INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Jammers for Mobile Cellular Systems applied to unauthorized UAVs

Karla Valentina de Freitas Lara

Master in Telecommunications and Computer Engineering

Supervisor:
PhD Pedro Joaquim Amaro Sebastião, Assistant Professor,
ISCTE-IUL

Co-supervisor:
PhD Nuno Manuel Branco Souto, Assistant Professor,
ISCTE-IUL

November, 2020

TECNOLOGIAS
E ARQUITETURA

Jammers for Mobile Cellular Systems applied to unauthorized UAVs

Karla Valentina de Freitas Lara

Master in Telecommunications and Computer Engineering

Supervisor:
PhD Pedro Joaquim Amaro Sebastião, Assistant Professor,
ISCTE-IUL

Co-supervisor:
PhD Nuno Manuel Branco Souto, Assistant Professor,
ISCTE-IUL

November, 2020

Acknowledgement

I would like to thank everyone who was part of this academic journey, from my work colleagues who always cheered for me to my friends and family who supported me and help me finish this step stone and life goal.

I would like to thank, in particular, to my colleague and friend, Renato Ferreira, who gave me an essential guideline throughout the whole process and had a lot of patience with me.

I also owe a huge thank you to my lovely boyfriend Diogo, who always supported me by giving me a lot of strength in those bad days when I doubted myself if I was capable of making it until the end.

Last but not least, I would like to thank to my supervisor, professor Pedro Sebastião, and my co-supervisor, professor Nuno Souto, who were very flexible with my full-time job schedule and, also were available to clarify any doubts even in these difficult pandemic times. Thanks for all the help and comprehension.

Lisbon, 2nd November 2020,
Karla Lara

Resumo

Neste estudo será feita uma abordagem ao jamming em sistemas móveis digitais, dando um maior foco inicial à tecnologia 2G, Sistema Global para Comunicações Móveis (GSM).

O objetivo principal será o desenvolvimento de um sinal jammer, diferente dos já existentes em termos de eficiência e complexidade, capaz de causar interferência em sistemas móveis celulares.

Será feito então uma análise às diferentes técnicas de interferência de sinal, capazes de perturbar a comunicação em sistemas móveis celulares, através da realização de simulações a partir da tecnologia Software Defined Radio (SDR) nomeadamente, a plataforma GNU Radio. As mesmas técnicas também serão estudadas e avaliadas num cenário real, de forma a fazer-se a seleção da melhor em termos de eficiência espectral, energia e complexidade.

Finalmente, a técnica de jamming que demonstrar melhores resultados, irá representar o jammer que poderá contribuir de forma sustentável para a problemática da circulação de drones em zonas restritas, como aeroportos e zonas residenciais, para a diminuição dos acidentes, atualmente registados, com este tipo de aeronaves.

Palavras-chave: GSM, Jamming, SDR, GNURadio, UAV

Abstract

This research aims to explore jamming on digital mobile systems, with an initial focus towards the 2G and Global System of Mobile Communications (GSM) technologies.

The main goal is to develop a jammer with an efficiency and complexity greater than the existent ones, capable to better disrupt digital mobile systems.

The study consists of an analysis of the different techniques of jamming, that can disrupt the mobile cellular system's communication, through a series of simulations using the Software Defined Radio (SDR) and the GNU Radio ecosystem. The same techniques will then be studied and evaluated in real life scenarios in order to select which one is the best regarding spectral efficiency, energy and complexity.

Finally, the jammer returning the best results will be the one chosen to contribute sustainably for the issue with flying drones on restrict areas, such as airports and residential zones, and thus, decrease the number of accidents which nowadays happen usually with this kind of aircrafts.

Keywords: GSM, Jamming, SDR, GNU Radio, UAV

Contents

List of Figures

List of Tables

Abbreviations

2G	**S**econd **G**eneration
3G	**T**hird **G**eneration
4G	**F**ourth **G**eneration
5G	**F**ifth **G**eneration
ADC	**A**nalog-to-**D**igital **C**onverter
A/D	**A**nalog-to-**D**igital
AFCS	**A**utonomous **F**light **C**ontrol **S**ystem
AGCH	**A**ccess **G**rant **CH**annel
AM	**A**mplitude**M**odulation
ANACOM	**A**utoridade **N**acional de **C**omunicações
ARFCN	**A**bsolute**R**adio **F**requency **C**hannel **N**umber
ASK	**A**mplitude **S**hift **K**eying
ATSC	**A**dvanced **T**elevision **S**ystem **C**ommittee
AuC	**A**uthentication **C**enter
BB	**B**ase **B**and
BCA	**B**orrowing **C**hannel **A**llocation
BCCH	**B**roadcast **C**ontrol **CH**annel
BLoS	**B**eyond **L**ine-of-**S**ight
BS	**B**ase **S**tation
BSS	**B**ase **S**tation **S**ubsystem
BSC	**B**ase **S**tation **C**ontroller
BT	**B**andwidth **T**ime
BTS	**B**ase **T**ransceiver **S**tation
CCH	**C**ontrol **CH**annels
CCCH	**C**ommon **C**ontrol **CH**annel

CDMA	**C**ode **D**ivision **M**ultiple **A**ccess
CIR	**C**arrier to **I**nterference **R**atio
CPM	**C**ontinuous **P**hase **M**odulation
D/A	**D**igital-to-**A**nalog
DCS	**D**igital **C**ommunication **S**ystems
DCCH	**D**edicated **C**ontrol **CH**annel
DSP	**D**igital **S**ignal **P**rocessing
DAC	**D**igital-to-**A**nalog **C**onverter
dBm	**D**ecibel **M**iliwatt
EIR	**E**quipment **I**dentity **R**egister
EU	**E**uropean **U**nion
FACCH	**F**ast **A**ssociated **C**ontrol **CH**annel
FCA	**F**ixed **C**hannel **A**llocation
FCCH	**F**requency **C**orrection **CH**annel
FDD	**F**requency **D**ivision **D**uplexing
FDM	**F**requency **D**ivision **M**ultiplexing
FM	**F**requency **M**odulation
FHSS	**F**requency **H**opping **S**pread **S**pectrum
FSK	**F**requency **S**hift **K**eying
GPS	**G**lobal **P**ositioning **S**ystem
GCS	**G**round **C**ontrol **S**tation
GDT	**G**round **D**ata **T**erminal
GMSK	**G**aussian **M**inimum **S**hift **K**eying
GNSS	**G**lobal **N**avigation **S**atellite **S**ystems
GPRS	**G**eneral **P**acket **R**adio **S**ervice
GSM	**G**lobal **S**ystem for **M**obile Communications
GUI	**G**raphical **U**ser**I**nterface
HALE	**H**igh **A**ltitude **L**ong **E**ndurance
HLR	**H**ome **L**ocation **R**egister
IMEI	**I**nternational **M**obile **E**quipment **I**dentity
IMU	**I**nertial **M**easurement **U**nit
ISDN	**I**ntegrated **S**ervice **D**igital **N**etwork

LA	**L**ocation **A**rea
LGPL	**L**esser **G**eneral **P**ublic **L**icense
LoS	**L**ine-of-**S**ight
LTE	**L**ong **T**erm **E**volution
MAC	**M**edium **A**ccess **C**ontrol
MALE	**M**edium **A**ltitude **L**ong **E**ndurance
MAV	**M**icro **A**erial **V**ehicle
MS	**M**obile **S**tation
MSC	**M**obile **S**witching **C**enter
MSK	**M**inimum **S**hift **K**eying
MT	**M**ulti **T**one
MUAV	**M**ini **U**nmanned **A**erial **V**ehicle
NAV	**N**ano **A**erial **V**ehicle
NSS	**N**etwork and **S**witching **S**ubsystem
OMC	**O**peration and **M**aintenance **C**enter
OSS	**O**peration **S**upport **S**ubsystem
PCH	**P**aging **CH**annel
PM	**P**hase **M**odulation
PSD	**P**ower **S**pectral **D**ensity
PSK	**P**hase **S**hift **K**eying
PSTN	**P**ublic **S**witched **T**elephone **N**etwork
QoS	**Q**uality of **S**ervice
RACH	**R**andom **A**ccess **CH**annel
RF	**R**adio **F**requency
RSS	**R**eceived **S**ignal **S**trength
RSS-H	**RSS** with **H**ysteresis
RSS-HT$_{\mathbf{new}}$	**RSS** with **H**ysteresis and **T**hreshold of the New Base Station
RSS-HT$_{\mathbf{ser}}$	**RSS** with **H**ysteresis and **T**hreshold of Servicing Base Station
RSSI	**RSS I**ndication
RSS-T	**RSS** with **T**hreshold
RX	**R**eception
SACCH	**S**low **A**ssociated **C**ontrol **CH**annel

SCH	**S**ynchronization **CH**annel
SDCCH	**S**tandalone **D**edicated **C**ontrol **CH**annel
SDM	**S**pace **D**ivision **M**ultiplexing
SDR	**S**oftware **D**efined **R**adio
SIM	**S**ubscriber **I**dentity **M**odule
ST	**S**ingle **T**one
SWIG	**S**implified **W**rapper and **I**nterface **G**enerator
TCH	**T**raffic **CH**annels
TDD	**T**ime **D**ivision **D**uplex
TDM	**T**ime **D**ivision **M**ultiplexing
TDMA	**T**ime **D**ivision **M**ultiple **A**ccess
TUAV	**T**actical **U**nmanned **A**erial **V**ehicle
TX	**T**ransmission
UAS	**U**nmanned **A**erial **S**ystems
UAV	**U**nmanned **A**erial **V**ehicle
UMTS	**U**niversal **M**obile **T**elecommunications **S**ystem
USB	**U**niversal **S**erial **B**us
UHF	**U**ltra **H**igh **F**requency
VHF	**V**ery **H**igh **F**requency
VCO	**V**oltage **C**ontrolled **O**scillator
VGA	**V**ariable **G**ain **A**mplifier
VLR	**V**isitor **L**ocation **R**egister
Wi-Fi	**W**ireless **F**idelity

Chapter 1

Introduction

In this first chapter, the motivation for the development of this dissertation will be introduced and the main objectives will be set as well. Furthermore the methods and questions of this research will be explained, along with the organization and structure of this dissertation.

1.1 Motivation and Background

Nowadays mobile communications exist on most devices used in everyday life: mobile phone, tablet, laptop, etc. This technology consists on the transmission of voice and multimedia data from a computer or a device without being connected to any physical or fixed links. This is done through a cellular communication network where the last link is wireless. These cells are distributed by territorial areas where each of them are served by at least one base station. These are the stations that provide the cells the necessary network coverage for voice or multimedia data transmission. In order to avoid interference and maintain service quality, it is usual to use for each cell a different "operation" frequency from the near cells.

With the development of technology, more specifically on mobile phones, the whole landscape of communication has changed. People have more and more urgency to communicate faster and comfortably. This journey of mobile communications emerged more consistent in the late 70s with the 1st Generation systems, where the cellular network was analog and only covered voice services. Currently, we are already at the end of the 4th Generation with a huge increase in data access speed through the Long Term Evolution

(LTE) standard. This technology focuses more on data traffic over voice, providing a faster and more stable data network. The 5th Generation is very close to being the most used in network infrastructures, promising better and faster video streaming.

With this inherent mobility in today's communications, signal inhibiting devices, called jammers, started to appear. A jammer is an equipment that introduces interference in communication or information exchange between devices.

Due to the recent notoriety of the SDR technology, jammers have become more flexible and easier to use and can now be purchased online at relatively affordable prices.

The misuse of this type of devices consists in a major problem for society because it compromises the quality and security of crucial wireless communications. Economically it can damage the revenues of mobile service providers if a large-scale attack occurs.

This dissertation will focus mainly in blocking the communication of a GSM receptor in order to battle the problem regarding the circulation of drones in unauthorized areas, while taking advantage of jamming in a non-malicious way. Drones are essentially unmanned aircraft that can be remotely controlled using a combination of microcontrollers, the Global Positioning System (GPS), Wireless Fidelity (Wi-Fi) and sensors. In the past most drones were military use only, although commercial use has grown exponentially lately. This has brought the need to have a greater control over the use of drones, with most countries creating their own flight laws and restrictions related to privacy, authorized areas for circulation and freight transportation.

Therefore, it is of great interest to approach this matter, in a bid to decrease the issue with drones on restrict areas as well as the number of accidents.

1.2 Objectives

First of all it is necessary to study the several basic concepts related to the technologies of cellular mobile network systems and SDR. It is also equally important to analyze the jamming related concepts.

The work developed in this dissertation consists in implementing and evaluating several jamming techniques applied to mobile cellular systems with previously selected targets. One of the main goals is to minimize possible interference in neighboring receivers.

To simulate the jamming techniques on the desired signal, interference signals will be generated and implemented from a SDR based device. This intervention needs to be achieved with the lowest energy possible in order to obtain the best energy efficiency ratio and reduce interference with near devices as well.

So, the jammer to be developed should be as energy-efficient as possible and its implementation should be of reduced difficulty so, that way, it can be as scalable and transversal as possible.

Finally, the jammer with the best performance will be chosen as the indicated jammer.

To achieve the goals of this dissertation, the work will be divided in the following phases:

1. Study and analysis of the different jamming techniques and signal generation procedures based on SDR devices;
2. Implementation of the software through the platform GNU Radio;
3. Implementation of the jammer in the SDR equipment;
4. Performing of the functional tests on the intended environments;
5. Analysis of the results obtained according to the set main goals.

1.3 Research Questions

According to the goals planned for this dissertation, it will be of great contribution to reach conclusions that answer the following research questions:

- Is there any unintentional interference with neighbouring receivers in performing the jamming? If so, how can you minimize it?
- Considering the energy efficiency, how far can the jammer disrupt the communication?
- Is the system response reasonably quick to be consider an effective solution?
- Is the solution found capable of combating the imminent risks of drones at a social level?

1.4 Research Methods

This dissertation is based on the Design Science Research methodology, which its main focus is the development and functional performance of the intended artifact. A method and instantiation of the artifact will, then, be elaborated.

This dissertation follows the problem-centered approach methodology since the research questions derive from the study and observation of the initial problem.

Thus, in order to achieve the proposed output, the work is divided into three components, as represented in figure 1.1:

1. The research starts with a theoretical study of the characteristics and operation modes of the mobile cellular systems' signals to be included in the jammers.

