phase-shift keying (BPSK). The GPS signals reach a GPS receiver from a series of satellites in terrestrial orbit allowing the positioning through trilateration. This is a method whereby the distances to three separate points, in this case satellites, are measured in order to calculate a location with an accuracy of only a few meters.

Each GPS satellite transmits two carrier waves: L1 and L2. They are generated from the fundamental frequency of 10.23 MHz, which is multiplied by 154 and 120, respectively. Thus, the frequencies (L) and the wavelengths (λ) of L1 and L2 are:

- $L1 = 10,23 \text{ MHz} \times 154 = 1575,42 \text{ MHz}$ and $\lambda = 19 \text{ cm}$ with a bandwidth of 15,345 MHz
- $L2 = 10,23 \text{ MHz} \times 120 = 1227,60 \text{ MHz}$ and $\lambda = 24 \text{ cm}$ with a bandwidth of 11 MHz

L1 is the target frequency for the proposed jammer as it is used by commercial UAVs. L1 is used for transmitting the Navigation Message, C/A and P Code. These codes are broadcasted to the receivers in the navigation message. In General, GPS satellites transmit three types of information: almanac, ephemeris and timing information. The spectrum representation of the GPS signal is shown in Figure 2.8.

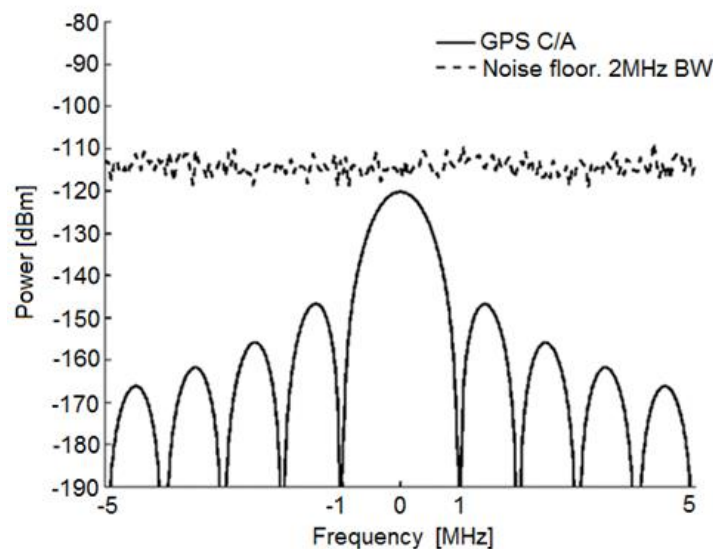


Figure 2.8. Spectrum of GPS signal and thermal noise power [47]

GPS signals are very weak, about 50 W, having about the same power as the TV signals transmitted by geostationary satellites. GPS signals suffer interference when they pass through most structures. As the satellite antenna diffuses the RF signal evenly over the Earth's surface

the transmitted energy is attenuated. This is mainly due to free space loss as the transmitted energy spreads spatially as it travels to the user (according to the surface of a sphere whose radius is increasing). The minimum energy level received for users on Earth is $-158,5$ dBW for L/C code at L1 and -160 dBW for P code at L2 according to GPS specifications [48].

2.4. Jamming

Any radio frequency signal from any unwanted source that is received by a GNSS receiver is considered interference. Such interference may result in inaccurate navigation or complete loss of signal to the receiver.

A jammer is a device with the ability to interfere with the transmission of signals, such as signals used in GNSS systems, signals from mobile communications systems, Wi-Fi signals and other signals.

There are several telecommunication devices that can suffer disturbances due to jammers. The main types of jammers are [49]:

- Mobile network jammers;
- Wi-Fi signal jammers;
- GPS jammers;
- Bluetooth jammers;
- VHF/UHF signal jammers;
- Walkie-talkie jammers.

Because the wireless medium is shared, a jammer can easily interfere with a communications channel used by RF technologies. It is possible to interfere with the channel through a signal that ignores MAC protocols or interferes with these same protocols.

2.4.1. Modulation

In general, it is common practice to use for the jammer architecture a similar architecture to the one used by the sender of the signal to be interfered. In this way, the interfering signal "mixes" with the target signal, since they have identical properties in order to destroy its information or make its reception virtually impossible in the receiver.

GPS systems use a transmission using BPSK (Binary Phase Shift Keying) modulation.

Regarding PSK modulation, the bipolar NRZ line coding can be used, facilitating the design of the transmitter. Since the bipolar line coding varies between a positive and negative voltage, the phase difference of 180° is obtained in this way. The block diagram describing this modulator is shown in Figure 2.9 [50].

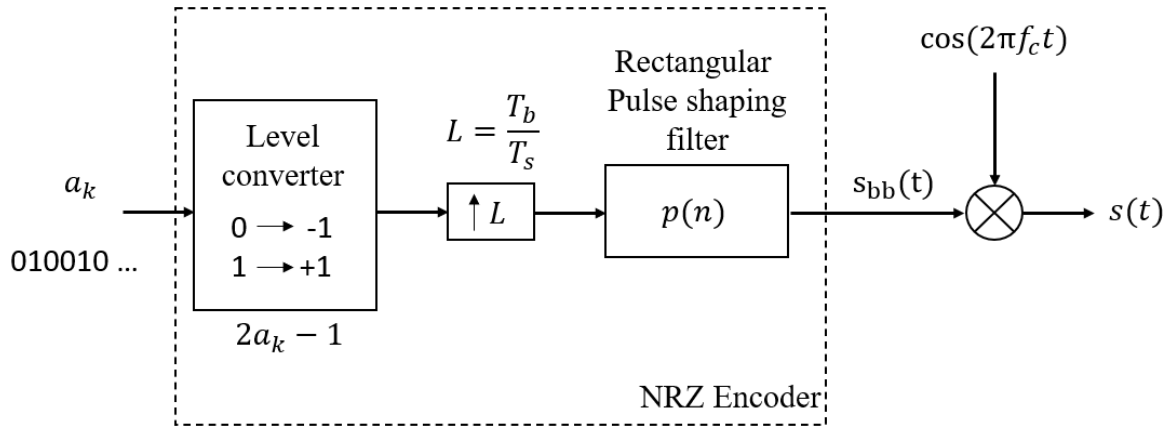


Figure 2.9. Binary PSK modulator

The PSK signal resulting from this modulation is represented in Figure 2.10. This modulation is also known as BPSK (Binary PSK).

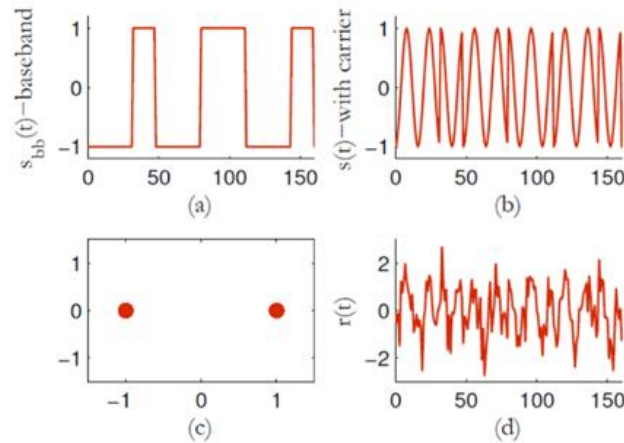


Figure 2.10. (a) Baseband BPSK signal, (b) Transmitted BPSK signal - with carrier, (c) constellation at transmitter and (d) received signal with AWGN noise [50]

For this modulation the values of amplitude and frequency of the carrier are constant, varying only the phase in 180° as represented in expression (10) [51].

$$S_{PSK}(t) = \begin{cases} A\cos(2\pi f_c t + 0); bit1 \\ A\cos(2\pi f_c t + \pi); bit0 \end{cases} \quad (10)$$

2.4.2. Main Components of a Jammer

Jammers were initially developed for security forces and military purposes to be used against criminals and terrorists. Later, the use of these devices extended to civilian applications, namely for use by governments to protect certain entities. GPS jammers were initially developed to be used in the military and spy agencies. As previously mentioned, there are two possible carrier frequencies that are used by these devices, one for the general public (1575,42 MHz) and another for the military (1227,6 MHz).

In the US, in October 2011, the FCC Enforcement Bureau carried out 20 actions against online shops illegally selling more than 200 models of jammers in 12 states. Different types of jammers were seized: Wi-Fi jammers, GPS jammers and jammers for other devices [52].

The main modules that make up a jammer are [53]:

- **Antennas** - Some less complex jammers have their antenna inside the device, while other more sophisticated ones have several antennas on the outside of the device, as this way it is possible to achieve a greater range and block several frequency bands simultaneously.
- **Voltage Controlled Oscillator (VCO)** - component that generates a signal.
- **Control circuit** - Allows you to adjust the frequency at which broadcasting will take place by imposing a voltage on the input of the VCO.
- **Noise generator** - It belongs to the control circuit. A random electronic signal is generated in this component at the frequency where communications jamming is to be done.
- **RF Amplifier** - Amplifies the output signal to the radio signal strength required to block communications.
- **Battery** - Powers the circuit. The charge depends on the complexity of the jammer.

Jammers are used in the military to prevent the exact location of a given object, such as missiles or bombs (with built-in GPS receivers) and other objects (also with GPS receivers) that allow troops to be located by the enemy. Thus, this device is useful both to hide the location of

the person who has it from the enemy, and also to prevent the enemy from using the functionalities of devices with GPS, if the jammer signal reaches these enemy devices.

GPS jammers have recently been used by civilians who want to ensure their own privacy. To do so, they use this device in their cars (a device of this type is shown in Figure 2.11). The aim of some users of these jammers is to block the GPS receiver of their car in order to prevent their location from being detected by devices with this capability.



Figure 2.11. GPS jammer for use in cars [54]

This device has also been recently used illegally for thefts of cars that have GPS receivers, since this jammer can disable the GPS locator of the car [54].

The jammer addressed in this dissertation aims to achieve the same purpose, in order to interfere in the communication of GNSS satellites with the target drone.

2.5. Antennas

An antenna is a transducer. It is a device which converts electrical power into electromagnetic waves and vice versa. An antenna can be used either as a transmitting antenna or a receiving antenna.

A transmitting antenna converts electrical signals into electromagnetic waves and radiates them. A receiving antenna converts electromagnetic waves from the received beam into electrical signals. Antennas have undergone many changes, in accordance with their size and shape. There are many types of antennas depending upon their wide variety of applications. The Table 2.2 shows examples of the various types of antennas and their applications.

Table 2.2 - Types of antennas according to the physical structure [55]

Type of antenna	Examples	Applications
Wire Antennas	Dipole antenna, Monopole antenna, Helix antenna, Loop antenna	Personal applications, buildings, ships, automobiles, space crafts
Aperture Antennas	Waveguide (opening), Horn antenna	Flush-mounted applications, air-craft, space craft
Reflector Antennas	Parabolic reflectors, Corner reflectors	Microwave communication, satellite tracking, radio astronomy
Lens Antennas	Convex-plane, Concave-plane, Convex-convex, Concave lenses	Used for very high frequency applications
Micro strip Antennas	Circular-shaped, Rectangular shaped metallic patch above the ground plane	Aircraft, spacecraft, satellites, missiles, cars, mobile phones etc.
Array Antennas	Yagi-Uda antenna, Micro strip patch array, Aperture array, Slotted wave guide array	Used for very high gain applications, mostly when needs to control the radiation pattern

The sole functionality of an antenna is power radiation or reception. The functioning of an antenna depends upon the radiation mechanism of a transmission line. Antennas may be divided into various types depending upon the physical structure of the antenna, the frequency ranges of operation, or the mode of applications.

The main communication parameters to consider when building an antenna are frequency carrier, wavelength, impedance matching (typically 50 ohm), radiation intensity, Voltage Standing Wave Ratio (VSWR) & reflected power, and bandwidth. According to the standard definition, “The ratio of maximum radiation intensity of the subject antenna to the radiation intensity of an isotropic or reference antenna, radiating the same total power is called the directivity.”

Considering the objective of a system to solve the problem of unauthorized drones, a directive antenna is needed. The aim of the system is to form a directional beam so that the signal can radiate more efficiently and not interfere with third party systems. The antenna that has these characteristics is the Yagi-Uda antenna. Yagi-Uda antenna is the most popular and easy-to-use type of antenna with better performance, which is famous for its high gain and directivity. The Yagi-Uda antenna consists of parasitic elements (reflector and directors) and a dipole. The directors are placed to increase the directivity of the antenna. The feeder is the bent dipole. The reflector is the length element, which is located behind the dipole [55].

The structure on which the elements are located is called as boom. The single element present at the back of the driven element is the reflector, which reflects all the energy towards

the direction of the radiation pattern. The other elements, before the driven element, are the directors which direct the beam towards the desired angle. The various components of the antenna can be seen in the Figure 2.12.

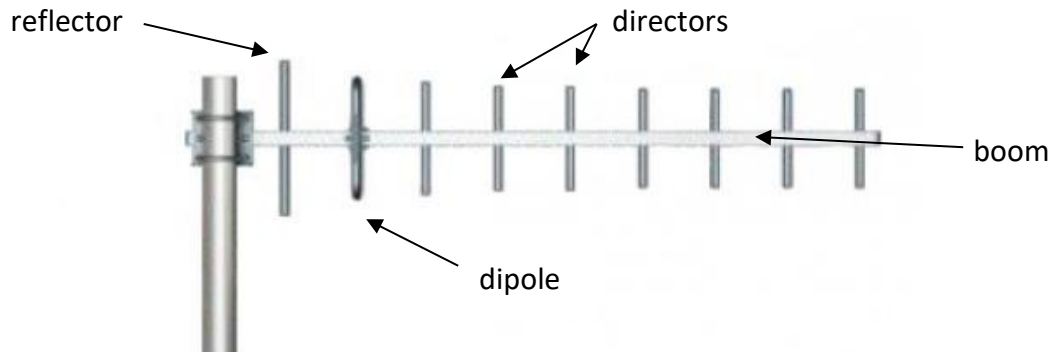


Figure 2.12. Yagi-Uda antenna

The directional pattern of the Yagi-Uda antenna is highly directive. The minor lobes are suppressed, and the directivity of the major lobe is increased by the addition of directors to the antenna. The advantages of Yagi-Uda antennas are the high gain, high directivity, ease of handling and maintenance, less amount of power is wasted, and broader coverage of frequencies. The Yagi-Uda antennas disadvantages are that they are easily affected by noise and atmospheric effects [55].

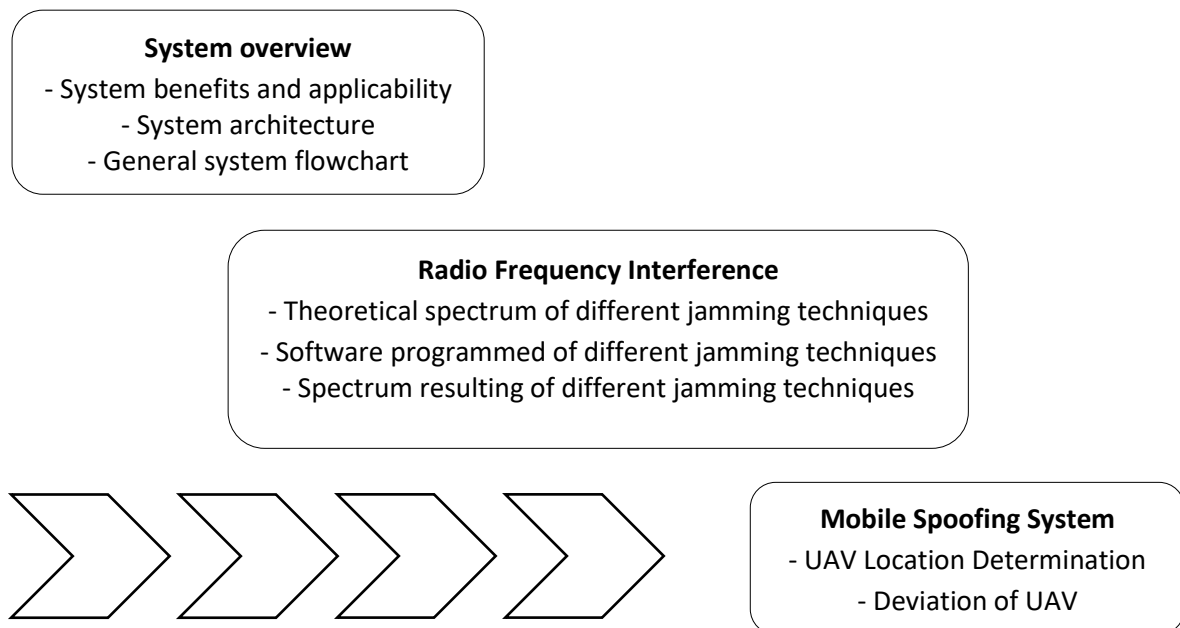
CHAPTER

3. System Functionalities

This chapter explains how the anti-drone system proposed as the main objective of the thesis works. It is divided into two sections, the first part discusses the jamming of GNSS signal communications, covering five different techniques and choosing which one is best considering spectrum analysis; and the second part describes how the system determines the location and gains control of the UAV.

3.1. Introduction to System Functionalities

The chart schematizes what is discussed in chapter 3 in a more perceptible way. The System overview section explains how the proposed anti-UAV system contributes to increase security and privacy. It is describing all the system modules. The Radio Frequency Interference section describes the software implementation of the different jamming techniques. The Mobile Spoofing System section demonstrates how the system can locate and divert the unauthorized drone.



3.2. System Overview

The great benefits that proposed anti-UAV system brings to society focus on two specific points: security and privacy. With the implementation of the studies and the creation of the prototype, proposed anti-UAV system contributes to increase the security of all citizens, since there are several possibilities of attempted attacks using bombs attached to drones. The intrusion of a drone in an airport causes many expenses for airlines. They may have their flights disrupted or even cancelled due to drone incidents. With the system this problem can be easily and quickly solved. Problems such as the traffic of illegal weapons or substances in prisons can also be solved by using this system. Regarding privacy issues, there are cases of invasion of privacy with drones, namely when capturing images on someone else's property. These were the main reasons for us to create a mobile solution, of quick intervention, user friendly and adaptable to any area of the planet.

The aim of the system described in this thesis is to prevent the intrusion of unauthorized drones, commercial or customized, which includes, for example, land, aerial and water drones operating in restricted areas such as airports, military areas, condominiums, occasional public events, or other areas where public safety needs to be guaranteed.

As possible applications, it can be used for protection against possible terrorist attacks at political speeches, festivals, sporting events or others, where terrorists may resort to bombs attached to drones. It can be used to reduce the trafficking of illegal substances and objects into prisons, where criminals use drones to transport them by air. It can also help to solve situations of negligent drone pilots who fly these devices to capture images of forest fires, obstructing aerial firefighting operations. There are many other cases and situations where this system can act as a non-destructive approach capable of forcing an invading drone to land. As it is a mobile system, it can be easily adapted to different geographical areas and different scenarios.

Through a touchscreen, the user of the system visualizes a map of the area where he is located, allowing him to select the intended landing spot for an eventual intruder drone. Once an invading drone is detected, the user just needs to point the system at the drone and press the trigger. The system will guide the invading drone to the previously selected site and force it to land. In order to be easily and quickly adapted to the areas to be protected, the system was designed so as to be portable. The modular system incorporates efficient technologies and materials, based on its ease of transportation and handling by defense forces (military and public security). Figure 3.1 represents the main modules that make up the system.

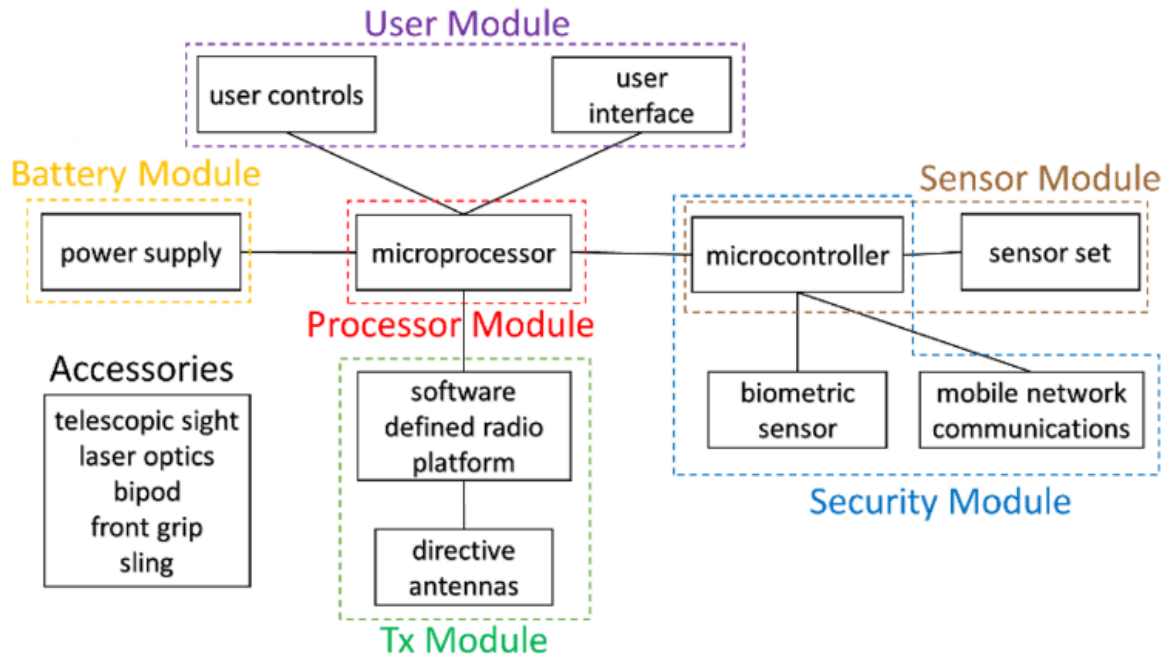


Figure 3.1. System architecture

The user module is composed of controls/commands and a user interface and is, thus, responsible for all user inputs. The battery module is responsible for powering the entire system. The processor module consists of the microprocessor, responsible for all system processing. The sensor module is composed of the microcontroller, which is directly connected to the microprocessor and is responsible for managing and collecting data from the whole set of sensors. The transmission module consists of the electronic equipment required for the transmission of radio signals and the directional antennas. The security module protects the system by resorting to authentication through a biometric sensor, which allows operation only to previously authorized users. Several accessories (e.g., telescopic sight, laser optics, bipod, front grip and sling) are incorporated into the system in order to help improve the user experience and, consequently, improves the performance of the operational system for the neutralization of target UAVs.

As previously stated, the main functionality of the system is the ability to divert the invading drone to a zone determined to be safe. To perform this task, the system needs to acquire the location of the target drone. To determine the location of the invading drone, a set of sensors are attached to the system such as: distance meter, accelerometer, location sensor and magnetometer.

In terms of security, to prevent the misuse of the equipment by unauthorized individuals, the system allocates a biometric sensor, as previously stated. Furthermore, through mobile

network communications, the system sends a periodic message (time configurable) with the information of the location of the system to a supervising entity. Complementarily, whenever someone initializes the system or initiates the transmission, a message is also sent with the respective username. This system minimizes interference in third party systems through the use of highly directive antennas.

In summary, the operation of the system can be divided into five stages, as shown in Figure 3.2.

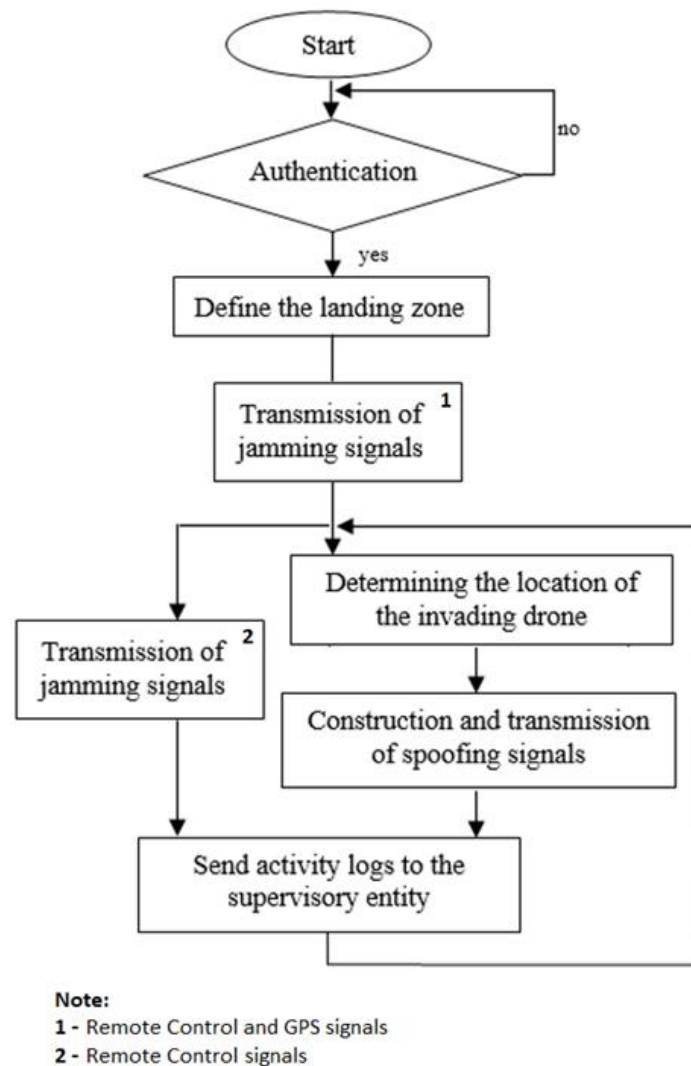


Figure 3.2. System flowchart

The first is the authentication step. Only a previously registered user can boot the system. The second step is the user input required for defining the zone where the invading drone will land. This is accomplished through the user module.

There are two types of jamming implemented in the system: jamming aimed at the communication link between the drone and the remote controller (typically 2,4 GHz or 5,8 GHz) and jamming aimed at the GPS signals received by the drone (around 1,5 GHz). Spoofing of GPS signals is only possible after jamming GPS signals. Therefore, the third step, which corresponds to jamming, comprises two different phases. In the first phase, jamming is applied to the communication between the drone and the remote controller and to the GPS signals. The second phase occurs in parallel to the spoofing steps and corresponds to jamming the control signal only. Jamming applied to the communication between the drone and the remote controller was not a research objective. The reasons that considered this decision was: first, it is the objective of the system to work for any type of drone or brand. Secondly, the system has no way of knowing what the modulation or signal encoding is. Thirdly, this type of links uses frequency hopping. Because of these reasons it was decided that the technique to use for jamming applied to the communication between the drone and the remote controller was the barrage jamming using the full bandwidth of the signal.

The fourth step consists of identifying the location of the invasive drone. The system determines the location of the system using a set of sensors that are managed using the sensor module. The fifth step is one of the main functions of the system and is the responsibility of the Tx module. In this case, this module starts by emitting spoofing signals targeted at the UAV, enabling the system to gain control over the drone. Finally, the sixth step comprises the generation of activity logs (date, time, signals issued, operator and location) which are sent to the supervisory entity.

3.3. Radio Frequency Interference

Most drones typically operate in one of two modes: the manual piloting mode (controlling the drone with the remote control) and the autonomous mode (previously plotting a route through geographic location coordinates). In both cases, the UAV relies on radio signals. In the case of the UAV being controlled by remote control, radio communications typically at 2,4 GHz or 5,8 GHz are used. When flying autonomously, they resort to GNSS signals. The implemented system can emit efficient signals to block these two types of operation. Since it is difficult to know which flight mode the unauthorized drone is in, the proposed anti-UAV mobile system transmits jamming signals on all frequencies of remote control and GNSS signals.

We conducted a study to understand which was the most effective approach for jamming the GPS signal. Five different techniques of jamming the GPS signal were considered: barrage jamming; tone jamming; sweep jamming; successive pulses jamming; and protocol-aware jamming. The different techniques were implemented and evaluated using low-cost SDR platforms and the GNU radio software development toolkit. The best performing jammer was protocol-aware jamming, which uses an architecture similar to that used by a transmitter of GPS signals. Using this approach, the interfering signal mixes more effectively with the main signal since they exhibit identical spectral behavior, requiring a lower transmitter power to successfully disable the correct reception of the GPS signal.

3.3.1. Barrage Jamming

It is the simplest form of interference and is generally defined as a jammer that transmits noise-like energy throughout the portion of the spectrum occupied by the target, as shown in Figure 3.3 a). It essentially increases the noise level in the receiver, making it difficult to operate the communication system.

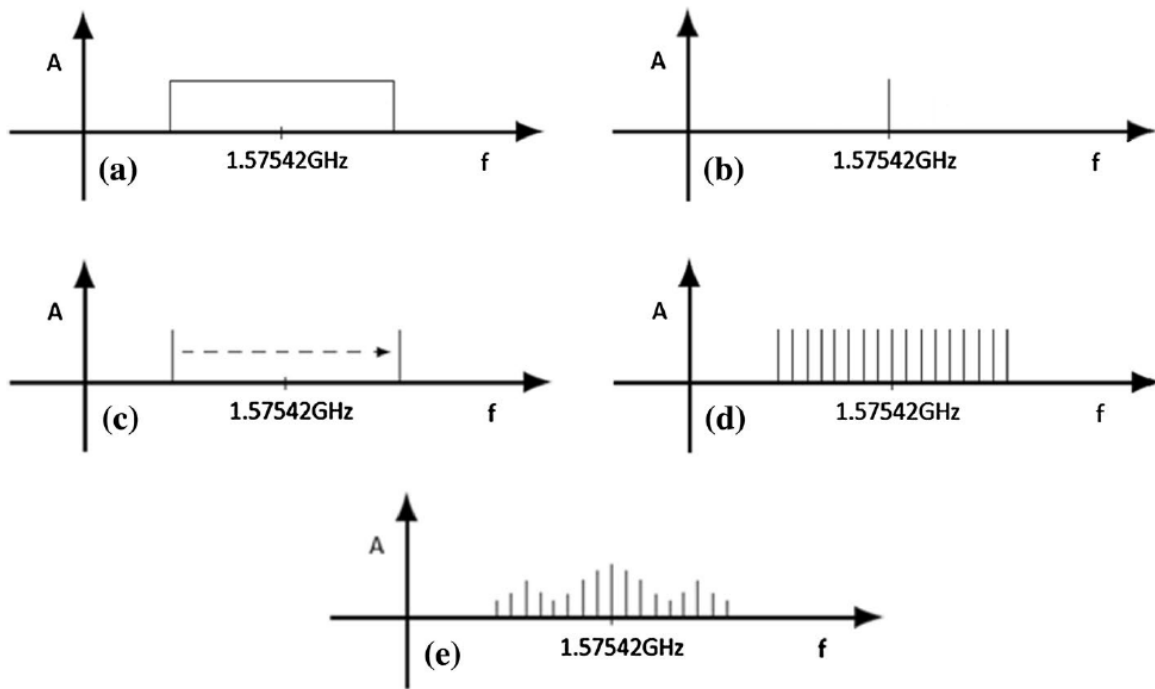


Figure 3.3. **a** Theoretical spectrum of barrage jamming; **b** theoretical spectrum of tone jamming; **c** theoretical spectrum of sweep jamming; **d** theoretical spectrum of successive pulses jamming; **e** theoretical spectrum of protocol-aware jamming

The Barrage Jamming is the best jammer that can be done in the absence of any knowledge of the target signal [56]. Blocking wireless networks can be accomplished by generating continuous noise with a power above the maximum the system supports. The negative side of this approach is the high amount of energy required which contributes to a low energy efficiency. Furthermore, it is not possible to select which signals to be affected in the RF band used. When applying this technique for GPS signal blocking, this last restriction is not an obstacle since what is intended to affect is the entire GPS frequency band.

The construction of the signal to be transmitted was programmed using the GNU Radio toolkit, where Gaussian noise is generated through the Noise Source block (Figure 3.4 (a)) and transmitted over the entire bandwidth of the L1 band GPS signal with a center frequency of 1,57542 GHz and a bandwidth of 14 MHz (Figure 3.4. (b)).

To analyze the power spectral density of the various types of jammers, the receiving antenna is connected for a spectrum analysis on the GNU Radio using the osmocom Source block (Figure 3.4. (c)), connected to the QT GUI Frequency Sink (Figure 3.4. (d)). This setting is possible because BladeRF is a transceiver. This configuration was adopted for all the techniques presented.

The BladeRF has a Variable Gain Amplifier (VGA) in the transmit module, TxVGA1 for BB (Base Band) Gain and TxVGA2 for RF (Radio Frequency) Gain. Generally, TxVGA1 should be increased before TxVGA2. Sliders for these parameters were provided in the GUI via the QT GUI Range block (Figure 3.4. (e)).

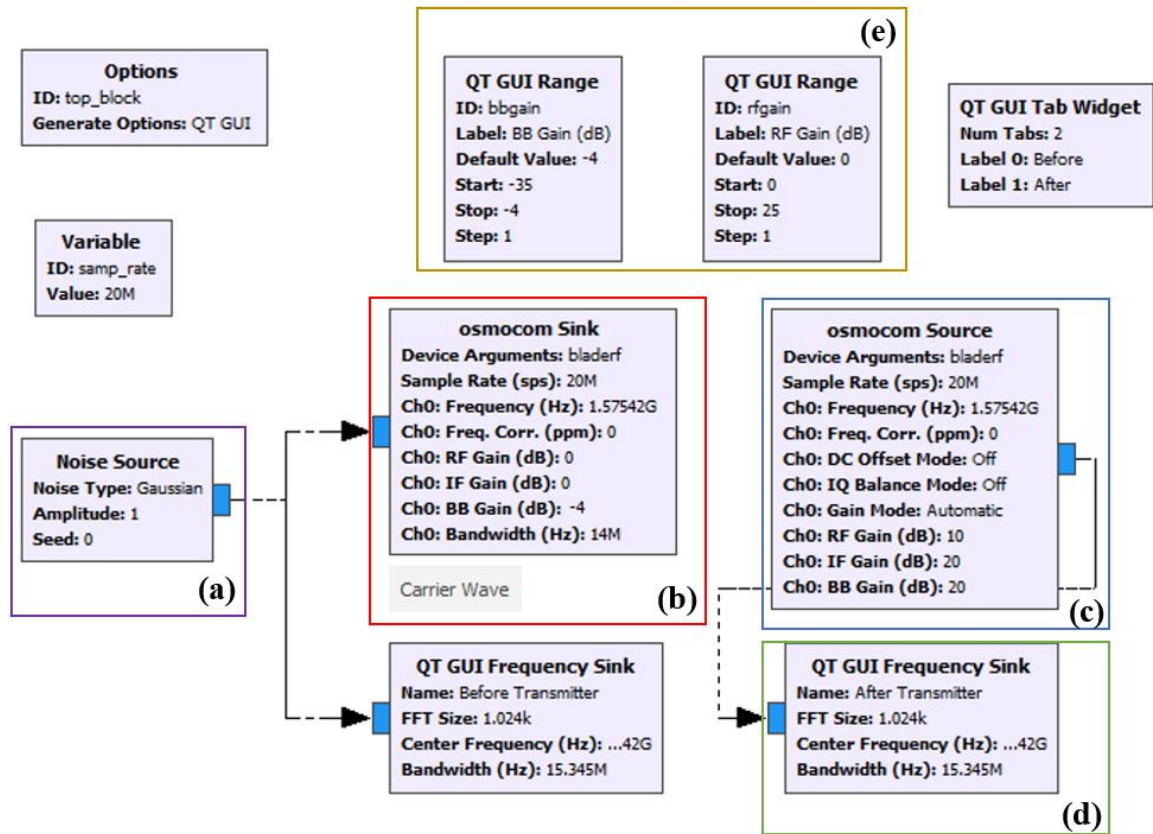


Figure 3.4. Barrage jamming programmed in GNU radio

Using the osmocomb Source block, the block responsible for the reception of the BladeRF, we can analyze the signal interconnecting this block to the QT GUI Frequency Sink to represent the transmitted signal spectrum (Figure 3.5).