2. The jammers will be implemented on the GNU Radio ecosystem.

3. Finally, the implemented jammers will be tested in a real environment.

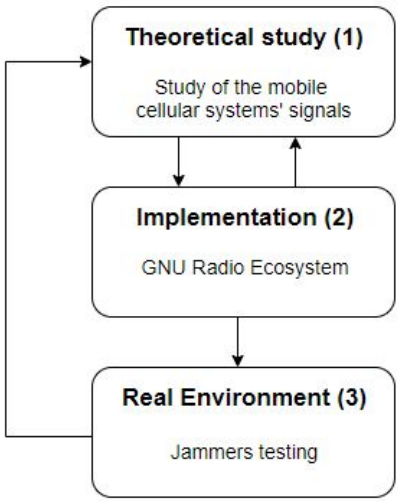


FIGURE 1.1: Work flow method

1.5 Thesis Outline

The first chapter has already been described earlier and it is a introductory section of the dissertation topic.

The second chapter is the literature review and overview of the main concepts of the dissertation like the UAV's, 2G communication technology and the SDR technology.

The third chapter consists in the description, study and configuration of the many jamming techniques, using a SDR device and the GNU Radio ecosystem.

The fourth chapter includes the tests on a real environment using the implemented jammers on the previous chapter, and also the study and selection of the jammer that showed better performance based on the obtained results.

Finally, the fifth chapter presents the main conclusions about the results achieved and also some future work recommendations.

1.6 Contributions

The elaboration of an article, based on the study made in this dissertation, is currently underway in order to be published in a conference.

Chapter 2

Literature Review

In this chapter, there is an approach on UAVs and its diverse characteristics. Therefore, it is important to explain the GSM technology and its related technical concepts. To build the intended jammer, it is necessary to study the jamming concept and how they work, and also look into the SDR technology and its mechanisms.

2.1 UAVs - Unmanned Aerial Vehicles

Nowadays the use of unmanned aerial vehicles in multiple tasks is quite usual, unlike in the past, where they were developed, built and commanded by military organizations, having not much contact with civil and commercial organizations.

UAVs, also known as drones, are devices that can be controlled remotely on all three space axes or fly autonomously through software controlled flight plans presented in their system. Combined with integrated sensors and a GPS system, drones are able to perform their functions.

Due to their composition, these types of aircraft can be used for different activities including urban planning, monitoring tasks, natural disaster warning or emergency situations.

2.1.1 UAV Types

UAVs are usually categorised by their size and reach capability. Therefore, they can be divided essentially into three major groups: High Altitude, Medium Altitude and Low Altitude [1]:

- **High Altitude Long Endurance (HALE):** This type of UAVs have the ability to achieve more than 15 km of altitude and perform flights of more than 24 hours. Thus, they are chosen for long-range (trans-global) military missions and are usually operated from fixed bases;

- **Medium Altitude Long Endurance (MALE):** This vehicle is similar to HALE but reaches lower altitudes (between 5 km and 15 km) and makes shorter flights (up to 24 hours). They are also controlled by fixed bases and cover shorter ranges with the minimum value of 500 km;

- **Tactical Unmanned Aerial Vehicle (TUAV):** Also named as Medium Range because their range goes between 100 km to 300 km. These aircrafts are smaller than HALE or MALE and therefore they operate in simpler systems also by land and naval forces;

- **Close-Range UAV:** They are usually used for mobile military/naval operations and many civilian purposes as well. This type of vehicles operate at ranges until around 100 km and have probably the most prolific of uses in both fields (military and civil);

- **Mini Unmanned Aerial Vehicle (MUAV):** This group of UAVs is defined by a certain mass (normally up to 20 kg) and are a little bigger than the MAV ones. They can operate at ranges up to about 30 km and are usually used for diverse civil purposes.

- **Micro Aerial Vehicle (MAV):** These vehicles are specially required for more civil tasks in urban environments because they are more affordable and easier to use. Their roles are different from the others above and for that, they need some specific configurations to be possible to achieve their tasks and some require slow flights with slow direction-changing movements.

- **Nano Aerial Vehicle (NAV):** These ones are very small (the size of a seed) and are used mostly for purposes like radar confusion and sub-systems control, having ultra-short ranges.

2.1.2 UAV Structural Types

Of the various existing UAVs, the most widely used are the fixed wing, represented in figure 2.1a and multi-rotor aircraft, represented in figure 2.1b. Each one has its own specificities:

- **Fixed-wing:** is defined by their high flight time and range [2], benefiting from their aerodynamic two-winged design. For that reason, they are mainly used for aerial mapping and military activities, since they can achieve high speeds. On the other hand they are expensive and require skill training to operate them. Although they need relatively more space for their launch and recovery, they are used to cover large areas using a gas engine as their power source [3];
- **Multi-rotor:** is considered the cheapest option available and easier to build, normally being used for tasks like filming and video surveillance. They can be divided into four types: tricopters, quadcopters, hexacopters, or octocopters, being that the most used are the quadcopters. Unlike the fixed-wing type, the multi-rotor is more limited in terms of flight time, speed and energy efficiency. For that reason they are not appropriate for flights of large-scale or longer distance monitoring [3].

(A) Fixed Wing UAV [4] (B) Multi-rotor UAV [5]

FIGURE 2.1: The two types of UAVs most widely used

These devices are now considered a low-cost solution (compared to the cost of using a manned aircraft) for obtaining data in a short period of time due to their ability of performing missions in almost all weather conditions and being relatively easy to use and maintain. Another useful feature of these aircrafts is the ability of enabling the

autonomous flight mode through the existent microcontroller on their system (the choice of the microcontroller depends on the type of UAV) [6].

The flight mission planning of these aircrafts must involve a balance between the volume of data to be transmitted (defined by the objectives set), the relationship between energy and power of the existing communication links, the availability on board power sources, the aircraft weight and also the operating range area.

2.1.3 UAV - Control and Communication

The communication between the UAV and the control station is made through data links systems. Two types of data links are generally used:

- **Line-of-Sight (LoS):** made by direct commands via Radio frequency (RF) and transmits data at high speeds, having a transfer rate around 274 Mbit/s [7]. To operate the system, two directional antennas are needed: one on the UAV and the other on the Ground Data Terminal (GDT), which provides communication between the control station and the UAV. The maximum achievable distance is about 200-250 km, having some limitations related to the link design;
- **Beyond Line-of-Sight (BLoS):** the communication is made through the use of geostationary satellites with a turnaround link latency of 0.48s or more [8], and for that reason it can reach more distances than LoS system. The distance achieved with this system is greater than 965 km.

Regarding the classification of the many types of UAV referred in the subsection 2.1.2, it is possible to indicate that the type of aircraft with high endurance like HALE and MALE use the BLoS system and the others with medium and low endurance like TUAV, Close-Range UAV, MUAV, MAV and NAV make use of the LoS system.

To operate a UAV, intermediate mechanisms are necessary for the communication between the aircraft and the user. These mechanisms can be:

2.1.3.1 Radio Controller

Within the complexity of operating a UAV, Radio Controller is the easiest, simplest and most affordable way to control an aircraft. In order to performed this task, the drone must

have a radio receiver capable of receiving RF data. This data is transmitted through the radio transmitter held by the user, capable of controlling the behavior of the aircraft [9]. A limitation inherent of this technology is the fact that the user can only control the UAV through LoS and when this does not happen the communication becomes compromised because the power is not high enough.

2.1.3.2 Ground Control Station (GCS)

GCS is an essential UAV monitoring and control tool, being more complete than the mentioned previously in subsection 2.1.3.1.

The user can monitor his flight parameters before the aircraft takes off via radio link established between the UAV and the GCS. When using the autopilot mode called Autonomous Flight Control System (AFCS), the UAV receives the proper GCS instructions through the existing system's telemetry, composed mainly for five components:

- Three-Axis Inertial Measurement Unit (IMU);
- Three-Axis magnetometer;
- GPS System;
- Radio system with servo interface and safety pilot;
- Flight computer (some of then already available for mobile devices like smartphones);

In terms of communication links, there are two types of links: uplink and downlink. The communication between the GCS and the UAV is made through the uplink, where commands are sent to the aircraft related to the position and intended direction of the mission. On the other hand, the downlink represents the connection between the UAV with the GCS where it is possible to sent telemetry data, images, information about the aircraft battery level or other data concerning to the state of the UAV.

Besides of the informative data that UAVs can transmit through the various sensors and usually through the existing cameras in the system, there is many important information that must be transmitted throughout the mission, namely flight status, control data, payload data and respective control. From this, it is possible to perform tasks like get the location of the UAV by reading data from the embedded GPS system.

There are many different types of software capable of playing the functions of a GCS for both operating systems: Windows and Linux. One of the known examples is Mission Planner, represented in figure 2.2. It is an open-source application compatible with the communication protocol used between the UAV and the GCS, MAVLink. This communication is made through telemetry equipment like Wi-Fi or RF transmitters and receivers [9].

FIGURE 2.2: Mission Planner App [10]

It is also relevant to take into consideration the data link protection and, consequently, the security and integrity of the transmitted data. This exchange of information between the aircraft and its ground control station could be disrupted either by environmental conditions or, above all, by voluntary attempts of signal interception.

Therefore, data can be protected through a complex set of protection resources such as robust coding techniques, high error tolerance protocols, systems to minimize electromagnetic exposure to jammers, the use of narrow or directed antennas and intelligent signal processing.

2.1.3.3 MAVLink

As mentioned earlier, the MAVLink is a protocol, which was released in 2009 under the Lesser General Public License (LGPL) by Lorenz Meier [11], with header-only message that uses a set of messages to transmit bidirectional data between the UAV and GCS. As the messages are transformed in a stream of bytes, they are typically of small sizes and can be safely transmitted across different wireless systems like Wi-Fi or telemetry equipment. Thus, in a Unmanned Aircraft Systems (UAS), the messages are interpreted by the GCS

or by a Raspberry Pi and are normally used for simple tasks like for the transmission of information about the UAV status, setting the flight mode or new waypoints [2].

With it, this protocol constitutes a reliable, fast and safe mechanism against error transmission. The figure 2.3 represents the structure of a MAVLink frame.

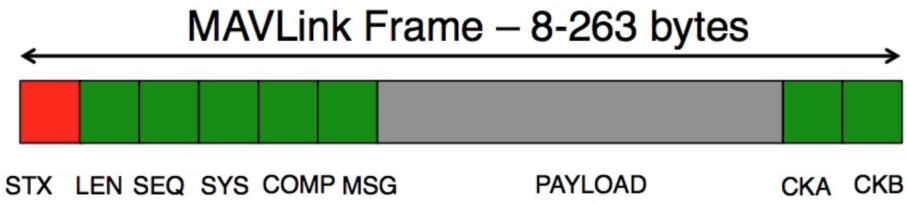


FIGURE 2.3: MAVLink protocol [12]

2.2 Cellular Mobile Networks

The communication of the jammer built in this dissertation it is based on a cellular mobile network. For that reason, it is important to understand the structure and operation of this system, provide a brief overview and how it emerged in historical terms, and finally focus on the type of mobile communication used in this research which is the GSM.

2.2.1 Overview

The basic concept related to cellular mobile communications is the division of densely populated regions into several small regions called cells. Each of these cells has a base station that provides radio coverage to the entire region bounded by the cell. Each base station is connected to a Mobile Switching Center (MSC), which is connected to a local center.

Thus, it is possible to identify the basic components of the architecture of a cellular mobile network, as represented in figure 2.4: the mobile devices, the base stations and the previously mentioned, MSC.

The base station is equipped to transmit, receive and route calls to or from any mobile device within a certain cell through the MSC. The cell covers a small area (usually between a radius of 1 km to 35 km, depending on the existing traffic), which enables the power output from the base station to be reduced to a level where the interference with

neighboring cells remains at reasonable limits. This way, the same radio frequency can be used in different cells without the danger of mutual interference [13].

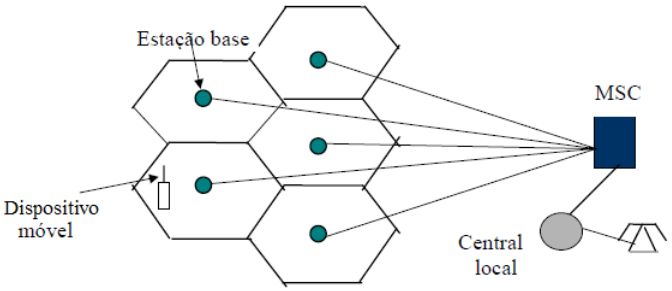


FIGURE 2.4: Cellular Mobile Network Architecture [14]

Therefore, by dividing the network into cells, it's possible to have:

- Frequency reuse: there is a reuse of channels in terms of frequency, time or code, thanks to the use of space-division multiplexing (SDM). The type of channel to reuse depends on the type of multiple access used on the system. Then, it's more likely to have a increase of the spectrum and improve the radio network efficiency;
- Capacity growth: as the need for better coverage and more capacity grows, it is possible to split the existing large cells into smaller cells, in order to increase the radio network capacity with a tighter reuse of the frequencies.
- Mobility: it is achievable through the existing handovers among the cells. That way, the users can roam through the network, using all the cells as one big service area;
- Robustness: if there is a failure in a single component, the cellular system is only compromised in a small area defined by the cell, without disabling the rest of the network, being thus a decentralized system [15].

On the other hand, the cellular network also holds some challenges [16]:

- Network structure: it is fundamental that the cells only cover the intended area in order to avoid interference resulting from the proximity of the cells. In order to connect the existing base stations for the system's operation, it is needed a complex infrastructure capable of supporting these links;
- Mobility: to achieve full mobility, the existence of the handover event is crucial. In order to perform its function efficiently, it requires complex measurements and

evaluation procedures in order to ensure to the user the continuity of the service at that time;

- Power control: to overcome the problem known as 'the-near-far problem', which appears derived from the proximity of a mobile to the base station that overpowers the low signal from the distant mobiles, it was necessary to introduce a power control in both uplink and downlink channels in order to increase radio quality and spectrum efficiency;

- Frequency planning: due to the existing limited number of frequencies available, the distribution of these frequencies must be carefully done in order to avoid interference [15].

Each cellular network is, then, assigned a set of frequencies or channels, and the number of channels allocated depends on the radio spectrum provided by the relevant regulatory authorities (in Portugal, the responsible entity is ANACOM), and also depends on the width of each channel in the standard used by the network. The cells are organized into clusters, as represented in figure 2.5, with disparate sets of frequencies in order for the available channel spectrum to be reused multiple times over a large area, with each cluster supporting the same number of users [14].

The allocation of frequencies to the cells can be done mainly through two methods:

- Borrowing Channel Allocation (BCA): at a given time, when the traffic on a cell increases, there is a dynamic allocation of frequencies in those peaks;

- Fixed Channel Allocation (FCA): there is a fixed assignment of frequencies to the cells resulting from a meticulous analysis process.

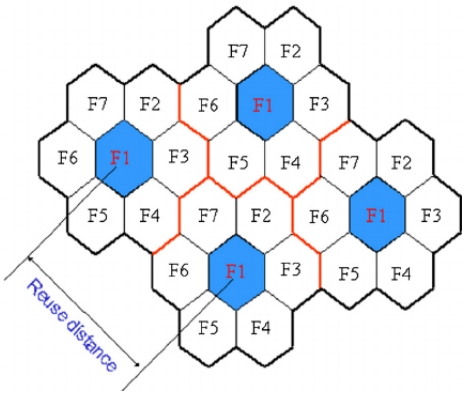


FIGURE 2.5: Cells Cluster System [17]

2.2.2 Historical Context

Chronologically describing the first generation of cellular communication systems emerged around the 1980s and was characterized by the use of voice only analog technology.

With the continuous interest in the evolution of this technology, the second generation of mobile communications was established, characterized by the GSM technology. Around this time, digital systems and small data transports began to be introduced, most of them still being voice data.

It was then in the third generation that digital technology was definitively affirmed through Universal Mobile Telecommunications System (UMTS), introducing data and multimedia transport with greater speed and quality.

Currently, we are in the fourth generation characterised by the LTE technology where it is possible to find a very high rate of data transmission compared to previous technologies [18].

The fifth generation it is currently under development and it promises to improve some features of the 4G technology and to be the future of telecommunications. The European Union (EU) gave 2020 as the deadline year for the 5G network to be commercially available in one city per country at least from the twenty three member states [19].

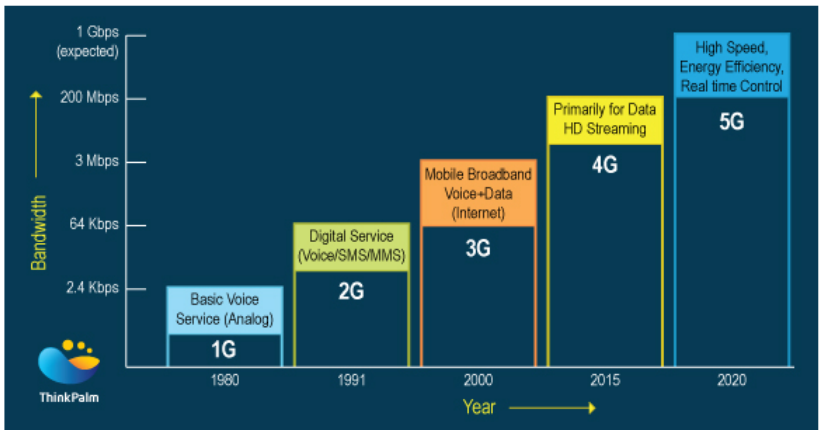


FIGURE 2.6: Mobile Communication Technology Evolution [19]

2.3 Global System for Mobile Communications (GSM)

One of the main focus of this dissertation is the GSM. Therefore, there is an overview of this technology and a study regarding its characteristics and associated technical details.

2.3.1 Overview and Network

The GSM technology is a globally recognized second generation (2G) standard for digital mobile communications. It emerged in 1982 to establish a standard European norm for the mobile cellular network [20].

Being a cellular network system, the GSM provides wireless communication through cells for subscribers close to them. There are four main cells in your network, where two of them (macro and micro) provide outdoor coverage and the other two (pico and femto) provide indoor coverage [21].

A GSM user is identified by a Subscriber Identity Module (SIM) card. This removable small chip contains the user's subscription information and allows the user to switch from one GSM device (normally a mobile phone) to another. In addition, the mobile equipment is uniquely identified by the International Mobile Equipment Identity (IMEI). These devices can be locked to a specific carrier but for those who are unlocked they can work with any SIM card of any carrier. This flexibility is a big advantage of the GSM technology where the ability to roam and switch carriers, by using individual mobile units, is given to the users.

In terms of structure, the GSM network includes the following elements [22]:

- **Mobile Station (MS)**: it is mainly composed by the mobile equipment, identified by the IMEI, and the user SIM card. The interaction between the MS and the Base Transceiver Station (BTS) basically forms the radio cell;

- **Base Station Subsystem (BSS)**: it represents the radio link and it is divided in two parts, the BTS and the Base Station Controller (BSC) [23]. A group of BTS's is controlled by a BSC. In short, the BSS is responsible for providing wireless connection to mobile device users via radio or air interface, making use of all nodes and functionalities of this subsystem [24];

- **Network and Switching Subsystem (NSS)**: it is basically the main network, which is responsible for the mobility, that "connects the wireless network with standard public networks" [15]. Thus, this subsystem contains all the nodes and features inherent to the service such as call switching and subscriber management. It is composed by the Mobile Switching Center (MSC) which is responsible for serving a group of BSS through the connection between a BSC [25], the Home Location

Register (HLR), the Visitor Location Register (VLR) and the Equipment Identity Register (EIR) databases, and finally the Authentication Center (AuC) which gives support to the HLR and VLR;

- **Operation Support Subsystem (OSS)**: it is the functional entity where the network operator monitors and controls the system, providing a network overview. It is composed essentially by the Operation and Maintenance Center (OMC) that "monitors and controls all other networks entities" [15]. Thus, this section has the main goal of delivering support for the many maintenance activities [20].

All these components, mentioned above, are explained in more detail in [15, 16] and are represented in the figure 2.7.

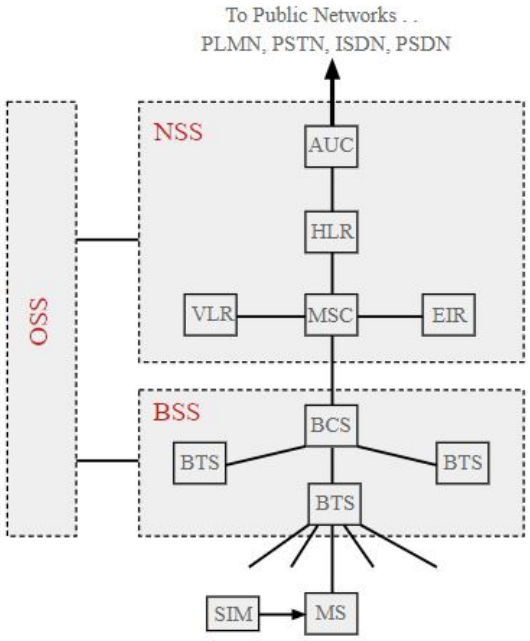


FIGURE 2.7: GSM Network Architecture [26]

It is possible to distinguish some aspects which made GSM gain wide acceptance and popularity within cellular mobile networks over the years:

- Spectral efficiency;
- The possibility of offering international roaming;
- Providing low cost base stations;

- Supporting new services;
- Being compatible with the set of communication norms for digital transmission, the Integrated Service Digital Network (ISDN).

Therefore, GSM technology is still widely used worldwide today, and some improvements have been introduced in recent years to achieve new features and reduce the operational cost for service providers [24].

2.3.2 Air Interface

The GSM Air Interface provides the physical link between the mobile terminal and the network. This digital system operates worldwide mainly in two bands: 900 MHz and 1800 MHz. Through the combination of frequency and time multiplexing, the GSM spectrum allocates time slots and frequencies in order to establish each user's communication and use the Gaussian Minimum Shift Keying (GMSK) modulation technique to transmit data. The above concepts will be explained in more detail in the further sections.

2.3.2.1 GSM Spectrum

Initially, in Europe, the GSM was specified as a 900 MHz system. Nowadays, this digital technology operates in bands around 800-900 MHz and 1800-1900 MHz all over the world [16].

There are mainly two radio spectrums for the GSM: GSM900 and GSM1800 (also known as DCS1800). The GSM900 has reserved a spectrum between 890-915 MHz for the uplink and 935-960 MHz for the downlink, which means a bandwidth of 25 MHz and a 45 MHz duplex distance between the bands. On the other hand, the GSM1800 uses the spectrum between 1710–1785 MHz for uplink and 1805–1880 MHz for the downlink, with a bandwidth of 75 MHz and a distance between the bands of 95 MHz.

In order to isolate the uplinks and downlinks, GSM incorporates two duplexing schemes: Time Division Duplex (TDD) and Frequency Division Duplex (FDD). FDD allows the mobile terminal and the base station to operate at the same time but on different frequencies to avoid interferences between each band and the TDD separates the transmission and reception of the signals, so that a single frequency is assigned to a user for both directions.

Thus, the spectrum is divided into radio channels with a bandwidth of 200 KHz through FDD. Similarly, each of these channels are then divided into eight time slots due to the use of TDD [16].

The figures 2.8 and 2.9 represent the radio spectrum of the GSM900 and the GSM1800 respectively.

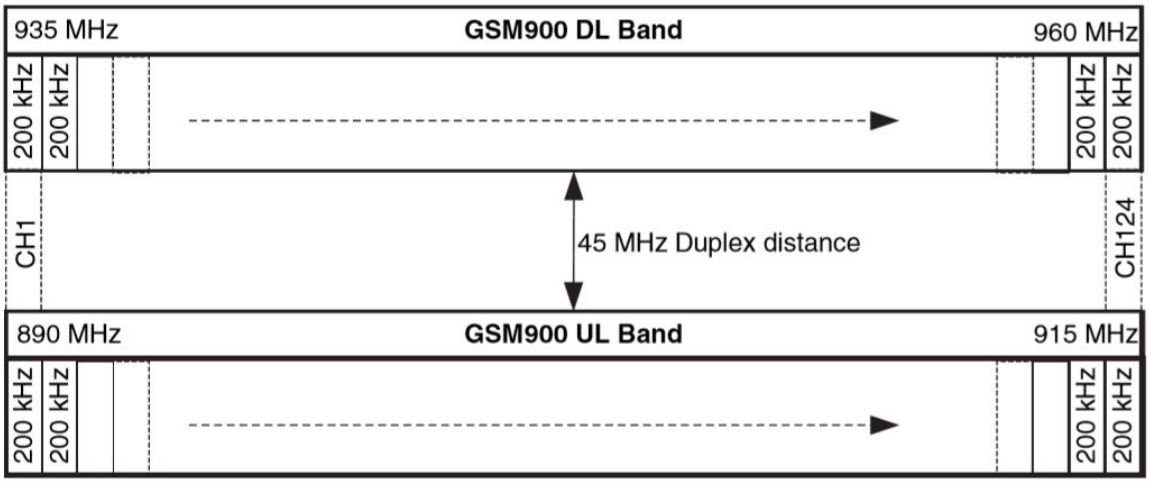


FIGURE 2.8: Radio Spectrum of GSM900 [16]

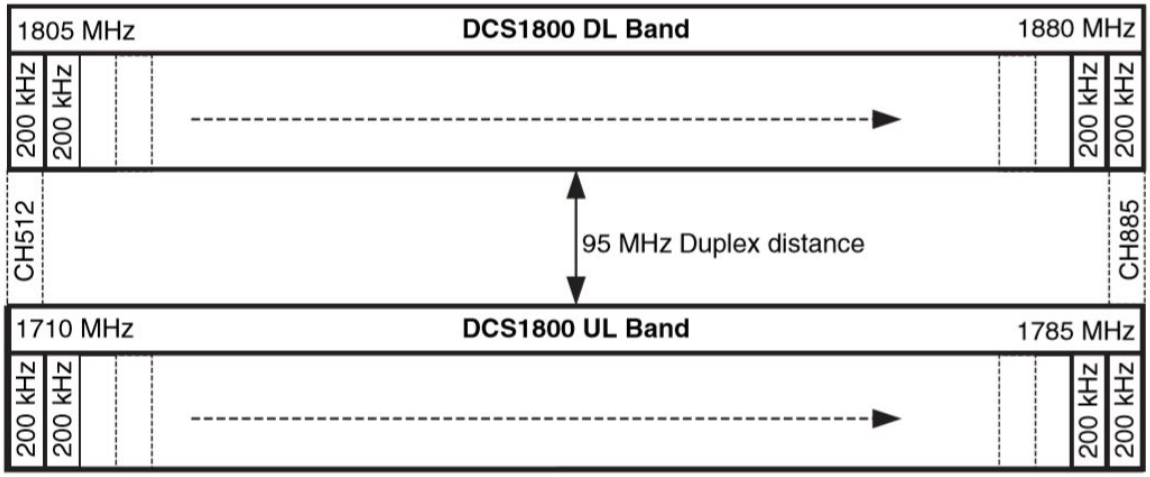


FIGURE 2.9: Radio Spectrum of GSM1800 [16]

2.3.2.2 Multiplexing and Multiple Access

Multiplexing is a functionality inherent to the communication systems, being responsible for the transmission of signal concurrently over a given communication medium such as

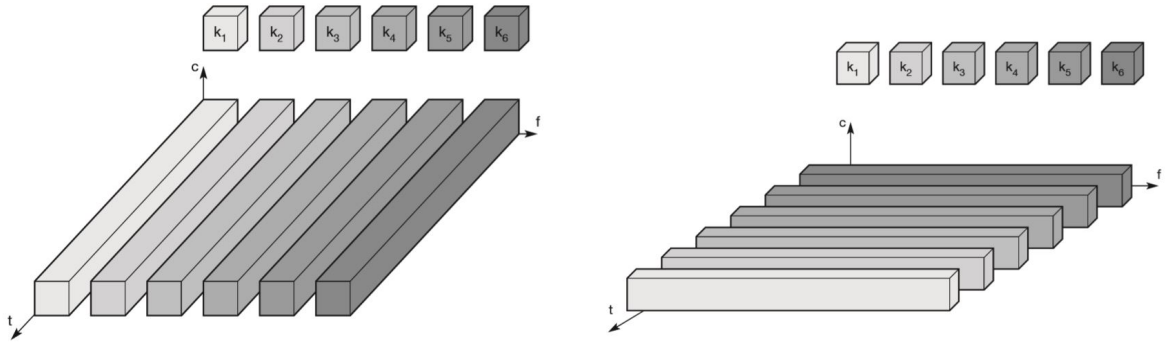
a frequency band [27]. Their schemes must ensure that the communication is made with the minimum or no interference at all between different senders.