The result in terms of spectrum of transmitted signal is the expected one according to theory, with the signal having a bandwidth of 14 MHz and an average power spectral density of -60 dBW/Hz. At the center frequency, there is a maximum peak due to the DC Offset problem. This problem lies in all the techniques presented below.

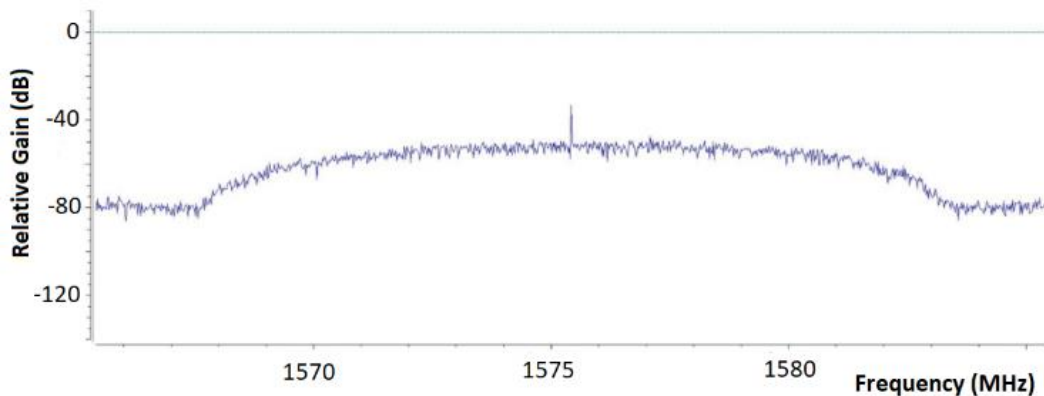


Figure 3.5. Spectrum resulting from barrage jamming

3.3.2. Tone Jamming

In this technique, only a sinusoid is transmitted on the same frequency as the carrier of the GPS signal. This means that the interference is created only at the central frequency and not over the whole bandwidth. Using this technique all energy is applied at the center frequency of the carrier. The spectrum is exemplified in Figure 3.3 b).

The Tone Jamming model was developed in GNU Radio, simply generating a sinusoid using Signal Source block with select cosine in waveform (Figure 3.6 (a)) which is transmitted in the central frequency of the GPS, 1,57542 GHz (Figure 3.6 (b)).

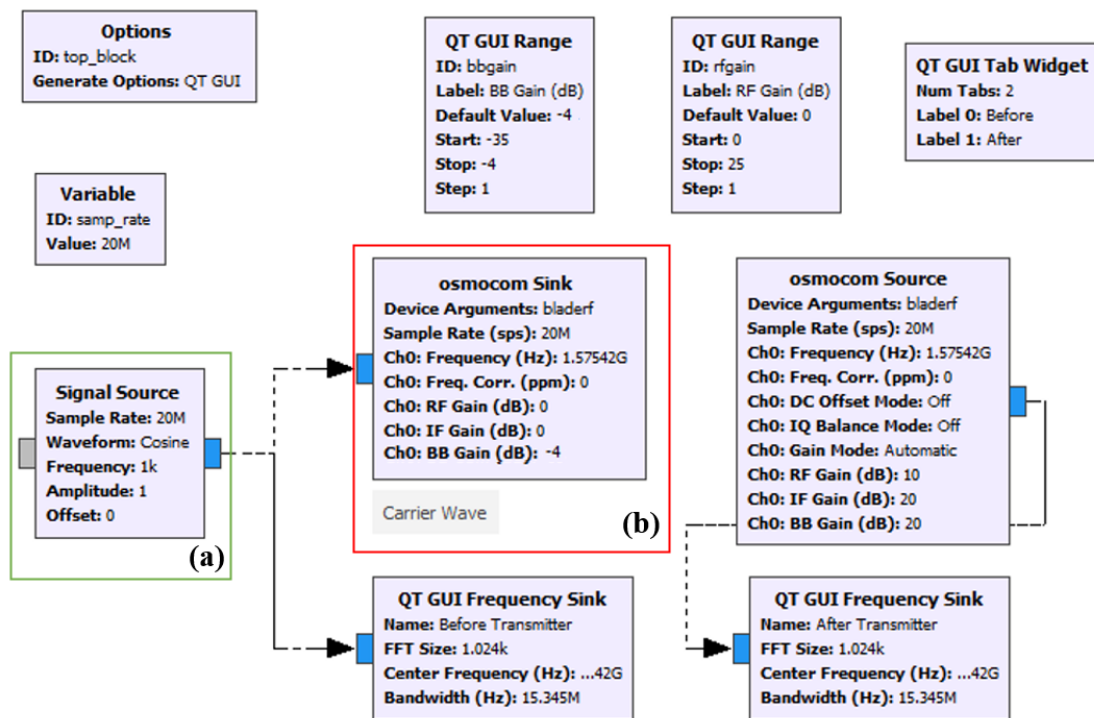


Figure 3.6. Tone jamming programmed in GNU radio

The interference results are shown in Figure 3.7. This jamming signal does not occupy the entire band of the GPS signal which is one of the possible disadvantages since the GPS signal is based on a spread spectrum approach which gives it some robustness against narrowband interference. The average power spectral density of the transmitted signal is -50 dBW/Hz.

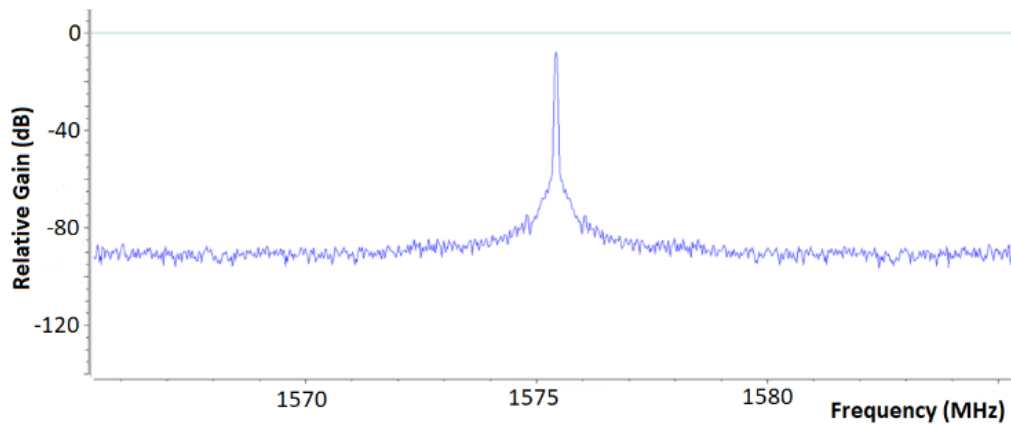


Figure 3.7. Spectrum resulting from tone jamming

3.3.3. Sweep Jamming

It is a technique that tries to replicate a behavior very similar to Barrage Jamming because it operates over the whole frequency band. The difference between these two techniques is that Sweep Jamming does not emit a static signal or a bandwidth of 15,345 MHz. This technique is more efficient with respect to power spectral density since it emits a low bandwidth signal and sweeps the frequency in order to traverse the entire bandwidth of the signal to be interfered with, as shown in Figure 3.3 c). It emits a signal known as Chirp Signal [57].

For the Sweep Jamming technique, it is necessary to create a Chirp Signal, i.e., a signal that increases or decreases its frequency over time. The result at the spectrum level corresponds to the continuous sweep of a range of frequencies. The base construction of the signal to be transmitted was accomplished on GNU Radio according to the flowgraph in Figure 3.8.

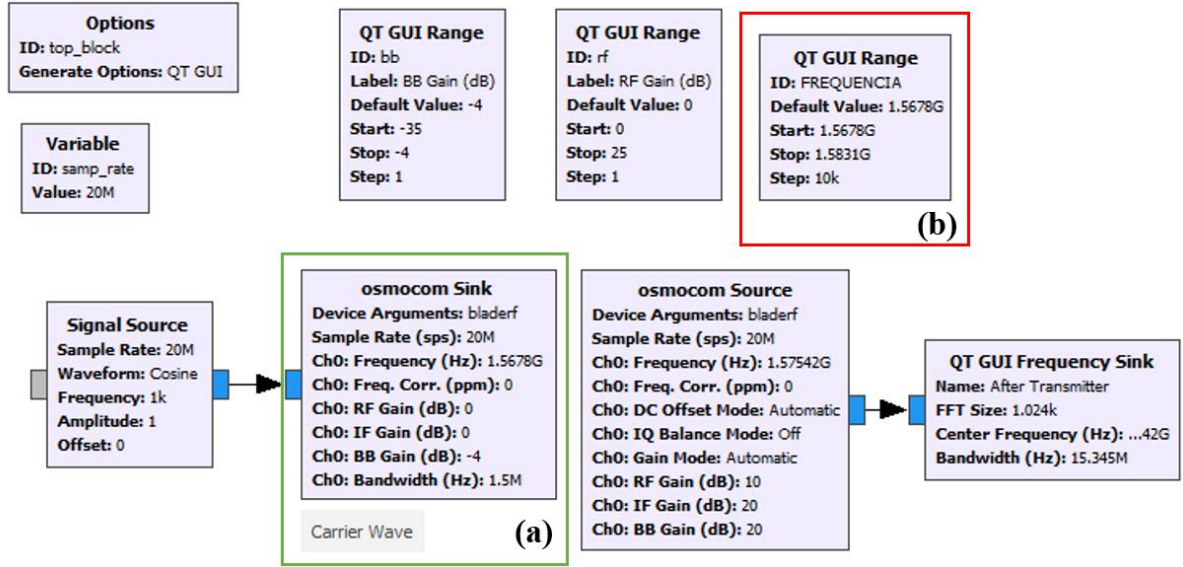


Figure 3.8. Sweep jamming programmed in GNU radio

It is transmitted with the minimum bandwidth supported by the BladeRF, 1,5 MHz (Figure 3.8 (a)). Knowing that the bandwidth of the GPS signal is 15,345 MHz, the frequency varies between 1,5678 and 1,5831 GHz, with 10 kHz jumps (Figure 3.8 (b)) calculated as in Equations 11 and 12.

$$f_{\min} = f_c - \frac{B}{2} \text{ [Hz]} \quad (11)$$

$$f_{\max} = f_c + \frac{B}{2} \text{ [Hz]} \quad (12)$$

The result in the frequency spectrum at a certain moment is shown in Figure 3.9. Using this rapid sweeping approach, it was observed that the transmitted signal has an average power spectral density of – 50 dBW/Hz and an overall bandwidth of 15,3 MHz.

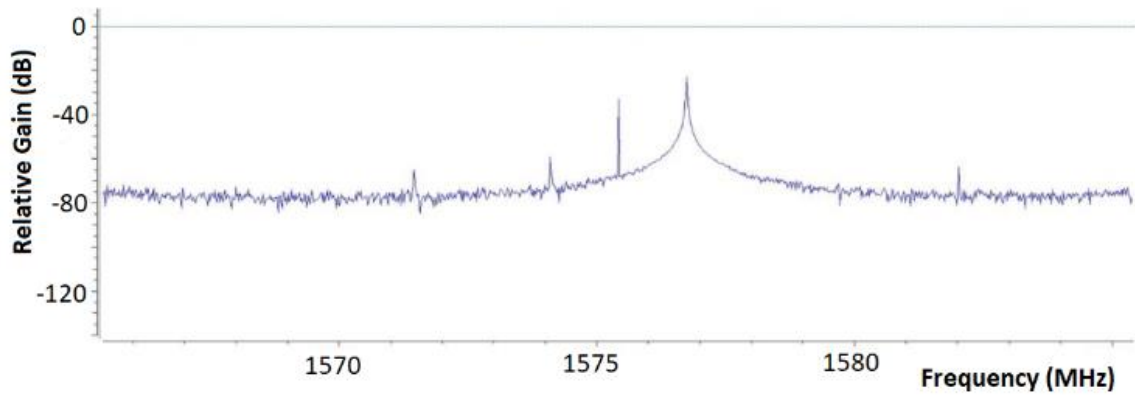


Figure 3.9. Spectrum resulting from sweep jamming

Using the waterfall spectrum from the Sharp SDR tool, Figure 3.10, it can be observed that the BladeRF is constantly transmitting and there are no perceptible jumps in the frequency because of the fast sweeping applied. The analysis of this waterfall is at the carrier frequency, 1575,42 MHz. The waterfall plot shows the variation of the frequency spectrum over time. The received power signal is declared by the color. Using the scale of Figure 3.10 it is possible to analyze the power received in different frequencies, being the color red the higher power and blue the lowest power.

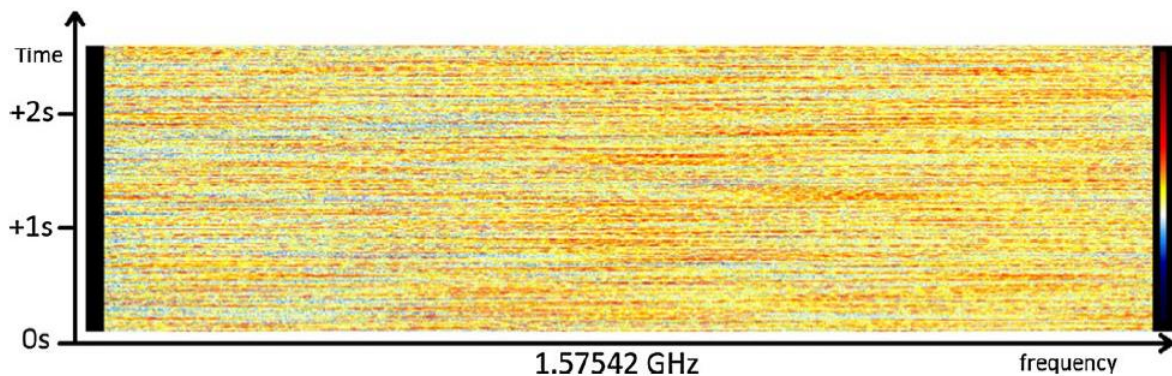


Figure 3.10. Waterfall analysis of sweep jamming (screenshot obtained from the sharp SDR software)

3.3.4. Successive Pulses Jamming

This approach consists in the generation of a sequence of pulses in time with low duty cycle. By using this technique, the jamming of the carrier wave frequency can be accomplished due to the resulting spectrum of the interfering signal, which is shown in Figure 3.3 d). The signal occupies the desired band with peaks located at multiples of the frequency of the corresponding pulse sequence.

This technique consists of sending a sequence of pulses with low duty cycle, on the GPS signal frequency 1,57542 GHz, occupying all its bandwidth, 14 MHz. It was implemented using the flow graph of Figure 3.11.

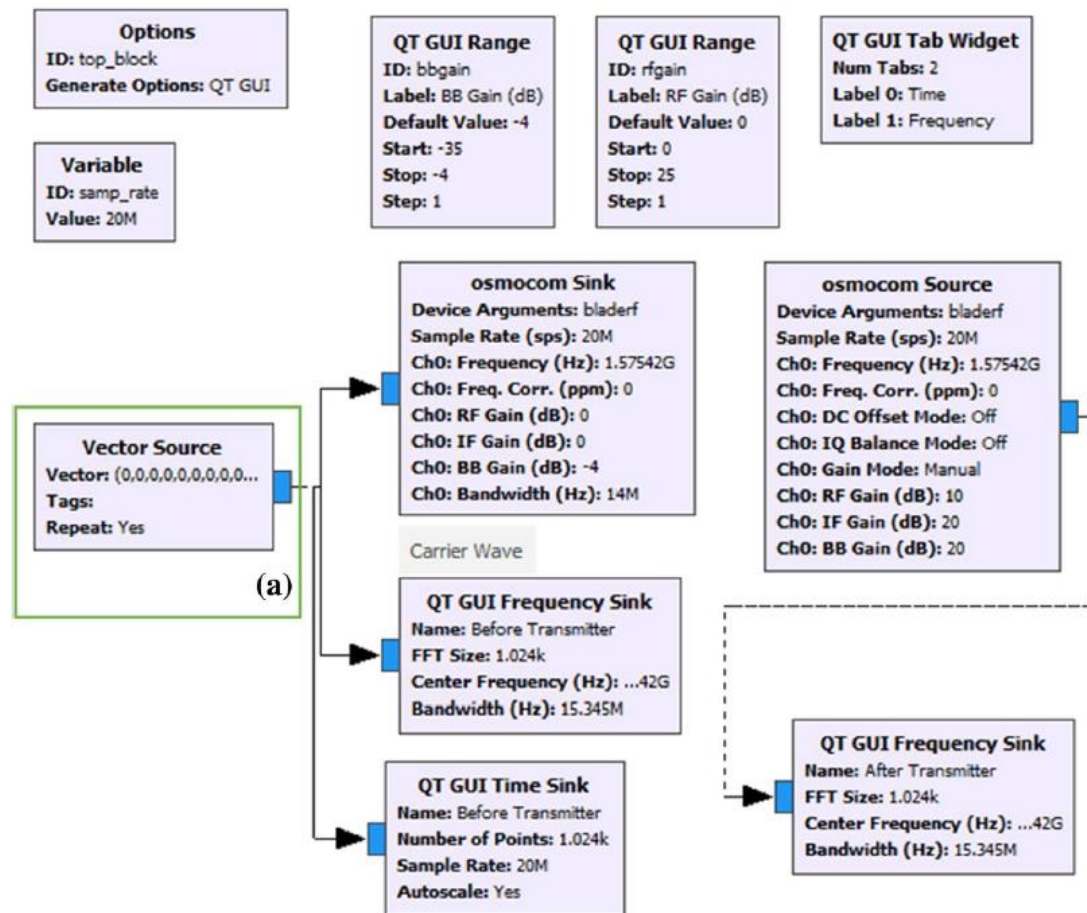


Figure 3.11. Successive pulses jamming programmed in GNU radio

[illegible]

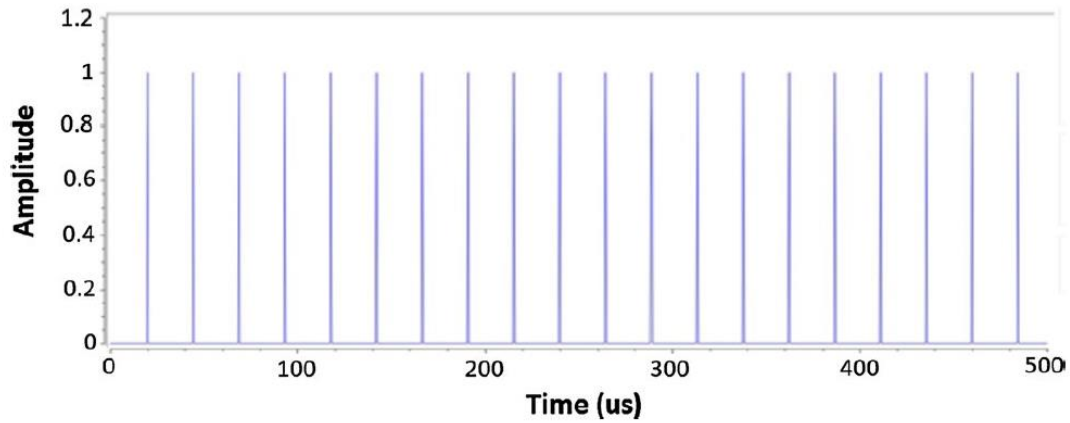


Figure 3.12. Impulses in time with low duty cycle

The spectrum of the transmitted signal is shown in Figure 3.13. Although the Successive Pulse Jamming technique takes up the full bandwidth of the GPS signal, it does not do it uniformly which may decrease its efficiency as a jammer. The average power spectral density of the transmitted signal is about -70 dBW/Hz, a little lower than the others.

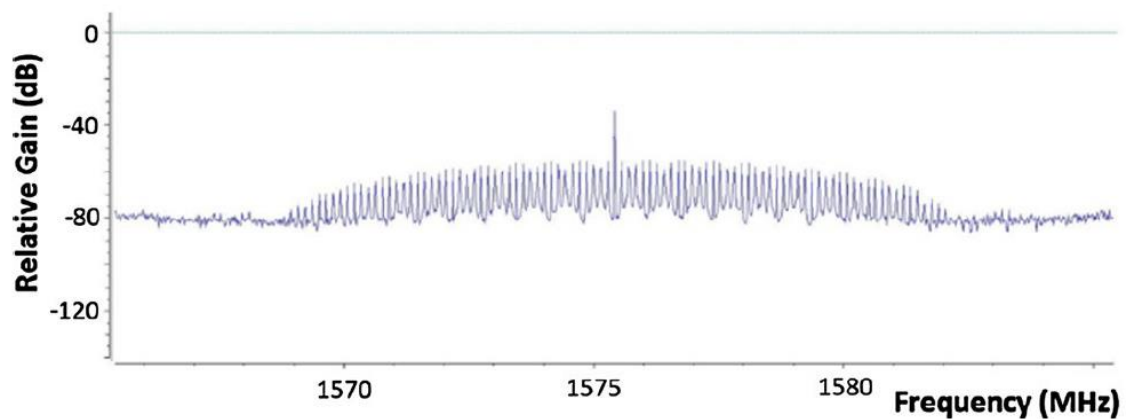


Figure 3.13. Spectrum resulting from successive pulses jamming

3.3.5. Protocol-Aware Jamming

The last interference technique presented is protocol-aware congestion. The feasibility of using protocol-aware jammers has been studied in IEEE 802.11-based wireless LAN communication systems. It was concluded that these can reach interference with very low energy requirements and low probability of protocol detection [58] [59]. Protocol-aware jammers also prevent interference with other communication systems operating on the same RF band. In this type of approach, it is a common practice to use a jammer with an architecture similar to that used by

the emitter of the target signal. In this way, the interfering signal mixes with the target signal using a similar spectrum to destroy the information thereof or otherwise make its reception virtually impossible at the receiver.

During the construction of the interference signal, the signal modulation (BPSK), the data rate (sample rate = 1,023 MHz) and the channel bandwidth (15,345 MHz) are considered. The resulting spectrum is illustrated in Figure 3.3 e). This technique is the one that results in a spectrum closer to the spectrum of real GPS signals.

The composition of the signal to be transmitted is represented in Figure 3.14 beginning by creating a random source of bits which are converted to float by applying the block UChar To Float (Figure 3.14 (a)). To map the '0's and '1's to -1 and 1 , respectively, there is a block that multiplies the sequence by 2 followed by an addition of -1 (Figure 3.14 (b)). It is only possible to transmit the signal if it is converted to a sequence of complex valued samples (Figure 3.14 (c)), since the osmocomb Sink block receives only complex values (this is the block responsible for interfacing with transmitter of the BladeRF board). The real part of the complex sequence carries the modulated signal (Figure 3.14 (b)) while the imaginary part is zero, the GPS signal L1 is not represented with a quadrature signal (Figure 3.14 (d)).

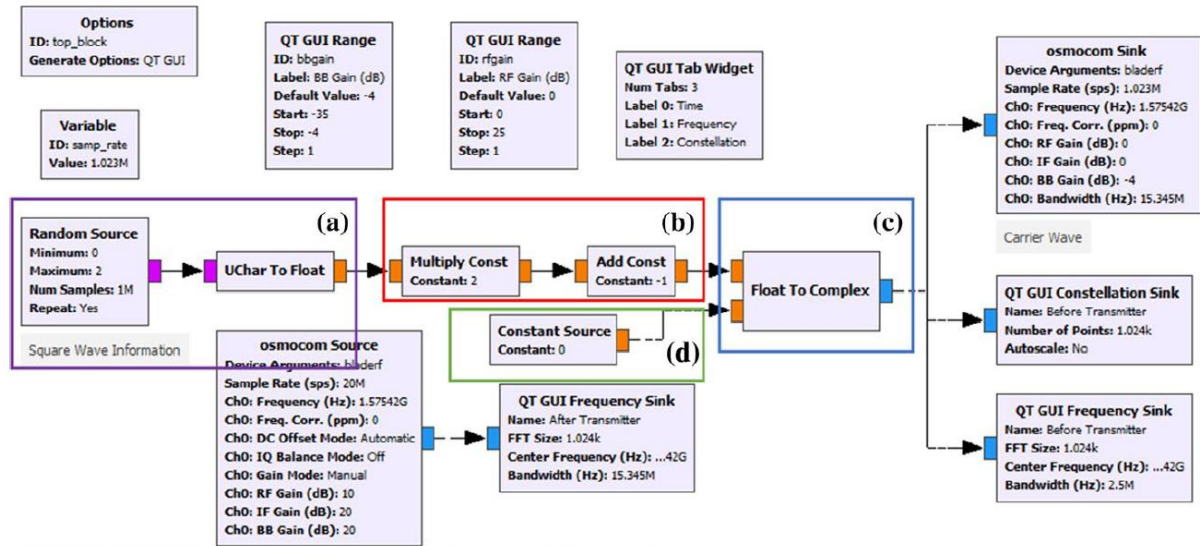


Figure 3.14. Protocol-Aware jamming programmed in GNU radio

The result of the BPSK modulated wave at the receiver, i.e., the jammer signal received with Additive White Gaussian Noise (AWGN), is shown in Figure 3.15.

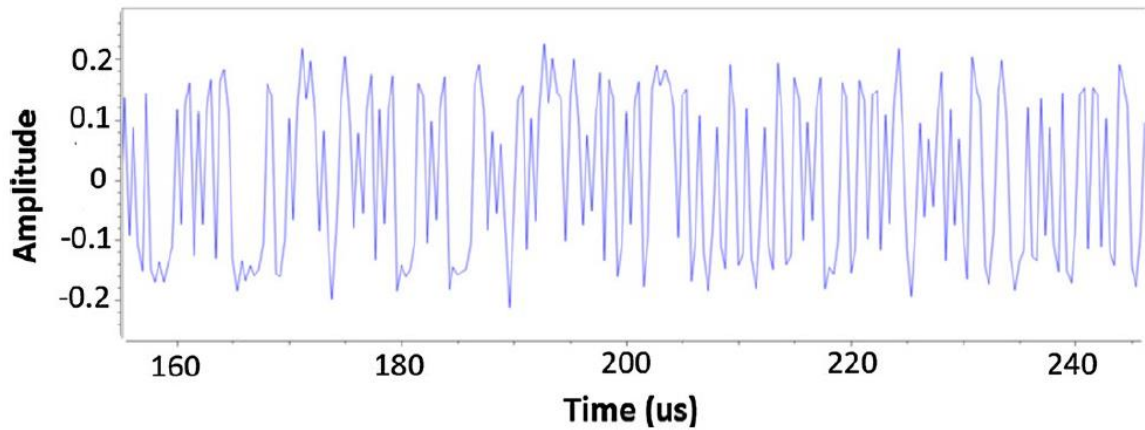


Figure 3.15. Received protocol-aware jamming signal in time

The corresponding frequency spectrum is shown in Figure 3.16. The average power spectral density of the transmitted signal is -60 dBW/Hz. It can be seen that it occupies the intended band with a shape similar to the GPS spectrum (i.e., stronger in the areas of the spectrum where the GPS signal is also stronger).

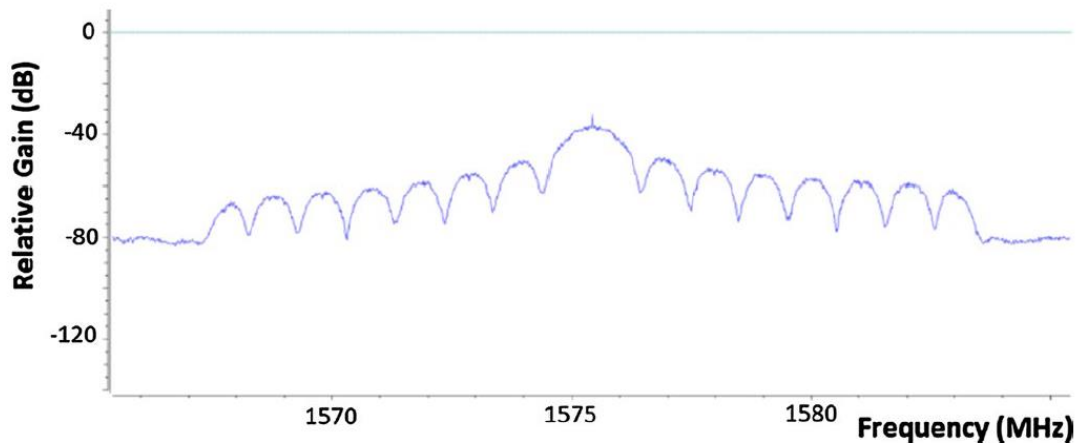


Figure 3.16. Spectrum resulting from protocol-aware jamming

Another solution for implementing this type of jammer is to transmit a copy of a real GPS signal. We tested this approach resorting to a GPS signal simulator and using a message with a nonexistent location. The simulator used is GPS-SDR-SIM¹ that generates GPS baseband signal data streams, which can be converted into RF using Software Defined Radio (SDR) platforms such as ADALM-Pluto, BladeRF, HackRF and USRP.

¹ <https://github.com/osqzss/gps-sdr-sim>.

The message is created through a.txt file and is based on other messages created by the simulator and then adapted to the situation in question. Example of a.txt message line:

```
$GPGGA,122455.00,9845.59709719,N,18924.22292476,W,1,24,0.9,100,M,-21.3213,M,*7C
```

The underlined digits are the coordinates of a point that does not exist on the planet Earth and so it is possible to shuffle the GPS receiver, translating into a GPS jammer signal. The resulting spectrum is shown in Figure 3.17, where it is visible that it resembles the one previously created (Figure 3.16). The average power spectral density is slightly less than -60 dBW/Hz.

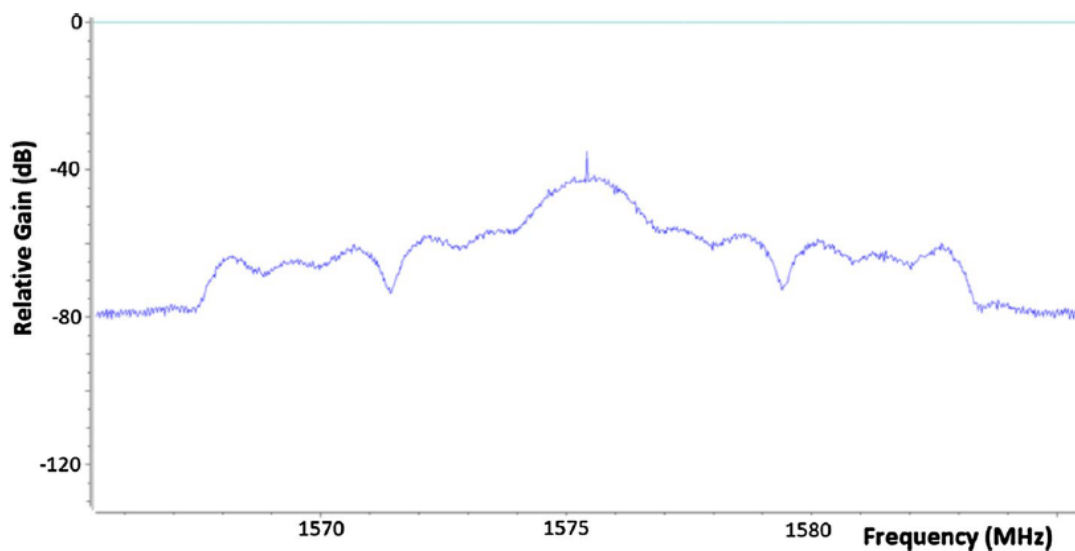


Figure 3.17. Spectrum resulting from protocol-aware jamming 2

3.4. Mobile Spoofing System

In this section is presented how UAV location is determined and how the UAV is diverted.

3.4.1. UAV Location Determination

There are already several systems that can detect invading drones through a radar (e.g. radar implemented at airports). These radars could be the first devices to identify the invading drone, as they work autonomously. However, there must be a complementarity/cooperation of both systems (localization and anti-UAV techniques). To determine the exact location of the UAV, the implemented system integrates three sensors and a receiver.

The Figure 3.18 illustrates how the estimation of the position of the intruder drone is carried out. The LIDAR Lite v3 [60] is responsible for measuring the distance to the UAV, which is marked as d) in the Figure 3.18. We can draw a right triangle between the system and the drone, as is visible in Figure 3.18. Through the 3D accelerometer MPU6050 [61], which is used for tilt/pitch measurements, it is possible to determine the angle p). With the angle p) and the distance d); using simple trigonometry, it is possible to determine the distance between the drone and the system in relation to the earth plane. Finally, using the e-compass LSM303D [62], which is responsible for measuring the system orientation, m), we can obtain the direction of the drone. By combining the information obtained from this set of sensors with the known location of the system itself, it is then possible to determine the location of the UAV [35]. Note that the system position is estimated through the GPS signal receiver [63].

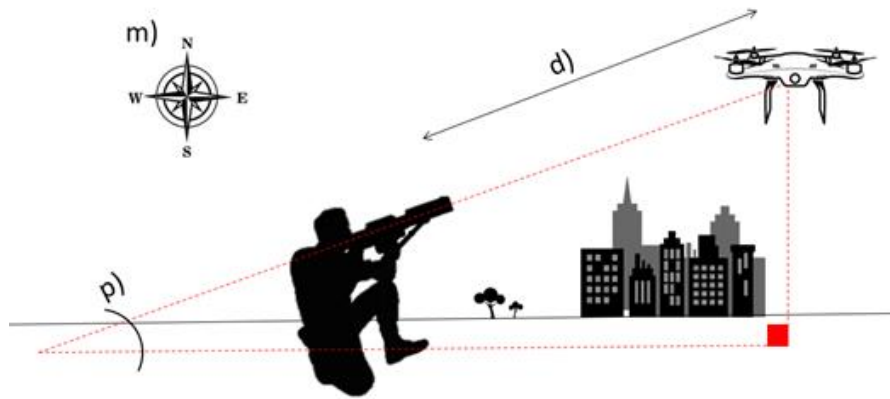


Figure 3.18. UAV localization method

3.4.2. Deviation of UAV

Spoofing, in general, is a fraudulent or malicious practice in which communication is sent from an unknown source, disguised as a source known to the receiver. The use of spoofing is more common in mechanisms and communication networks that do not have a high level of security. In the civil GPS signal, there is not any type of encryption or authentication to protect or to prove that the signal comes from a reliable source or the non-occurrence of repudiation of the signal. Thus, to accomplish spoofing and deceive a GPS receiver, one can simulate GPS signals as if they are coming from real satellites.

The spoofing developed in this system is based on our previous study [35], which considered an open hardware electronic prototype platform, sensors, an SDR module and a

system on chip (SoC) as the central processor of the system. The adopted approach used a simple spoofing technique, which could generate and transmit false GPS signals.

The indirect acquisition of the drone control is carried out through the use of the ephemeris files, provided that they allow the simulation of a set of satellites, thus, forming a hypothetical constellation, which subsequently generates baseband signal data streams that are transmitted in the frequency range of the satellite location system. The system was designed with two spoofing modes of operation, one that worked by taking into account only the drone's location, and another, which took into account not only the location but also the direction and speed. Using these parameters, it is possible to implement and apply the spoofing more smoothly and less noticeably to the target. In [35], the spoofing functionalities were studied and tested on different GPS receivers such as smartphones, u-blox M8 GNSS Evaluation Kit, and u-blox MAX-7Q. We gave more focus to testing the spoofing functionality integrated into the complete anti-UAV system and targeted at the GNSS receivers in UAVs.