In wireless communications, multiplexing can be carried out in four dimensions: space, time, frequency and code. The GSM standard uses a combination of frequency and time to make it possible to communicate between the user terminal and the base station [15]:

- **Frequency Division Multiplexing - FDM**: the frequency medium is divided into several non-overlapping frequency bands. To avoid adjacent channel interference, guard spaces are used to separate each frequency. This scheme is very simple so, there is no need to have coordination between the sender and the receiver, however having a fixed assignment of a frequency to a sender makes this mechanism very restrictive and inflexible;

- **Time Division Multiplexing - TDM**: the entire bandwidth is given to a channel for a certain amount of time, and so all senders use a certain frequency band in different periods of time. Just as in FDM, here the guard spaces also exist in order to separate the senders' time slots. This mechanism is more flexible than FDM but it is more demanding because it needs a strict synchronization between the senders in order to avoid collisions.

The figures 2.10a and 2.10b are a representation of the FDM and TDM schemes, respectively.



(A) FDM (B) TDM

FIGURE 2.10: The two multiplexing techniques used in GSM [15]

The combination of frequency and time division multiplexing, represented in the figure 2.11, results in a given sender transmitting at a certain frequency in a particular point of time.

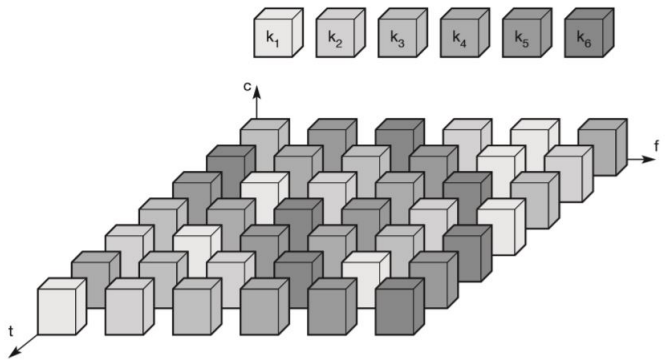


FIGURE 2.11: Frequency and time division multiplexing combined [15]

Multiple Access is the use of multiplexing techniques to provide communication service to multiple users over a single channel. It allows many users to share a common spectrum resource.

In the case of GSM, the multiple access to the spectrum is possible by combining time and frequency:

- **Frequency Division Multiple Access (FDMA)**: allocates frequencies according to the FDM scheme already described [15]. In the specific case of the GSM900, the 25 MHz bandwidth is divided into 124 carriers all spaced 200 KHz apart. The same happens in the GSM1800: the 75 MHz bandwidth is divided into 374 radio channels, all spaced 200 KHz apart as well;

- **Time Division Multiple Access (TDMA)**: allocates time slots for communicating through TDM. In the GSM, there is a fixed access pattern where each TDMA frame, with the duration of 4.615ms [28], is separated into eight time-divided channels called time slots[16]. Each of those 577μs time slots represents a physical TDM channel with approximately 156.25 bits. Then, these time slots are the fundamental unit of time in a TDMA scheme and are also named as bursts. More information about the TDMA trama of the GSM can be found in [15] and [28].

While a slot represents the physical separation of the spectrum, in other words, the physical channels, when these are grouped into a TDMA frame in order to transmit user or signalling data, they become the basic unit for the definition of logical channels. GSM channels can be named as dedicated channels when they are allocated to a mobile station

or can be named as common channels when they are used to distribute data to several mobile stations.

2.3.2.3 Modulation

Modulation is needed to transmit digital data via certain frequencies [15]. What modulation techniques do is to transport information into a radio-frequency carrier wave, changing one of their particular characteristics. The most commonly modified characteristics include amplitude, frequency, phase, pulse sequence, and pulse duration.

In wireless communications, the information cannot be transmitted via digital format. So the digital modulation has the purpose of translating binary data (0 or 1) into a analog signal, becoming a baseband signal. To perform this digital modulation, there are three basic methods: Amplitude Shift Keying (ASK), Frequency Shift Keying (FSK) and Phase Shift Keying (PSK) [15]. After the digital modulation, it is also necessary an analog modulation in order to shift "the center frequency of the baseband signal generated by the digital modulation up to the radio carrier" [15], so that it can be transmitted through the antenna. In the same way as digital modulation, there are three basic forms of analog modulation: Amplitude Modulation (AM), Frequency Modulation (FM) and Phase Modulation (PM).

For the 2G communications, the main focus will be the FSK, the Minimum Shift Keying (MSK) and more specific, the modulation scheme used on the GSM standard, the Gaussian Minimum Shift Keying (GMSK).

The FSK is a digital modulation where the frequency of the carrier signal varies according to the digital signal changes, and therefore, it constitutes a frequency modulation scheme. For example, for each binary input, 0 or 1, it is assigned a specific frequency output: for the input 0 the frequency is lower and for the input 1 the frequency is higher. In order to avoid abrupt changes in the signal's phase, there is a need to use frequency modulators that have Continuous Phase Modulation (CPM) [15].

The MSK is a FSK scheme with no phase discontinuities because "the frequency changes occur at the carrier zero crossing points" [29], representing itself a form of CPM.

In the MSK, the rectangular data pulse is replaced with a half sinusoidal pulse, [30], representing a modulation index of 0.5. MSK has some relevant characteristics that makes

it very useful: more immune to noise, relatively narrow bandwidth and coherent detection capability [31].

The result of a binary signal modulated through MSK can be shown in the figure 2.12.

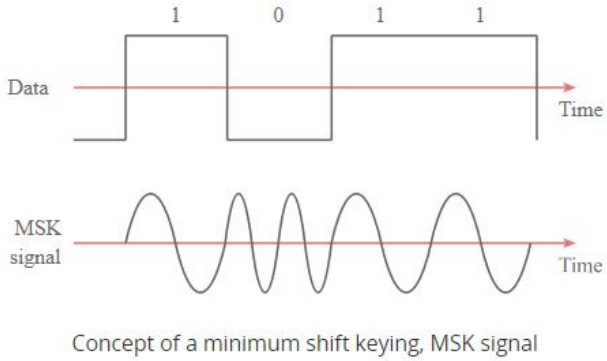


FIGURE 2.12: MSK Scheme [29]

However, the spectrum of a native MSK signal shows sidebands extending beyond the bandwidth of the original data, which it is not intended. So, this issue can be adjusted by passing the modulating signal through a low pass filter in some sort of pre-modulation. The filter that met the requirements is the Gaussian filter, which decreases the large spectrum needed by the MSK modulation. It was from this need, that the basic MSK signal was evolved into a GMSK modulation [29].

So, in the GMSK scheme, the modulating signal passes through a Gaussian filter with an appropriate bandwidth to then follow the normal process of being modulated by the MSK method. Therefore, the generated signal of the Gaussian filter is more compact, with low side lobes and a narrow bandwidth, being more capable of suppressing the high-frequency components [31].

GSMK was the modulation scheme selected for the GSM standard due to its properties being "easy to handle and implement into hardware" [28] and its low level of interference with neighboring channels.

2.3.3 Frequency Hopping

The GSM technology has two ways to use its available frequencies. One is the Frequency Hopping Spread Spectrum (FHSS), which is simplest and most common. In this scenario both FDM and TDM schemes, as described in the section 2.3.2.2, are implemented, where

the total available bandwidth is divided into several channels of lower bandwidth plus guard spaces between them, and each transmitter and receiver stay in a channel for a certain time and then hop to another.

In GSM standard, the FHSS is implemented using a constant carrier frequency for each channel called Absolute Radio-Frequency Channel Number (ARFCN) [28]. There are two FHSS variants: the slow hopping and the fast hopping. The slow hopping, used in GSM, refers to when "the transmitter uses one frequency for several bit periods" [15]. On the other hand, in the fast hopping, "the transmitter changes the frequency several times during the transmission of a single bit" [15]. The slow hopping is more tolerant to narrowband interference than the fast hopping scheme.

In order to make the system more robust and improve the service quality, it is also possible to use alternating frequencies for a single cell channel. This way, the carrier frequency is changed in every burst of the TDMA frame transmitted [28].

2.3.4 Handover

Handover, also known as Handoff, is the event of transferring users, which are the mobile stations, from a radio network to another. In the GSM standard the hard handover is implemented, where the MS is linked to a single BS at the time, opposed to the soft handover, where the MS is linked to more than one BS. This means that using hard handover breaks the connection with the source cell before establishing the link with the new cell's BS, which follows the "break-before make" approach [32].

There are many reasons to perform handover in cellular systems such as GSM. Normally, the MS tries to use the channel with the best Carrier to Interference Ratio (CIR) or signal strength [33]. The MS, in combination with the BTS, performs the measurement and report of not only its serving cell conditions, but also the signal strength of neighbor cells, to assure that it is safe to move a MS to a certain cell. Therefore, when a channel achieves a low value of CIR or signal strength, it is necessary to perform the handover, carried out by the BSC, in order to not compromise the communication. Thus, the need to perform a handover can happen due to [33]:

- Mobility: when a mobile station moves out of a BTS range, the execution of handover is crucial in order to preserve the service continuity;

- Network Management: when the traffic on one cell is too high, it is necessary to shift some mobile stations to neighboring cells in order to balance the coverage;
- Service-Related: in this case, the handover is performed when the channel in use presents a degradation in the Quality of Service (QoS).

Considering the many changes presented in the radio channel environment, it is necessary to execute a handover method that is effective with a relatively fast adaptive capacity in order to avoid unnecessary handoff and preserve a certain level of QoS. Having these needs in consideration, the most common criteria used for handover analysis is the Received Signal Strength (RSS) [32]. Thus, the hard handover algorithms presented in GSM are the following [33]:

- RSS based handover algorithm: the handoff occurs when the signal strength of a neighboring BS in a MS is greater than the RSS of the current cell BS;
- RSS based handover algorithm with Threshold (RSS-T): the handoff occurs when the signal strength of the current cell's BS is lower than a threshold value, indicated by T1 and T2 in figure 2.13, and lower than the signal strength of a neighboring BS as well;
- RSS based handover algorithm with Hysteresis (RSS-H): the handoff occurs when the signal strength of a neighboring BS is greater than the signal strength of the current cell's BS by a hysteresis margin identified by the value h of the figure 2.13;
- RSS based handover algorithm with Hysteresis and Threshold of Servicing BS (RSS-HT_{ser}): the handoff occurs when the current signal level drops below a threshold and the RSS of the new BS is stronger than the current one by a given hysteresis margin;
- RSS based handover algorithm with Hysteresis and Threshold of the New BS (RSS-HT_{new}): the handoff occurs when the RSS of a neighboring BS is strong enough to achieve the threshold value of the ideal new BS based on the RSS-H algorithm.

Figure 2.13 represents a GSM handover scheme, where a MS moves between two BSs, while passing through the already explained threshold (T1 and T2) and the hysteresis margin (h) parameters.

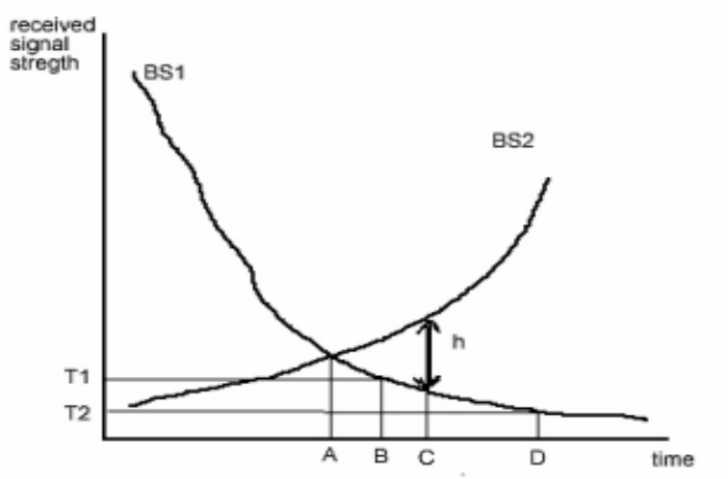


FIGURE 2.13: GSM Handover scheme [34]

The implementation of the handover algorithms is left to the operator, following their policies.

The GSM handovers can be classified in four types [15]:

- Intra-cell handover: inside the cell, the BSC can change the carrier frequency;
- Inter-cell, intra-BSC handover: it is the usual handover scheme. The MS moves to another cell but remains controlled by the same BSC;
- Inter-BSC, intra-MSC handover: the MS moves to another cell controlled by a different BSC belonging to the same MSC as before;
- Inter MSC handover: this last type of handover occurs between two cells with different MSCs.

2.4 Jamming

Jamming is the intentional disruption of the communication signal. This effect is caused by the so-called jammers that are devices capable of interfering in the transmission of signals in many communication systems such as GNSS systems, mobile communication systems, Wi-Fi network, among others.

Initially, jammers for cellular mobile communications were designed for military use. The interest in this technology for other types of uses appeared due to the utility resulting

from the main idea: to deny the successful transport of information between a sender and a receiver.

Generally, to perform jamming, the power of the signal jammer on the pretend receiver must overlap the signal from the transmitter. That way, the ratio of jamming power to signal power necessary to obtain an effective jamming is called the Jamming-to-Signal ratio (J/S). Usually this value is expressed in dB and has to be positive to represent an inhibition of a successful communication [35].

The jamming of mobile devices is done through the transmission of a RF signal by the jammer, in the same frequency band the mobile device operates, which results in a signal loss, leaving the antenna of the mobile device unable to communicate with the antenna of the belonging base station and, consequently, the mobile device will be unable to establish connections with another mobile terminal. Likewise, all devices within the jammer radius will also be deactivated. Most mobile devices use bands of different frequencies to communicate with the base stations. Then, low power jammers are designed to block all bands between 800MHz and 1900MHz with a maximum range of approximately 9 meters, depending on the surrounding environment (existence of mountains or buildings walls that can block the interference signal) [36]. The most sophisticated jammers are capable of blocking several bands at the same time, which is useful in mobile double-band and triple-band devices where it is possible to have an automatic switching of the band type in order to find an available channel.