In our implementation, a spoofing trajectory can be specified in either a CSV file, which contains the Earth-centered, Earth-fixed (ECEF) user positions, or an NMEA GGA directly from the command line. First, the user specifies the GPS satellite constellation through a GPS broadcast ephemeris file. The daily GPS broadcast ephemeris file (brdc) is a merge of the individual site navigation files into one (the archive for the daily file can be downloaded from <https://cddis.nasa.gov/archive/gnss/data/daily/> accessed on 10 January 2022). These files are then used to generate the simulated pseudorange and Doppler for the GPS satellites in view. This simulated range data is then used to generate the digitized I/Q samples for the GPS signal. As an example of a static mode transmission via the command line we can execute

```
> gps-sdr-sim -e brdc0250.22n -l 38.747839, -9.153623,100
```

In this command line, option `-e <gps_nav>` denotes RINEX navigation file for GPS ephemerides (required), `brdc0250.22n` is the filename and `-l <location>` is used for providing latitude, longitude and height coordinates (static mode). This command creates a `.bin` file corresponding to the simulated GPS signal file, named “`gpssim.bin`”, which can be loaded into the bladeRF board for playback as exemplified below:

```
> set frequency 1575.42M
> set samplerate 2.6M
> set bandwidth 2.5M
> set txvga1 -25
> cal lms
> cal dc tx
> tx config file=gpssim.bin format=bin
> tx start
```

After executing the 'tx start' command, BladeRF starts the transmission and will be able to deceive the target receiver.

[This page is deliberately left blank.]

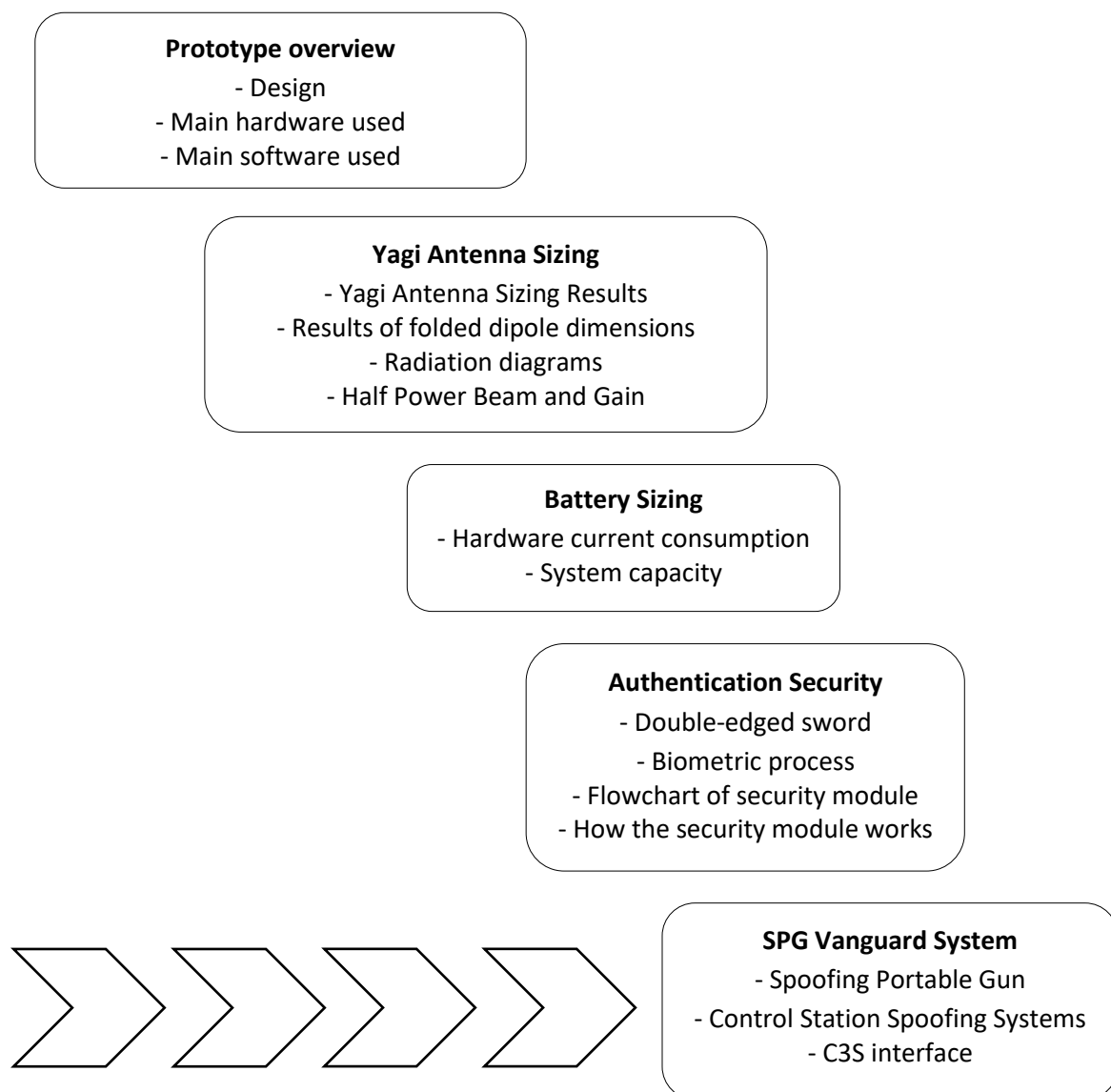
CHAPTER

4. Prototype System

In this chapter we applied our learning system methodology to create a prototype. The chapter begins with the study to produce the Yagi-Uda antenna for the GPS frequency. The battery was dimensioned for the system, considering the consumption of each component. For safety reasons it was felt the need to restrict the use of the system developed.

4.1. Introduction to Prototype System

The chart schematizes what is discussed in chapter 4 in a more perceptible way. The Prototype overview section presents the version 1 of System Anti-UAs prototype. The Yagi-Uda Antenna Sizing section describes how the directive antenna was planned and developed. The Battery Sizing section provides a forecast of system consumption and system capacity. The Authentication Security describes the authentication and data submission system. The SPG Vanguard System section presents the two Minimum Viable Product (MVPs) resulting from several iterations.



4.2. Prototype Overview

The objective of this work was to build a final prototype of an anti-UAV system, which should be portable and easily manageable by an operator.

The design of the implemented prototype is shown in Figure 4.1. The main hardware supports the implementation of three distinct modules, which were introduced Figure 3.1. The processor module, which is the brain of the entire system being responsible for all interconnecting sensors/actuators, is implemented using a raspberry pi 3 board. A microcontroller which is part of two different modules, the sensor module, and the security module, is implemented using an Arduino uno (AtMega329p microcontroller). It has the functionality of collecting and processing all the information coming from the sensors. The Tx module is responsible for transmitting jamming and spoofing signals and is implemented on a software defined radio platform, namely, the BladeRF x40.



Figure 4.1. System Anti-UAVs version 1

To create and transmit the jamming signals, the GNU radio toolbox was used [34], whereas the spoofing signals are generated resorting to the simulator GPS-SDR-SIM available on GitHub [35].

4.3. Yagi Antenna Sizing

To minimize interference with GPS receivers in the vicinity of the target UAV, there was the need for implementing a directive antenna. With a smaller transmission beam, it is possible to direct the signal to the target and, thereby, to increase the power of the signal in that direction while reducing unwanted interference. The Yagi-Uda antenna is a high-power antenna that can be used to transmit signals over relatively long distances, as well as to pick up weak signals. In wireless networks, Yagi antennas are the ones that offer the longest range, but they can only cover a small area where they are aimed. For the Yagi antenna design, a Yagi Calculator-VK5DJ simulator developed by John Drew [64] was used. Yagi Calculator-VK5DJ is a program whose purpose is to produce dimensions for a DL6WU style Yagi antenna. It is designed for frequencies between 144 MHz and 2,4 GHz.

The Yagi DL6WU model is easy to build and with very positive results. For a frequency of 1575,42 MHz and with simulator recommendation to use a minimum of eight directors, the results of the antenna dimensions are expressed in Figure 4.2a. The simulator also presents in its results the dimensions of the folded dipole in Figure 4.2b.

VK5DJ's YAGI CALCULATOR

Yagi design frequency =1575,42 MHz
Wavelength =190 mm
Parasitic elements contacting a square section metal boom 15 mm across:
Folded dipole mounted same as directors and reflector
Director/reflector diam =4 mm
Radiator diam =4 mm

REFLECTOR
103,4 mm long at boom position = 30 mm (IT = 44,0 mm)

RADIATOR
Single dipole 97,0 mm tip to tip, spaced 38 mm from reflector at boom posn 68 mm (IT = 36,0 mm)
Folded dipole 100,8 mm tip to tip, spaced 38 mm from reflector at boom posn 68 mm (IT = 43,0 mm)

DIRECTORS

Dir (no.)	Length (mm)	Spaced (mm)	Boom position (mm)	IT (mm)	Gain (dBd)	Gain (dBi)
1	89,4	14,3	82,3	37,0	4,8	6,3
2	88,2	34,3	116,6	36,5	6,5	8,6
3	87,1	40,9	157,5	36,0	7,8	9,9
4	86,1	47,6	205,1	35,5	8,9	11,0
5	85,2	53,3	258,4	35,0	9,8	11,9
6	84,3	57,1	315,4	34,5	10,5	12,7
7	83,5	59,9	375,4	34,0	11,2	13,3
8	82,8	62,8	438,2	34,0	11,7	13,9
9	82,1	65,7	503,9	33,5	12,2	14,4
10	81,5	68,5	572,3	33,0	12,7	14,9
11	80,9	71,4	643,7	33,0	13,1	15,3
12	80,3	73,3	717,0	32,5	13,5	15,7
13	79,8	74,2	791,2	32,5	13,8	16,0
14	79,4	75,2	866,3	32,0	14,2	16,3
15	78,9	76,1	942,5	32,0	14,5	16,6

(a)

COMMENTS

The abbreviation "IT" means "Insert To", it is the construction distance from the element tip to the edge of the boom for through boom mounting

Spacings measured centre to centre from previous element
Tolerance for element lengths is +/- 1 mm

Boom position is the mounting point for each element as measured from the rear of the boom and includes the 30 mm overhang. The total boom length is 972 mm including two overhangs of 30 mm

The beam's estimated 3dB beamwidth is 30 deg

FOLDED DIPOLE CONSTRUCTION

Measurements are taken from the inside of bends
Folded dipole length measured tip to tip = 101mm
Total rod length =202mm
Centre of rod=101mm
Distance BC=CD=48mm
Distance HI=GF=46mm
Distance HA=GE=50mm
Distance HB=GD=53mm
Distance HC=GC=101mm
Gap at HG=4mm
Bend diameter BI=DF=4mm

If the folded dipole is considered as a flat plane (see ARRL Antenna Handbook) then its resonant frequency is 1408,4MHz and K is 0,947

MATERIALS GUIDE for purchase. Allow extra, do NOT use these figures for cutting
NO allowance for saw cuts or purchased lengths resulting in waste
1) Length used by directors and reflector 1353mm of round 4mm rod
2) Length used by single dipole 87mm or folded dipole 202mm of round 4mm rod
3) Length used for boom 972mm (allows for 30mm each end) square section 15mm

(b)

Figure 4.2. Results of a VK5DJ's Yagi Calculator.

(a) Yagi Antenna Sizing Results; (b) Results of folded dipole dimensions.

The simulator also calculates the antenna gain, which was 14,8 dB with approximately 29° beamwidth for both planes (vertical and horizontal).

The result of the handmade Yagi antenna, respecting the dimensions provided by the simulator, is shown in Figure 4.3.



Figure 4.3. Handmade Yagi Antenna

As shown in Figure 4.4, the radiation diagrams of the handmade Yagi antenna were obtained for the XY (a) and YZ (b) planes. Spectral power density was measured with the RTL SDR 820T2 with five degrees spacing. The blue line represents the measured values. The red line represents the trendline.

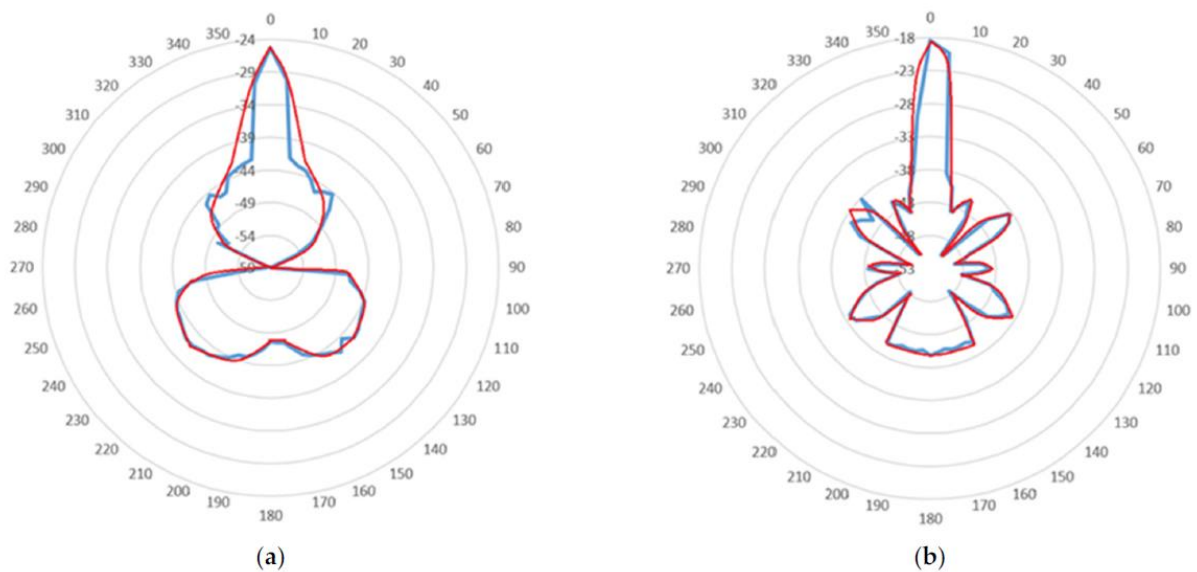


*Figure 4.4. Radiation diagrams of the handmade Yagi antenna
(a) XY plane radiation diagram; (b) YZ plane radiation diagram.*

It is important to note that the conditions (open field) under which measurements were taken to draw the diagrams were not ideal. For the results to be more assertive, measurements should have been made in an anechoic chamber to avoid reflections that influence the intended results.

The angular distance between half power points is defined as the beamwidth [65]. The beam width in both planes XY, Figure 4.4a; and YZ, Figure 4.4b, corresponds to a beam width of about 5 degrees for both cases.

To calculate the antenna gain, it is necessary to use the free space propagation model (Equation (13)), since the radiation diagrams presented refer to the received powers.

$$P_{Rx} = P_{Tx} \left(\frac{c}{4\pi df} \right)^2 \cdot G_{Tx} \cdot G_{Rx} \quad (13)$$

As P_{Rx} should be equal in both planes, for the purpose of calculations, an average of the two measured values was taken, resulting in P_{Rx} -21,5 dBW. Using the equation (14) we can determine the transmission gain as 18,72 dB.

$$G_{Tx} = \frac{P_{Rx}}{P_{Tx} \left(\frac{c}{4\pi df} \right)^2 \cdot G_{Rx}} \quad (14)$$

The signal emitted through GNU radio for measuring the values had a transmission gain of -4dB, so the actual antenna gain is 14,72 dBi:

$$G_{antenna}[dBi] = G_{Tx}[dB] + G_{TxGNUradio}[dB] \quad (15)$$

The Table 4.1 compares the resulting simulator values with the measured values.

Table 4.1 - Spectral power density of different jammers

	Half Power Beam Width [°]	Antenna Gain [dBi]
Simulator Values	29	14,8
Real Values	5	14,7

The results obtained through the simulator, compared to the experimental values, were slightly different regarding the half power beam width, which translates into the antenna directivity. In this case, a more directive antenna than expected was obtained. Values may differ due to fabrication imperfections and due to measurement conditions,

which were not perfect. Regarding antenna gain, the result was very close to the expected one.

A low-cost amplifier SPF5889Z was used as we can see in Figure 4.5. It is important to note that, while not being the ideal power amplifier, it was sufficiently capable for the outlined objective. According to the specifications, the SPF5189Z possesses a gain of 17,9 dB of at 1000 MHz and 13,8 dB at 1700 MHz.

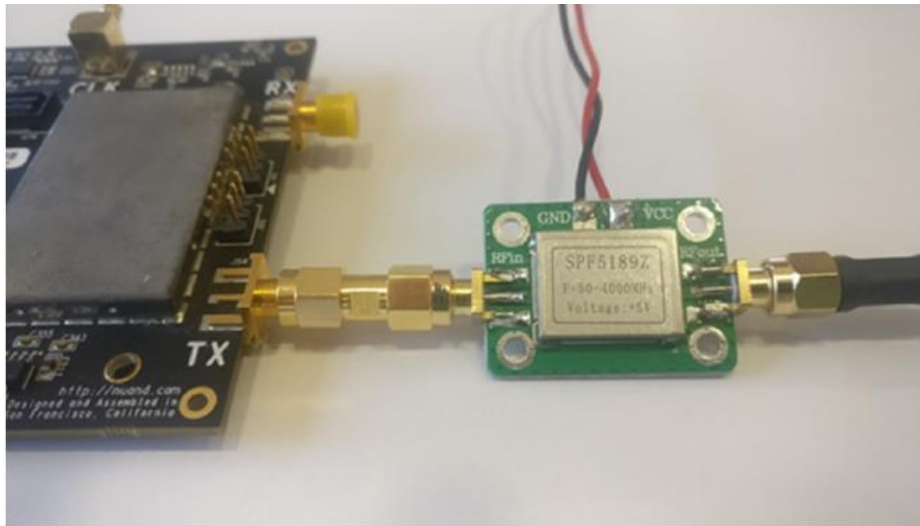


Figure 4.5. Power amplifier SPF5189Z.

4.4. Battery Sizing

As the objective was to implement a mobile anti-UAV system, it is necessary to perform the sizing of the battery to be adopted.

Considering that the adopted Raspberry Pi 3, Arduino Uno and BladeRF work with a voltage of about 5 V, the power supply module was designed so as to supply the same voltage to all those boards. The BladeRF, which was used for generating the jamming and spoofing signals, according to Nuand's official specifications, possesses a maximum consumption of 4,5 W. To increase the transmitted power, we also adopted a Nuand XB-300 board. The Nuand XB-300 is an amplifier expansion card that greatly increases the range of the BladeRF. On the receive side, the XB-300 featured a low-noise amplifier (LNA) and a combiner for antenna diversity. The transmit side featured a power amplifier (PA), TRX switch, and a highly accurate ADC for measuring output power of the PA. The PA exhibited a typical gain of 20 dB at 2,45 GHz with a bandwidth of 100 MHz (2,4-2,5 GHz). The BladeRF, combined with the XB-300 module with Tx ON and Rx OFF,

exhibited a consumption of 10W; consumptions available from the official Nuand specifications.

Total instantaneous current consumption was 3,74 A. In Table 4.2, we summarize the hardware consumption.

Table 4.2 - Hardware current consumption

Hardware	Electric current [A]
BladeRF x40	0,73
BladeRF x40 + xb300	1,72
Arduino Uno	0,05
Raspberry Pi 3	0,24
Power Amplifier (SPF5189Z) ($\approx 1,5$ GHz)	1
Total	3,74

If we assume a hypothetical military scenario where a soldier works an 8 h shift and the battery is intended to be able to power the system about 20% of the shift time (1,6 h), then we can estimate the required capacity at about 6 hours.

4.5. Authentication Security

Technology has the possibility of being used for evil purposes. For this reason, it was felt the need to restrict the use of the system developed for safety. Only previously authorized users can use the system, being monitored who initialized, or transmitted jamming or spoofing signals. Due to the space limitations in system implementation, the authentication factor has to be compact, small and lightweight. Biometric sensor, fingerprint scanner - TTL (GT-521F32), has been chosen as the authentication factor.

A fingerprint scanner primarily converts biometric information, i.e., the surface or subsurface of the skin of a finger, into a digital signal, typically a digital image. In practice, this conversion process can never be perfect. The persistent and largely invariant part of the imperfections induced by the fingerprint scanner in this process is called the scanner pattern. The variations of the process parameters in semiconductors are indirect evidence of the existence of the sweep pattern [66].

The biometric process has four distinct steps (Figure 4.6): scan, extraction, pattern creation, and comparison. Fingerprint readers can use different technologies to capture the unique characteristics that exist in prints. The most common fingerprint reader is the

optical reader, which uses lenses to reflect light on complementary metal oxide semiconductor sensors, which then convert light into electronic signals. Other readers capture impressions using capacitive sensors. The grooves and valleys of the fingerprints create different electric currents in different areas of the finger. Each of the ridges and valleys of its finger act as insulators, restricting the flow of current produced by the reader [67].

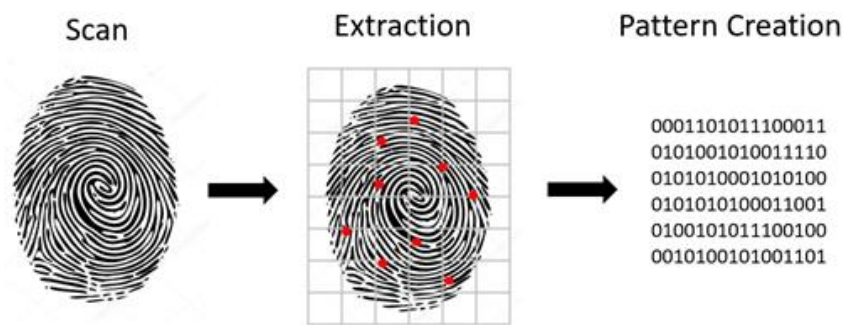


Figure 4.6. Biometric process (scan, extraction and pattern creation)

Once these details are stored, whenever the fingerprint is scanned the identity can be authenticated. To build a complete and more accurate fingerprint image, the scanner often asks to take multiple prints from the same finger.

As a means of preventing and enhancing system security through mobile network communication, the system sends periodically (configurable time) message with the location information of the system to a supervisory entity. In addition, whenever someone initializes the system or initiates the transmission, a message with the respective username is also sent. For the communication with a supervisory entity, later identified, a shield was used for Arduino SIM900 that allows the sending of SMS. This shield features Global System for Mobile (GSM) Communications and General Packet Radio Service (GPRS) technologies with which you can make a connection, send and receive text messages and even use the internet from a SIM card (Subscriber Identity Module).

This shield is Quad-Band and works on the following frequencies: EGSM 900MHz / DCS 1800MHz and GSM850 MHz / PCS 1900MHz. It is not necessary to change the frequency band to work. It is configured in All Band mode which makes it work anywhere in the world. This GSM / GPRS module is programmed through AT commands (GSM07.07, 07.05 and SimCom). The shield also includes a high-gain onboard antenna and uses a SimCom SIM900 chip.

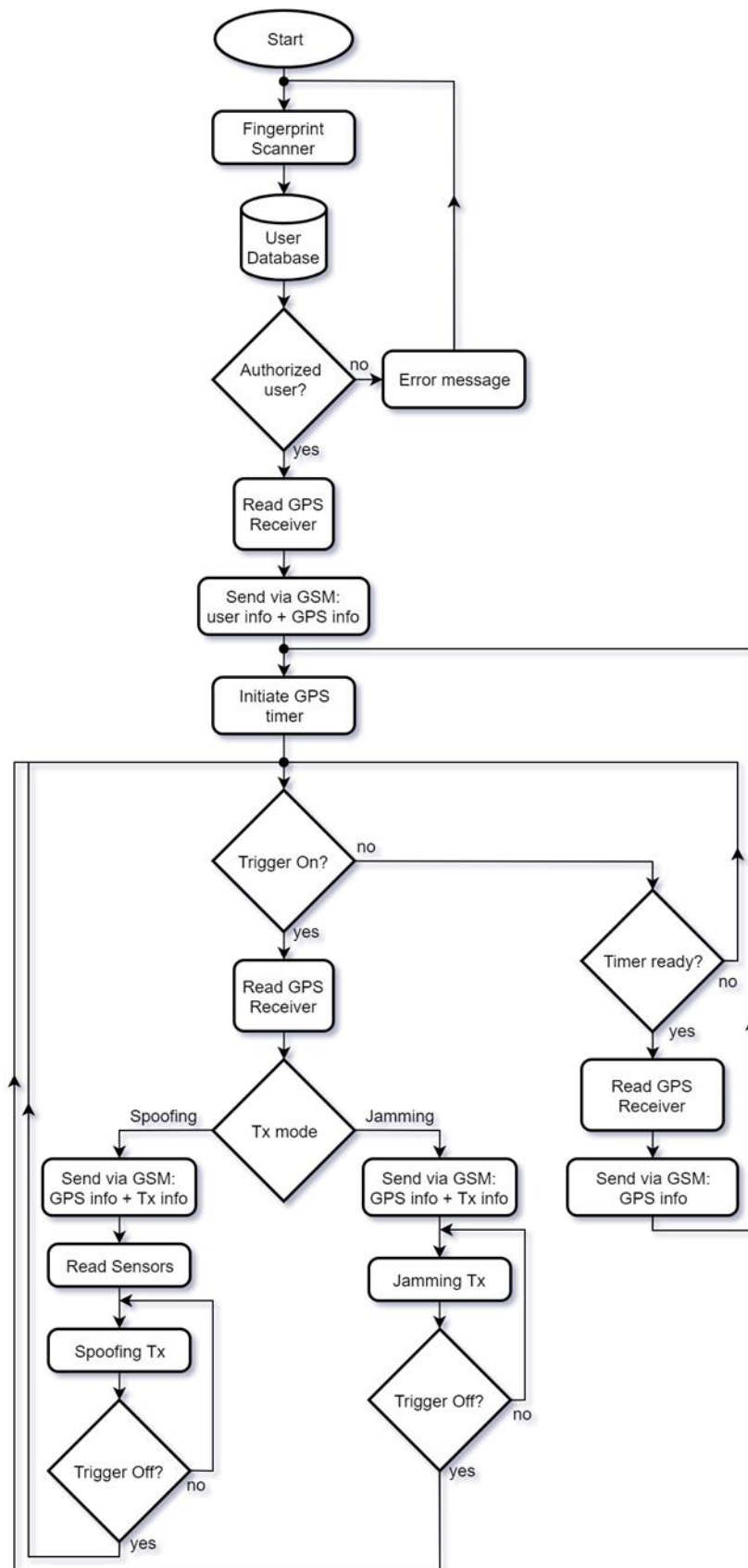


Figure 4.7. Flowchart of the general functioning of the security system

Figure 4.7 shows a block diagram of the general functioning of the system security, which is then reported in stages.

First step: Scan your finger on the biometric sensor; Second step: Use the database, where all registered users are located; Third step: Compare if the user is registered in the system. If there is no registration, alert the user with a message of misuse; Fourth step: Register the current location of the system, through the GPS receiver; Fifth step: Send a message with the name of the user who accessed the system, location and date/time of the current moment; Sixth step: Initialize the timer and send the periodic message that contains the system location information; Seventh step: Compare whether the trigger is pressed. In case it is not pressed, it will compare if the time for sending the periodic message has passed. If the time for sending the periodic message has already passed, the system updates the current location data and sends a new message with the most updated location information. If the time for sending the periodic message is not due, the program returns to the beginning of seventh step. Eighth step: If the trigger is pressed, the system updates the location through the GPS receiver. Ninth step: Comparison of the operating mode, whether the system is operating in spoofing or jamming mode. Tenth step: Sending a message that contains, who is the user of the system, date/time of the start of the transmission, detail if it is a spoofing or jamming transmission and the current location of the system. Eleventh step: In case the user is operating in spoofing mode, the system registers the location of the target drone, through the set of sensors to estimate its location. Twelfth step: Initiation of the transmission. Thirteenth step: While the trigger is pressed, the transmission is maintained. When the trigger is released, the system returns to seventh step.

4.6. SPG Vanguard System

The evolution of the prototype was continuous. Some technologies were changed or improved, such as the communication between the system and the supervising entity. As one of the objectives would be not to depend on third-party systems, we stopped making the communication between the supervising entity and the system using GSM, since we would always be limited to the coverage of the GSM network. We obtained a point-to-point communication using a Grove Lora radio 868MHz.

The Anti-UAV system consists of two hardware devices, the Spoofing Portable Gun (SPG) and the Control Station Spoofing Systems (C3S).

The SPG is an improved system from the previous prototype presented, with an improved design and more efficient functions at the structure level (Figure 4.8).



Figure 4.8. Spoofing Portable Gun (SPG)

The C3S (Figure 4.9) arises from the need not to depend on third party systems. The system is remotely controlled by C3S with the use of a key. One of the developments for this new prototype was that we modified the biometric sensor to a key and remote authentication control. The biometric sensor was not practical since soldiers normally wear gloves. At any time, the C3S user may block the system and the SPG will no longer function.



Figure 4.9. Control Station Spoofing Systems (C3S)

On the other hand, with the incorporation of this hardware it was possible to monitor the entire system. Through C3S we have the GPS location data, the SPG battery level, the C3S battery level, and the SPG status (transmission ON or OFF). The C3S user has an overview of the entire operation scenario. The C3S interface are presented in Figure 4.10.

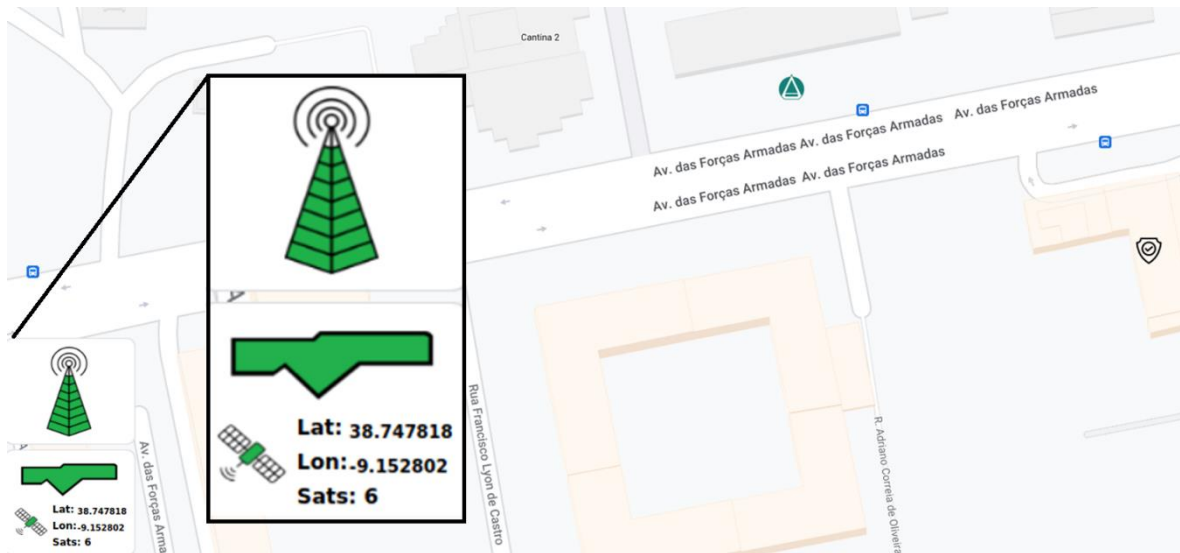


Figure 4.10. C3S Interface

In the Table 4.3 it is possible to observe all the symbols/images available in the C3S interface. The C3S interface has as outputs the real-time tracking of the SPG on the map. We were able to find out the status of the SPG, whether it is on standby, transmitting or without authorization to operate. With C3S is possible at any time allow or deny access to SPG operations. It is also possible to check the status of the SPG battery status, how many satellites are in view, if it get a fix and what are their coordinates. Its main function is to determine the safe zone with the help of a joystick. The safe zone can be changed at any time.

Table 4.3 - Interpretation of the C3S interface

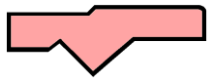
Illustration	Meaning
	SPG location
	Safe-zone
	C3S battery level (5/8)
	SPG GPS: no fix
	SPG GPS: fix
	No Communication C3S ↔ SPG
	SPG battery level (6/8)
	System block
	SPG transmission ON

Figure 4.11 describes the correct operation of the SPG Vanguard System. First, the safe zone is selected in the C3S unit, i.e., the zone to which the user wants to divert the unauthorized drone. Once the intrusion of an unauthorized drone has been detected, the SPG operator targets the unauthorized drone and pulls the trigger. Start transmission of jamming signals and the drone can no longer be controlled. The spoofing signal transmission is initiated, and the drone is diverted to the previously selected safe zone.



Figure 4.11. How SPG Vanguard System work

The Anti-UAV system has completed the R&D phases. It is currently in the deployment phase (TRL 7). Technology Readiness Levels (TRLs) are a method for understanding the technical maturity of a technology during its acquisition phase. TRLs allow engineers to have a consistent datum of reference for understanding technology evolution. All phases are presented in more detail in Table 4.4.

Table 4.4 - Technology Readiness Level (TRL)

Deployment	9	Actual System Proven in Operational Environment
	8	System Complete and Qualified
	7	System Prototype Demonstration in Operational Environment
Development	6	Technology Demonstration in Relevant Environment
	5	Technology Validated in Relevant Environment
	4	Technology Validated in LAB
Research	3	Experimental Proof of Concept
	2	Technology Concept Formulated
	1	Basic Principles Observed

[This page is deliberately left blank.]

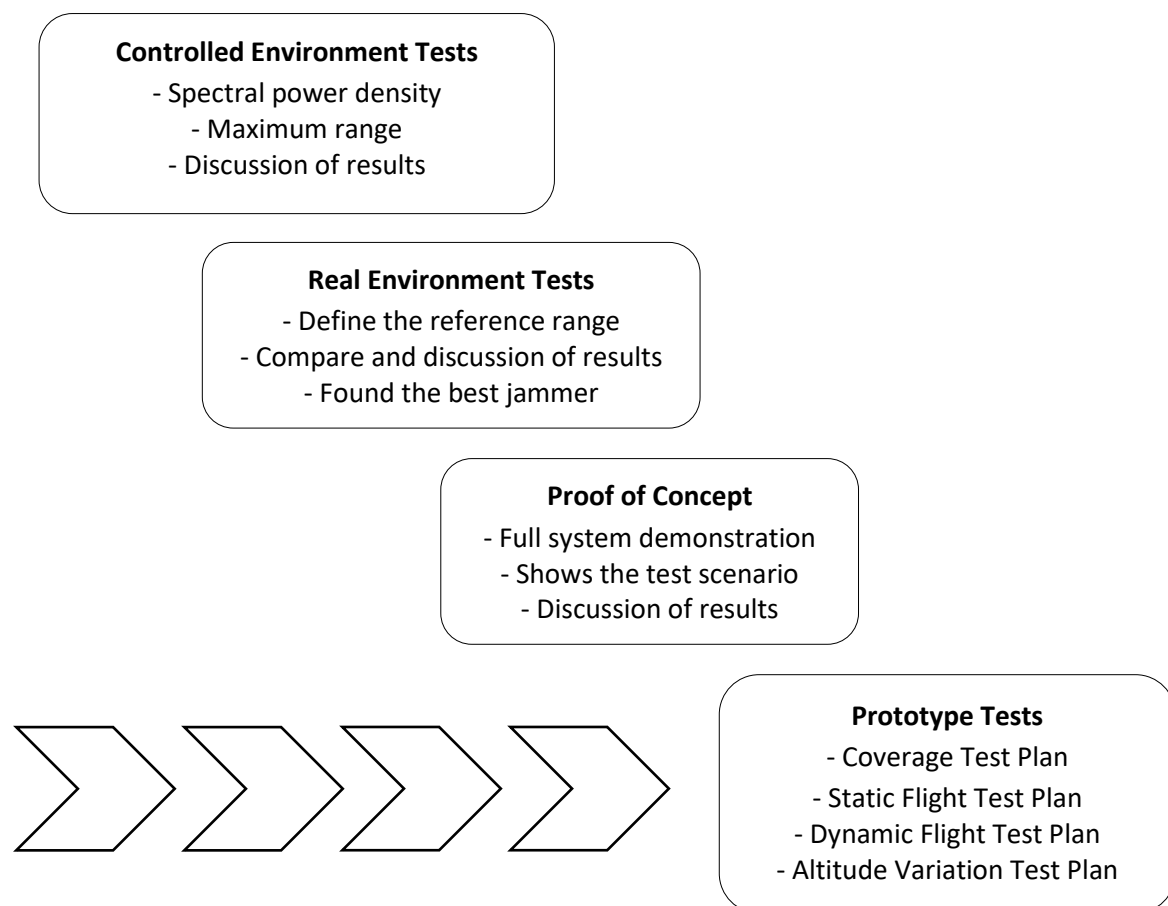
CHAPTER

5. Experimental Results

In this chapter the developed system was integrated and tested in a controlled environment and in a real environment. Several tests were accomplished to evaluate the performance of the complete anti-UAV mobile system under the influence of real GNSS signals.