Therefore, the jammer broadcasts a radio signal with a higher power at the operating frequency of the mobile device in order to have a collision between the two signals and consequently the communication is canceled. However, the mobile terminals are prepared to increase the signal power if they detect any type of attack, so, the jammer must be able to identify this change and adjust its power again in line with the mobile terminal power. Since mobile devices are full-duplex, which means, they use two different frequencies: one for the transmitter channel and one for the receiving channel, the jammer must disturb one of the channels to compromise the normal functioning of the device [37].

Depending on their final objective, a jammer can be essentially classified as elementary or advanced. Also, these two main categories can be divided into two sub-categories as shown in figure 2.14:

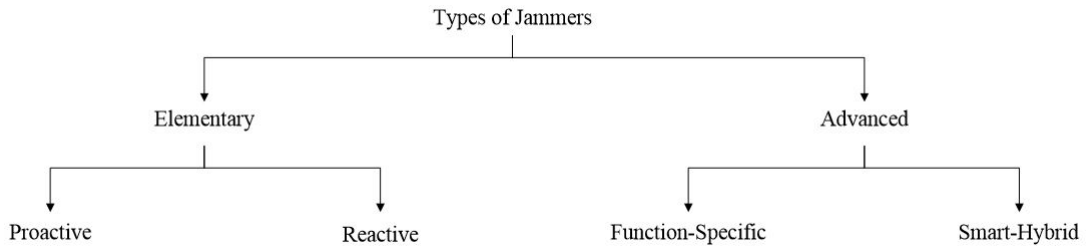


FIGURE 2.14: Type of jammers [38]

The proactive jammers interfere whether or not there is activity on a certain channel of the network while the reactive jammers only start jamming when communication exists on a certain channel. On the advanced jammers, the function-specific ones, as the name suggests, have a well established function being able to act in a single channel or in multiples as well and the smart-hybrid jammers are characterized by their power efficiency and effective jamming [38].

The main components common to any type of jammer are [39]:

- Antennas: while the less complex jammers normally have their antenna inside the device, the more sophisticated ones have several antennas on the outside in order to ease the reach of bigger actuation radiuses and the blocking of several frequency bands simultaneously;
- Battery: it is the power supply of the system, whose duration depends on the complexity of the jammer;
- Voltage-Controlled Oscillator (VCO): responsible for generating the emitted radio signal;
- Tuning circuit: it allows to define the frequency which the signal will be broadcasted, inserting a voltage at the VCO input;
- Noise Generator: it is part of the control circuit and it is in this component that a random electronic signal is generated at the same frequency as the pretended signal to interfere;
- RF Amplifier: it amplifies the output signal in order to reach the necessary radio signal power to block the communication.

To build the pretended jammer for this thesis, it is necessary to study, implement and analyze jamming techniques in order to choose the jammer with the best performance. The techniques used in this study are the following: barrage jamming, tone jamming, sweep jamming and protocol-aware jamming. These methods will be explained in more detail and also implemented on chapter 3 through the SDR technology.

2.5 Software Defined Radio (SDR)

2.5.1 Overview

According to the Institute of Electrical and Electronic Engineers (IEEE) P1900.1 Working Group, the definition for Software-Defined Radio is "radio in which some or all of the physical layer functions are software defined" [40]. In other words, it is the implementation of operating functions on the radio system or device processed through software without the need to change the hardware.

This technology was first introduced by Joseph Mitola in 1992. It emerged by the limitation and lack of flexibility of protocols mostly hardware based. There was the need of a solution capable of being reconfigured to perform others purposes beyond what the hardware itself allowed [41].

Some applications and advantages for its use can already be identified, such as [42]:

- Interoperability: the interest in this technology, including from the military, lies in the fact that SDR can communicate with different radios, acting as a translator for all of them;
- Efficient resources adaptation: a system based on SDR can adjust a waveform to a specific scenario in order to maximize user experience;
- Frequency reuse: an SDR can use an underutilized spectrum and that way, increase the amount of available spectrum;
- Reduced obsolescence: this technology can support and sustain the latest communication protocols through mostly software updates;
- Lower cost: a SDR is designed to have multiple purposes, so the cost of maintenance needs to be reduced;

- Research and development: like it is used in this research, the SDR technology allows the implementation of many waveforms and study its real-time performance.

2.5.2 Architecture

An ideal SDR, represented in the figure 2.15, must include an antenna, a micro-processor and Digital-to-Analog (D/A) and Analog-to-Digital (A/D) modules for a transmitter and receiver respectively. The SDR is also described as the application of Digital Signal Processing (DSP) to radio waveforms. The micro-processor replaces the DSP block of the traditional radio receivers and transmitters.

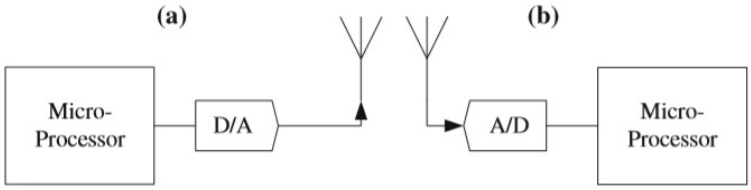
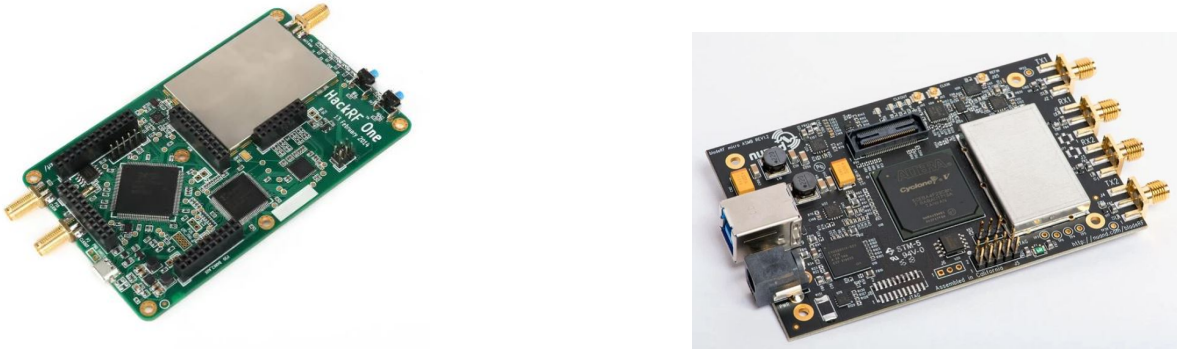


FIGURE 2.15: Ideal SDR: (a) Transmitter, (b) Receiver [42]

The data is transformed into a pretended waveform in the microprocessor and then converted into a RF signal on the D/A component to finally being sent through the antenna. Then, the transmitted signal enters the receiver antenna, is transformed into digital samples on the A/D module and processed in real time in a generic micro-processor [42].

2.5.3 SDR Equipment

Nowadays, there is a wide variety of SDR devices in the market, which can be characterized in terms of price, application, frequency and usability. Among them, it is possible to highlight two equipment that best suit in this study: the HackRF One and the BladeRF, which are represented in figure 2.16a and 2.16b respectively.



(A) HackRF One [43]

(B) BladeRF [44]

FIGURE 2.16: SDR Equipment

The HackRF One is an open source hardware equipment design to build SDR projects. It is capable to operate in frequencies from 1 MHz to 6 GHz covering most devices operating with Bluetooth, FM radio, and cellular technology. The HackRF One can be used to transmit or receive radio signals but it cannot do both at the same time. For this reason, it is considered a half-duplex transceiver. It has a 8-bit resolution of the Analog-to-Digital Converter (ADC) and up to 20 MHz of bandwidth [45].

As well as the HackRF One, the BladeRF is also an open source SDR transceiver. It was designed to be highly reprogrammable, being capable "to act as a custom RF modem, a GSM and LTE picocell, a GPS receiver, an ATSC transmitter or a combination Bluetooth/WiFi client" [46]. It can tune from 300 MHz to 3.8 GHz and it can operate in full-duplex which means it can receive and transmit simultaneously. It has a 12-bit of ADC and up to 28 MHz of instantaneous bandwidth [47].

The table 2.1 combines both characteristics of the HackRF One and the BladeRF mentioned above.

	HackRF One	**BladeRF**
Open Source	Yes	Yes
Frequencies Range (MHz)	1 - 6000	300 - 3800
Duplex	Half-duplex	Full-duplex
ADC Resolution (Bit)	8	12
Bandwidth (MHz)	20	28
Price (Euros)	250	550

TABLE 2.1: Comparison between HackRF One and BladeRF

Given the main purpose of building a jammer in this study, the chosen equipment must be able to transmit and receive at the same time. It also must cover the frequency ranges of the GSM standard and cover, at least, one of its bandwidth as well. Therefore, the SDR equipment that meets the requirements mentioned above is the BladeRF. The BladeRF is described in more details in chapter 3.

2.5.4 SDR Software - GNU Radio

Nowadays, one of the most popular SDR softwares is the GNU Radio and it was founded by Eric Blossom. The "GNU Radio is a free & open-source software development toolkit that provides signal processing blocks to implement software radios. It can be used with readily-available low-cost external RF hardware to create software-defined radios, or without hardware in a simulation-like environment" [48].

This software uses two programming languages: C++ for creating signal processing blocks and Python for higher-level connections and generation of signal flow graphs. The integration between these two languages is possible through an interface compiler called Simplified Wrapper and Interface Generator (SWIG) [49]. The GNU Radio runs under several operating systems like Linux, MacOS and Windows, having more support on Linux.

The GNU Radio is mainly composed by the following elements [42]:

- Flow graph: it is series of interconnected signal processing blocks;
- Source blocks: they represent the beginning of a flow-graph, having no inputs but one or more outputs;
- Sink blocks: they represent the end of a flow-graph, having no outputs but one or more inputs;
- Scheduler: it is responsible for activating each processing block and managing data transfer between blocks.

In order to simplify the use of GNU Radio and have a smaller learning curve, the GNU Radio Companion (GRC) extension can be used.

The GRC is a Graphical User Interface (GUI) for GNU Radio, where users place functional blocks into a processing chain known as a flowgraph. These blocks can be

easily configured through its inherent parameters. With this free open-source tool, Python knowledge is not required because after the user creates the pretended signal flow graph and consequently executes the GRC, a Python file is generated that will allow us to run the application [49].

An illustrative example of a flow graph made in the GRC is shown in figure 2.17.

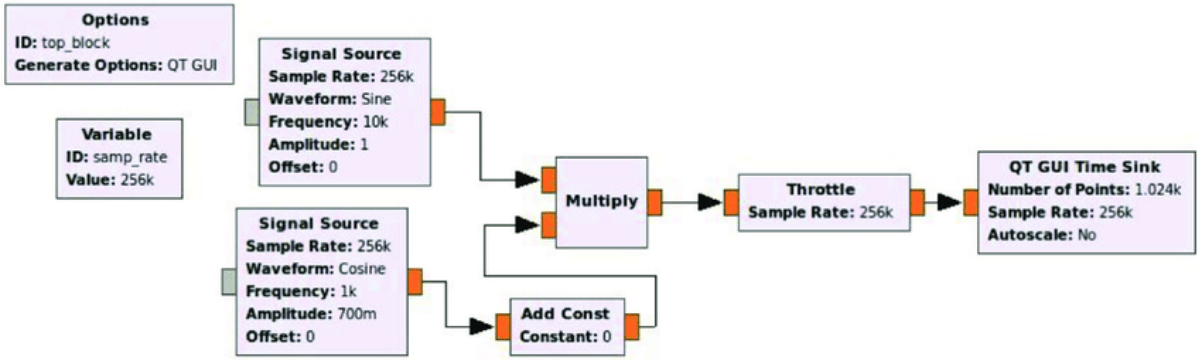


FIGURE 2.17: A GRC flow graph [50]

2.6 Related Work

2.6.1 GSM Jamming in Mobile Phones

The GSM standard is a mature technology with many years of improvements. For that reason, the interest on this topic and its vulnerabilities has been growing over the years. There are many publications where GSM jammers are built and studied with different outcomes.

In studies done in [51] and [52], the authors designed and implemented a GSM jammer to be applied on mobile phones. On the first study, their main intention was to transmit a RF signal in the frequency band of the mobile device used in order to corrupt the communication, leaving the device and other devices that were within range of action of the jammer, with the "no network" alert on the screen. The results obtained were as intended, with the experiment, illustrated in figure 2.18, being able to jam the three main cell phone carriers of the country under study with the developed jammer working in a dual band, both on the GSM900 and GSM1800.

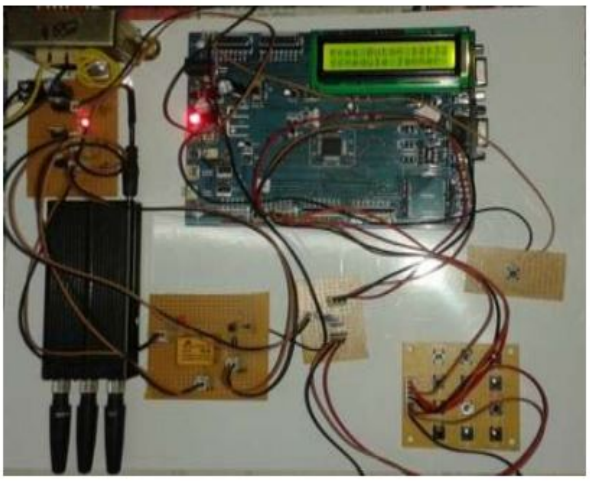


FIGURE 2.18: System built on study [51]

On the other hand, the results obtained in [52] were satisfactory as well but the authors have realized that the jammer was not so effective at certain points, and those situations were when the power of the jammer input signal was greater than its output signal.

2.6.2 Jamming applied to UAVs

Initially, UAVs were designed for military purposes. Over the years, they evolved in order for their commercialization to be possible. Nowadays, this type of aircrafts is available for many civilian purposes, which also means that they can be used in illegal activities.

Therefore, many research articles such as the ones described in [53] and [54] try to use jammers to mitigate the misuse of commercial UAVs. The authors in [53] have done a research using available commercial jammers, more specifically the JYT/J08 and VG5W20, in order to test if those jammers can really work against the threat of misusing UAVs. After the appropriate experiences, it was verified that the jammers within the band of 2.4 GHz were not efficient but in the frequency band used for the GPS signal, they were sufficient and agile on cases where the UAV was in an autonomous flight mode. In [54], the authors had the same concern about the social risks related to the use of UAVs. The proposed reactive jamming would transmit a relatively weak interference signal, through a Yagi antenna, to the narrow band of the UAV in order to disable the frequency hopping communication. The experiences made, represented on the figure 2.19, revealed that the

developed jammer in [54] was able to work as an anti-drone, interrupting the communication between the UAV and its radio controller by detecting the operating frequency of the drone.

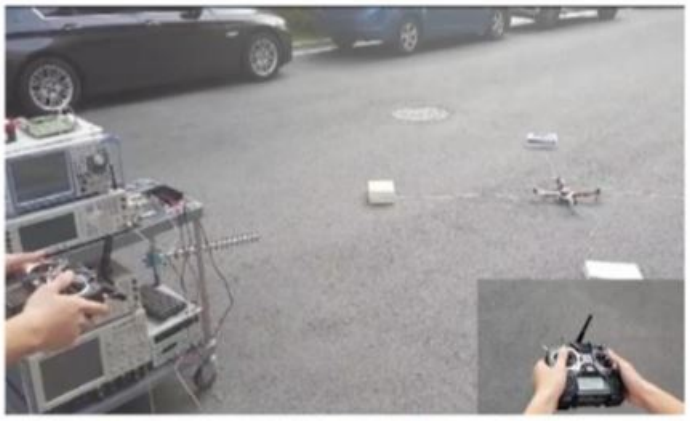


FIGURE 2.19: Experimental setup of study [54]

2.6.3 Jamming using SDR technology

With the emergence of the SDR technology, building jammers and studying the jamming techniques became more reachable among civilians due to its easier hardware commercialization and its open-source software. Therefore, some SDR and jammers researches applied to wireless communications systems are already available.

In [55] and [56], the authors used SDR for Wi-Fi and GPS jamming, respectively. The author in [55] used the GRC as the main platform to interact with the USRP B210 equipment. It was through the broadcast of unmodulated Gaussian noise methodology, as represented in the figure 2.20, that the author obtained the parameters to achieve his main goal: an effective jamming. Also, the author in [55] reinforced the viability of SDR to perform an efficient Wi-Fi jamming by being able to reach to a minimum power value of 75 dBm. To perform the GPS jamming in [56], the author used the software GRC as well and a BladeRF as hardware. On this study, five known jamming techniques were tested: barrage jamming, tone jamming, sweep jamming, protocol-aware jamming and sucessive pulses jamming. Given the specific scenario and taking into account the range factor, the author in [56] considered the protocol-aware jamming to be the most effective in performing GPS jamming, accomplishing these concrete results with the SDR technology as well.

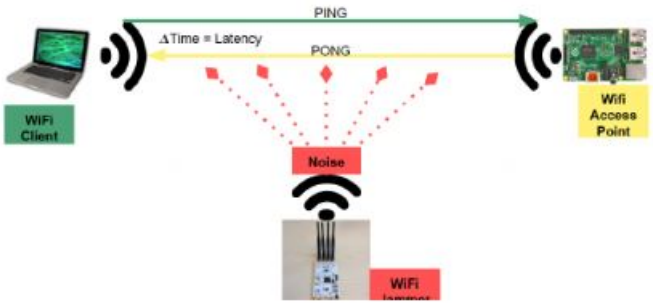


FIGURE 2.20: Experimental setup of study [55]

Taking into account the researches and study concepts described above related to jamming, GSM, SDR and UAV, this dissertation will then propose the development of a efficient jammer for mobile cellular systems, more specifically a GSM jammer, based on the SDR technology, in order to contribute to the reduction of unauthorized activities from UAVs.

The researchers presented so far, related to the mobile networks, are more focused on the GSM technology and the reason why is because it will serve as a starting point for the exploration of jamming on cellular mobile systems.

Chapter 3

Implementation of Jamming Techniques

To build the pretended jammer, it is necessary to study the many jamming techniques and how they work. Therefore, in this chapter, there is an approach of the chosen techniques and, consequently, its implementation using the SDR technology.

3.1 Hardware

In the section 2.5.3, there is a brief description about the main hardware chosen for this research, the BladeRF x40 and the others devices and platforms used to implement the jamming techniques.

As stated earlier, the BladeRF x40 is a SDR transceiver covering the frequency range of 0.3 GHz to 3.8 GHz, capable of achieving full-duplex 28MHz channels, with appropriate software.

To maximize the use of this device, it is important to know its features in more detail, as listed below [47] [57]:

- Flexible clocking architecture for arbitrary sample rates up to 40 million samples per second (MSPS);
- 12-bit quadrature sampling;
- Supported by GNU Radio, Pothos, SDR Console, MathWorks MATLAB & Simulink and more;
- Independent RX and TX signal paths;

- Fully bus-powered USB 3.0;
- +6dBm TX power;
- 2 SMA female antenna connectors.

To have a better perspective of the BladeRF composition, the figure 3.1 shows its architecture and its main components.

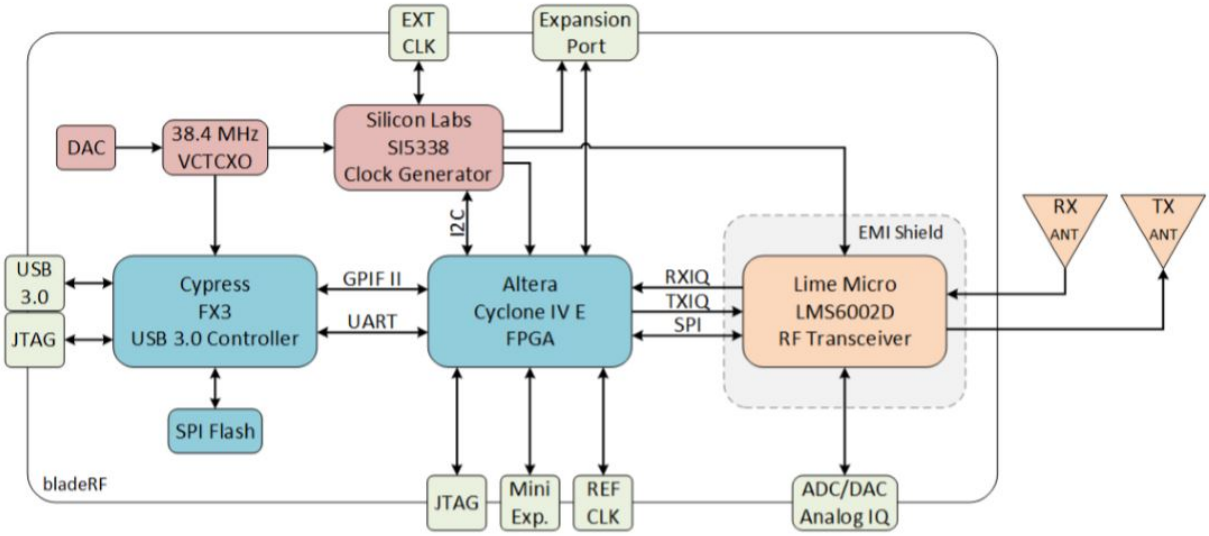


FIGURE 3.1: BladeRF Architecture [47]

As figure 3.1 shows, the transceiver employed by the BladeRF is the Lime Microsystems LMS6002D. This single chip has the following specific programmable modulation bandwidth values [58], as shown in table 3.1.

1.5	**1.75**	**2.5**	**2.75**	**3**	**3.84**	**5**	**5.5**	**6**	**7**	**8.75**	**10**	**12**	**14**	**20**	**28**

TABLE 3.1: Microsystems LMS6002D bandwidth values, in MHz

The GSM900 signals have a bandwidth of 25 MHz. Using the 20 MHz value, it will not cover the entire bandwidth of the GSM900 signal. On the other hand, using the 28 MHz value, the entire bandwidth will be covered, having only a waste of 3 MHz. Therefore, these two values will be applied in the jamming techniques where it makes sense, and the most efficient value will be identified for each case.

In the BladeRF, the TX gain is implemented through Variable Gain Amplifier (VGA), using two gain stages: TXVGA1 for the Base Band (BB) Gain and TXVGA2 for the Radio

Frequency (RF) Gain. The values for the TXVGA1 vary from -35 dB to -4 dB, and for the TXVGA2 the values vary from 0 dB to 25 dB [59]. For the implementation of each jammer the maximum value will be applied for the BB Gain and RF Gain, which is, -4 dB and 25 dB respectively.

The BladeRF has a maximum value of 40 MHz, in regard to the sample rate values [47]. The most suitable sample rate value for each jammer implementation will be identified, in order to avoid samples' losses.

To better analyze and visualize the spectrum, the LimeSDR mini was used. This device, in line with the platform CubicSDR, was capable to play the role of a receiver when the BladeRF receiver was not able to dynamically reproduce the result of the signal transmitted in the spectrum.

The LimeSDR mini, represented in figure 3.2, is an open source SDR transceiver, a smaller and cheaper version of the full sized LimeSDR [60]. It has two coaxial RF SMA connectors, one for reception and the other for transmitting, and a USB3.0 (type A) plug. The LimeSDR mini covers a frequency range from 10 MHz up to 3.5 GHz in full-duplex and a bandwidth value of up to 30.72 MHz. As a main RF chip, a Lime Microsystems LMS7002M with a 12-bit ADC is used [61].

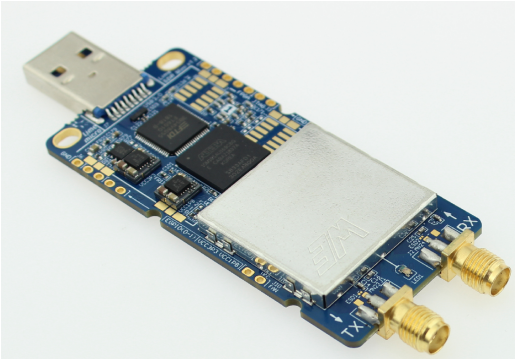


FIGURE 3.2: LimeSDR Mini [62]

The two antennas used with the BladeRF are an omnidirectional antenna and an Apex TG.30 ultra-wideband antenna, shown in figure 3.3a and 3.3b respectively. Both can operate over a wide range of frequencies from 698 MHz to 960 MHz, covering the frequencies of the GSM900 [63] [64]. There is no need to have any type of adaptor because these antennas have a SMA male connector allowing direct connection to the BladeRF.

(A) Omnidirectional antenna [63]

(B) Apex TG.30 antenna [65]

FIGURE 3.3: Antennas

3.2 Software

The main software used to build the flow graphs needed to implement the studied jamming techniques was the GNURadio, more specifically, the GRC. This software was already explained, in detail, on the section 2.5.4.

As explained in the previous section, it was necessary to use the CubicSDR platform to analyse the spectrum. The CubicSDR is a cross-platform that, in combination with a hardware, works as a SDR receiver. Using a supported hardware, which makes the conversion of the RF spectrum into a digital stream, it is possible to explore any types of airborne signals such as satellite. It is included in the Pothos SDR development environment, supporting many types of SDR hardware such as BladeRF, HackRF, Airspy, RTLSDR and Red Pitaya [66]. In the figure 3.4, the user interface of the CubicSDR platform is presented.

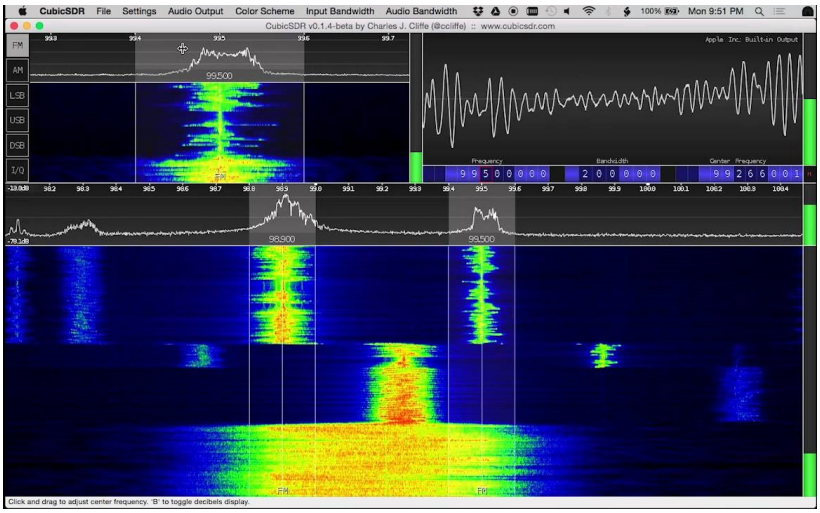


FIGURE 3.4: CubicSDR user interface [67]

Another helpful free tool used to observe and analyze the reception status of the GSM receptor used when the jammer is transmitting, is an Android app from the Play Store called "NetMonitor Cell Signal Logging", represented in figure 3.5. This app can monitor the network traffic, indicate the power received by the smartphone and indicate from which channel is receiving its coverage, and finally determine which mobile network technology has been used.

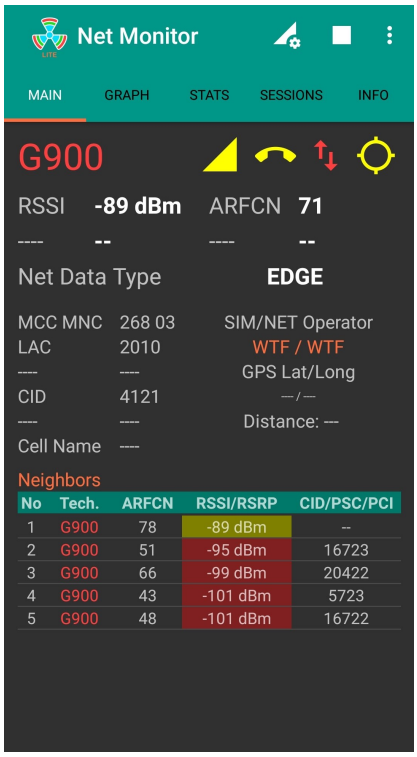


FIGURE 3.5: Interface from NetMonitor App

3.3 Frequency values used

To affect the communication system of the GSM receptor, it is intended to attack its downlink channel since it is through this link that the BS covers the cell where the GSM receptor is located. As already mentioned in section 2.3.2.1, the frequency range of the GSM900 downlink channel is from 935 MHz to 960 MHz. The bandwidth of 25 MHz is then divided in 124 channels. In the GSM, each uplink/downlink channel pair is identified by the ARFCN code as explained in section 2.3.3. There are two formulas to calculate the frequency of each GSM900 uplink/downlink channel pairs based on the ARFCN code.

$$f_{ul}(n) = 890.0 + 0.2 \times n \tag{3.1}$$

$$f_{dl}(n) = f_{ul}(n) + 45 \tag{3.2}$$

The equation (3.1) represents the uplink frequency and the equation (3.2) represents the downlink frequency, where n is the ARFCN code.