5.1. Introduction to Experimental Results

The chart schematizes what is discussed in chapter 5 in a more perceptible way. The Controlled Environment Tests section performs the study and compares the different jamming techniques discussed without the influence of real GNSS signals. The Real Environment Tests section performs the study and compares the different jamming techniques discussed with the influence of real GNSS signals. The Proof-of-Concept Tests section demonstrates the jamming and spoofing technique working in a real scenario simulating an intrusion from an unauthorized drone. The Prototype Test details a set of tests performed on the system.



5.2. Controlled Environment Tests

To evaluate and compare the different GPS jammer signal generation techniques, several tests were performed using the previously discussed techniques, considering different distances between jammer and target receiver.

To analyze the power spectral density of the various types of jammers, the receiving antenna was connected to the BladeRF for a spectrum analysis on the GNU Radio. This setting is possible due to the full duplex support of the BladeRF. The distance between the receiving antenna and the transmitting antenna is almost zero (< 10 cm). Figure 5.1 represents the hardware configuration adopted for implemented jammers.

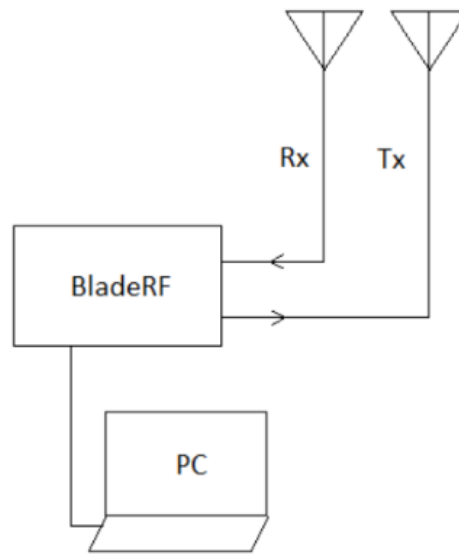


Figure 5.1. Emitter block diagram (jammer)

Table 5. presents some power spectral density measurements obtained with the five techniques. The values selected for the gains TxVGA1 and TxVGA2 were -4 dB and 25 dB respectively. The power spectral density shown in Table 5.1 is the maximum value.

Table 5.1 - Spectral power density of different jammers

	Maximum power spectral density [dBW/Hz]	Average power spectral density [dBW/Hz]
Barrage jamming	– 28	– 60
Sweep jamming	– 8	– 50
Successive pulses jamming	– 24	– 70
Tone jamming	2	– 50
Protocol-aware jamming	– 14	– 60

The measured power output matches the expected ones, where the lowest values are those of Barrage Jamming and Successive Pulses Jamming, because they use all the GPS frequency range, 14 MHz. The fact that Successive Pulses Jamming achieves a slightly higher value than Barrage Jamming is because, even though it occupies 14 MHz, it does not do it evenly. Although Protocol-Aware Jamming also uses the 14 MHz of bandwidth it concentrates more energy in the center frequency than Barrage Jamming and Successive Pulses Jamming. For that reason, it achieves higher peak on the power spectral density. Jamming Tone is the one that has a high-power density concentrated in a small area of the spectrum. Sweep Jamming in theory should get values equal to Tone Jamming, since they are the same, although Sweep Jamming sweeps the frequency. This does not happen due to the DC Offset error effect. To ensure that the conditions of the various tests are the same, it was decided to not use the actual GPS signals but to transmit a false GPS signal. This is to ensure that the intensity and reception quality is always the same, as throughout the day these two factors change using the actual GPS signals due to the orbital motion of the satellites.

A GPS transmitting ephemeris file specifies the constellation of GPS satellites to use. The ephemeris contains information regarding the position and the clock error of the satellites required in the positioning.

Figure 5.2 shows the setup employed for the tests, where it is shown the adopted GPS receiver as well as a second BladeRF board used for the emission of the false GPS signal.

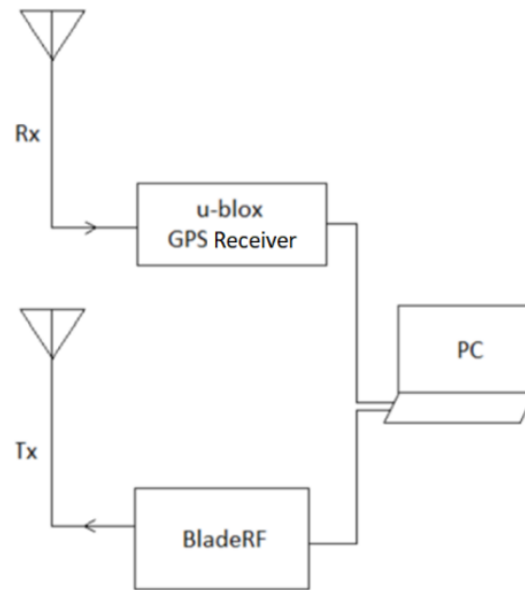


Figure 5.2. Block diagram reference setup comprising a GPS receiver and false GPS transmitter

The receiver used for the tests, shown in Figure 5.2, is the ublox receiver shown in Figure 5.3.



Figure 5.3. Ublox receiver (EVK-M8T)

The GPS receiver antenna is connected to the u-blox module and it is connected to the computer as shown at the top of Figure 5.2. The distance between the receiving antenna and the transmitting antenna ranges from 5 to 25 meters considering steps of 5 meters.

For the tests it was important to transmit the simulated GPS signal using a realistic power, considering the typical power received by an actual GPS signal. For this we used the following approach.

The process begins with the GNSS signal propagating through space until arrives at the user's GNSS receiving antenna. The power received is extremely poor, corresponding to a guaranteed signal power of -160 dBW in the case of the Global Positioning System (GPS). Considering a bandwidth of 2 MHz (the approximate null-to-null bandwidth of the GPS C/A code signal), the power of the received GPS signal is lower than the thermal noise power, as defined by Equation 16 [68].

$$P_{thermal_noise} = k_B \cdot T \cdot \Delta f \text{ [W]} \quad (16)$$

Applying the bandwidth of 2 MHz and assuming a temperature of 290 K results in 8 fW (or $-140,97$ dBW).

Knowing that the transmission powers of the GPS satellites lie between 20 and 50 W, with a transmission antenna with a gain of 12 dB [69] and that the satellites are located 20200 km high (90° elevation), the maximum power received on the earth's surface is calculated using the free space path loss equation.

$$L_{fs} = \frac{(4\pi)^2 d^2}{\lambda^2} = \frac{(4\pi)^2 d^2}{\left(\frac{c}{f}\right)^2} \quad (17)$$

Inserting all the specified values into Equation 17 we obtain $1,78 \times 10^8$ (or 182,5 dB).

The maximum power emitted by the GPS satellite in dBW is 17 dBW and considering the power transmitted and considering the losses in free space previously calculated, one can easily compute the power received using

$$P_{Rx} = P_{Tx} + G_{Tx} - L_{fs} \quad (18)$$

The BladeRF with a gain $TxVGA1 = -4 \text{ dB}$ and $RxVGA1_{min} = 5 \text{ dB}$ [70] results in a false GPS signal with -122 dBW of power, measured with the BladeRF without any type of filtering. For the signal to have a power of $-153,5 \text{ dBW}$ adjustments are required.

Without the VGA1 emission and reception gains is equal to -123 dBW . The $TxVGA1$ gain adjustment can also be set to -35 dB , losing 31 dB compared to the previous case. Adding the loss of 31 dB applied through the gain adjustment $TxVGA1$, results in a received power of -153 dBW . The GPS receiver and the false GPS transmitter must be located close to each other and with a $TxVGA1$ setting = -35 dB , so that the received signal power can be close to the received signal power in a real case.

In the first evaluation phase, maximum range tests were performed for each of the jammers studied in a controlled environment (Table 5.2).

Table 5.2 - Maximum range of various jammers in a controlled environment

	5 m	10 m	15 m	20 m	25 m
Barrage jamming	✓	✓	✓	✓	✓
Sweep jamming	✓	✓	✓	✓	✓
Successive pulses jamming	✓	×	×	×	×
Tone jamming	✓	✓	✓	✓	×
Protocol-aware jamming	✓	✓	✓	✓	✓
✓ - GPS receiver without location × - GPS receiver with location					

Based on the results, a conclusion cannot be reached yet, although the best-performing jammers are Barrage Jamming, Sweep Jamming and Protocol-Aware Jamming, with a maximum range of 25 meters. Successive Pulses Jamming managed to interfere only up to 5 meters away with the receiver. The Tone Jamming achieved a maximum range of 20 meters.

The five techniques presented have advantages and disadvantages which are presented next, before the experimental tests in a realistic environment.

Barrage Jamming has as its main advantage the capability to jam the entire GPS signal band. The major problem is the power resource, since the power distributes evenly inside the bandwidth of $15,345 \text{ MHz}$ which can result in a low power spectral density at every frequency.

The Tone Jamming only emits a sinusoid at the center frequency, concentrating all the energy on the carrier frequency of the GPS signals but in practice this is not the case because the LimeMicro LMS6002D chip, which is responsible for the BladeRF emission, has a minimum emission bandwidth of 1,5 MHz, bandwidth than the jammer. The great advantage is to concentrate all your energy on the carrier frequency of the GPS signals.

It will be expected that the technique is not one of the most effective but has the advantage of simplicity in terms of signal generation.

The great advantage of Sweep Jamming is the ability to apply a power spectral density which can momentarily become much higher than Barrage Jamming on a specific frequency using a signal with a lower bandwidth. As the bandwidth of the signal is smaller, the signal power does not disperse and is more concentrated around the central frequency of the signal which can be changed over time. This technique uses a frequency sweep so that it is possible to cover the entire bandwidth of the GPS signal. The disadvantage is the need for the hardware to support frequency sweeping fast enough for this technique to succeed.

Successive Pulses Jamming can also obtain higher power spectral density values than the Barrage Jamming, because although it occupies the entire bandwidth of the GPS signal, it does not do so uniformly. The fact that jamming spacing between frequencies exists throughout the entire band of the GPS signal is a disadvantage since the receiver may be able to recover the GPS signal.

Finally, Protocol-Aware Jamming (BPSK random signal created using GNU Radio or using GPS-SDR-SIM is the same results) has a very similar behavior to Barrage Jamming, although this does not consist of noise emitting itself, but random bits modulated in BPSK. Setting the identical sample rate to GPS, makes the Protocol-Aware Jamming spectrum very similar to that of GPS.

5.3. Real Environment Tests

The aim of the second phase of the tests was to evaluate the performance of the jamming techniques with real GPS signals.

The Barrage Jamming is used as the reference technique against which the other jammers are compared. The tests consist of first evaluating the maximum distance at which the Barrage Jamming can interfere in the real environment. The maximum range

obtained for the Barrage Jamming was 18 meters. This distance was defined as the reference range so that if we could place the receiver farther from the jammer, as shown in Figure 5.4, we could then conclude that specific jammers had a higher range than Barrage Jamming. For these tests, the BladeRF was powered by USB 3.0, with gains of $TxVGA1 = -4$ dB and $TxVGA2 = 25$ dB.

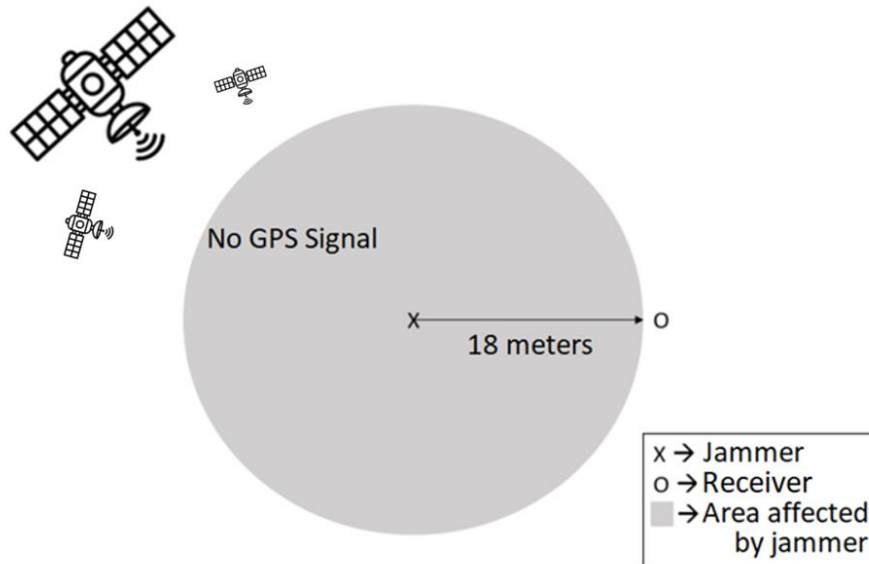


Figure 5.4. Test in real environment

The Successive Pulses Jamming as expected failed to interfere with the receiver. The fact that there is not a complete coverage of all frequencies throughout the bandwidth of the GPS signal makes this technique inefficient.

The Tone Jammer can interfere with the receiver by lowering all power levels of the satellites but still, it was not able to continuously maintain the inhibition of the localization functionality of the receiver. It is important to remind that this technique does not occupy uniformly all the bandwidth of the GPS.

Sweep Jamming and Protocol-Aware Jamming (BPSK random signal created using GNU Radio or using GPS-SDR-SIM achieved the same results) were able to block the GPS signals at the receiver and were shown to be more efficient techniques compared to Barrage Jamming.

Based on these results, these two techniques deserve a more detailed analysis. Both can cause the receiver to fail to determine the location, although the analysis of signal strengths of the GPS satellites in the receiver are different, as can be seen in Figure 5.5 and Figure 5.6.

The graphs presented in both figures relate the received power level (vertical axis) and the time instants on the horizontal axis (each square corresponds to 1 s), with the oldest being represented on the left and the current on the right. The graphs of Figure 5.5 and Figure 5.6 were constructed using the u-center, GNSS evaluation software for Windows. It is possible to observe that with Sweep Jamming the received power associated to each satellite never vanishes completely, whereas in Protocol-Aware Jamming as soon as the jammer is activated, the powers of the satellites gradually diminish in the following instants of time until they completely disappear for all satellites. It was concluded that Protocol-Aware Jamming was the most viable jammer in terms of its scope compared to the rest. Sweep Jamming is also a simple and effective solution, but the equipment can limit the efficiency of the technique approached. If the hardware does not allow sufficiently performance to have an efficient frequency sweep, the jamming's effectivity cannot be guaranteed.

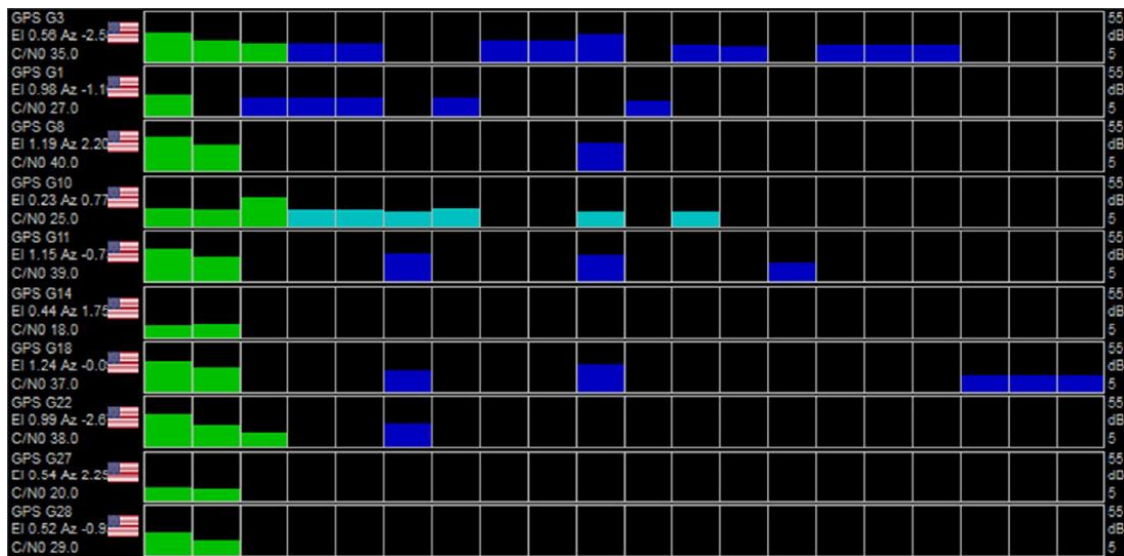


Figure 5.5. Power of GPS satellite signals with sweep jamming (screenshot obtained from the U-Center software)

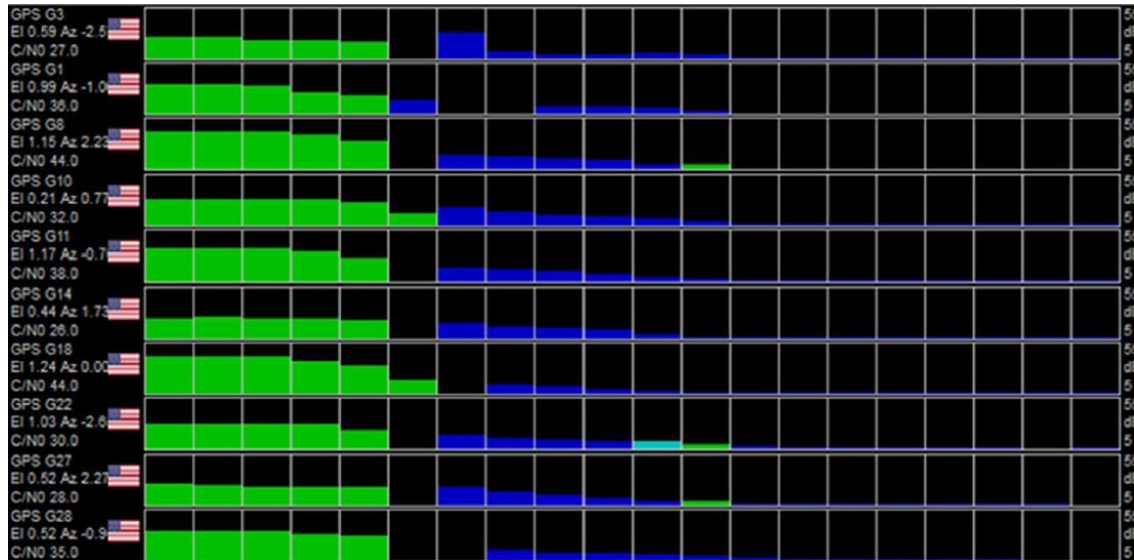


Figure 5.6. Power of GPS satellite signals with protocol-aware jamming (screenshot obtained from the U-Center software)

Once we found the best jammer, we used it to test over a drone in flight. The drones used for the real-life tests were the DJI Spark and Parrot Bebop 2 FPV. In both cases similar behavior was observed. Selecting the auto flight mode and with the drone already in flight, whenever the jammer signal transmission was started, the drone's behavior automatically changed, stopping its flight path and gliding in the same place. It was observed that the time between starting jammer transmission and drone gliding is almost instantaneous. If the jammer is started before the drone takes off, the drone will not even perform any action. All tests were performed safely, away from air traffic and outside prohibited areas. After the drone halts its operation due to jamming it could then be possible to emit spoofing signals so that the drone is deflected and indirectly controlled.

Figure 5.7 shows a prototype of an unauthorized drone protection system, which includes the proposed jamming solution.



Figure 5.7. Unauthorized drone protection system

5.4. Proof of Concept

Several tests were accomplished to evaluate the performance of the complete anti-UAV mobile system under the influence of real GNSS signals. It is important to note that, in those tests, we focused mostly on the evaluation of the overall system against drones operating in automatic flight mode. Still, in a previous work of some of the authors [71], we had already presented several experimental interference tests using the adopted jamming solution, which showed that it was possible to disrupt the UAV communication link.

For the tests presented in this thesis, the BladeRF was powered by USB 3.0, with gains of $TxVGA1 = -4$ dB and $TxVGA2 = 25$ dB.

For the operation of the system, it is necessary to select the forced landing site, intended for the forced landing of possible invading drones. We can see the selection adopted for the tests in Figure 5.8.



Figure 5.8. Real test scenario with selected forced landing site.

In the following figures, we illustrate the real test scenario, which corresponded to a countryside environment, wherein it was possible to visualize the roof of a one-story house, bushes, some ground vegetation and a few trees. The tests were carried out in a fully controlled and safe environment.

The drone used for the real-life tests was a DJI Phantom 3 Standard, illustrated in Figure 5.9.



Figure 5.9. DJI Phantom 3 Standard

Selecting the auto flight mode and with the drone already in flight, whenever the jammer signal transmission was started, the drone's behaviour automatically changed, stopping its flight path and gliding in the same place. It was observed that the time between starting jammer transmission and drone gliding is almost instantaneous. If the jammer is started before the drone takes off, the drone will not even perform any action. All tests were performed safely, away from air traffic and outside prohibited areas. After the drone halts its operation due to jamming it could then be possible to emit spoofing signals so that the drone is deflected and indirectly controlled.

Figure 5.10 shows the test scenario. The UAV was pre-configured with an autonomous route marked in red in Figure 5.10. As soon as the operator started transmitting jamming signals, the drone was hovering in the same place (ball marked in red).

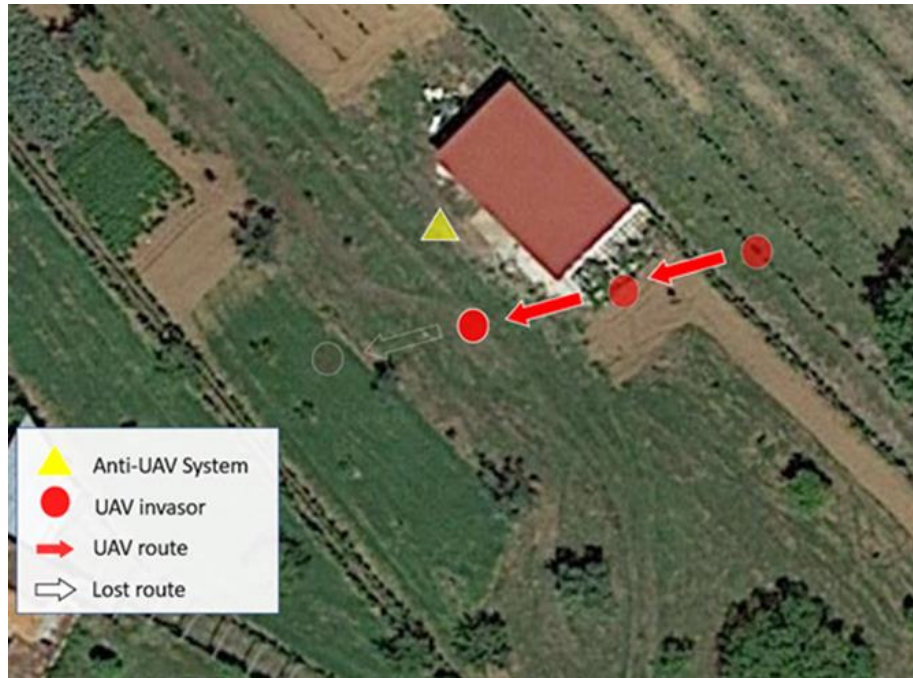


Figure 5.10. Real test scenario using jamming signals

The remaining pre-configured route was not completed by the UAV.

The operator of the mobile anti-UAV system (Figure 5.11) keeps aiming at the drone and keeping the trigger pressed. The system starts transmitting spoofing signals.



Figure 5.11. Anti-UAV mobile system operator

With the operator pointing towards the target UAV, using the telescopic sight, if necessary, the geographical determination of the UAV is initiated.

Through the Sensor Module the location of the UAV is determined and through the Processor Module the spoof route to the forced landing site is generated.

We can observe the whole scenario in Figure 5.12.

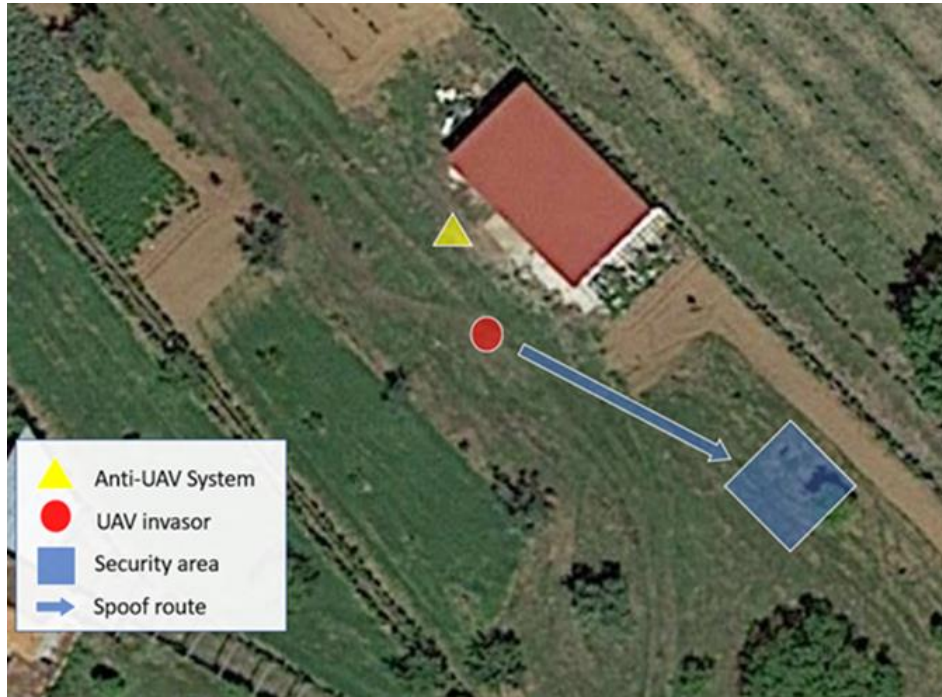


Figure 5.12. Real test scenario using spoofing signals

When the UAV receives the spoofing signals it assumes its new route and moves to the forced landing site as desired. The system's performance was positive and we managed to divert the drone at the four cardinal points. The spoofing behaved as shown previously in [35] regarding several well-known GPS receivers.

5.5. Prototype's Tests

In this section, several tests in different environments (urban and suburban) of the final prototype resulting from this thesis are reported. After the Anti-UAV system had demonstrated this technology works, detailed tests of all the technologies that the system includes were carried out. The maximum ranges of the system, coverage tests, and behavior of the UAV with the various technologies, jamming and/or spoofing was tested.

5.5.1. Coverage Test Plan

The maximum link distance between C3S and SPG was tested. Both hardware were connected and the distance between these devices was increased at the same time as the communication was analyzed.

In an urban environment with Line-of-Sight (LoS) between receiver and transmitter the maximum range was 305,20 meters (Figure 5.13) and Non-Line-of-Sight (NLoS) was 172,60 meters (Figure 5.14). In both figures the point A represents the SPG and the point B represents the C3S.

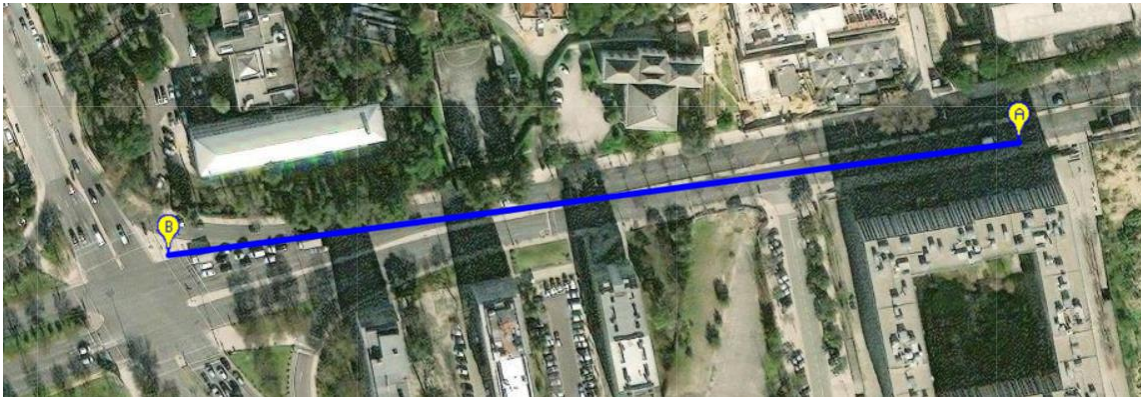


Figure 5.13. Urban environment with LoS between SPG ↔ C3S

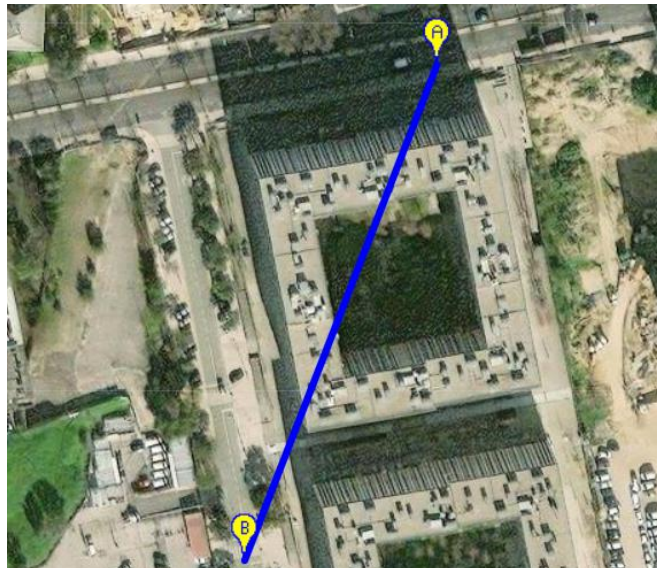


Figure 5.14. Urban environment with NLoS between SPG ↔ C3S

The expectation is that in a suburban environment the range will be greater than in an urban environment. This is because in urban environments there are more fixed or moving obstacles (e.g., buildings and cars) that interfere with the signal.

In suburban environment with LoS between receiver and transmitter the maximum range was 327,10 meters (Figure 5.15). In Figure 5.15 the point A represents the SPG and the point B represents the C3S.

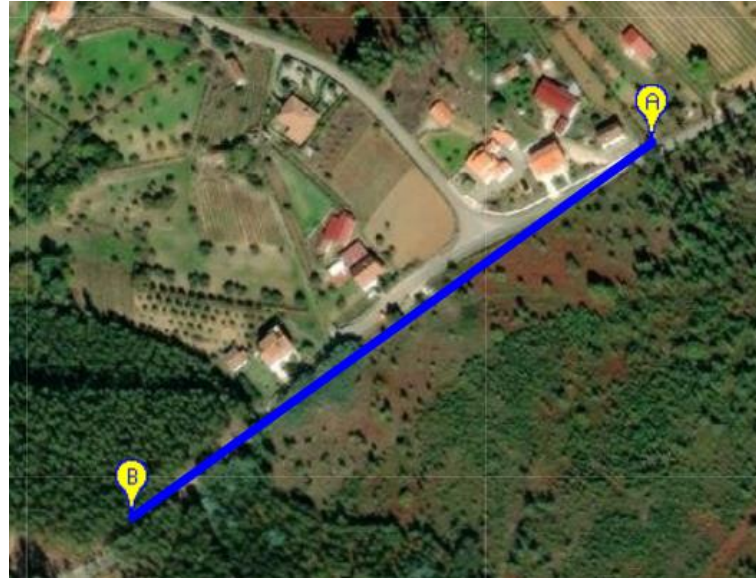


Figure 5.15. Suburban environment with LoS between SPG ↔ C3S

The maximum range of SPG's 2,4 GHz jammer was tested. The 2,4 GHz jammer is used to jamming the communication between the remote control and the invading drone. By jamming this communication, the user of the invading drone can no longer control the drone. The test was conducted in a controlled environment with the drone landed on the ground. The remote control and the drone are 1 meter apart so that there is a high-power connection (worst case scenario for the SPG function). The SPG transmitting 2,4GHz jamming moves away until the drone and remote control are reconnected. The distance between the drone and the SPG is measured once the remote control and the drone have connected. The maximum range of the 2,4GHz jammer in suburban environment is 183,30 meters.

Using the Rohde Schwarz FSH3 spectrum analyzer the spectrum of the jammer 2,4 GHz is represented in Figure 5.16. It can be seen that the jammer emits noise in the frequency range between 2,368 GHz and 2,4625 GHz. The jammer power is about 40 dBm. This measurement was made through free space propagation with the transmitter and receiver 10 cm apart.

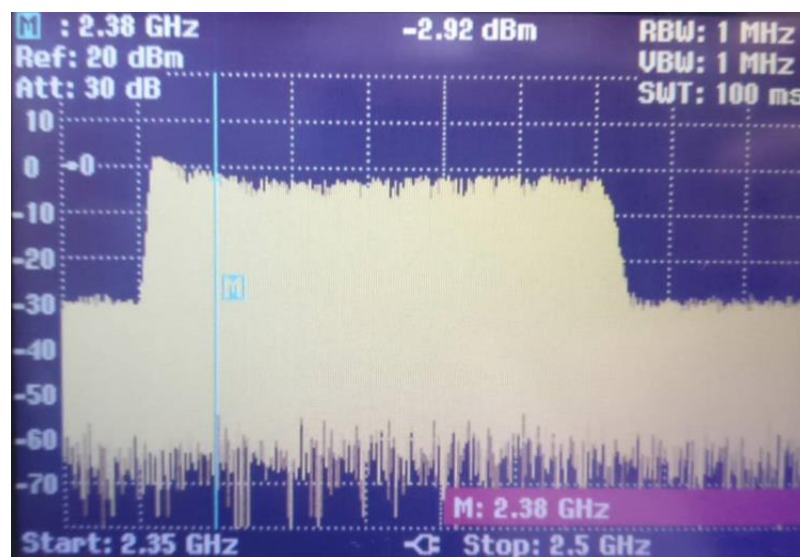


Figure 5.16. Jammer 2,4GHz spectrum analyser

The maximum range of SPG's GNSS jammer (GPS and GLONASS) was tested. The GNSS jammer is used to not allow the invading drone to receive satellite signals from the GPS and GLONASS navigation systems. By blocking this reception of signals, the user of the invading drone can no longer control the drone in an autonomous way. The test was conducted in a controlled environment with the drone landed on the ground. While GNSS jamming transmission is performed the GSP operator geographically moves away from the drone until the drone receives GNSS signals. The distance between the drone and the SPG is measured once the drone has received GNSS signals. The maximum range of the GNSS jammer in suburban environment is 87,60 meters.

The spectrum of the jammer GNSS is represented in Figure 5.17. It can be seen that the jammer emits noise in the frequency range between 1,5686 GHz and 1,6117 GHz. The jammer power is about 40 dBm. This measurement was made through free space propagation with the transmitter and receiver 10 cm apart.