Since the number of channels to cover is considerably high in some jammer implementations (duly indicated later), it was decided to restrict the target to a frequency range used by a Portugal mobile network operator. The main three mobile network operators in Portugal are NOS, MEO and Vodafone. The chosen GSM receptor for this simulation is covered by NOS, so the downlink frequency range used will be between 943.1 MHz and 950.9 MHz [68].

3.4 Jamming Techniques

In order to achieve the desired jammer, four jamming techniques were studied and implemented. For simulation purposes, a smartphone is used as a GSM receptor, with the 2G mode active only, in order to test the jamming techniques performance.

3.4.1 Barrage Jamming

The barrage jamming, shown in figure 3.6, transmits noise energy across the entire bandwidth of the target and for this reason, it is also known as full band jamming. This type of jamming essentially raises the background noise level in the receiver, disturbing its

communication system, being the easiest scheme to use when the characteristics of the target channel are not known [69].

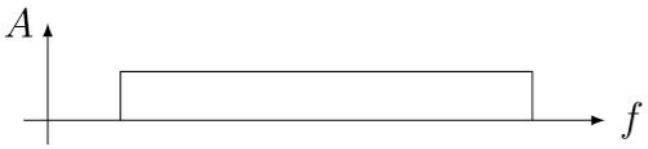


FIGURE 3.6: Barrage Jamming Scheme [70]

The implementation of this technique on the GRC, represented in figure 3.7, uses the Noise Source block to introduce a Gaussian noise signal across all the GSM900 bandwidth, through the transmission block represented by the osmocom Sink block. The center frequency chosen was 947.4 MHz, which is the center frequency of the downlink spectrum, corresponding to the channel with the ARFCN code equal to 62. Therefore, the table 3.2 indicates the configuration values used for this jammer implementation.

Parameter	**Value**
Bandwidth	20 MHz
Sample Rate	8 MHz
Frequency	947.4 MHz
Center Frequency	947.4 MHz

TABLE 3.2: Configuration values used on the Barrage Jamming

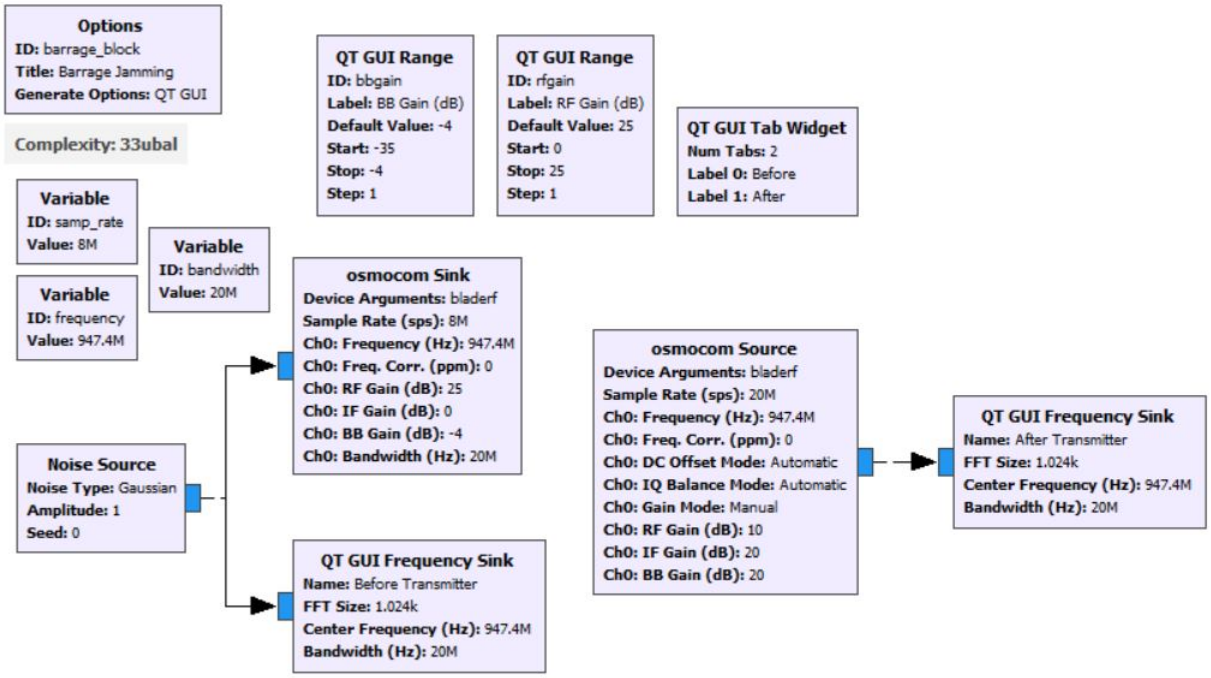


FIGURE 3.7: Barrage Jamming Flow graph

Through the BladeRF receiving block represented by the osmocom Source and the QT GUI Frequency Sink block responsible for the signal emitted representation, it is possible to analyse the resulting spectrum graph illustrated in figure 3.8.

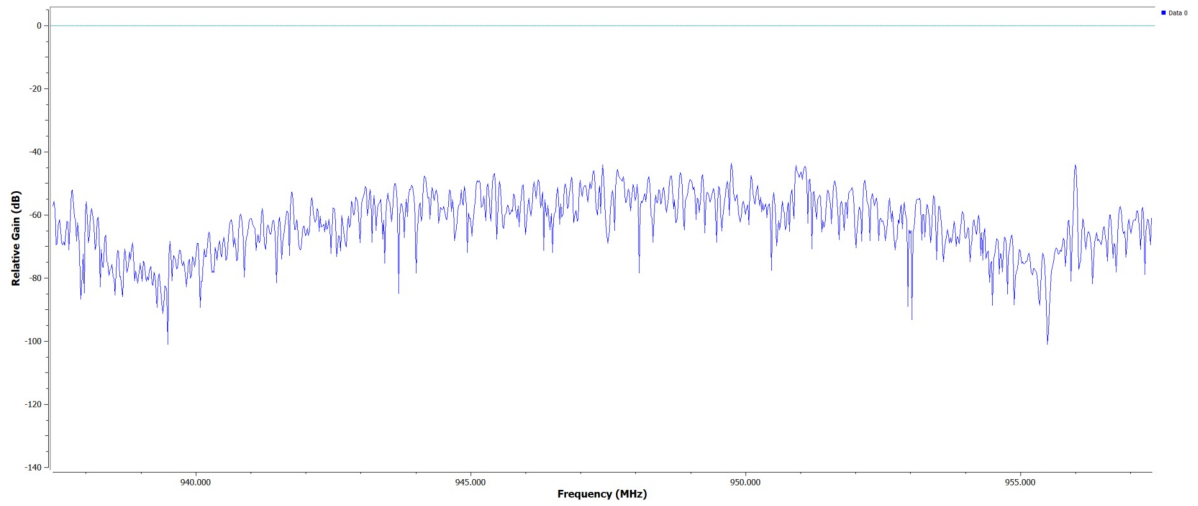


FIGURE 3.8: Barrage Jamming resulting spectrum

The signal developed has a bandwidth of 20MHz and an average Power Spectral Density (PSD) of, approximately, -60 dBW/Hz.

3.4.2 Tone Jamming

This jamming scheme has two versions: the single tone (ST) and the multi tone (MT). In the ST, the jammer puts all its power at a single pre-selected frequency that has been considered as an interest target. On the other hand, the MT distributes its power among several tones, generating tones in possible strategic frequencies [69]. Due to the fact that the BladeRF can only transmit one frequency at a time, in this study the ST version will be implemented, as represented in figure 3.9.

FIGURE 3.9: Single Tone Jamming Scheme [70]

In this scheme, the Signal Source block is used , responsible for the generation of a sine wave transmitted through the osmocom Sink block. This wave is emitted in a frequency of 949.2 MHz, value calculated through the formula (3.2) with a ARFCN code equal to 71, which is the channel code with the best Received Signal Strength Indication (RSSI) of the GSM receptor used at the moment of implementation. The figure 3.10 illustrates the GRC flow graph of the ST jamming and the configuration values used for the implementation are indicated in the table 3.3.

Parameter	**Value**
Sample Rate	12 MHz
Frequency	949.2 MHz
Center Frequency	947.4 MHz

TABLE 3.3: Configuration values used on the Tone Jamming

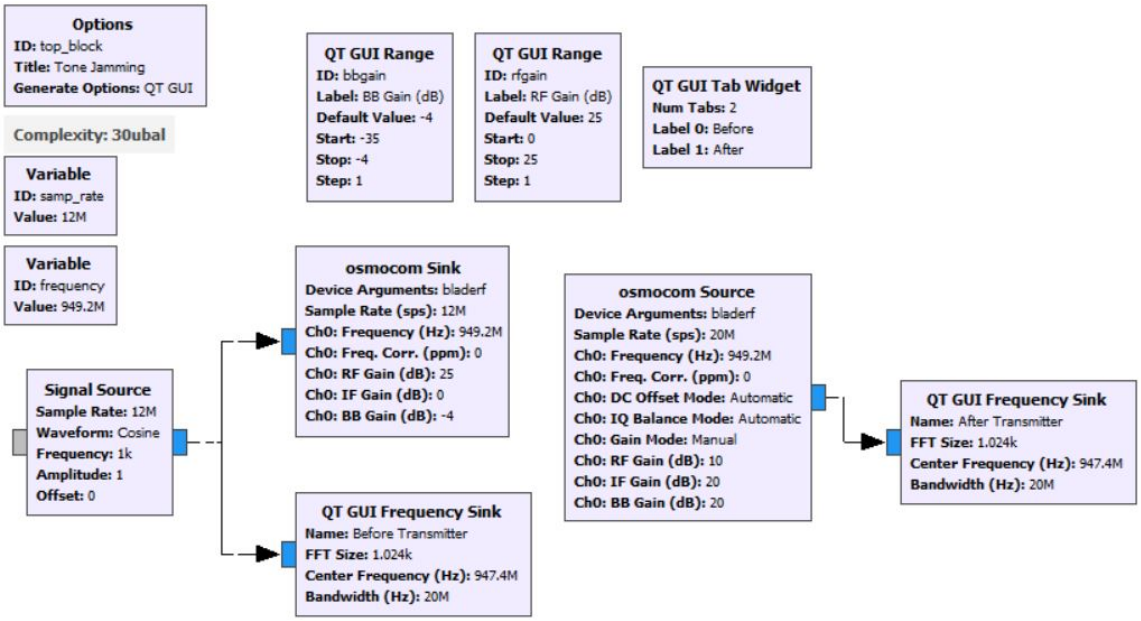


FIGURE 3.10: Single Tone Jamming Flow graph

The figure 3.11 represents the resulting spectrum graph obtained through the osmocom Source block, displayed graphically by the QT GUI Frequency Sink block.

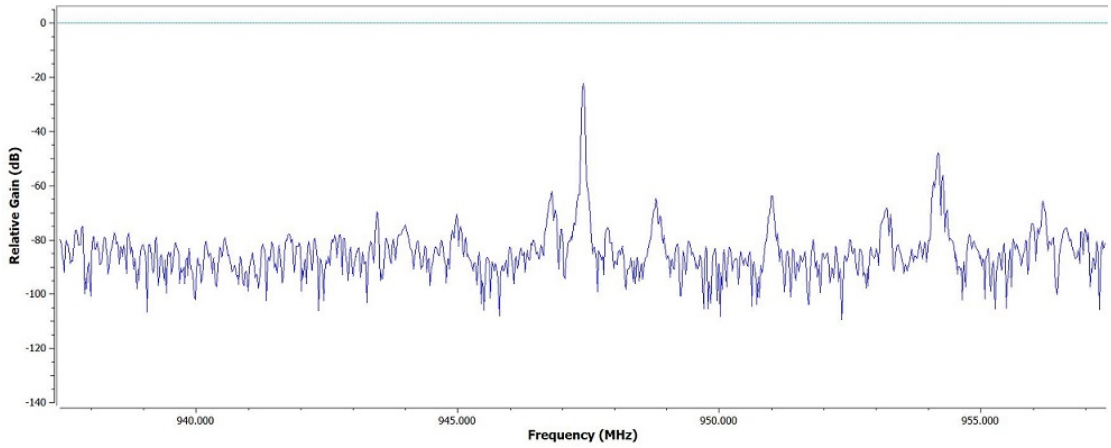


FIGURE 3.11: Single Tone Jamming resulting spectrum

The signal developed has an average PSD of, approximately, -85 dBW/Hz.

3.4.3 Sweep Jamming

The sweep jamming technique gathers concepts from both barrage and tone jamming, as a relatively narrowband signal, usually referred as chirp signal, which is swept in time across the entire target bandwidth [70]. Therefore, this jammer is more efficient in terms

of spectral density since employs its full power on a specific frequency over a period of time, jamming only the portion of the spectrum around that frequency. In order to make this jammer efficient, it is important to know the characteristics of the target receivers and adjust the jammer frequency hops speed [69]. The figure 3.12 represents the theoretical spectrum of the sweep jamming.

FIGURE 3.12: Sweep Jamming Scheme [70]

For the implementation of this technique, it is necessary to transmit a Chirp Signal that will make hops over a desired frequency range. That way, the Signal Source block was used to transmit a signal, more specifically, a sinusoidal wave, that will change its transmission frequency value, over time, through a set of frequency options inserted in the QT GUI Chooser block. As mentioned in the section 3.3, to cover the frequency range of the NOS operator, which is the operator used by the GSM receptor, it was possible to calculate, through the formula (3.2), the downlink frequency range of the NOS operator, reaching the values between 943 MHz and 950.8 MHz, with a frequency hops value equal to the bandwidth value of each GSM channel, which is 0.2 MHz.