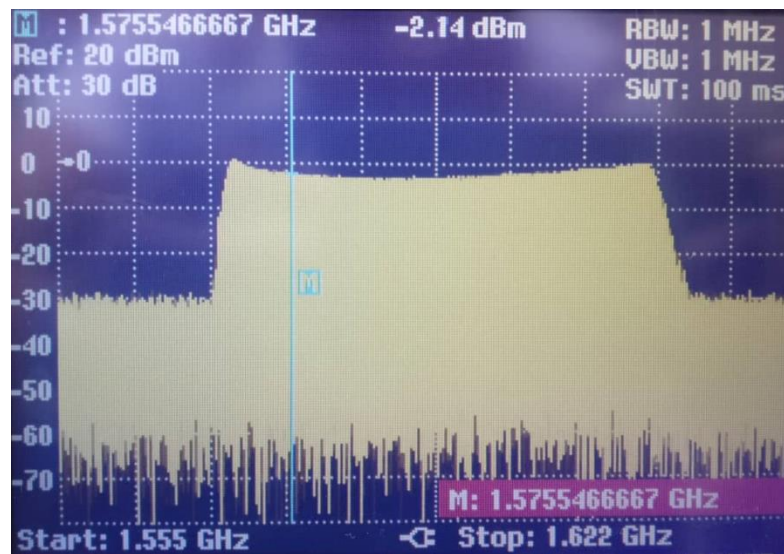


Figure 5.17. Jammer GNSS spectrum analyser

The maximum range of SPG's GPS spoofing was tested. GPS spoofing is used to spoof the location of the invading drone. Through GPS spoofing we are able to divert the invading drone to a security zone previously chosen by the C3S user. The test was conducted in a controlled environment with the drone landed on the ground. While GPS spoofing transmission is performed the GSP operator geographically moves away from the drone until the drone receives GNSS signals. The distance between the drone and the SPG is measured once the drone has not received false GNSS signals. The maximum range of the GPS spoofing in suburban environment is 216,20 meters.

The spectrum of the spoofing GPS is represented in Figure 5.18. It can be seen that the emitted signal is at the carrier frequency of 1,5754 GHz and has a bandwidth of 3,5 MHz. The spoofing power is about 31 dBm. This measurement was made through free space propagation with the transmitter and receiver 10 cm apart.

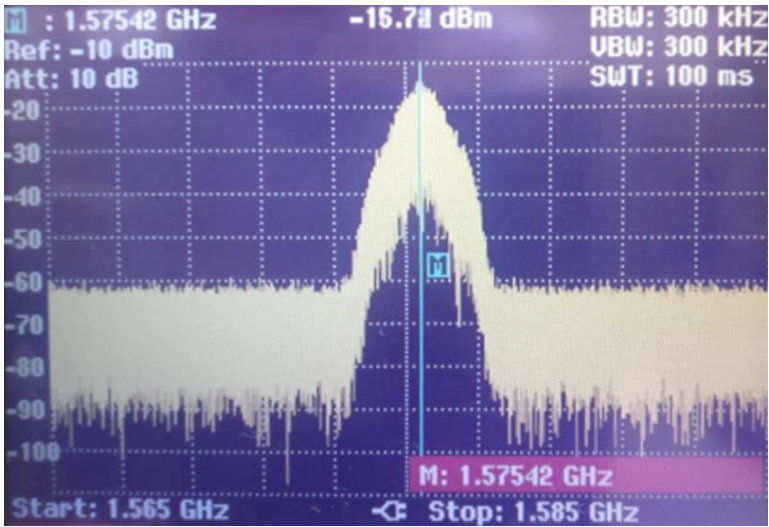


Figure 5.18. Spoofing GPS spectrum analyser

Table 5.3 shows a summary of the tests performed, describing the steps, expected results and the practical results.

Table 5.3 – Coverage Test Plan

Coverage testing	Stages	Expected results	Practical results
Distance of communication Lora (C3S ↔ SPG) in an urban environment	1) Connect C3S and GSP with a distance of 1 meter; 2) Check on the C3S screen that the GSP is already connected; 3) Gradually move the GSP away until the connection is lost. 4) Measure the distance between the two devices.	It enables data transmission over distances of up to approx. 800 meters, using the cable as an antenna.	LoS = 305,20 meters NLoS = 172,60 meters
Distance of communication Lora (C3S ↔ SPG) in a suburban environment	1) Connect C3S and GSP with a distance of 1 meter; 2) Check on the C3S screen that the GSP is already connected; 3) Gradually move the GSP away until the connection is lost. 4) Measure the distance between the two devices.	It enables data transmission over distances of up to approx. 800 meters, using the cable as an antenna.	327,10 meters
Maximum distance of Jammer 2,4GHz	1) Connect remote control and drone, with distance of 1 meter. 2) Check with the smartphone that the drone and the remote control are paired. 3) Transmit the 2,4GHz jammer signal with SPG and move away gradually. 4) Detect the point at which the drone can reconnect to the remote control. 5) Measure the distance between the drone/remote control and the SPG.	---	183,30 meters

Maximum distance of jammer 1,57542 GHz (GPS) + 1,602 GHz (GLONASS)	1) Connect remote control and drone, with distance of 1 meter. 2) Check with the smartphone that the drone and the remote control are paired and that the drone has a GPS signal. 3) Transmit the 1,57542GHz jammer signal with SPG and gradually move away. 4) Detect the point at which the drone can get GPS signals back. 5) Measuring the distance between the drone and the SPG.	---	87,60 meters
Maximum distance of GPS Spoofing	1) Connect remote control and drone, with distance of 1 meter. 2) Check with the smartphone that the drone and the remote control are paired and that the drone has a GPS signal. 3) Transmit the GPS spoofing signal with SPG and move away gradually. 4) Detect the point at which the drone stops receiving spoofing signals. 5) Measuring the distance between the drone and the SPG.	---	216,20 meters

5.5.2. Static Flight Test Plan

After testing the maximum distances using the drone without taking off, some tests were carried out with the drone flying manually controlled and in controlled environment.

We start by testing the GNSS Jammer with the drone in flight, hovering in the air. After take-off, the drone is controlled to a safe position and signals from the GPS jammer and Glonass jammer are transmitted. As soon as transmission begins the drone stops receiving GNSS signals and loses its location. The drone can no longer compensate for drag due to wind. Drone control becomes more unstable but it is still possible to control the drone.

Next the Jammer 5.8GHz was tested with the drone flying, hovering in the air. After take-off, the drone is controlled to a safe position and 5.8GHz jamming signals are transmitted. Once the jammer transmission is initiated the drone stops receiving the remote control signals and the drone operator can no longer control the drone. The drone detects that it no longer has the connection with the remote control and activates the go home algorithm. The drone autonomously lands at the same location where it took off.

The jammers were tested simultaneously with the drone flying, hovering in the air. After take-off, the drone is controlled to a safe position and GPS jammer, Glonass jammer and 5,8GHz jamming signals are transmitted. Once the jammer transmission is initiated the drone stops receiving GNSS signals and loses its location. The drone no longer receives the signals from the remote control and the drone operator can no longer control the drone. The drone hovers in the air, but no longer performs wind compensation and is blown by the wind.

The following test is the GPS spoofing together with the GNSS jammer with the drone flying, hovering in the air. After take-off, the drone is controlled to a safe position and GNSS jammer and GPS spoofing signals are transmitted. After the drone receives the spoofing signals (approximately 20s), the drone moves in the direction of the previously selected zone. There is always the possibility for the drone pilot to intervene and manually control the drone by remote control.

To complete the static flight tests the GPS spoofing was tested together with the GNSS jammer and 5,8GHz jammer with the drone flying, hovering in the air. After take-off, the drone is controlled to a safe position and GNSS jammer, 5,8GHz jammer and GPS spoofing signals are transmitted. The behaviour is the same as in the previous test but there is no possibility for the drone pilot to intervene and manually control the drone by remote control. Table 5.4 shows a summary of the tests performed, describing the steps, expected results and the practical results. With the realization of the static flight tests we can conclude that the time to achieve spoofing the drone GNSS receiver is around 20 seconds. We can also state that the system had a positive behavior for all the static flight tests.

Table 5.4 - Static Flight Test Plan

Static Testing	Stages	Expected results	Practical results
Jammer GNSS	1) Drone take-off; 2) Control the drone to a safe position; 3) Starting GNSS Jammer transmission; 4) Observe the drone behaviour.	When the Jammer GNSS signals start to be transmitted the drone does not receive satellite positioning signals. The drone can only be controlled manually.	The drone does not receive satellite positioning signals and no longer performs wind compensation. Controlling the drone is more difficult but possible.
Jammer 2,4GHz	1) Drone take-off; 2) Control the drone to a safe position; 3) Starting 2,4GHz Jammer transmission; 4) Observe the drone behaviour.	When Jammer 2,4GHz starts transmission, the drone stops receiving the signals from remote control. The return home function is activated automatically and using GNSS signals the drone returns autonomously to the place where it took off.	The connection with the remote control remains stable. The smartphone stops receiving image and data with the information from the drone.
Jammer 5,8GHz	1) Drone take-off; 2) Control the drone to a safe position; 3) Starting 5,8GHz Jammer transmission; 4) Observe the drone behaviour.	When Jammer 5,8GHz starts transmission, the drone stops receiving the signals from remote control. The return home function is activated automatically and using GNSS signals the drone returns autonomously to the place where it took off.	The connection to the remote control no longer exists. The return home function is activated automatically and using GNSS signals the drone returns autonomously to the place where it took off.

Jammer GNSS + Jammer 2,4GHz	1) Drone take-off; 2) Control the drone to a safe position; 3) Starting GNSS Jammer and 2,4GHz Jammer transmission; 4) Observe the drone behaviour.	When the Jammers 2,4GHz and GNSS signals start to be transmitted the drone does not receive satellite positioning signals and stops receiving the signals from remote control. The drone hovers in the air.	The drone hovers in the air but no longer performs wind compensation. The drone is blown away by the wind. The smartphone stops receiving image and data with the information from the drone.
Jammer GNSS + GPS Spoofing	1) Drone take-off; 2) Control the drone to a safe position; 3) Starting GNSS Jammer and GPS Spoofing transmission; 4) Check when the drone receives GPS spoofing signals; 5) Observe the drone behaviour.	By starting the transmission of Jammer GNSS and GPS spoofing signals simultaneously the drone stops receiving the satellite positioning signals. After the drone receives the spoofing signals (approximately 20s), the drone moves in the direction of the previously selected zone. There is always the possibility for the drone pilot to intervene and manually control the drone by remote control.	After 20s from the start of the transmission the drone moved to the desired direction. The user can control the drone through the remote control.
Jammer GNSS + Jammer 5,8GHz + GPS Spoofing	1) Drone take-off; 2) Control the drone to a safe position; 3) Starting 5,8GHz Jammer, GNSS Jammer and GPS Spoofing transmission; 4) Check when the drone receives GPS spoofing signals; 5) Observe the drone behaviour.	By starting the transmission of Jammer GNSS and GPS spoofing signals simultaneously the drone stops receiving the satellite positioning signals. After the drone receives the spoofing signals (approximately 20s), the drone moves in the direction of the previously selected zone. There is no possibility for the drone pilot to intervene and manually control the drone by remote control.	After 20s from the start of the transmission the SPG gains control of drone. The user cannot control the drone.

5.5.3. Dynamic Flight Test Plan

After testing the drone flying manually, some tests were carried out with the drone flying autonomously and in controlled environment.

Jammer GNSS was tested with the drone flying an autonomous route. After take-off, the drone started its own pre-configured route and signals from the GPS jammer and Glonass jammer are transmitted. The drone is no longer receiving GNSS signals, has lost its location and was unable to continue the mission plane. The drone hovers in the air, but no longer performs wind compensation and is blown away by the wind. Although the drone is more unstable, the operator can have control over the drone.

The 5.8GHz Jammer was tested with the drone flying an autonomous route. After take-off, it started its own route and 5.8GHz jamming signals are transmitted. The drone stopped receiving the signals from the remote control and its operator could no longer control the drone. The drone detected that it no longer had the connection with the remote control and activated the homing algorithm. It landed autonomously in the same place where it took off.

Next, GPS spoofing with GNSS jammer was tested and with the drone flying an autonomous route. After take-off, the drone started its own route and GNSS jamming and GPS spoofing signals were transmitted. After the drone has received the spoofing signals (approximately 20s), it moves towards the previously selected zone. During this test there was always the possibility for the pilot of the aircraft to intervene and manually control the aircraft by remote control.

To complete the dynamic flight tests the GPS spoofing was tested together with the GNSS jammer and the 5.8GHz jammer with the drone flying an autonomous route. After take-off, the drone started its own route and the GNSS jammer, 5.8GHz jammer and GPS spoofing signals were transmitted. The behaviour was the same as in the previous test but there is no possibility for the drone pilot to intervene and manually control the drone by remote control.

Table 5.5 shows a summary of the tests performed, describing the steps, expected results and the practical results. By conducting the dynamic flight tests, we can conclude that the time to achieve the spoofing of the drone's GNSS receiver remained around 20 seconds. We can also say that the system performed very good, and it is possible to divert the drone into a pre-defined zone.

Table 5.5 – Dynamic Flight Test Plan

Dynamic Testing	Stages	Expected results	Practical results
Jammer GNSS	1) Drone take-off; 2) Control the drone to a safe position; 3) Setting a planned route safely and without obstacles; 4) Start autonomous flight; 5) Starting GNSS Jammer transmission. 6) Observe the drone behaviour.	When the Jammer GNSS signals start to be transmitted the drone does not receive satellite positioning signals and in turn is no longer able to perform the autonomous flight.	The drone stops receiving GPS signals. The drone cannot continue the mission plane. The drone hovers in the air, but no longer performs wind compensation. The drone is blown away by the wind.
Jammer 2,4GHz	1) Drone take-off; 2) Control the drone to a safe position; 3) Setting a planned route safely and without obstacles; 4) Start autonomous flight; 5) Starting 2,4GHz Jammer transmission; 6) Observe the drone behaviour.	When Jammer 2,4GHz starts transmission, the drone stops receiving the signals from remote control. As the drone is on an autonomous flight mission, it will continue its pre-defined route. When it finishes the programmed route the drone returns home and lands at the place where it took off.	The drone continues its mission plane normally. The 2,4Ghz jammer has no influence on the remote control. The smartphone no longer communicates with the drone. Drone image and data reception are no longer available.

Jammer GNSS + Spoofing	1) Drone take-off; 2) Control the drone to a safe position; 3) Setting a planned route safely and without obstacles; 4) Start autonomous flight; 5) Starting 5,8GHz Jammer and GNSS Jammer transmission; 6) Check when the drone receives GPS spoofing signals; 7) Observe the drone behaviour.	By starting the transmission of Jammer GNSS and GPS spoofing signals simultaneously the drone stops receiving the satellite positioning signals and autonomous flight is no longer able and drone stop the route. After the drone receives the spoofing signals (approximately 20s), the drone moves in the direction of the previously selected zone. There is always the possibility for the drone pilot to intervene and manually control the drone by remote control.	The drone cannot continue the mission plane. After 20s from the start of the transmission the drone moved to the desired direction. The user can control the drone through the remote control.
Jammer GNSS + Jammer Remoto Control + GPS Spoofing	1) Drone take-off; 2) Control the drone to a safe position; 3) Setting a planned route safely and without obstacles; 4) Start autonomous flight; 5) Starting 5,8GHz Jammer, GNSS Jammer and GPS Spoofing transmission; 6) Check when the drone receives GPS spoofing signals; 7) Observe the drone behaviour.	By starting the transmission of Jammer GNSS and GPS spoofing signals simultaneously the drone stops receiving the satellite positioning signals and autonomous flight is no longer able and drone stop the route. After the drone receives the spoofing signals (approximately 20s), the drone moves in the direction of the previously selected zone. There is no possibility for the drone pilot to intervene and manually control the drone by remote control.	The drone cannot continue the mission plane. After 20s from the start of the transmission the drone moved to the desired direction. The user cannot control the drone.

5.5.4. Altitude Variation Test Plan

Changing the altitude of the drone to a lower altitude with reference to the GNSS signals was tested. With the drone hovering at a height of 10 meters, the transmission of the GNSS jammer and GPS spoofing signals with altitude variation was initiated. We waited until the drone received the false GNSS signals and observed what the drone's behavior was.

The same procedure was carried out for the increase in altitude. The drone in both tests did not change its altitude. What we can conclude is that the drone does not rely solely on the GPS message to change its altitude position. The drone has other sensors. Most DJI drones measure altitude using a barometric sensor with an AGL (Above Ground Level) reference.

Table 5.6 shows a summary of the tests performed, describing the steps, expected results and the practical results.

Table 5.6 - Altitude Variation Test Plan

Static testing	Stages	Expected results	Practical results
Jammer GNSS + Spoofing + Altitude	1) Drone take-off; 2) Control the drone to a safe position ready to start the test; 3) Start transmitting of GNSS Jammer and Spoofing signals with decreasing altitude; 4) Check the Drone's remote control display if no GPS signals is received; 5) Check the Drone's remote control display when GPS Spoofing signals are received; 6) Visually check if the drone varies its altitude.	After the drone has calculated its position through GPS spoofing signals (approx. 20s) the drone will move upwards.	The drone does not receive satellite positioning signals and no longer performs wind compensation. The drone did not change its altitude.
Jammer GNSS + Spoofing - Altitude	1) Drone take-off; 2) Control the drone to a safe position ready to start the test; 3) Start transmitting of GNSS Jammer and Spoofing signals with increasing altitude; 4) Check the Drone's remote control display if no GPS signals is received; 5) Check the Drone's remote control display when GPS Spoofing signals are received; 6) Visually check if the drone varies its altitude.	After the drone has calculated its position through GPS spoofing signals (approx. 20s) the drone will move downwards.	The drone does not receive satellite positioning signals and no longer performs wind compensation. The drone did not change its altitude.

[This page is deliberately left blank.]

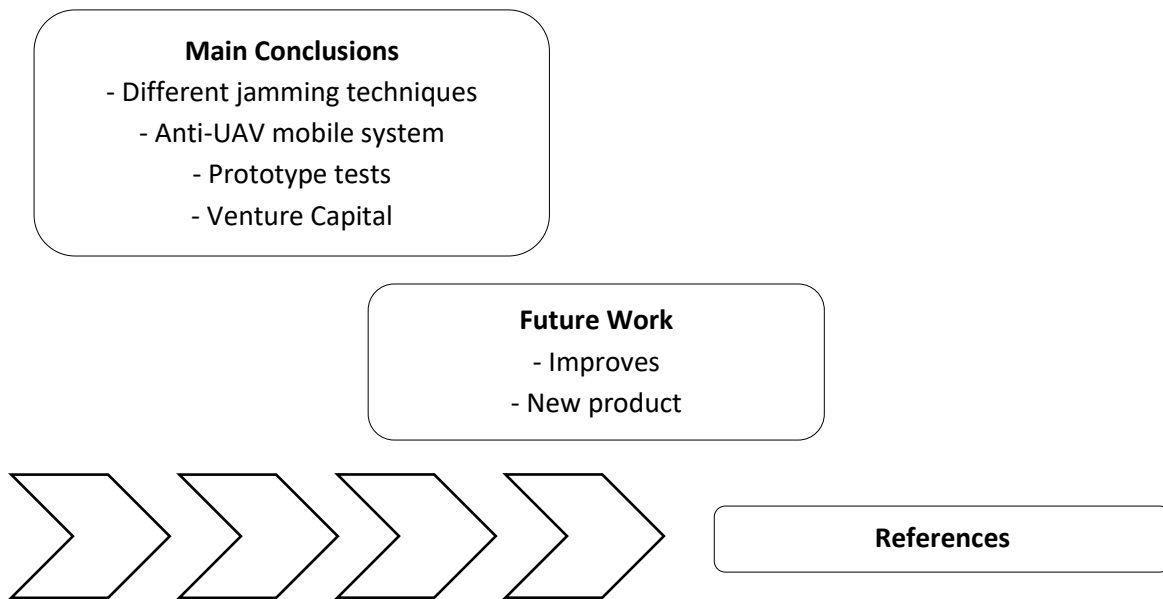
CHAPTER

6. Conclusions

In this chapter we present the main conclusions and discuss future directions of research.

6.1. Introduction to Conclusions

The chart schematizes what is discussed in chapter 6 in a more perceptible way. The Main Conclusions section makes a general conclusion about the different jamming techniques, the main conclusions of the tests made with the Anti-UAV mobile system and with the prototype and explains how it is relating to the companies and the market. The Future Work section refers to the improvements that can be made on the system and the new products that can arise from technology transfer with this technology.



6.2. Main Conclusions

Recalling the main objective of this thesis, which was to produce a system capable of estimating the geolocation of the invading drone through a set of sensors; having the functionality to emit efficient signals to block these two types of communication with drones (connection between remote control and drone, and connection between drone and GNSS systems); and diverting unauthorised drones to a pre-selected safe zone using a non-destructive approach, through GPS spoofing. In addition to these technical characteristics, the system had to be mobile and adapted to any area of the planet, not depending on or interfering with third party systems for its complete operation.

This study begins to compare five possible techniques capable to interfere with GPS signals resulting in the possible loss of localization and navigation capabilities of an UAV.

The different jamming techniques were implemented and evaluated using low-cost SDR platforms and the GNU Radio software development toolkit. Several tests were performed to evaluate the effectivity in accomplishing the jamming of GPS signals. The best-performing jammer was Protocol-Aware Jamming (Figure 5.6) which uses a similar architecture to that used by a transmitter of GPS signals. Using this approach, the interfering signal mixes more effectively with the main signal since they exhibit identical spectral behaviour, making its reception virtually impossible to perform at the receiver with lower transmitter power required.

We described an anti-UAV mobile system that was developed to protect areas from unauthorized drones. The system incorporated localization with jamming and spoofing techniques which were used in a coordinated approach. The system was able to estimate the position of the invading vehicle and could then apply jamming to neutralize the GPS signal, followed by spoofing to gain control of the vehicle. In addition, it also supported jamming directed to the control signal, thus, making manual control unfeasible. The barrage jammer was used to jam the connection between the remote control and the drone because Frequency-hopping spread spectrum (FHSS) was used. The system did not analyse the spectrum of the signal.

Through carefully conducted real-life tests using the implemented prototype, we observed the effectiveness of the proposed solution, which was capable of blocking the autonomous flight of an UAV by jamming its GPS receiver, followed by the successful

acquisition of the vehicle control through the transmission of spoofing signals, which allowed its forced landing on a predefined site.

We can conclude that it is possible to block an autonomous flight of a drone by blocking its GPS receiver and remote control. We can also conclude that it is possible to gain control of the autonomous flight of a drone by emitting spoofing of GNSS signals.

This Anti-UAV system is the result of technology transfer. It was developed and produced with the main objective of diverting the drone. The system has been designed according to the standardization required for its application in the context of Defence and Security. As the thesis work progressed, several entities were interested in the project and it was supported by the Public Venture Capital Fund Management Company, Portugal Ventures. This investment allowed the researcher to apply the investigation to a business model, constituting his own start-up. Incubated in Audax - Centro de Empreendedorismo e Inovação do ISCTE-IUL since 2021, the start-up Swatter Company started to take its first steps in the world of defence and security. The Swatter Company is working together with the Estado Maior das Forças Armadas (EMFA) to obtain PRT Army Tested and Combat Proven Certificates. Because it is a very innovative system, the research team together with ISCTE-IUL registered the system's national patent and have applied for two more international patents which are in progress. A functional prototype has been completed and the next step is to approach the DefenseTech market. The strategy is to develop pilots and travel to international fairs, so that we can present and demonstrate the technology. We aim to complete the deployment phase, TRL 9. For this we need system prototype demonstration in operational environment, system qualified, and proven in operational environment.

6.3. Future Work

As future work, besides extending the maximum operational range using better amplifiers and integrated circuit antennas with higher directivity, it is intended to extend the system for fixed position surveillance applications, where it can be deployed for continuous monitoring of a predefined area. In this case, beamforming technologies can be applied, thus, enabling it to defend against an intrusion of multiple unauthorized drones. Based on different beamforming approaches often used in communication systems, it should be possible to rely on two algorithms: a Direction of Arrival (DOA) algorithm and an adaptive beamforming algorithm. The DOA algorithm calculates the direction of arrival of the received signals. Then, the adaptive beamforming algorithm is used to update the system parameters. The weights of each element of the antenna arrays change the phase shift and amplitude attenuation of the received signal, so that the main beam is directed towards the desired signal direction and the nulls are placed in the interference directions. By studying and using this kind of adaptive beamforming algorithm it could be possible to transmit the jamming signals without interfering with neighbouring systems and being precise in its targets to be affected.

In fact, in the specific type of scenario with a multiple drone attack, the system presented in this thesis will have difficulties in being able to provide an effective response. In this situation, an individual system and an operator would be needed for each invading drone, which makes the solution less appealing. Therefore, for this type of scenario, a fixed system incorporating beamforming technologies can constitute a better approach.

Another product derived from Anti-UAV system is already in the planning process. The international patent application for this new system has already been submitted and the planning is that by 2023 it will be possible to design, engineer and build the prototype. A technology transfer from C3S will take place for a fully autonomous drone that will protect a certain area from the intrusion of unauthorized drones by diverting them to a safe zone. Our objective is to be able to transfer technology to more systems, including military systems.

[This page is deliberately left blank.]

References

- [1] *Easy Access Rules for Unmanned Aircraft Systems* (Regulation (EU) 2019/947 and Regulation (EU) 2019/945). Available online: <https://www.easa.europa.eu/document-library/easy-access-rules/easy-access-rules-unmanned-aircraft-systems-regulationeu> (accessed on 12 January 2021).
- [2] Ong, T. *Dutch Police Will Stop Using Drone-Hunting Eagles since They Weren't Doing What They're Told*. Available online: <https://www.theverge.com/2017/12/12/16767000/police-netherlands-eagles-rogue-drones> (accessed on 1 July 2021).
- [3] Recognition, A. *New Russian Rex-1 Anti-Drone Rifle System Ready to Be Tested-Weapons Defence Industry Military Technology UK*. Available online: https://www.armyrecognition.com/weapons_defence_industry_military_technology_uk/new_russian_rex-1_anti-drone_rifle_system_ready_to_be_tested.html (accessed on 1 July 2021).
- [4] Matić, V.; Kosjer, V.; Lebl, A.; Pavić, B.; Radivojević, J. *Methods for Drone Detection and Jamming*. In Proceedings of the 10th International Conference on Information Society and Technology (ICIST), Kopaonik, Serbia, 8–11 March 2020.
- [5] Lebl, A.; Vujić, A.; Pavić, B.; Petrović, P.; Kosjer, V. *SDR COTS Components Applications to Military Systems for Radio Surveillance and Jamming*. In Proceedings of the 9th International Scientific Conference OTEH 2020, Belgrade, Serbia, 15–16 October 2020; pp. 264–269.
- [6] Ferreira, R.; Gaspar, J.; Souto, N.; Sebastião, P. *Effective GPS Jamming Techniques for UAVs Using Low-Cost SDR Platforms*. In Proceedings of the 2018 GlobalWireless Summit (GWS), Chiang Rai, Thailand, 25–28 November 2018; pp. 27–32.
- [7] *Drone Incidents All over the World*. Available online: <https://www.dedrone.com/resources/incidents/all> (accessed on 25 October 2021).
- [8] Chamola, V.; Kotes, P.; Agarwal, A.; Naren; Gupta, N.; Guizani, M. *A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques*. *Ad Hoc Netw.* 2021, 111, 102324.
- [9] Kim SG, Lee E, Hong IP, Yook JG. Review of Intentional Electromagnetic Interference on UAV Sensor Modules and Experimental Study. *Sensors (Basel)*. 2022 Mar 20;22(6):2384. doi: 10.3390/s22062384. PMID: 35336557; PMCID: PMC8950540.

- [10] Batoul Achaal, Mohamad Rida Mortada, Ali Mansour, Abbass Nasser. Wireless Communication Attack Using SDR and Low-Cost Devices. 14th International KES Conference on Intelligent Decision Technologies, KES-IDT 2022, Jun 2022, Rhodes, Greece. pp.417-428, <10.1007/978-981-19-3444-5_36>. <hal-03772364>
- [11] Castrillo, V.U.; Manco, A.; Pascarella, D.; Gigante, G. A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones. *Drones* 2022, 6, 65. <https://doi.org/10.3390/drones6030065>.
- [12] N. Souli, P. Kolios and G. Ellinas, "An Autonomous Counter-Drone System with Jamming and Relative Positioning Capabilities," ICC 2022 - IEEE International Conference on Communications, 2022, pp. 5110-5115, doi: 10.1109/ICC45855.2022.9838783.
- [13] Lyu, C.; Zhan, R. Global Analysis of Active Defense Technologies for Unmanned Aerial Vehicle. *IEEE Aerosp. Electron. Syst. Mag.* 2022, 37, 6–31.
- [14] Rahman, A.D.B.A.; Ghani, K.A.; Khamis, N.H.H.; Sidek, A.R.M. *Unmanned Aerial Vehicle (UAV) GPS Jamming Test by using Software Defined Radio (SDR) platform*. *J. Physics Conf. Ser.* 2021, 1793, 012060.
- [15] Khan, S.Z.; Mohsin, M.; Iqbal, W. *On GPS spoofing of aerial platforms: A review of threats, challenges, methodologies, and future research directions*. *PeerJ Comput. Sci.* 2021, 7, e507.
- [16] Shepard, D.P.; Bhatti, J.A.; Humphreys, T.E.; Fansler, A.A. *Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks*. In Proceedings of the 2012 ION GNSS Conference, Nashville, TN, USA, 19–21 September 2012; pp. 3591–3605.
- [17] Kerns, A.J.; Shepard, D.P.; Bhatti, J.A.; Humphreys, T.E. *Unmanned aircraft capture and control via GPS spoofing*. *J. Field Robot.* 2014, 31, 617–636.
- [18] Lin, H.; Qing, Y. *GPS spoofing low-cost GPS simulator*. In Proceedings of the DEF CON 23 Hacking Conference, at Paris/Bally's, Las Vegas, NV, USA, 6 August 2015.
- [19] Gaspar, J.; Ferreira, R.; Sebastião, P.; Souto, N. *Capture of UAVs Through GPS Spoofing*. In Proceedings of the 2018 Global Wireless Summit (GWS), Chiang Rai, Thailand, 25–28 November 2018; pp. 21–26.
- [20] Shattil, S.; Sen, R. Unmanned Aerial Vehicle Intrusion Detection and Countermeasures, US 20170094527 A2. Available online: https://pt.espacenet.com/publicationDetails/biblio?II=0&ND=3&adjacent=true&locale=pt_PTPT&FT=D&date=20170330&CC=US&NR=2017094527A1&KC=A1 (accessed on 30 May 2017).

- [21] *Portable Drone Jammer*, K.; Jin, S. WO 2018147604 A1. Available online: https://pt.espacenet.com/publicationDetails/biblio?II=0&ND=3&adjacent=true&locale=pt_PT&FT=D&date=20180816&CC=WO&NR=2018147604A1&KC=A1 (accessed on 16 August 2018).
- [22] Yunfeng, Y. *Energy-Saving Gun Barrel Type Directional Unmanned Aerial Vehicle (UAV) Jammer*, CN 107612655 A. Available online: https://pt.espacenet.com/publicationDetails/biblio?II=0&ND=3&adjacent=true&locale=pt_PT&FT=D&date=20180119&CC=CN&NR=107612655A&KC=A (accessed on 19 January 2018).
- [23] Davidovich, B.; Nassi, B.; Elovici, Y. Towards the Detection of GPS Spoofing Attacks against Drones by Analyzing Camera's Video Stream. *Sensors* 2022, 22, 2608. <https://doi.org/10.3390/s22072608>.
- [24] Dudczyk, J.; Czyba, R.; Skrzypczyk, K. Multi-Sensory Data Fusion in Terms of UAV Detection in 3D Space. *Sensors* 2022, 22, 4323. <https://doi.org/10.3390/s22124323>.
- [25] Łukasiewicz, J., Kobaszyńska - Twardowska, A. (2022). Proposed method for building an anti-drone system for the protection of facilities important for state security. *Security and Defence Quarterly*, 39(3), 88-107. <https://doi.org/10.35467/sdq/149268>.
- [26] Kong, L.; Chen, B.; Hu, F. Blockchain-Assisted Adaptive Reconfiguration Method for Trusted UAV Network. *Electronics* 2022, 11, 2549. <https://doi.org/10.3390/electronics11162549>.
- [27] Wei, X.; Sun, C.; Lyu, M.; Song, Q.; Li, Y. ConstDet: Control Semantics-Based Detection for GPS Spoofing Attacks on UAVs. *Remote Sens.* 2022, 14, 5587. <https://doi.org/10.3390/rs14215587>.
- [28] Wei, X.; Wang, Y.; Sun, C. PerDet: Machine-Learning-Based UAV GPS Spoofing Detection Using Perception Data. *Remote Sens.* 2022, 14, 4925. <https://doi.org/10.3390/rs14194925>.
- [29] Murtaza S.; Celestine I.; Kniezova J.; Noble A.. Analysis on security-related concerns of unmanned aerial vehicle: attacks, limitations, and recommendations[J]. *Mathematical Biosciences and Engineering*, 2022, 19(3): 2641-2670. doi: 10.3934/mbe.2022121.
- [30] B. S. Margana, D. S. Achanta, K. K. Songala and S. R. Ammana, "A Simple SDR based Method to Spoof Low-End GPS aided Drones for Securing Locations," 2021 IEEE International Conference on Robotics, Automation, Artificial-Intelligence and Internet-of-Things (RAAICON), 2021, pp. 32-36, doi: 10.1109/RAAICON54709.2021.9929965.
- [31] Haoyan Chen, Changbiao Lei, Lei Wang, "Research on navigation spoofing for UAV and UAV group," *Proc. SPIE 12161*, 4th International Conference on Informatics Engineering & Information Science (ICIEIS2021), 1216105 (14 February 2022); <https://doi.org/10.1117/12.2626900>.

- [32] Kožović, D., & Đurđević, D. (2021). Spoofing in aviation: Security threats on GPS and ADS-B systems. *Vojnotehnički Glasnik*, 69, 461-485.
- [33] Klar, G. *Drone Interceptor System, and Methods and Computer Program Products Useful in Conjunction Therewith*, US20190285388. Available online: https://pt.espacenet.com/publicationDetails/biblio?II=0&ND=3&adjacent=true&locale=pt_PT&FT=D&date=20190919&CC=US&NR=2019285388A1&KC=A1 (accessed on 13 March 2018).
- [34] Ferreira, R.; Gaspar, J.; Sebastião, P.; Souto, N. *Effective GPS Jamming Techniques for UAVs Using Low-Cost SDR Platforms*. *Wirel. Pers. Commun.* 2020, 115, 2705–2727.
- [35] Gaspar, J.; Ferreira, R.; Sebastião, P.; Souto, N. *Capture of UAVs Through GPS Spoofing Using Low-Cost SDR Platforms*. *Wirel. Pers. Commun.* 2020, 115, 2729–2754.
- [36] Different Types of Drones and Uses (2022 Full Guide), JOUAV, Unmanned Aircraft System. Updated at: Jul 27, 2022.
- [37] UAVision, Products Skypro, 2022. [Online]. Available: <https://www.uavision.com/spyro?lang=pt>
- [38] Tekever, AR5, 2022. [Online]. Available: <https://www.tekever.com/models/ar5/>
- [39] X. Wang, J. Guo, N. Cui. "Adaptive extended Kalman filtering applied to low-cost MEMS IMU/GPS integration for UAV". *International Conference on Mechatronics and Automation*, 2009.
- [40] Faculdade de ciências da universidade de lisboa—DEGGE-hidrografia, GNSS and Earth Observation: recent results and challenges, 2013.
- [41] S. Pullen and G. Gao, "GNSS jamming in the name of privacy," *Inside GNSS*, pp. 34–43, March/April 2012.
- [42] NETFLIX, Bruce Kennedy, Simon George and Ian Russel. Producer/Director: Emma Webster. "History 101, Season 2 Ep.10: GPS", 2022.
- [43] W. Hoffmann, B.H. Lichtenegger and J. Collins, *GPS: Theory and Practice* (Springer-Verlag, New York, 1994), 3rd ed.
- [44] J. Monico, *Posicionamento Pelo GNSS: Descrição, Fundamentos e Aplicações* (Unesp, São Paulo, 2008).
- [45] Parque Newton Freire Maia, "A tecnologia GPS - Parte II" [Online]. Available: <http://parquedaciencia.blogspot.pt/2013/08/a-tecnologia-gps-parte-ii.html>. [Accessed: 4-Jan-2022].

- [46] G. Blewitt, "Basics of the GPS Technique: Observation Equations" [Online]. Available: <http://www.nbmj.unr.edu/staff/pdfs/blewitt%20basics%20of%20gps.pdf>. [Accessed: 4-Jan-2022].
- [47] what-when-how—In depth tutorials and information, GNSS antennas and front ends (GPS and Galileo Receiver) Part 1. Retrieved July 14, 2018, from <http://what-when-how.com/a-software-defined-gpsand-galileo-receiver/gnss-antennas-and-front-ends-gps-and-galileo-receiver-part-1/>.
- [48] Misra, P., & Enge, P. (2010). Global Positioning System: Signals, measurements and performance. Lincoln, MA: Ganga-Jamuna Press.
- [49] Graham, A. Communications, Radar and Electronic Warfare. s.l. : John Wiley & Son Ltd, 2011.
- [50] Sklar, B. Digital Communications: Fundamentals and Applications. s.l. : Prentice Hall, 2001.
- [51] Lloyd N. Trefethen, David Bau III, Numerical linear algebra, Philadelphia: Society for Industrial and Applied Mathematics, ISBN 978-0-89871-361-9, pp.56.
- [52] Federal Communications Commission, Website Notices [Online]. Available: <http://www.fcc.gov> [Accessed: 4-Jan-2022].
- [53] Cell Phone Jammer, jammer berkualitas [Online]. Available: www.signaljammerblockers.com [Accessed: 4-Jan-2022].
- [54] Tech-Faq, GPS Jammer [Online]. Available: <http://www.tech-faq.com/gps-jammer.html> [Accessed: 4-Jan-2022].
- [55] Tutorialspoint, Learn Antenna Theory, simply easy learning, [Online]. Available: https://www.tutorialspoint.com/antenna_theory/index.htm
- [56] Basar, Tamer. (1983). The Gaussian test channel with an intelligent jammer. IEEE Transactions on Information Theory, 29(1), 152–157.
- [57] Smith, S. The scientist and engineer's guide to digital signal processing, Chapter 11: Fourier transform pairs/chirp signals.
- [58] Hussain, A., Saqib, N., Qamar, U., Zia, M., & Mahmood, H. (2014). Protocol-aware radio frequency jamming in Wi-Fi and commercial wireless networks. Journal of Communications and Networks, 16(4), 397–406.
- [59] Thuente, D., & Acharya, M. (2006). Intelligent jamming in wireless networks with applications to 802.11 b and other networks. In Proceedings of the MILCOM (Vol. 6, p. 100).

- [60] Lite, L., Specifications, T. Able of Contents Lidar Lite v3 Operation Manual and Technical Specifications Wiring Harness, Garmin: Olathe, KS, USA, 2016; pp. 1–14.
- [61] Ave, B.; Number, D.; Date, R. MPU-6000 and MPU-6050 Product Specification; InvenSense: San Jose, CA, USA, 2012, Volume 1, p. 408.
- [62] Ecopack, E.F., Lsm, T. 3D Accelerometer and 3D Magnetometer Module. Patent LSM303DLHC, November 2013.
- [63] U-Blox, Max-7 Series| U-Blox. Available online: <https://www.u-blox.com/en/product/max-7-series> (accessed on 4 July 2021).
- [64] Drew, J. Yagi Calculator DL6WU Download Version 2.6.18-May 2016. Available online: <http://www.vk5dj.com/yagi.html> (accessed on 8 March 2022).
- [65] Vieira, M. Glossário Sobre Antenas. Janeiro 2010. Available online: https://wirelesspt.net/wiki/Gloss%C3%A1rio_sobre_antenas (accessed on 2 January 2022).
- [66] P. G. Drennan, “Device mismatch in BiCMOS technologies,” pp. 104–111, 2003.
- [67] J. L. Wayman, D. Maltoni, D. Maio, A. K. Jain, and R. Cappelli, “Performance evaluation of fingerprint verification systems,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 28, no. 1, pp. 3–18, 2006.
- [68] what-when-how—In depth tutorials and information, GNSS antennas and front ends (GPS and Galileo Receiver) Part 1. Retrieved July 14, 2018, from <http://what-when-how.com/a-software-defined-gpsand-galileo-receiver/gnss-antennas-and-front-ends-gps-and-galileo-receiver-part-1/>.
- [69] Global Position System Low Noise Amplifier. GPS, LNA, Sensitivity, Jamming, Cohabitation, TTFF. NXP founded by Philips. Date of release: May 2009.
- [70] bladeRF Power Consumption—FX3 GPIF, FPGA, and RF Active—bladeRF x40. Retrieved March 12, 2018, from <https://github.com/Nuand/bladeRF/wiki/bladeRF-Power-Consumption>.
- [71] Brito, A.; Sebastiao, P.; Souto, N. Jamming for Unauthorized UAV Operations-Communications Link. In *Proceedings of the 2019 International Young Engineers Forum (YEF-ECE)*, Costa da Caparica, Portugal, 10 May 2019; pp. 94–98.

APPENDIXES

[This page is deliberately left blank.]

Appendix A

SISTEMA MÓVEL PARA IMOBILIZAR E DESVIAR DRONES NÃO AUTORIZADOS



Número de Publicação: PT 115663 B

Classificação Internacional:
G05D 1/00 (2006)

PATENTE DE INVENÇÃO

Data de pedido: **2019.07.19**

Data de publicação do pedido: **2021.01.19**

Data da Concessão: **2021.07.26**

Data da Publicação da Concessão: **2021.07.29**

Titular(es):

**RENATO BRANCO FERREIRA
JOÃO FILIPE DE QUADROS GASPAR
PEDRO JOAQUIM AMARO SEBASTIÃO
NUNO MANUEL BRANCO SOUTO
ISCTE- INSTITUTO UNIVERSITÁRIO DE
LISBOA**

Inventor(es):

**RENATO BRANCO FERREIRA
JOÃO FILIPE DE QUADROS GASPAR
PEDRO JOAQUIM AMARO SEBASTIÃO
NUNO MANUEL BRANCO SOUTO**

Mandatário:

**RUI DO NASCIMENTO GOMES
J. PEREIRA DA CRUZ, S.A.
RUA VITOR CORDON, 14 1249-103 LISBOA**

Resumo: NOS ÚLTIMOS TEMPOS, VÁRIOS TÊM SIDO OS RELATOS DE INCIDENTES COM DRONES QUE ENVOLVEM AVIÕES NAS IMEDIAÇÕES DE AEROPORTOS OU AERÓDROMOS. COM O «SISTEMA MÓVEL PARA IMOBILIZAR E DESVIAR DRONES NÃO AUTORIZADOS» É POSSÍVEL PROTEGER A INTRUSÃO DE DRONES NÃO AUTORIZADOS (COMERCIAIS E DE FABRICO CUSTOMIZADO), TERRESTRES, AÉREOS E AQUÁTICOS EM ZONAS RESTRITAS, E.G., AEROPORTOS, ÁREAS MILITARES, CONDOMÍNIOS E SITUAÇÕES PONTUAIS DE EVENTOS PÚBLICOS OU ZONAS ONDE É NECESSÁRIO GARANTIR A SEGURANÇA PÚBLICA. TRATANDO-SE DE UM SISTEMA MÓVEL, CONSEGUISE ASSIM UMA FÁCIL E RÁPIDA ADAPTAÇÃO ÀS ZONAS A PROTEGER. ESTE SISTEMA MINIMIZA A INTERFERÊNCIA EM SISTEMAS TERCEIROS E, POR OUTRO LADO, IMPLEMENTA TÉCNICAS AVANÇADAS DE EMISSÃO DE SINAIS DE ELEVADA EFICIÊNCIA ENERGÉTICA, MINIMIZANDO A PEGADA AMBIENTAL. ATRAVÉS DA UTILIZAÇÃO DE TECNOLOGIAS E MATERIAIS EFICIENTES PROJETOUSE O SISTEMA MODULAR, REPRESENTADO NA FIGURA 1, TENDO POR BASE A SUA FACILIDADE DE TRANSPORTE E MANUSEAMENTO POR FORÇAS DE DEFESA (MILITARES E SEGURANÇA PÚBLICA).

Resumo

Sistema Móvel para Imobilizar e Desviar Drones Não Autorizados

A invenção apresentada visa a proteção contra a intrusão de drones não autorizados (comerciais e de fabrico customizado), terrestres, aéreos e aquáticos em zonas restritas, e.g., aeroportos, áreas militares, condomínios e situações pontuais de eventos públicos ou zonas onde é necessário garantir a segurança pública. Tratando-se de um sistema móvel, consegue-se assim uma fácil e rápida adaptação às zonas a proteger.

Através da utilização de tecnologias e materiais eficientes projetou-se o sistema modular, representado na **figura 1**, tendo por base a sua facilidade de transporte e manuseamento por forças de defesa (militares e segurança pública). O sistema é composto pelos seguintes módulos independentes que agrupados implementam todas as funcionalidades do sistema: módulo de processamento (**20**) responsável por processar e coordenar toda a lógica do sistema; módulo de sensorização (**19**) com o objetivo de estimar a localização do drone; módulo de transmissão (**21**) onde estão presentes todas as tecnologias para a emissão de sinais de jamming e spoofing; módulo de alimentação (**18**) responsável por fornecer energia para todo sistema; módulo utilizador (**17**) que trata de todas as interações do sistema com o utilizador; e módulo de segurança (**22**) que contém medidas de prevenção e aumento da segurança do sistema.

O sistema apresentado minimiza a interferência em sistemas terceiros e, por outro lado, implementa técnicas avançadas de emissão de sinais de elevada eficiência energética, minimizando a pegada ambiental.

Descrição

Sistema Móvel para Imobilizar e Desviar Drones Não Autorizados

Domínio técnico da invenção:

A presente invenção diz respeito a áreas de segurança e privacidade, sendo um Sistema Móvel para Imobilizar e Desviar Drones não autorizados.

A técnica anterior:

Existem algumas soluções idênticas para o problema apresentado, como é o exemplo do sistema KNOX desenvolvido pela empresa MyDefence. Trata-se de um sistema fixo, pelo que a instalação num local demora algum tempo e é necessário investimento para cada local a proteger. O sistema apresentado é móvel e facilmente adaptado a qualquer zona, e.g., prisões, grandes aeroportos internacionais, eventos pontuais (como é o caso de festivais), presenças de entidades (e.g. presidentes, Papa, deputados, atletas de alta competição, figura públicas, etc.). Existe outra solução móvel, a REX-1 desenvolvida pela companhia Russa ZALA Aero. O KNOX e a REX-1 ainda não introduzem a técnica de spoofing apresentada no sistema proposto, significando uma ausência de uma funcionalidade importante num sistema com estas características. Apenas com as funcionalidades destes projetos comerciais é possível forçar a aterragem dos drones comerciais. Para drones manufaturados por terroristas, ou para outros fins maléficos a sua configuração é desenvolvida pelo técnico, sendo que neste caso o drone pode não ser forçado a aterrar apenas com o bloqueio dos sinais de navegação. O potencial subjacente ao sistema proposto, quando comparado com estas, é a generalização de um sistema que consegue controlar o drone alvo (não autorizado) para zonas seguras, minimizando níveis de interferência emitidos para dispositivos terceiros (telemóveis, aviões, drones autorizados, redes móveis celulares e rede de comunicação sem fios).

Descrição das figuras:

Figura 1.1: Representação ilustrativa do sistema, em perspetiva com vista lateral esquerda e superior. Equipado com um rail longo para acoplação de mira telescópica (1); sensor acelerómetro (2); caixa para microcontrolador (3); e receptor de localização (4).

Figura 1.2: Representação ilustrativa do sistema, em perspetiva com vista lateral esquerda e superior. Antena directiva para transmissão de sinais de posicionamento por satélite (5); ecrã táctil com mapa para interface com utilizador para definir zona segura (6); caixa para equipamento eletrónico para transmissão de sinais rádio (7); LEDs de sinalização de estado de funcionamento e sensor magnetómetro (8); e sensor biométrico para identificação do utilizador (9).

Figura 1.3: Representação ilustrativa do sistema, em perspetiva com vista lateral direita e inferior. Interruptor ON/OFF e selectores para diferentes modos de funcionamento (10); caixa para microprocessador (11); equipado com um rail curto para braço de apoio/ bipé (12).

Figura 1.4: Representação ilustrativa do sistema, em perspetiva com vista lateral direita e inferior. Alojamento da bateria (13); gatilhos para controle da transmissão (14); Antena directiva para transmissão de sinais na banda do controlo remoto (15); e medidor de distância ao alvo (16).

Figura 2.1: Sendo este um sistema modular, a figura representa os módulos principais que constituem o sistema. O módulo do Utilizador (17) é composto por Comandos do Utilizador e Interface Utilizador. Nos Comandos do Utilizador (10) estão localizados os botões ON/OFF para alimentar o sistema, botões para seleccionar vários modos de funcionamento e os gatilhos (14) para inicialização das transmissões de jamming e spoofing. Na Interface Utilizador encontra-se o ecrã (6) e LEDs (8) para interação com o utilizador. O módulo de Alimentação (18) é responsável pela alimentação de todo o sistema. O módulo de Processamento (20) é composto por o Microprocessador (11), responsável por todo o processamento do sistema. O módulo de Sensorização (19) é composto pelo Microcontrolador (3) que está directamente ligado ao Microprocessador (11) e é responsável por toda a leitura do Conjunto de Sensores (2) (4) (8) (9) (16) do

sistema. O módulo de Transmissão **(21)** é constituído por equipamentos electrónicos **(7)** para a transmissão de sinais rádio e pelas antenas directivas **(5)** **(15)**. O módulo de segurança **(22)** protege o sistema por autenticação através de sensor biométrico **(9)** o qual permite a utilização apenas a utilizadores previamente autorizados protegendo contra a utilização para efeitos que não sejam os devidos. Estão incorporados no sistema acessórios **(1)** **(12)** que servem de auxílio para a melhoria da experiência do utilizador e, consequentemente contribuir para a melhoria do desempenho no ataque aos drones.

Descrição pormenorizada da invenção:

É objectivo da presente invenção proteger a intrusão de drones não autorizados (comerciais e de fabrico customizado): terrestres, aéreos e aquáticos em zonas restritas, e.g., aeroportos, áreas militares, condomínios e situações pontuais de eventos públicos ou zonas onde é necessário garantir a segurança pública. Sendo um sistema móvel, consegue-se assim uma fácil e rápida adaptação às zonas a proteger.

Através da utilização de tecnologias e materiais eficientes projectou-se o sistema modular, tendo por base a sua facilidade de transporte e manuseamento por forças de defesa (militares e segurança pública).

Tendo o drones dois modos de funcionamento, o modo de pilotagem manual (controlando o drone com o controlo remoto) e o modo autónomo (traçando previamente uma rota através de coordenadas de localização geográfica), o sistema a patentear tem a funcionalidade de emitir sinais eficientes para bloquear estes dois tipos de comunicação com o aparelho.

A grande inovação e funcionalidade do sistema é a capacidade de poder desviar o drone invasor para uma zona determinada como segura. Para a realização desta tarefa, o sistema tem a necessidade de conhecer a localização do drone alvo. Para determinar a localização do drone invasor, estão acoplados ao sistema um conjunto de sensores como: medidor de distância **(16)**, acelerómetro **(2)**, sensor de localização **(4)** e magnetómetro **(8)**. Este sistema requer que o utilizador consiga apontar para o drone. Neste sentido, o sistema disponibiliza um conjunto de acessórios para ajudar o utilizador, e.g., bandoleira (que serve de apoio ao utilizador, aquando está em modo repouso para não existir fadiga física), mira telescópica **(1)**, laser óptico **(1)**, braço frontal de apoio **(12)** e bipé **(12)** (para facilitar a interceção com o drone). Para uma interacção com o utilizador, o sistema disponibiliza um ecrã táctil **(6)** e LEDs **(8)** (para definição de zonas seguras e visualização da interface do sistema, e visualização da alimentação do sistema).

A aquisição indireta do controlo do drone é efetuada através da utilização dos ficheiros efemérides disponibilizados que permitem a simulação de um conjunto de satélites, formando assim uma hipotética constelação, que posteriormente gera fluxos de dados

de sinal banda base que são transmitidos na gama de frequência do sistema de localização por satélite. O sistema foi projetado com dois modos de funcionamento de spoofing, um que funciona tendo apenas em conta a localização do drone, e outro, que tem em conta não apenas a localização mas também a direcção, sentido e velocidade, utilizando estes parâmetros em algoritmos desenvolvidos para que o spoofing seja suave e menos perceptível.

Em termos de segurança, para que não exista um uso indevido do equipamento, o sistema aloca um sensor biométrico (9), o qual permite a utilização apenas a utilizadores previamente autorizados protegendo contra a utilização para efeitos que não sejam os devidos. Além disso, através de comunicação de rede móvel, o sistema envia uma mensagem periódica (tempo configurável) com a informação da localização do sistema para uma entidade supervisora. Complementarmente, sempre que alguém inicialize o sistema ou inicie a transmissão é enviada também uma mensagem com o respectivo nome de utilizador.

Este sistema minimiza a interferência em sistemas terceiros devido à utilização de antenas altamente directivas (5) (15) e, por outro lado, implementa técnicas avançadas de emissão de sinais de elevada eficiência energética, aumentando a autonomia do sistema e contribuindo para a diminuição da pegada ambiental.

Os desenhos do sistema proposto não estão limitados à configuração apresentada, sendo possível realizar implementações modificadas do mesmo.

Descrição de modos particulares de realização:

O sistema móvel modular para localizar, neutralizar e desviar drones (aéreos, terrestres e aquáticos) não autorizados em determinadas áreas desenvolvido é caracterizado por:

- Detectar e localizar aparelhos não tripulados;
- Transmitir sinais electromagnéticos para bloqueio do controlo remoto e para bloqueio de sinais de localização via satélite;
- Gerar e transmitir de sinais falsos de localização por satélite.

Num modo de realização do sistema desenvolvido este é constituído por vários módulos independentes, nomeadamente módulos de Processamento (20), Sensorização (19),

Transmissão **(21)**, Alimentação **(18)**, Utilizador **(17)** e Segurança **(22)**, os quais podem funcionar de forma isolada, mas que acoplados constituem o sistema, possibilitando assim que sejam actualizados com novas tecnologias.

Num outro modo de realização do sistema desenvolvido, o módulo de sensorização **(19)** é responsável por executar a leitura de um conjunto de sensores, nomeadamente sensores para medição de distância **(16)**, inclinação **(2)**, orientação **(8)** e localização **(4)**, enviando as medições para o módulo de processamento **(20)** o qual efectua a estimação da localização do drone.

Num outro modo de realização do sistema desenvolvido, o módulo de transmissão **(21)** é responsável pela emissão de sinais eletromagnéticos, para bloquear os sinais emitidos pelo controlo remoto do drone e os sinais de radionavegação provenientes dos satélites de localização geográfica, neutralizando assim o modo de funcionamento manual e o modo de funcionamento autónomo do drone alvo.

Num outro modo de realização do sistema desenvolvido, o módulo de processamento **(20)** e o módulo de transmissão **(21)** têm em conjunto a capacidade de simular e transmitir uma hipotética constelação de satélites de localização geográfica, adquirindo o controlo do drone.

Num outro modo de realização do sistema desenvolvido, este caracteriza-se por ser móvel e por possuir um módulo de alimentação **(18)** baseado em baterias recarregáveis **(13)** e de fácil acesso tornando-o adaptável a qualquer tipo de local ou terreno a ser utilizado.

Num outro modo de realização do sistema desenvolvido, este recorre a antenas altamente diretivas **(5)** **(15)**, adaptadas para cada tecnologia, para que não exista uma interferência em receptores vizinhos que não sejam o alvo (e.g., aviões, redes móveis, redes de comunicação sem fios).

Num outro modo de realização do sistema desenvolvido, o módulo de utilizador **(17)** é constituído por interruptores de modo de funcionamento **(10)**, LEDs indicadores de estado de funcionamento **(8)** e um ecrã **(6)** onde é possível visualizar os mapas,

determinar as zonas seguras para uma aterragem do drone invasor em segurança e por ser adaptável tanto para destros como para utilizadores canhotos.

Num outro modo de realização do sistema desenvolvido, o módulo de processamento **(20)** é onde se alocam algoritmos inteligentes que consoante a distância ao drone, medida por um sensor **(16)**, controlam a potência de transmissão suficiente para afetar o drone, não existindo desperdício de energia e diminuindo a pegada ecológica.

Num outro modo de realização do sistema desenvolvido, este caracteriza-se por ser complementado com um conjunto de acessórios que auxiliam o utilizador a ter um melhor desempenho nomeadamente: uma mira telescópica **(1)**, um laser óptico **(1)**, um bipé **(12)** e um braço frontal de apoio **(12)**.

Num outro modo de realização do sistema desenvolvido, o módulo de segurança **(22)** protege o sistema por autenticação através de sensor biométrico **(9)** o qual permite a utilização apenas a utilizadores previamente autorizados protegendo contra a utilização para efeitos que não sejam os devidos.

Num outro modo de realização do sistema desenvolvido, o módulo de segurança **(22)** contém medidas de prevenção e aumento da segurança:

- Envio de uma mensagem periódica (tempo configurável) com a informação da localização do sistema para uma entidade supervisora usando rede móvel.
- Envio de uma mensagem usando rede móvel com o nome de utilizador, sempre que este inicialize o sistema ou inicie uma transmissão.

Reivindicações

1. Sistema móvel para imobilizar e desviar drones não autorizados caracterizado por compreender:

- um módulo de sensorização (19) adaptado a recolher dados relativos a distância, inclinação, orientação e localização;
- um módulo de processamento (20) compreendendo capacidade de processamento configurada para:
 - (i) determinar a localização de um drone a partir dos dados recolhidos pelo módulo de sensorização (19);
 - (ii) com base na localização do drone, simular uma constelação de satélites a partir de ficheiros efemérides, de forma a gerar fluxos de dados de sinal de banda base; e
 - (iii) programar um módulo de transmissão (21) para transmitir os fluxos de dados numa gama de frequência do sistema de localização por satélite;
- um módulo de transmissão (21) configurado para:
 - (i) emitir sinais eletromagnéticos adaptados a bloquear sinais emitidos por um controlador remoto e sinais de radionavegação; e
 - (ii) emitir sinais eletromagnéticos adaptados a realizar spoofing através de sinais de radionavegação.

2. Sistema de acordo com a reivindicação 1, caracterizado por o módulo de processamento (20) estar adicionalmente configurado para:

- determinar a direção, sentido e velocidade do drone a partir dos dados recolhidos pelo módulo de sensorização (19); e
- gerar fluxos de dados de sinal de banda base baseados na localização, direção, sentido e velocidade do drone.

3. Sistema de acordo com qualquer uma das reivindicações anteriores, caracterizado por o módulo de processamento estar adicionalmente programado para controlar a potência de transmissão do sinal emitido pelo módulo de transmissão (21), com base na distância entre o sistema e o drone.

4. Sistema de acordo com qualquer uma das reivindicações anteriores, caracterizado por o módulo de sensorização compreender o conjunto de sensores incluindo: sensor medidor de distância (16), acelerómetro (2), sensor de localização (4) e magnetómetro (8).
5. Sistema de acordo com qualquer uma das reivindicações anteriores, caracterizado por o módulo de transmissão (21) compreender antenas diretivas (5)(15).
6. Sistema de acordo com qualquer uma das reivindicações anteriores, caracterizado por compreender adicionalmente um módulo de utilizador (17) constituído por interruptores de modo de funcionamento (10), LEDs indicadores de estado de funcionamento (8) e um ecrã (6) adaptado à visualização de mapas.
7. Sistema de acordo com qualquer uma das reivindicações anteriores, caracterizado por compreender adicionalmente um módulo de alimentação (18) compreendendo baterias recarregáveis (13).
8. Sistema de acordo com qualquer uma das reivindicações anteriores, caracterizado por o compreender adicionalmente um módulo de segurança (22) que inclui mecanismo de autenticação através de sensor biométrico.
9. Sistema de acordo com a reivindicação 8, caracterizado por o módulo de segurança estar configurado a:
 - (i) Enviar uma mensagem periódica através de rede móvel, com informação da localização do sistema para uma entidade supervisora;
 - (ii) Enviar uma mensagem através de rede móvel com o nome do utilizador, sempre que este inicialize o sistema.
10. Sistema de acordo com qualquer umas das reivindicações anteriores, caracterizado por compreender adicionalmente pelo menos um ou uma combinação entre os seguintes acessórios: mira telescópica (1), laser óptico, bipé (12), braço frontal de apoio.

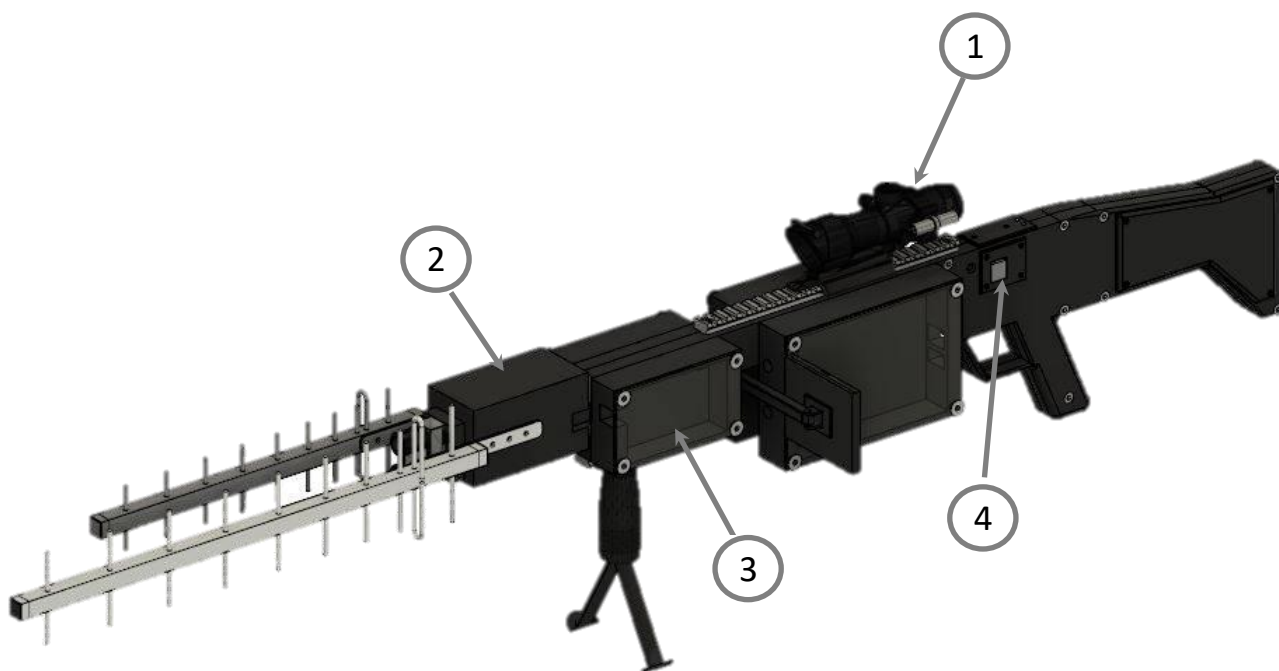


Figura 1.1

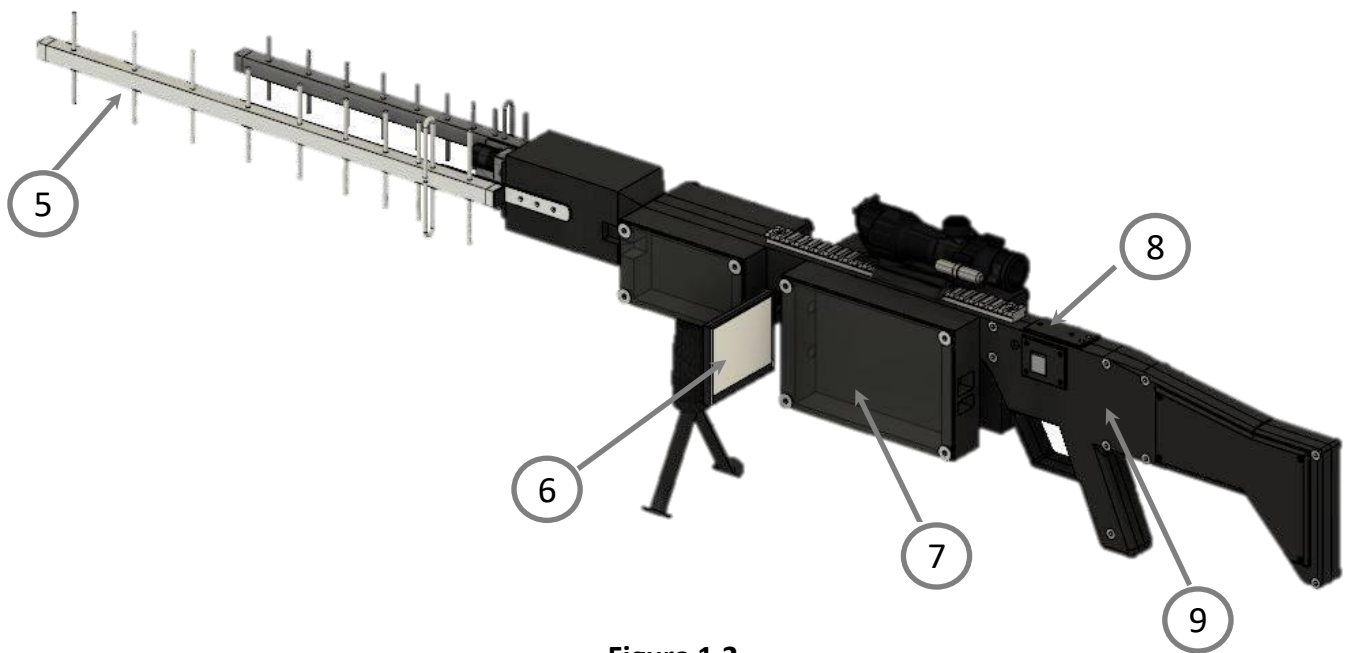


Figura 1.2

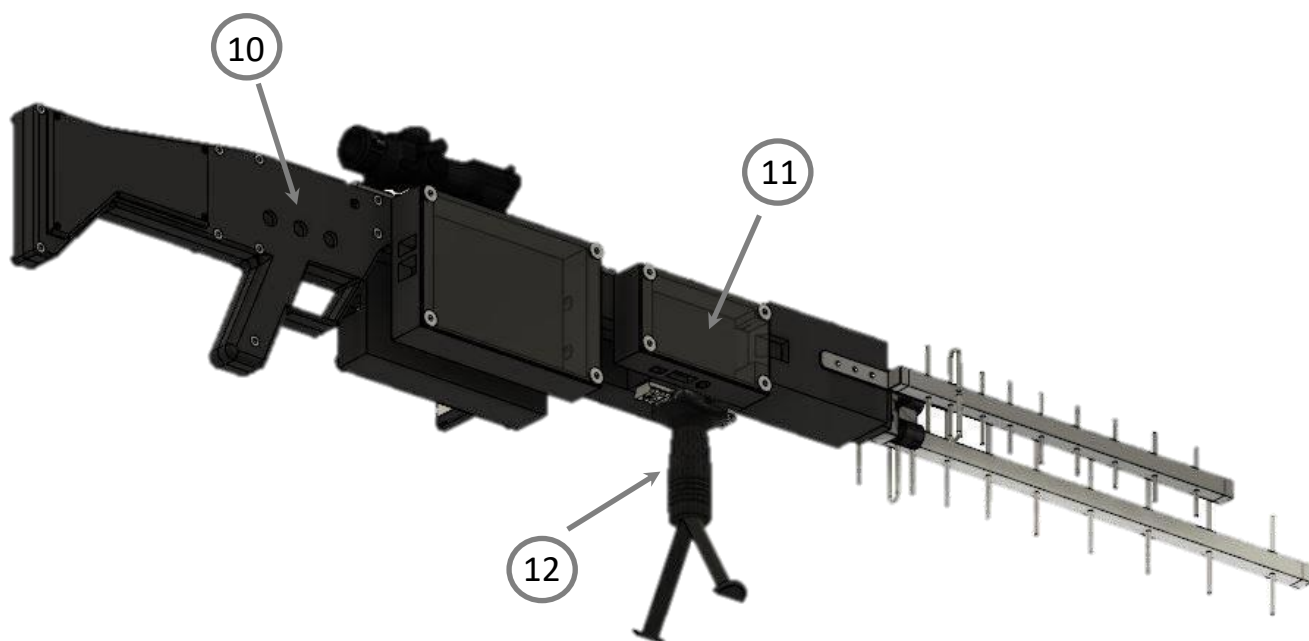


Figura 1.3

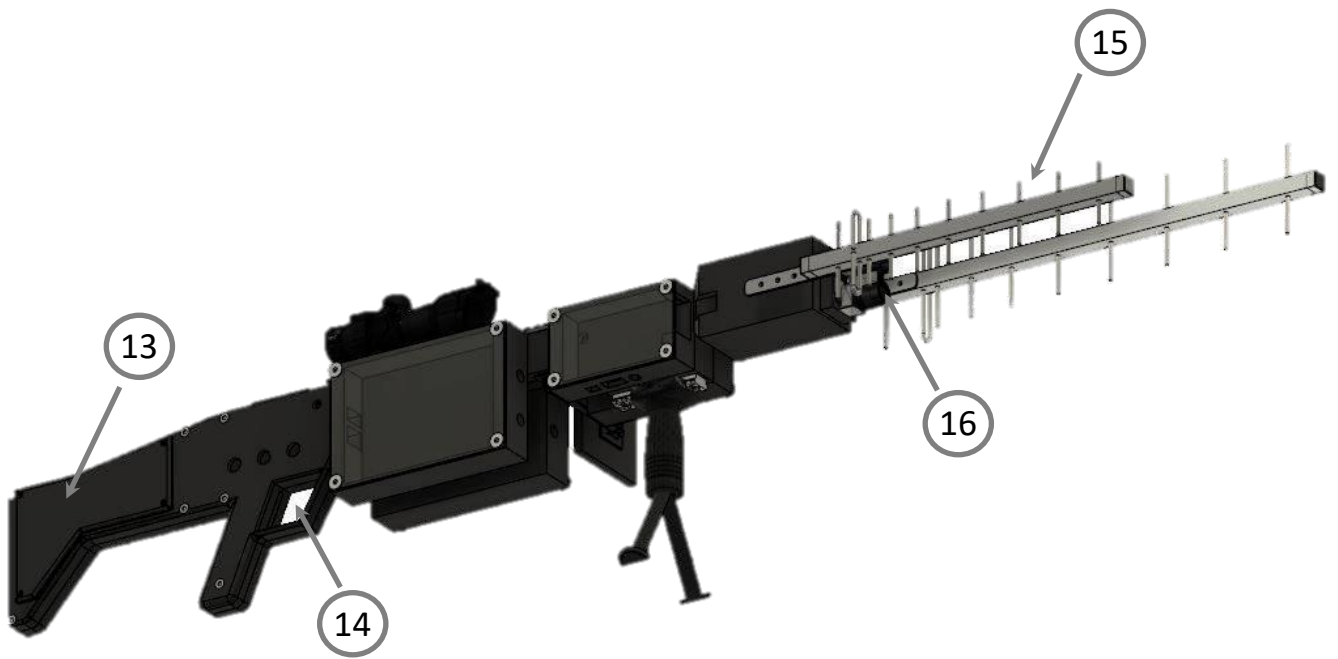


Figura 1.4

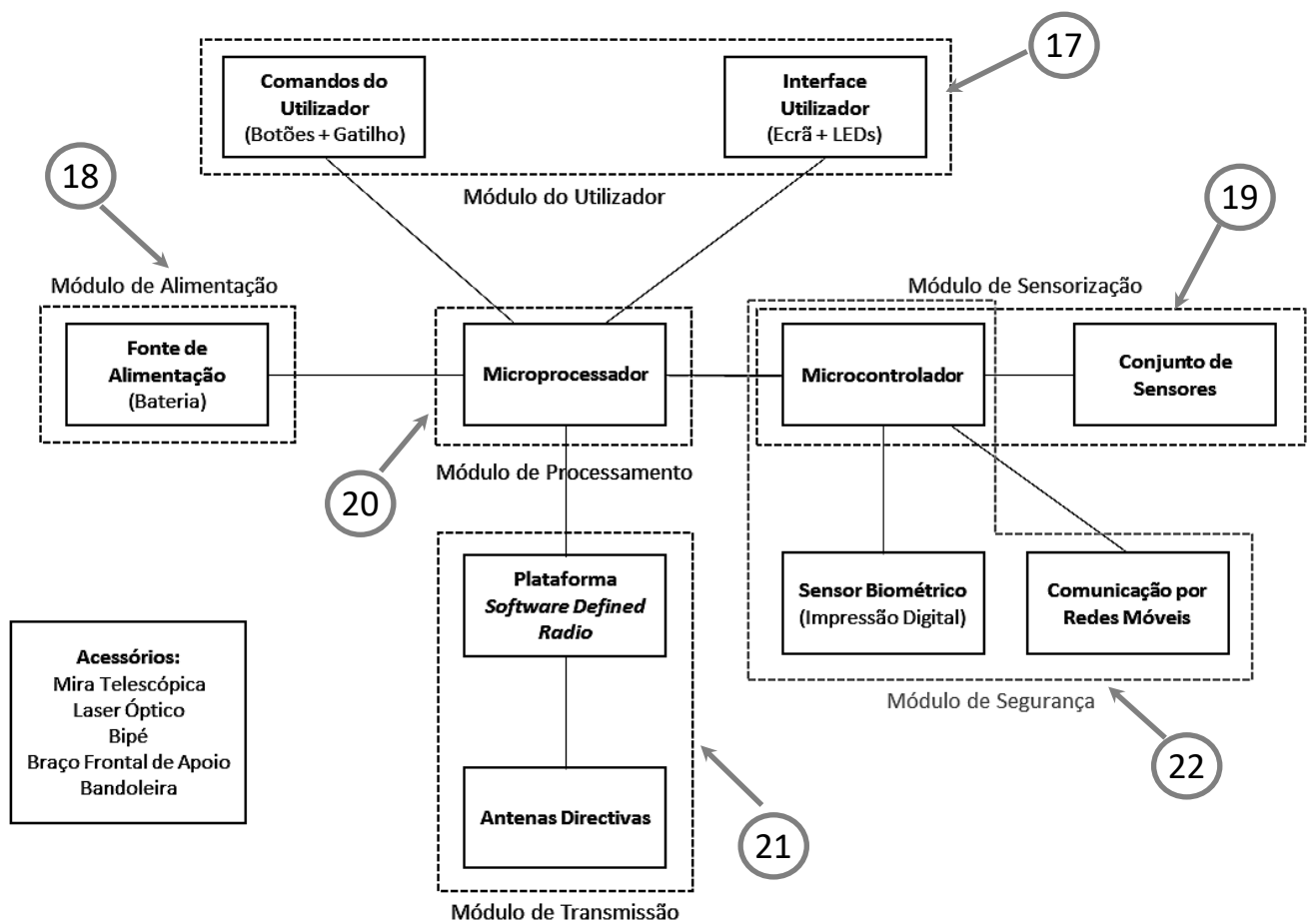


Figura 2.1

Appendix A – translated version

MOBILE SYSTEM TO IMMOBILIZE AND DIVERT UNAUTHORIZED DRONES



Publication Number: PT 115663 B

International Classification:
G05D 1/00 (2006)

INVENTION PATENT

Date of request: **2019.07.19**

Date of request's publication: **2021.01.19**

Date of grant: **2021.07.26**

Date of grant's Publication: **2021.07.29**

Owner(s):

**RENATO BRANCO FERREIRA
JOÃO FILIPE DE QUADROS GASPAR
PEDRO JOAQUIM AMARO SEBASTIÃO
NUNO MANUEL BRANCO SOUTO
ISCTE- INSTITUTO UNIVERSITÁRIO DE
LISBOA**

Inventor(s):

**RENATO BRANCO FERREIRA
JOÃO FILIPE DE QUADROS GASPAR
PEDRO JOAQUIM AMARO SEBASTIÃO
NUNO MANUEL BRANCO SOUTO**

Trustee:

**RUI DO NASCIMENTO GOMES
J. PEREIRA DA CRUZ, S.A.
RUA VITOR CORDON, 14 1249-103
LISBOA**

Abstract: IN RECENT TIMES, THERE HAVE BEEN SEVERAL REPORTS OF DRONE INCIDENTS INVOLVING AIRCRAFT NEAR AIRPORTS OR AERODROMES. WITH THE MOBILE SYSTEM FOR IMMOBILIZING AND DIVERTING UNAUTHORIZED DRONES, IT IS POSSIBLE TO PROTECT THE INTRUSION OF UNAUTHORIZED DRONES (COMMERCIAL AND CUSTOM-MADE), LAND, AIR AND WATER DRONES IN RESTRICTED AREAS, E.G. AIRPORTS, MILITARY AREAS, CONDOMINIUMS AND SPECIFIC SITUATIONS OF PUBLIC EVENTS OR AREAS WHERE PUBLIC SAFETY NEEDS TO BE ENSURED. AS IT IS A MOBILE SYSTEM, IT CAN BE EASILY AND QUICKLY ADAPTED TO THE AREAS TO BE PROTECTED. THIS SYSTEM MINIMISES INTERFERENCE IN THIRD PARTY SYSTEMS AND, ON THE OTHER HAND, IMPLEMENTS ADVANCED, HIGHLY ENERGY EFFICIENT SIGNAL EMISSION TECHNIQUES, MINIMISING THE ENVIRONMENTAL FOOTPRINT. BY USING EFFICIENT TECHNOLOGIES AND MATERIALS, THE MODULAR SYSTEM, REPRESENTED IN FIGURE 1, WAS DESIGNED BASED ON ITS EASE OF TRANSPORT AND HANDLING BY DEFENCE FORCES (MILITARY AND PUBLIC SECURITY).

Abstract

Mobile System to Immobilise and Divert Unauthorized Drones

The invention aims to protect against the intrusion of unauthorized drones (commercial and customised), land, air and water drones in restricted areas, e.g. airports, military areas, condominiums and occasional public events or areas where it is necessary to guarantee public safety. As it is a mobile system, it can be easily and quickly adapted to the areas to be protected.

Using efficient technologies and materials the modular system was designed, represented in the **figure 1**, being easy to transport and handle by defence forces (military and public security). The system is composed of independent modules that together implement all the functionalities of the system: processing module **(20)** responsible for processing and coordinating all system logic; sensing module **(19)** in order to estimate the drone's location; transmission module **(21)** for all technologies for jamming and spoofing signals; power supply module **(18)** responsible for providing energy for the entire system; user module **(17)** for all system users' interactions; and security module **(22)** which contains measures to prevent and increase the security of the system.

The presented system minimises interference with third party systems and, on the other hand, implements advanced signal emission techniques with high energy efficiency, minimising the environmental footprint.

Description

Mobile System to Immobilise and Divert Unauthorized Drones

Technical field of invention:

The present invention relates to the areas of security and privacy, as it is a Mobile System for Immobilising and Diverting Unauthorized Drones.

The previous technique:

There are some identical solutions to the problem presented, such as the KNOX system developed by the company MyDefence. It is a fixed system, so installation on a site takes time and investment is needed for each site to be protected. The system presented is mobile and easily adapted to any area, e.g., prisons, international airports, events and festivals, presences of entities (e.g., presidents, the Pope, MPs, public figures, etc.). There is another mobile solution, the REX-1 developed by the Russian company ZALA Aero. KNOX and REX-1 do not introduce the spoofing technique presented in the proposed system, meaning an absence of an important functionality in a system with these characteristics. Only with the features of these commercial projects is it possible to force commercial drones to land. For drones manufactured by terrorists, or for other evil purposes their configuration is developed by the technician, in which case the drone may not be forced to land just by blocking the navigation signals. The underlying potential of the proposed system, when compared to these, is the generalisation of a system that can control the target (unauthorized drone) to safe zones, minimising interference levels emitted to third party devices (mobile phones, aircraft, authorized drones, cellular mobile networks and wireless communication network).

Figures' Description:

Figure 1.1: Illustrative representation of the system, in perspective with left and top side view. Equipped with a long rail for attaching a telescopic sight (1); accelerometer sensor (2); microcontroller box (3); and receiver location (4).

Figure 1.2: Illustrative representation of the system, in perspective with left and top side view. Directive antenna for the transmission of satellite positioning signals (5); touch screen with map for user interface to define safe zone (6); electronic equipment for transmission of radio signals (7); Operating status LEDs and magnetometer sensor (8); and biometric sensor for user identification (9).

Figure 1.3: Illustrative representation of the system, in perspective with right and bottom side view. ON/OFF switch and selectors for different operating modes (10); microprocessor box (11); fitted with a short rail for support arm/bipod (12).

Figure 1.4: Illustrative representation of the system, in perspective with right and bottom side view. Battery compartment (13); triggers to control the transmission (14); Directional antenna for transmitting signals in the remote-control band (15); and distance-to-target meter (16).

Figure 2.1: As this is a modular system, the figure represents the main modules of the system. The User module (17) consists of User Commands and User Interface. In the User Commands (10) are located the ON/OFF buttons to power the system, buttons to select various operating modes and the triggers (14) for jamming and spoofing transmissions. On the User Interface is the touch screen (6) and LEDs (8) for interaction with the user. The Power Supply Module (18) for powering the entire system. The Processing module (20) is composed by the Microprocessor (11), responsible for all system processing. The Sensing Module (19) is composed by Microcontroller (3) which is directly connected to the Microprocessor (11) and is responsible for all the reading of the system's Sensor Set (2) (4) (8) (9) (16). The Transmission module (21) is composed of electronic equipment (7) for the transmission of radio signals and by directive antennas (5) (15). The security module (22) protects the system by authentication through biometric sensor (9) which allows to use only by previously authorised users and protects against use for purposes other than those intended. Accessories are

incorporated in the system **(1)** **(12)** which help to improve the user experience and consequently contribute to improved performance in attacking drones.

Detailed description of the invention:

It is an object of the present invention to protect against intrusion by unauthorized drones (commercial and customised manufacturing): terrestrial, aerial and aquatic in restricted zones, e.g. airports, military areas, condominiums and occasional public event situations or zones where it is necessary to guarantee public safety. As it is a mobile system, it can be easily and quickly adapted to the areas to be protected.

Through the use of efficient technologies and materials, the modular system was designed, based on its ease of transport and handling by defence forces (military and public security).

Drones having two modes of operation, manual piloting mode (the drone is controlled with the remote control) and autonomous mode (plotting a route in advance using geographical location coordinates), the system to be patented has the functionality of emitting efficient signals to block these two types of communication with the device.

The great innovation and functionality of the system is the ability to be able to divert the invading drone to a zone determined to be safe. To perform this task, the system has the need to know the location of the target drone. To determine the location of the invading drone, a set of sensors are attached to the system such as: distance meter (**16**), accelerometer (**2**), location sensor (**4**) and magnetometer (**8**). This system requires the user to be able to aim the drone. In this sense, the system provides a set of accessories to help the user, e.g., shoulder strap (which serves as a support for the user, when in rest mode to avoid physical fatigue), telescopic sight (**1**), optical laser (**1**), front support arm (**12**) and bipod (**12**) (to facilitate interception with the drone). For user interaction, the system provides a touch screen (**6**) and LEDs (**8**) (for defining safe zones, viewing the system interface and viewing the system power supply).

The indirect acquisition of the drone control is carried out using the ephemeris files provided, which allow the simulation of a set of satellites, thus forming a hypothetical constellation, which subsequently generates baseband signal data streams that are transmitted in the frequency range of the satellite positioning system. The system is designed with two spoofing modes of operation, one that works by considering only the location of the drone, and another, which takes into account not only the location but

also the direction, direction and speed, using these parameters in algorithms developed to make spoofing smooth and less noticeable.

In terms of security, so that there is no misuse of the equipment, the system allocates a biometric sensor (9), which allows it to be used only by pre-authorised users and protects against use for purposes other than those intended. In addition, via mobile network communication, the system sends a periodic message (configurable time) with information on the location of the system for a supervisory entity. In addition, whenever someone initialises the system or starts the transmission, a message is also sent with the respective username.

This system minimises interference to third party systems due to the use of highly directive antennas (5) (15) and, on the other hand, implements advanced techniques for the emission of highly energy efficient signals, increasing the autonomy of the system and contributing to the reduction of the environmental footprint.

The design of the proposed system is not limited to the configuration presented, and modified implementations of it are possible.

Description of modes:

The modular mobile system to locate, neutralise and divert unauthorized drones (air, land and water) in certain developed areas is characterised by:

- Detecting and locating unmanned aircraft;
- Transmit electromagnetic signals for jamming remote control communications and for jamming satellite location signals;
- Generating and transmitting false satellite positioning signals.

The developed system is composed of several independent modules: Processing module (20), Sensing (19), Transmission (21), Power Supply (18), User (17) and Security (22), which can work in isolation, but which together constitute the system, thus enabling them to be updated with new technologies.

In another realisation mode of the developed system, the Sensing Module (19) is responsible for carrying out the reading of a set of sensors, such as sensors for distance

measurement **(16)**, tilt **(2)**, orientation **(8)** and location **(4)**, sending the measurements to the processing module **(20)** which estimates the drone's location.

In another realisation mode of the developed system, the transmission module **(21)** is responsible for the emission of electromagnetic signals, to jamming the signals emitted by the drone's remote control and the radio navigation signals coming from geo-location satellites, thus neutralising the manual and autonomous operating mode of the target drone.

In another realisation mode of the developed system, the processing module **(20)** and the transmission module **(21)** together have the ability to simulate and transmit a hypothetical constellation of geo-location satellites, acquiring control of the drone.

In another way of realising the developed system, it is characterised by being mobile and by having a power supply module **(18)** based on rechargeable batteries **(13)** and easy to access making it adaptable to any type of location or setting.

In another way of realising the developed system, it uses highly directive antennas **(5)** **(15)**, adapted for each technology, so that there is no interference in neighbouring receivers that are not the target (e.g., aircraft, mobile networks, wireless communication networks).

In another realisation mode of the developed system, the user module **(17)** consists of operating mode switches **(10)**, LEDs operating status indicators **(8)** and a screen **(6)** where it is possible to view the maps and determine the safe zones for a safe landing of the invading drone. The system is adaptable for both right-handed and left-handed users.

In another realisation mode of the developed system, the processing module **(20)** responsible for the intelligent algorithms that depending on the distance to the drone, measured by a sensor **(16)**, controls the transmission power sufficient to affect the drone, so no energy is wasted and the environmental footprint is reduced.

In another realisation mode of the developed system, it is characterised by being complemented with a set of accessories that help the user to have a better performance

such as: a telescopic sight **(1)**, an optical laser **(1)**, a bipod **(12)** and a front support arm **(12)**.

In another way of realising the developed system, the security module **(22)** protects the system by authentication through biometric sensor **(9)** which allows use only by pre-authorised users and protects against use for purposes other than those intended.

In another way of realising the developed system, the security module **(22)** contains measures to prevent and increase security:

- Sending a periodic message (configurable time) with the system location information to a supervising entity using mobile network.
- Sending a message using the mobile network with the user name, every time the user initialises the system or starts a transmission.

Claims

1. Mobile system to immobilise and divert unauthorized drones featuring:
 - a Sensing Module (19) adapted to collect data on distance, tilt, orientation and location;
 - a processing module (20) incorporating processing capacity configured for:
 - (i) determine the location of a drone from the data collected by the Sensing Module (19);
 - (ii) based on the location of the drone, simulate a constellation of satellites from ephemeris files in order to generate baseband signal data streams; and
 - (iii) programming a transmission module (21) to transmit the data streams in a frequency range of the satellite positioning system;
 - a transmission module (21) configured to:
 - (i) emit electromagnetic signals adapted to jamming signals emitted by a remote controller and radio navigation signals; and
 - (ii) emitting electromagnetic signals adapted to perform spoofing via radio navigation signals.
2. System according to the claim 1, characterised by the processing module (20) be additionally configured to:
 - determine the drone's direction, direction and speed from the data collected by the Sensing Module (19); and
 - generate baseband signal data streams based on location, direction, and speed of the drone.
3. System according to any of the preceding claims, characterised by the processing module being additionally programmed to control the transmit power of the signal emitted by the transmission module (21), based on the distance between the system and the drone.
4. System according to any of the preceding claims, characterised in that the sensing module comprises the sensor array including: distance measuring sensor (16), accelerometer (2), location sensor (4) and magnetometer (8).

5. System according to any of the preceding claims, characterised by the transmission module (21) is composed of directional antennas (5)(15).
6. System according to any of the preceding claims, characterised by additionally comprising a user module (17) consisting of operating mode switches (10), LED operating status indicators (8) and a screen (6) adapted to the visualisation of maps.
7. System according to any of the preceding claims, characterised by additionally comprising a power supply module (18) including rechargeable batteries (13).
8. System according to any of the preceding claims, characterised by the additionally comprising a security module (22) which includes authentication mechanism through biometric sensor.
9. System according to claim 8, characterised by the security module being configured to:
 - (i) Send a periodic message via mobile network, with information on the location of the system to a supervising entity;
 - (ii) Send a message via the mobile network with the user's name every time the user initialize the system.
10. System according to any of the preceding claims, characterised by additionally comprising at least one or a combination of the following accessories: telescopic sight (1), optical laser, bipod (12), front support arm.

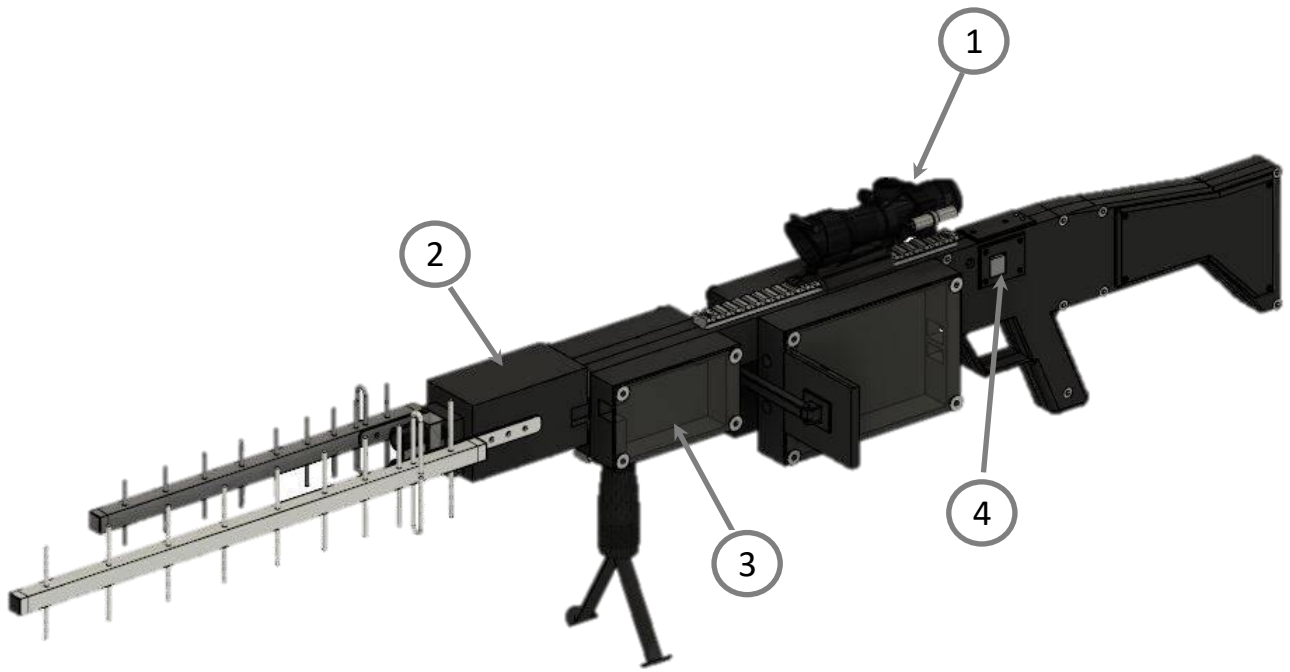


Figure 1.1

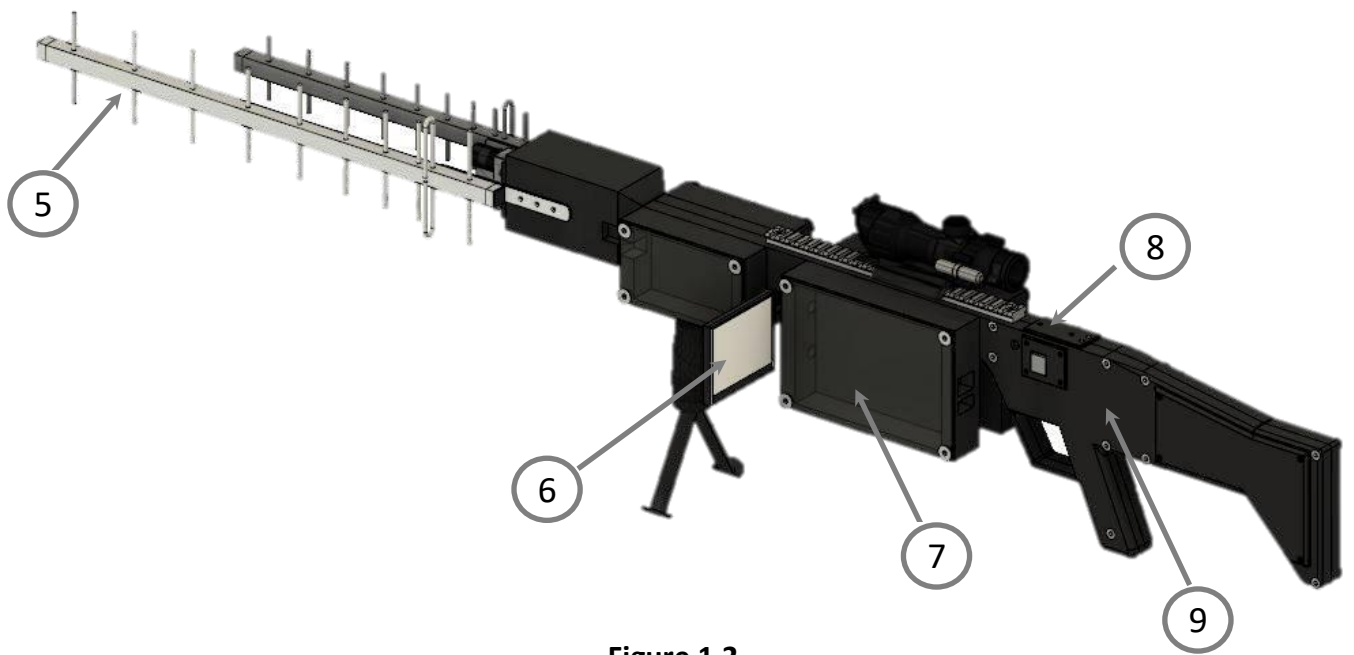


Figure 1.2

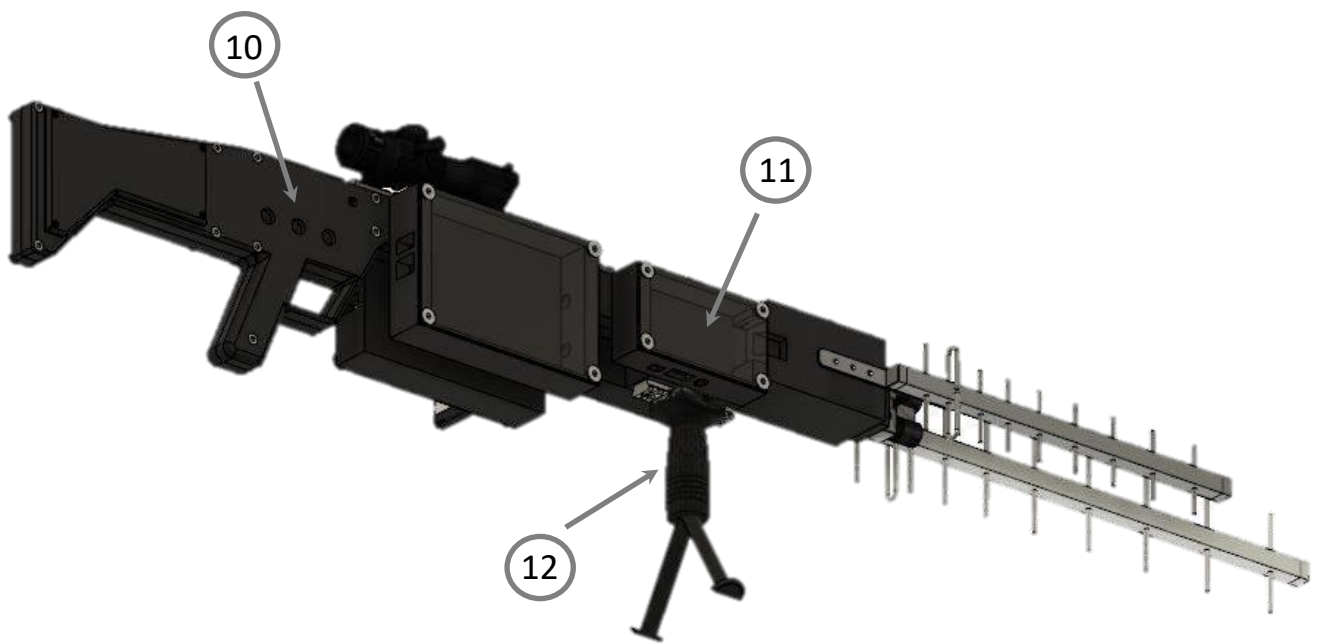


Figure 1.3

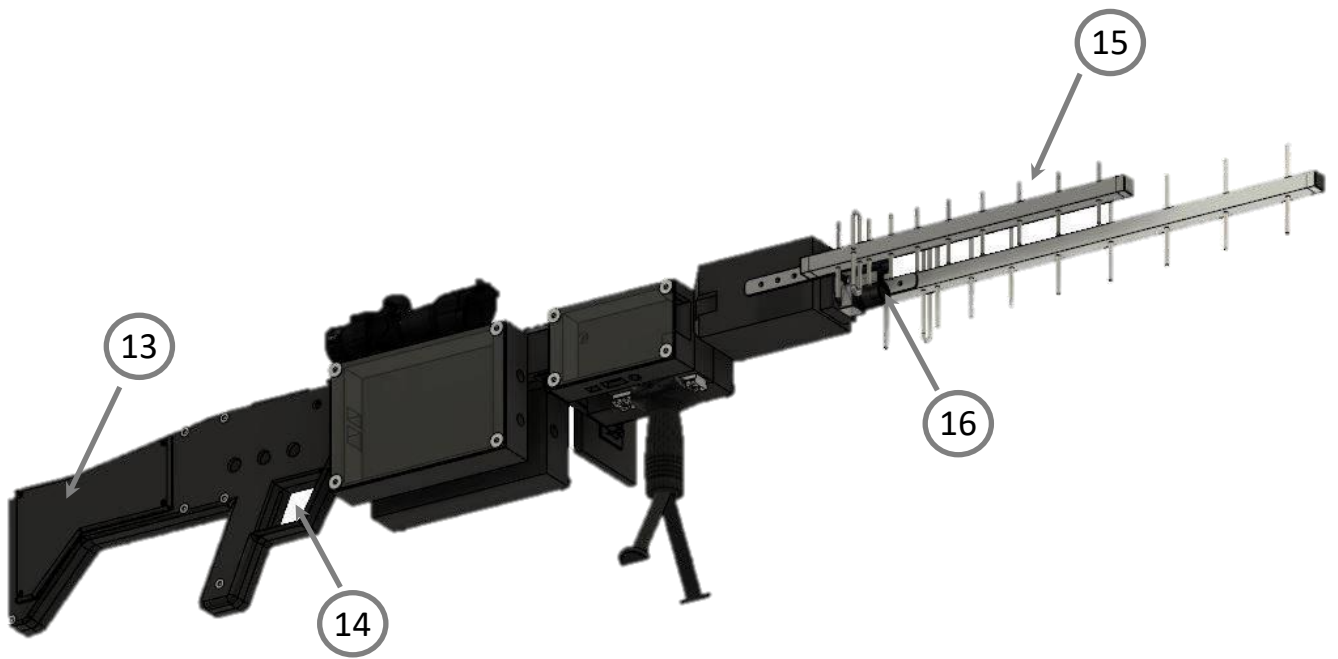


Figure 1.4

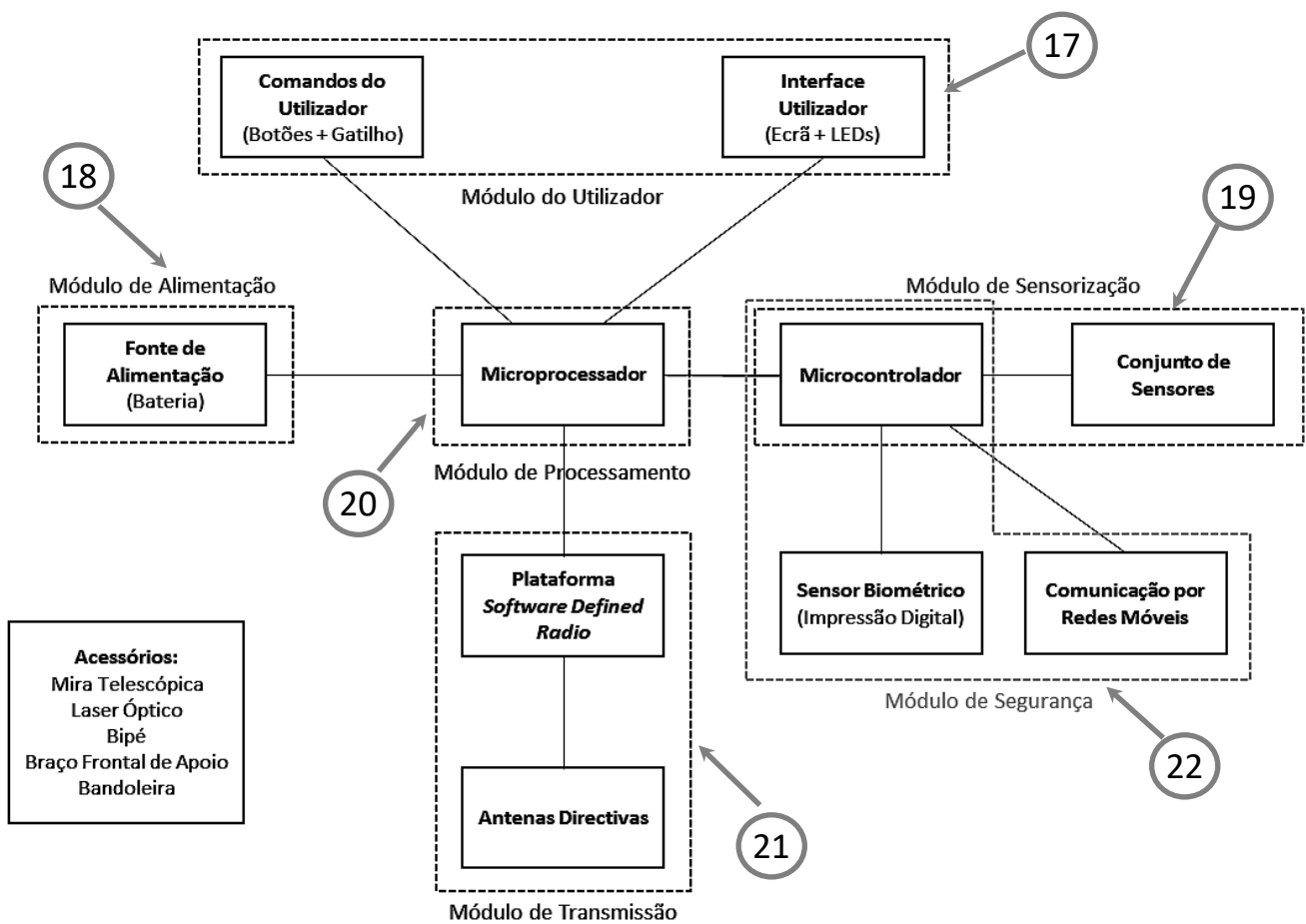


Figure 2.1

17 - User module (user commands and User Interface)

18 - Power Supply module (battery)

19 - Sensing Module (microcontroller and sensor set)

20 - Processing module (microprocessor)

21 - Transmission module (software defined radio and directional antennas)

22 - Security module (microprocessor, biometric sensor, and mobile network communications)

Appendix B

A PORTABLE EQUIPMENT FOR TRANSPORTING COUNTERMEASURE DEVICES



Comprovativo da submissão eletrônica

O Organismo receptor (RO/IB) acusa a recepção de um pedido internacional do PCT depositado através do ePCT-Filing. An Application Number and Date of Receipt have been automatically assigned (Administrative Instructions, Part 7).

Número de submissão:	057947	
Número de pedido:	PCT/IB2021/057947	
Data de recepção:	31 Agosto 2021	
Organismo receptor:	Secretaria Internacional da OMPI	
A sua referência:	2021-1183TA	
Requerente:	SWATTER COMPANY, LDA	
Número de requerentes:	1	
Título:	A PORTABLE EQUIPMENT FOR TRANSPORTING COUNTERMEASURE DEVICES	
Documentos submetidos:	20211183TA-appb-000004.pdf	382354
	(2021-1183TA vdepósito 24082021.pdf)	
	20211183TA-appb.xml	976
	20211183TA-fees.xml	1984
	20211183TA-requ.xml	6269
	20211183TA-vlog.xml	784
Submetido por:	CRUZ JOÃO PEREIRA (ID de cliente: user_PT_JOAO-PEREIRA_CRUZ_4876)	
Carimbo de hora do comprovativo:	31 Agosto 2021 16:25 UTC+2 (CEST)	
Sumário oficial da submissão:	E9:6A:AB:23:C2:72:FE:28:04:35:9E:43:40:FA:B8:A1:7B:01:6B:A1	

/Genebra, Organismo receptor/IB/

DESCRIPTION

A PORTABLE EQUIPMENT FOR TRANSPORTING COUNTERMEASURE DEVICES

FIELD OF THE INVENTION

The present invention is enclosed in the area of countermeasure devices adapted to act on unmanned systems. More particularly, the present invention relates to equipment for storing, charging, and transporting countermeasure devices.

PRIOR ART

Unmanned systems or autonomous aerial vehicles ("UAV), more commonly known as "drones", have become more and more prevalent in both the military and civilian context. Known, commercially available drones embody technology that was until recently, solely within the purview of governmental entities. The drones available to the civilian and military markets include navigation systems, various types of eavesdropping components, high-definition or real-time video output, long life lithium batteries, and the like. Furthermore, known civilian models may be operated by any individual, without regarding to licensing or regulation. The propagation of civilian drone usage has resulted in invasions of privacy, interference with official governmental operations, spying on neighbours, spying on government installations, and myriad other offensive operations.

This widespread use of drones has led to security and privacy concerns for the military, law enforcement, and the private citizen, driving a rapid growth in defence technologies embedded in countermeasure devices making them more advanced and effective for the task at hand. However, there is a limitation associated with the operation of these devices, which is related to their operating range and autonomy, as they concern complex apparatus, which need to be charged periodically. In fact, in a practical scenario in which the countermeasure device is programmed to operate in a remote area, away from an area surrounding its main base station, it is necessary to transport it to the appropriate location, while guaranteeing the operability of the device in terms of autonomy. In this regard, the state of the art, despite disclosing

new technologies related to both police-drones or handheld devices, seems to disregard the issues related to the operating range and autonomy of said devices, which may impose geographic limitations on the action to said devices.

The present solution intended to innovatively overcome such issues.

SUMMARY OF THE INVENTION

It is therefore an object of the present invention a portable equipment for transporting at least one countermeasure device adapted to act on an unmanned system. Such equipment therefore provides a portable base station that allows the storage and transport of countermeasure devices to remote locations, ensuring their operability for long periods of time. This is particularly relevant in scenarios where the operation of the countermeasure device takes place in remote locations, away from a main base station, ensuring that the operability of the devices is not compromised.

For that purpose, the portable equipment is comprised by a docking platform formed for detachable attachment of at least one countermeasure device. Additionally, the docking platform integrates a battery charging station comprising at least one charging terminal configured to apply charging power to a countermeasure device. By means of this portable docking station, the operation of the countermeasure devices is ensured for long periods of time.

The portable equipment is further comprised by a geolocation module and by a communication module designed in such a way that an information item relating to the location of the equipment is remotely accessible to an external system. In this way it is ensured that the location of the portable equipment is always known, which is important in the case where the operation of countermeasure devices takes place in remote and inaccessible places, so that the collection of the equipment can easily occur.

The present application also relates to a system comprised by a plurality of portable equipment and a central unit, working as an external system and configured to centralize all the information acquired from each portable equipment. Said information can then be accessed by authorized users. The connection between

portable equipment and the central unit is performed by means of a communication network.

DESCRIPTION OF FIGURES

Figure 1 – representation of an embodiment of the portable equipment with a rigid envelope. The portable equipment being in a closed state, and the reference signs represent:

- 1 – portable equipment;
- 2 – rigid envelope;
- 3 – handle.

Figure 2 – representation of an embodiment of the portable equipment with a rigid envelope. The portable equipment being in an open state, and the reference signs represent:

- 1 – portable equipment;
- 2 – rigid envelope;
- 4 – screen display of the user interface unit.

DETAILED DESCRIPTION

The more general and advantageous configurations of the present invention are described in the Summary of the invention. Such configurations are detailed below in accordance with other advantageous and/or preferred embodiments of implementation of the present invention.

The present invention relates to a portable equipment for transporting at least one countermeasure device adapted to act on unmanned systems. In the context of the present application, a countermeasure device may be in the form of a drone or it may be man-portable having a handheld form factor body. More particularly, in the context of the present application, a countermeasure device in the form of a drone is designated as a police-drone.

In a preferred aspect of the portable equipment of the present invention, the docking platform allows the storage of at least one countermeasure device. Therefore, the size of the equipment, particularly, the volume of the equipment's envelope may vary depending on the number of devices to be transported. The battery charging station, integrated in the docking platform is adapted to charge the countermeasure devices by means of charging terminals. The technology involved in developing such charging terminals is known from the art. The battery capacity of the charging station may vary depending on the size of the portable equipment which may be dependent on the number of countermeasure devices to be transported. Said charging station's capacity is adapted to provide at least two additional full charges for each countermeasure device being transported. Particularly, if the equipment is projected to store and transport one 10000 mAh handheld countermeasure device, the charging station capacity will be of at least 20000 mAh. It is important to mention that the portable equipment itself comprises a separate power unit used to feed all its electric components, modules and units.

In a preferred embodiment of the portable equipment of the present invention, combinable with any of the above described, it further comprises an access control unit, configured to restrict access to the interior of the envelope responsive to at least one access credential.

In another preferred embodiment, the access control unit is configured to restrict access to the at least one countermeasure device attached to the docking platform responsive to at least one access credential.

More particularly, according to another preferred embodiment, the access control unit is programmed to configure access criteria and security rules adapted to provide different levels of access responsive to access credentials, wherein each countermeasure device being associated to a level of access. In this way it is possible to establish different levels of access either for opening the envelope and for operating a countermeasure device stored inside the equipment, which is useful to establish an adequate interaction of the equipment with several users, each one with different skills

of expertise or assigned to different functions within a security scheme of an organization, by ensuring that only a specific user will be able to access the interior of the envelope and to operate a countermeasure device stored therein. Consequently, an unauthorized user will not be able to open the equipment, and a user being associated to a level of access will only be able to access a countermeasure device which is of the same level of access. The access criteria and security rules used to implement such security protocols are known from the art, and are applied in the context of accessing to the interior of the envelope and also to a countermeasure device.

More particularly, in one embodiment, the access control unit comprises a biometric sensor adapted to collect biometric data from a user. In this context, the access credentials relate to biometric data of a user. Alternatively, any face recognition system may be used and incorporated in the access control unit.

In another embodiment the access credential is a password, which may be remotely or locally inserted by means of input means.

More particularly, and in connection with the previous embodiments, the access control unit is programmed to configure access criteria and security rules adapted to provide different levels of access responsive to a primary or a secondary password.

Issues related to security, in particular access to the interior of the equipment and devices stored in it, are especially relevant when the operation takes place in locations far from main base station, where access to countermeasure devices may be easily controlled using any state-of-the-art system. So, the portable equipment developed includes the referred security measures/protocols/systems in order to ensure that an appropriate level of security can be achieved, even in a remote location.

In another preferred embodiment of the portable equipment of the present invention, combinable with any of the above described, the communication module is further configured to establish a communication data link with the at least one countermeasure device for collecting operational data related to said countermeasure device.

In a preferred aspect, the operational data may relate to unmanned system's landing position and/or countermeasure device's flight routes and/or data

related to countermeasure device's transmitted redirection signals. In this way, the portable equipment may also work as a remote base station, where a user may obtain information regarding operational data of the device.

In another preferred embodiment of the portable equipment of the present invention, combinable with any of the above described, it further comprises a user interface unit. Said user interface unit comprises at least a screen display adapted to display a user interface including displaying at least the following information: battery level of the battery charging station, location of the portable equipment, user interaction data records, and technical information related to the at least one countermeasure devices.

More particularly, in a preferred aspect, the countermeasure device's technical information may relate to at least one of the following parameters: type of countermeasure device; battery level; operational data records relating to unmanned system's landing position and/or countermeasure device' flight routes and/or data related to countermeasure device's transmitted redirection signals.

Additionally, in a preferred aspect, user interaction data records may include information related to the identification of the user accessing to the equipment and time and date of access. In this way it is possible to keep track of all the information related to the operation of the device which may be useful for its maintenance in order to avoid wear and foresee possible anomalies.

In another preferred embodiment of the portable equipment of the present invention, the user interface unit comprises input means. Particularly, the screen display is a touch screen display and the input means is provided by the touch screen display. Alternatively, the input means may be of a keyboard type.

In another preferred embodiment of the portable equipment of the present invention, combinable with any above described, the envelope is rigid, in order to protect the countermeasure devices stored inside.

In another embodiment, the portable equipment comprises at least one handle, installed in the outer surface of the envelope, enabling it to be carried.

Additionally, in another preferred embodiment, combinable with any of the above described, the equipment comprises means of displacement installed in the outer surface of the envelope proving the contact with the ground. More particularly, the means of displacement being at least one wheel, and optionally, the envelope further comprising a handle enabling the equipment to be rolled along by means of the at least one wheel.

In another preferred embodiment, combinable with any above described, equipment further comprises attaching means installed in the outer surface of the envelop. Said attaching means are adapted to provide connection of the portable equipment to a parachute module.

In this way, the transportation of the portable equipment is ensured in different ways, whether by land or air, which, combined with the security mechanisms and communication and geolocation capabilities provided by the equipment, allow the continuous monitoring of its operation as well as of the countermeasure devices stored in it.

As will be clear to one skilled in the art, the present invention should not be limited to the embodiments described herein, and a number of changes are possible which remain within the scope of the present invention.

Of course, the preferred embodiments shown above are combinable, in the different possible forms, being herein avoided the repetition all such combinations.

CLAIMS

1. A portable equipment for transporting at least one countermeasure device adapted to act on an unmanned system; the equipment comprising an envelope, defining a loading volume containing at least:

- a docking platform formed for detachable attachment of at least one countermeasure device; the docking platform integrating a battery charging station comprising at least one charging terminal configured to apply charging power to a countermeasure device;
- a geolocation module and a communication module designed in such a way that an information item relating to the location of the equipment is remotely accessible to an external system.

2. The portable equipment according to claim 1, further comprising an access control unit configured to restrict access to the interior of the envelope responsive to at least one access credential.

3. The portable equipment according to claim 1 or 2, further comprising an access control unit configured to restrict access to the at least one countermeasure device attached to the docking platform responsive to at least one access credential.

4. The portable equipment according to claim 3, wherein the access control unit is programmed to configure access criteria and security rules adapted to provide different levels of access responsive to access credentials; each countermeasure device being associated to a level of access.

5. The portable equipment according to any of the previous claims 2 to 4, wherein the access control unit comprises a biometric sensor adapted to collect biometric data from a user; and an access credential is biometric data related to a user.

6. The portable equipment according to claims 4 and 5, wherein the user is associated to a level of access, so that the user is only able to access to a countermeasure device which is of the same level of access.

7. The portable equipment according to any of the previous claims 2 to 6, wherein an access credential is a password.

8. The portable equipment according to claims 4 and 7, wherein the access control unit is programmed to configure access criteria and security rules adapted to provide different levels of access responsive to a primary or a secondary password.

9. The portable equipment according to any of the previous claims, wherein the communication module is further configured to establish a communication data link with the at least one countermeasure device for collecting operational data related to said countermeasure device; the operational data relating to unmanned system's landing position and/or countermeasure device's flight routes and/or data related to countermeasure device's transmitted redirection signals.

10. The portable equipment according to any of the previous claims further comprising a user interface unit comprised by at least a screen display adapted to display a user interface including displaying at least the following information: battery level of the battery charging station, location of the portable equipment, user interaction data records, and technical information related to the at least one countermeasure devices.

11. The portable equipment according to claim 10, wherein the countermeasure device's technical information relates to at least one of the following parameters: type of countermeasure device; battery level; operational data records relating to unmanned system's landing position and/or countermeasure device' flight routes and/or data related to countermeasure device's transmitted redirection signals.

12. The portable equipment according to claims 10 or 11, wherein a user interaction data record includes information related to the identification of the user accessing to the equipment and time and date of access.

13. The portable equipment according to any of the previous claims 10 to 12, wherein the user interface unit comprises input means; wherein the screen display is a touch screen display and the input means being provided by the touch screen display; and/or the input means are of a keyboard type.

14. The portable equipment according to claims 7 or 8 and claim 13, wherein the password is inserted by the input means.

15. The portable equipment according to any of the previous claims, wherein a countermeasure device is a police-drone or a handheld, man-portable countermeasure device having a handheld form factor body.

16. The portable equipment according to any of the previous claims, wherein the envelope is rigid.

17. The portable equipment according to any of the previous claims, further comprising at least one handle, installed in the outer surface of the envelope, enabling it to be carried.

18. The portable equipment according to any of the previous claims, further comprising means of displacement installed in the outer surface of the envelope, providing the contact with the ground; the means of displacement being at least one wheel, and, optionally, the envelope further comprising a handle enabling the equipment to be rolled along by means of the at least one wheel.

19. The portable equipment according to any of the previous claims, further comprising attaching means installed in the outer surface of the envelope; said attaching means adapted to provide connection of the portable equipment to a parachute module.

20. A system comprising:

- a plurality of portable equipment of claims 1 to 19;
- a central unit,

wherein,

the central unit is an external system; and

the plurality of portable equipment and the central unit are connected by means of a communication network.

ABSTRACT

A PORTABLE EQUIPMENT FOR TRANSPORTING COUNTERMEASURE DEVICES

It is an object of the present invention a portable equipment for transporting at least one countermeasure device adapted to act on unmanned system. It provides a portable base station that allows the storage and transport of countermeasure devices to remote locations, ensuring their operability for long periods of time. The equipment (1) is comprised by an envelope (2), defining a loading volume containing at least a docking platform comprising a battery charging station, geolocation module and a communication module. The equipment may also comprise a handle (3) enabling it to be carried.

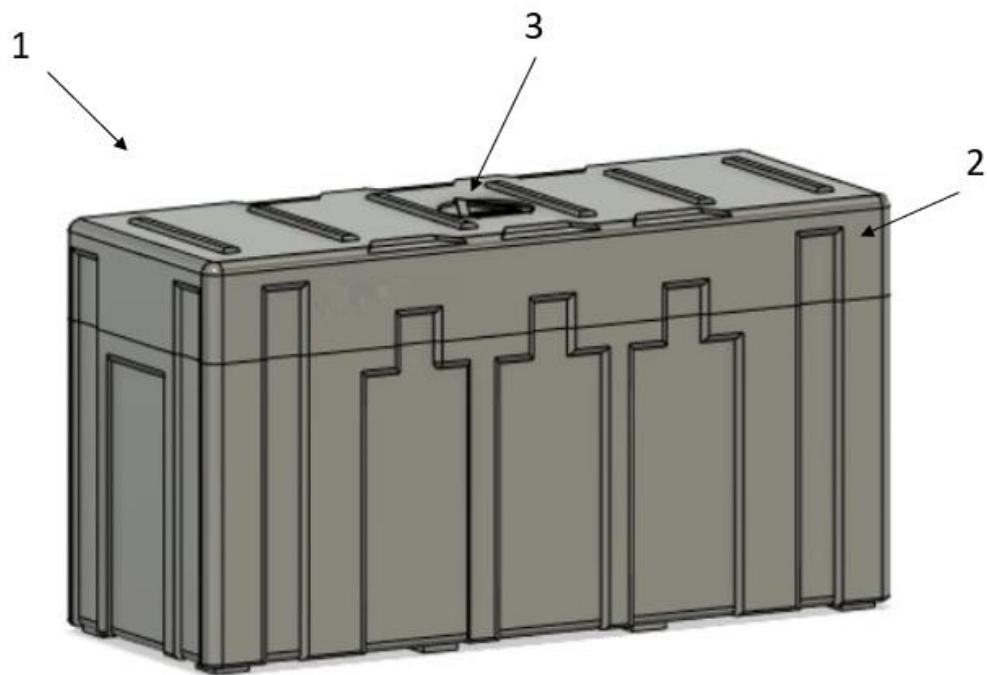


Figure 1

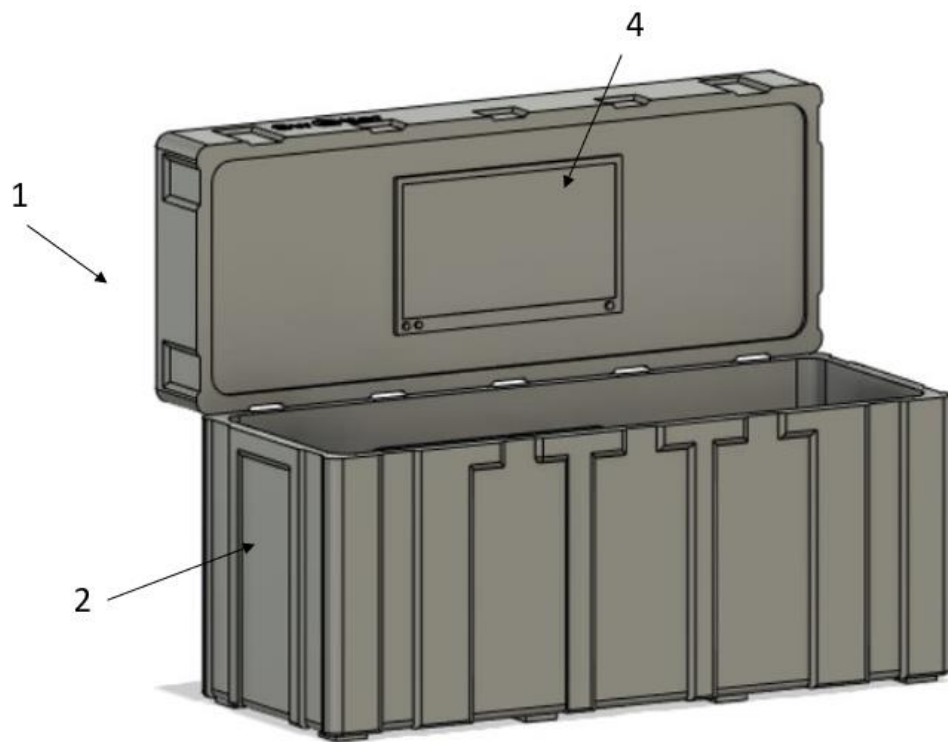


Figure 2

Appendix C

METHOD AND SYSTEM FOR INTERCEPTING AND CONTROLLING TARGET-DRONES



Comprovativo da submissão eletrônica

O Organismo receptor (RO/IB) acusa a recepção de um pedido internacional do PCT depositado através do ePCT-Filing. An Application Number and Date of Receipt have been automatically assigned
(Administrative Instructions, Part 7).

Número de submissão:	057202	
Número de pedido:	PCT/IB2021/057202	
Data de recepção:	05 Agosto 2021	
Organismo receptor:	Secretaria Internacional da OMPI	
A sua referência:	2021-0928TA	
Requerente:	SWATTER COMPANY, LDA	
Número de requerentes:	1	
Título:	METHOD AND SYSTEM FOR INTERCEPTING AND CONTROLLING TARGET-DRONES	
Documentos submetidos:	20210928TA-appb-000004.pdf (2021-928TA vdepósito.pdf)	481562
	20210928TA-appb.xml	976
	20210928TA-fees.xml	1984
	20210928TA-requ.xml	6261
	20210928TA-vlog.xml	774
Submetido por:	CRUZ JOÃO PEREIRA (ID de cliente: user_PT_JOAO-PEREIRA_CRUZ_4876)	
Carimbo de hora do comprovativo:	05 Agosto 2021 16:00 UTC+2 (CEST)	
Sumário oficial da submissão:	65:78:F6:4F:C7:9B:45:5C:CF:E1:D5:7B:E3:BB:B5:04:1B:6D:0E:7E	

/Genebra, Organismo receptor/IB/

DESCRIPTION

METHOD AND SYSTEM FOR INTERCEPTING AND CONTROLLING TARGET-DRONES

FIELD OF THE INVENTION

The present invention relates to detection and interception of drones or remotely controlled aircrafts within the vicinity of restricted areas.

PRIOR ART

An unmanned aerial vehicle, commonly known as a drone, is an aircraft without any human pilot, crew or passengers on board. The flight of drones may operate under remote control by a human operator, as remotely-piloted aircraft, or with various degrees of autonomy, such as autopilot assistance, up to fully autonomous aircraft that have no provision for human intervention. Drones have become popular in recent years due to the availability of relatively cheap recreational models with improved flight characteristics that can be controlled by almost anyone. Because of that, regulatory bodies around the world are developing unmanned aircraft system traffic management solutions to better integrate drones into airspace. As a consequence, the use of drones is becoming increasingly regulated by the national aviation authority of individual countries. However, media reports of negligent, criminal, and/or malicious drone is around airports, military bases, and prisons have become a common occurrence. For this reason, there are systems that aim to protect high security areas, which may use different protection schemes.

As an example, document US20190285388A1 discloses a system operative to down a target-drone comprising a processor-controlled interceptor drone bearing a processor-controlled flexible elongate intercepting agent cannon and an onboard processor to receive sensed wind conditions and configured to track the target drone including at least once, when said wind conditions exist, guiding the interceptor drone to a firing position and commanding the cannon to fire streamer rolls, once said

firing position is achieved, thereby to use the flexible elongate intercepting agent to down target drones. Document KR102034494B1 has a similar approach but the interceptors are projected to fire a catching net instead of streamer rolls in order to neutralize the target-drone.

In a different approach, document KR102001181B1 describes a shooting drone, which flies toward a target-drone and emits a jamming signal that prevents reception of GPS signals and communication frequencies, and which prevents damage due to the emitted jamming signal. The drone for downing target-drones, according to the referred document, comprises: a flight control unit provided inside a body of the drone flying based on a control signal generated and transmitted by a controller manually controlled by a user and controlling the flight of the drone based on the control signal transmitted from the controller; a jammer mounted at a distance from a lower part of the body of the drone to emit a jamming signal toward an unlicensed drone in flight; and a jammer control unit controlling the jammer based on aiming and firing signals from the controller. A similar approach is also described in KR20200099818A which relates to an anti-drone responding system that enables responses and defence with respect to target-drones invading a restricted area. The system uses police-drones adapted to identify one or more target-drones and to transmit jamming signals by detecting a frequency and generating a disturbing frequency signal for incapacitating the target-drone.

As such, the state of the art discloses systems that allow to control the airspace of restricted areas, preventing their access by target-drones, using police-drones that, either by means of firing physical elements such as stream rollers or catching nets, or by transmitting jamming signals are able to incapacitate and neutralize the invading drone, which in many cases leads to its total destruction and/or the need for repair. However, notwithstanding in such restricted areas the flight of drones is strictly restricted, there are occasions when a target-drone is inadvertently or intentionally penetrated into restricted areas. For this situation a destructive approach is not adequate, so the state of the art fails to disclose a strategy for the protection of restricted areas that is equally effective but that does not destroy or cause physical

damage to the target-drone. The present solution intended to innovatively overcome such issues.

SUMMARY OF THE INVENTION

It is therefore an object of the present invention a method for intercepting and controlling target-drones, which allows to control the target-drone's flight route, causing it to land in a predetermined landing position.

For that purpose, the method of the invention provides the configuration of flight routes for controlling the target-drone's flight path in order to direct it to the landing position, without causing any physical damage to the target-drone. This control is achieved by using police-drones which are adapted to transmit redirecting signals to the target-drone, as way to program a new flight route for the at least one target-drone to a landing position. The redirecting signals include spoofing signals.

It is also an object of the present invention a system for intercepting and controlling target-drones, adapted to operate in accordance with the method of the invention.

DESCRIPTION OF FIGURES

Figure 1 – representation of an embodiment of the method of the invention, wherein the reference signs represent:

- 1 – police-drone;
- 2 – target-drone;
- 3 – redirection signals;
- 4 – new flight route for the target-drone.

Figure 2 – representation of an embodiment of a police-drone of the invention, wherein the reference signs represent:

- 1 –police-drone;
- 3 – redirection signals;
- 5 – transmitting antenna;
- 6 –vertical camera;
- 7 – horizontal camera.

DETAILED DESCRIPTION

The more general and advantageous configurations of the present invention are described in the Summary of the invention. Such configurations are detailed below in accordance with other advantageous and/or preferred embodiments of implementation of the present invention.

In the context of the present application, a restricted area is a controlled environment area or facilities that have a need to limit access for security, safety and/or privacy concerns. Said restricted areas may be entirely or partially surrounded by a no-drone zone, which means that if a drone is in the designated no-drone zone or is on a flight route toward or near the restricted area, it may be designated as hostile. In the context of the present application a drone designated as hostile is named target-drone (2). Also, in the context of the present application, a police-drone (1) is directed by the control unit of the system of the invention to intercept a target-drone (2).

The present invention relates to a method for intercepting and controlling target-drones (2). In a first step of the method of the invention, it is determined the location in space of at least one target-drone (2) that is positioned in a vicinity of or within a restricted area. In one embodiment of the method, the position of a target-drone (2) is acquired by an auxiliary detection system, such as a radar system.

In a second step of the method of the invention, at least one police-drone (1) is activated and it is displaced to an operating position in a vicinity of at least one target-drone (2). In another embodiment of the method of the invention, the displacement of a police-drone (1) to the operating position is carried out autonomously by programming a flight route. Yet in another embodiment, the police-drone (1) may

continuously update the flight route by capturing video of a target-drone (2) and processing said video capture in order to detect and track said target-drone (2). Alternatively, in another embodiment of the method of the invention, the displacement of a police-drone (1) to the operating position is performed remotely under the control of a user by means of a remote controller. Yet in another embodiment, said remote controller may include a screen adapted to transmit the video signal captured by the police-drone (1), in order to help the user in his task of remotely operating the police-drone (1).

In a third step of the method of the invention, redirection signals (3) are transmitted by at least one police-drone (1) to the at least one target-drone (2). The redirection signals (3) include spoofing signals, which are configured to program a new flight route (4) for the at least one target-drone (2) to a landing position. For that purpose, in one embodiment of the method, the transmission of spoofing signals may use ephemeris files adapted to simulate a set of satellites, forming a hypothetical constellation, which are configured to generate baseband signal data streams to be transmitted in a frequency range of a satellite tracking system so as to be able to program the flight route (4) of at least one target-drone (2) to the landing position.

In one preferred embodiment of the method of the invention, the redirection signals (3) further include jamming signals. More particularly, the jamming signals are transmitted prior to the transmission of the spoofing signals.

Yet in another embodiment of the method, the redirection signals (3) further include jamming signals. More particularly, the jamming signals and the spoofing signals are transmitted simultaneously. As a consequence of this preferred configuration, the signal strength of the spoofing signals transmitted by a police-drone (1) may be decreased compared with the scenario where only spoofing signals are transmitted. In fact, even though in addition to spoofing signals also jamming signals are generated and transmitted, this particular configuration allows to achieve a better relationship between the power consumed by the police-drone (1) and the efficiency of the redirection signals (3) in redirecting the flight route (4) of the target-drone (2) for a pre-defined landing position.

In another embodiment of the method of the invention, the transmission of jamming signals involves the transmission of radio frequency signals adapted to jam terrestrial positioning signals or remote-control signals. The configuration and subsequent transmission of jamming signals implies detecting the frequency of operation of the target-drone (2) and generating a disturbing frequency signal for incapacitating the target-drone (2). Then the police-drone (1) by means of an antenna element (5) transmits the disturbing frequency signal with respect to the target-drone (2), thereby blocking remote control frequencies, image transmission frequency bands that may be used to control the flight path of the target-drone, and Global Navigation Satellite System signals.

In another embodiment of the method of the invention, the operating position is based on the location of a target-drone (2) at any time; and the operating position being defined as a position for a police-drone (1) that is at a radial distance between 3 to 10 meters from the target-drone (2).

Yet in another embodiment of the method of the invention, the operating position is defined as a position for the police-drone (1) which is at an altitude higher than the altitude of the target-drone (2). More particularly, in another embodiment of the method of the invention, the operating position is defined as a position for the police-drone (1) with the same geographic latitude and longitude coordinates as the target-drone (2) but the police-drone (1) being at an altitude higher than the altitude of the target-drone (2). This operating position proved to be more efficient for the transmission of the redirection signals (3).

In another embodiment of the method of the invention, the landing position is predetermined as a function of the restricted area, more particularly, the landing position can be inside or outside the restricted area.

The present invention also relates to a system for intercepting and controlling target-drones (2), adapted to operate in accordance with the method of the invention. The system comprises a control unit and at least one police-drone (1). The

control unit comprises processing means configured to program flight routes and to monitor the position of police-drones (1) and target-drones (2).

In one embodiment of the system of the invention, the control unit is configured to program a flight route (4) for at least one target-drone (2).

In another embodiment of the system of the invention, the police-drone (1) comprises at least one or a combination of the following sensory elements: Lidar sensor, at least one camera, barometer, accelerometer, gyroscope, compass, geolocation sensor. Yet in another embodiment, the police-drone comprises at least one camera with attached gimbal. Yet in another embodiment, the police-drone comprises a horizontal camera (7) and a vertical camera (6).

In another embodiment of the system of the invention, the police-drone (1) comprises a computational module with processing capability adapted to process sensory information collected by the sensory elements.

Yet in another embodiment of the system of the invention, it further comprises an auxiliary detection system adapted to determine the position of a target-drone (2). In this embodiment, the control is being further configured to program a flight route (4) base on the position of a target-drone (2) acquired by said auxiliary detection system.

Yet in another embodiment of the system of the invention, it further comprises at least one remote controller adapted to remotely control at least one police-drone (1); said remote controller being operated by a user. Yet in another embodiment, the remote controller comprises a biometric sensor configured to identify the user operating the remote controller. In this embodiment, the control unit is additionally configured to disable the remote controller if the user identified by the biometric sensor is not a certified user. A certified user is a user that is authorized to operate a remote controller. Finally, in another embodiment of the system of the invention, the remote controller comprises a touch screen in order to improve the control operation of the police-drone (1) executed by the user.

As will be clear to one skilled in the art, the present invention should not be limited to the embodiments described herein, and a number of changes are possible which remain within the scope of the present invention.

Of course, the preferred embodiments shown above are combinable, in the different possible forms, being herein avoided the repetition all such combinations.

CLAIMS

1. Method for intercepting and controlling target-drones, the method comprising the following steps:

- i. determining the location in space of at least one target-drone that is positioned in a vicinity of or within a restricted area;
- ii. activating at least one police-drone and its displacement to an operating position in a vicinity of at least one target-drone;
- iii. transmitting redirection signals by at least one police-drone to the at least one target-drone; the redirection signals being configured to program a flight route for the at least one target-drone to a landing position;

wherein,

the redirection signals include spoofing signals.

2. The method according to claim 1, wherein the redirection signals further include jamming signals; the jamming signals being transmitted prior to the transmission of spoofing signals.

3. The method according to claim 1, wherein the redirection signals further include jamming signals; the jamming signals and the spoofing signals being transmitted simultaneously.

4. The method according to any of the preceding claims, wherein the position of a target-drone is acquired by an auxiliary detection system.

5. The method according to claim 4, wherein the auxiliary detection system is a radar system.

6. The method according to any of the preceding claims, wherein the displacement of a police-drone to the operating position is carried out autonomously by programming a flight route.

7. The method according to claim 6, wherein a police-drone continuously updates the flight route by capturing video of a target-drone and processing said video capture in order to detect and track said target-drone.

8. The method according to any of claims 1 to 5, wherein the displacement of a police-drone to the operating position is performed remotely under the control of a user by means of a remote controller.

9. The method according to any of the preceding claims, wherein the operating position is based on the location of a target-drone at any time; and the operating position being defined as a position for a police-drone that is at a radial distance between 3 to 10 meters from the target-drone.

10. The method according to claim 9, wherein the operating position is defined as a position for the police-drone which is at an altitude higher than the altitude of the target-drone.

11. The method according to claim 10, wherein the operating position is defined as a position for the police-drone with the same geographic latitude and longitude coordinates as the target-drone.

12. The method according to any of the claims 2 to 11, wherein the transmission of jamming signals involves the transmission of radio frequency signals adapted to jam terrestrial positioning signals or remote-control signals.

13. The method according to any of the preceding claims, wherein the transmission of spoofing signals uses ephemeris files adapted to simulate a set of satellites forming a hypothetical constellation; the set of satellites being configured to generate

baseband signal data streams to be transmitted in a frequency range of a satellite tracking system so as to be able to program the flight route of at least one target-drone to the landing position.

14. The method according to any of the preceding claims, wherein the landing position is predetermined as a function of the restricted area.

15. The method according to any of the previous claims, wherein the landing position is inside or outside the restricted area.

16. A system for intercepting controlling target-drones, adapted to operate in accordance with the method of claims 1 to 15; said system comprising:

- a control unit;
- at least one police-drone;

the control unit comprising processing means configured to program flight routes and to monitor the position of police-drones and target-drones.

17. The system according to claim 16, wherein the control unit is configured to program a flight route for at least one target-drone.

18. The system according to claims 16 or 17, wherein a police-drone comprises at least one or a combination of the following sensory elements: Lidar sensor, at least one camera, barometer, accelerometer, gyroscope, compass, geolocation sensor.

19. The system according to claim 18, wherein the police-drone comprises at least one camera with attached gimbal.

20. The system according to claims 18 or 19, wherein the police-drone comprises a horizontal camera and a vertical camera.

21. The system according to any of claims 18 to 20, wherein the police-drone comprises a computational module with processing capability adapted to process sensory information collected by the sensory elements.

22. The system according to any of the preceding claims, further comprising an auxiliary detection system adapted to determine the position of a target-drone; the control unit being further configured to program a flight route base on the position of a target-drone acquired by said auxiliary detection system.

23. The system according to any of the preceding claims, comprising at least one remote controller adapted to remotely control at least one police-drone; said remote controller being operated by a user.

24. The system according to claim 23, wherein the remote controller comprises a biometric sensor configured to identify the user operating the remote controller; the control unit being additionally configured to disable the remote controller if the user identified by the biometric sensor is not a certified user.

25. The system of claim 23 or 24, wherein the remote controller comprises a touch screen.

ABSTRACT

METHOD AND SYSTEM FOR INTERCEPTING AND CONTROLLING TARGET-DRONES

The present application relates to a method and a system for intercepting and controlling target-drones (2), allowing to control the target-drone's flight route (4), causing it to land in a predetermined landing position. For that purpose, the method of the invention provides the configuration of flight routes (4) for controlling the target-drone's flight path in order to direct it to the landing position, without causing any physical damage to the target-drone (1). This control is achieved by using police-drones (1) which are adapted to transmit redirection signals (3) used as a way to program a new flight route (4) for the at least one target-drone (2) to a landing position.

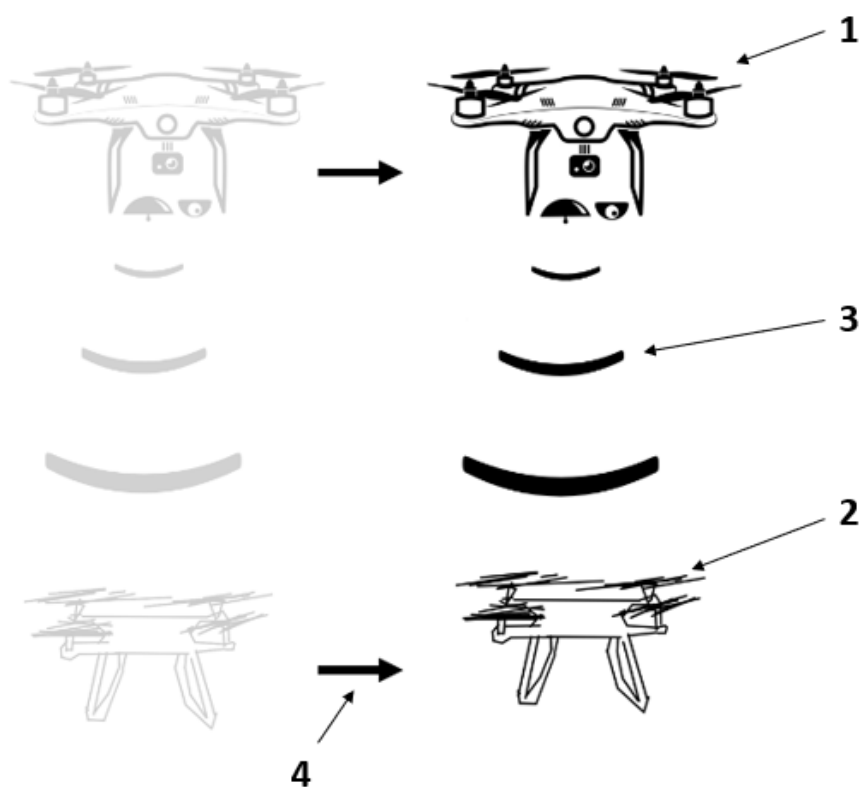


Figure 1

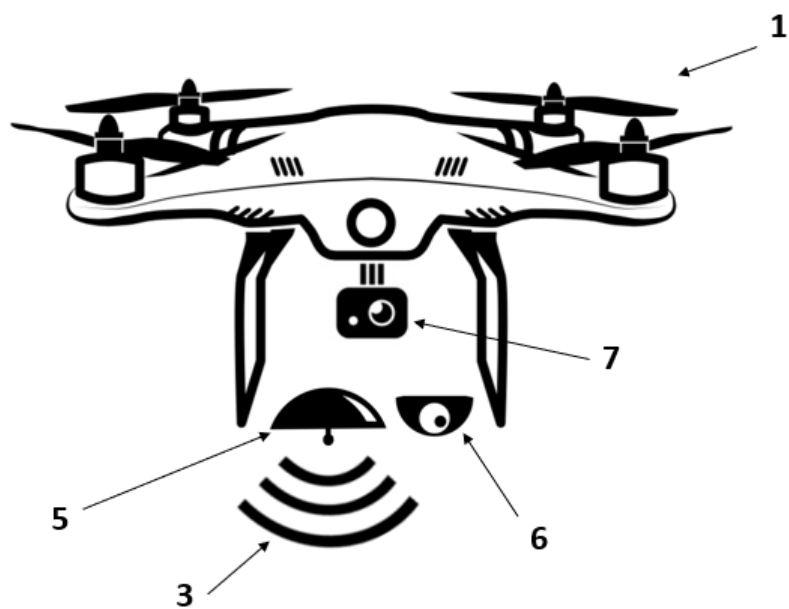


Figure 2