The table 3.4 summarizes the main configuration values used for the Sweep Jamming implementation and the figure 3.13 illustrates the GRC flow graph of the Sweep jamming.

Parameter	**Value**
Bandwidth	20 MHz
Sample Rate	20 MHz
Frequency	943 MHz - 950.8 MHz
Center Frequency	947.4 MHz

TABLE 3.4: Configuration values used on the Sweep Jamming

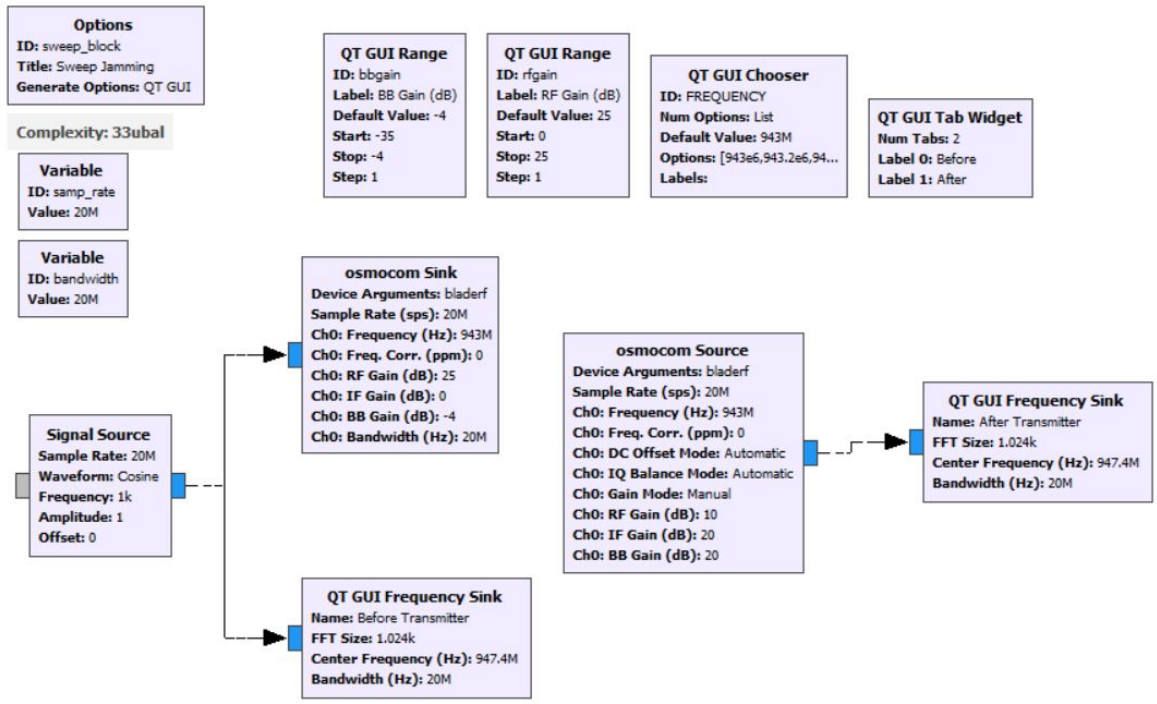


FIGURE 3.13: Sweep Jamming Flow graph

In order to set the center frequency automatically on the osmocom Sink block using the available frequencies of the QT GUI Chooser block, the python code file generated by the GRC was modified, with the following changes:

1. A function called "get_FREQUENCY_Options" was created, as represented in the figure 3.14 a), to return the array "self._FREQUENCY_options" which contains the frequencies values of the QT GUI Chooser block that will be swept;

2. On the main function, a loop cycle was implemented to scroll through the frequencies list values obtained, by calling the existing function

   "get_FREQUENCY_Options";

3. Then, the current loop frequency value was set to the center frequency value of the osmocom Sink block by calling the function "set_FREQUENCY";

4. Finally, the code line "print tb.get_FREQUENCY()" outputs the BladeRF current frequency value transmitted.

The modifications made in points 2, 3 and 4 are shown in figure 3.14 b).

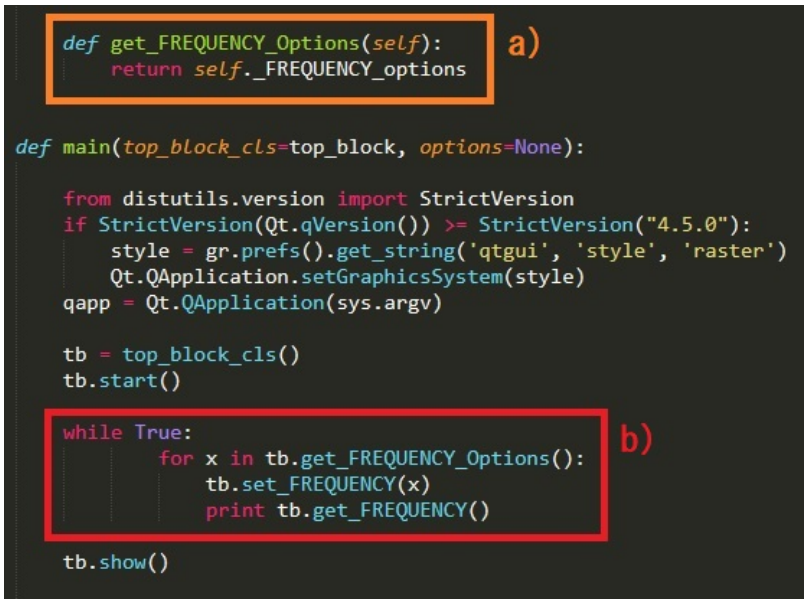
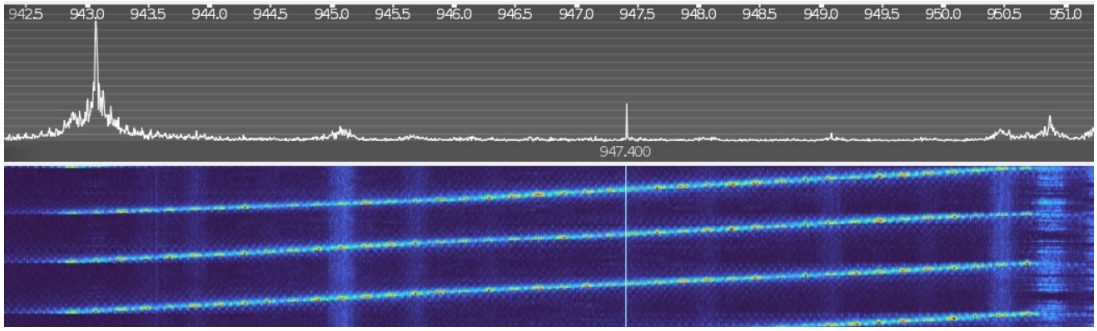
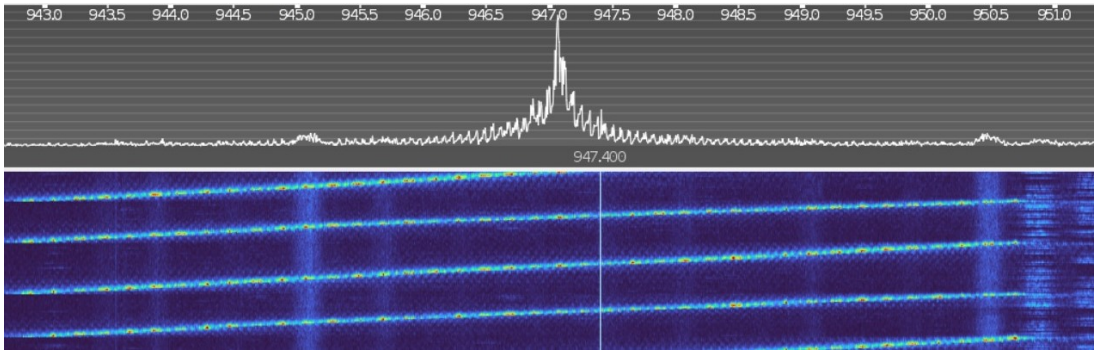


FIGURE 3.14: Changes made on the generated GRC Python file to transmit the chosen frequencies automatically

For this technique, the resulting spectrum of the Chirp Signal transmitted was analyzed using the LimeSDR mini as a receptor and the CubicSDR as a visualization interface, both mentioned in section 3.1 and 3.2 respectively. Thus, the figures 3.15a and 3.15b show the frequency hops of the current study spectrum in the CubicSDR platform.



(A) Frequency hop at 943.2 MHz



(B) Frequency hop at 947.2 MHz

FIGURE 3.15: The frequency hops visualization of the Sweep Jamming in the CubicSDR platform

The resulting spectrum graph in a certain instant of time is presented in figure 3.16, where the BladeRF has transmitted the Chirp Signal at the frequency of 949.2 MHz, verifying an average PSD of, approximately, -90 dBW/Hz.

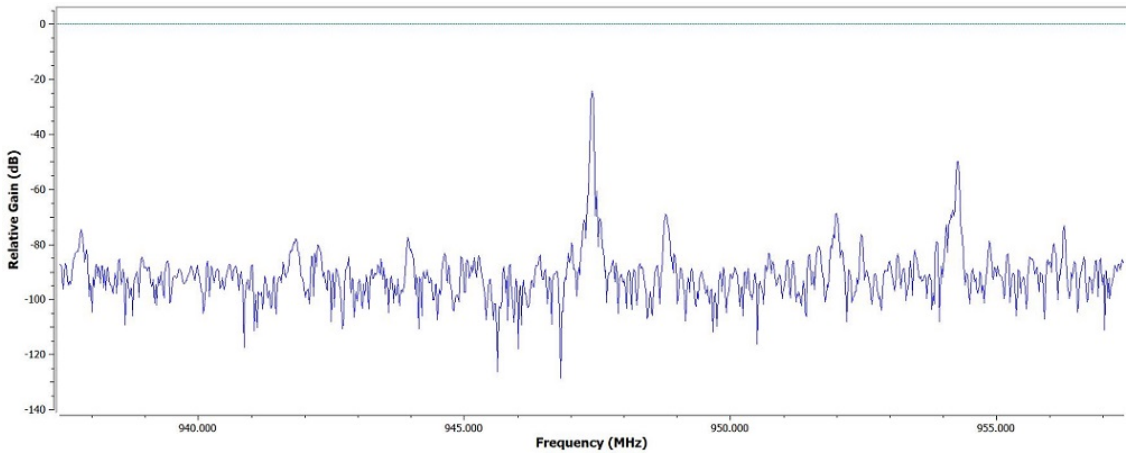


FIGURE 3.16: Sweep Jamming resulting spectrum at 949.2 MHz

3.4.4 Protocol-Aware Jamming

The implementation of this jamming technique is more specific since it is necessary to know some relevant parameters of the target signal protocol which are the modulation type, the data rate and the channel bandwidth. In cases where the FHSS method is used, it is important to have knowledge related to channel frequencies, hopping patterns and hopping rate. The application of this technique in other technologies, apart from GSM, has already been studied in [71] and [72], proving its efficiency even with low energy sources and also its low detection probability. In general, one of the main advantages pointed to the protocol-aware jamming technique is its low interference with other communication systems since it operates only on the band portion occupied by the target signal [70]. A spectrum scheme of the protocol-aware jamming is presented in figure 3.17.

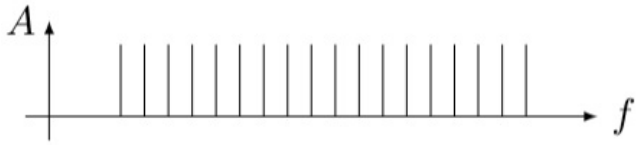


FIGURE 3.17: Protocol-Aware Jamming Scheme [70]

As mentioned in section 2.3.2.3, the GSM technology uses the GMSK modulation scheme. Therefore, the implementation of this jammer, represented in figure 3.18, uses the GMSK modulation as well.

There are two ways to build GMSK modulated signals: the most intuitive way is using a Gaussian filter to filter the modulating signal and then to apply a frequency modulation with a modulation index equal to 0.5. The other way it is to use a quadrature modulator often called an I-Q modulator. The GMSK Mod block follows the first approach described above.

With that being said, the Random Source block was used to create a binary random sequence, which means, a sequence of 0s and 1s bits. The GMSK Mod block receives the binary sequence created by the Random Source block and transforms them into NRZ (Non Return Zero) data, in other words a sequence of -1s and 1s. It then implements the Gaussian filter, generates a Gaussian response and then applies the FM modulation. Finally, the output generated by the GMSK Mod block, which is the complex modulated signal at baseband, will be transmitted by the BladeRF through the osmocom Sink block.

There is a relation between the sample rate, symbol rate and samples per symbol which can be expressed by the following formula:

$$Fs = sps \times F, \tag{3.3}$$

where sps is the number of samples per symbol, Fs is the resulting sample rate and F is the symbol rate. The symbol rate specified for the GSM standard is 270.833 KHz and the chosen number of samples per symbol was 8. Thus, based on the formula (3.3), the resulting sample rate with these conditions is 2.166664 MHz.

The Bandwidth-Time (BT), represented in the GMSK Mod block with the same nomenclature, is defined in the GSM technology with the value 0.3.

Same as the previous Sweep Jamming implementation, the frequencies values used to cover the NOS operator (between 943 MHz and 950.8 MHz) were set, separated by intervals of 0.2 MHz, in the QT GUI Chooser block. Once again, the generated GRC python file was modified according to the figure 3.14 in order to change automatically the frequency value of the osmocom Sink block, based on the values of the QT GUI Chooser block, in order to transmit the implemented signal across the desired frequency range.

The main configuration values used for the Protocol-Aware Jamming implementation are indicated in table 3.5.

Parameter	**Value**
Bandwidth	20 MHz
Sample Rate	2.166664 MHz
Frequency	943 MHz - 950.8 MHz
Center Frequency	947.4 MHz
Samples/Symbol	8
BT	0.3

Table 3.5: Configuration values used on the Protocol-Aware Jamming

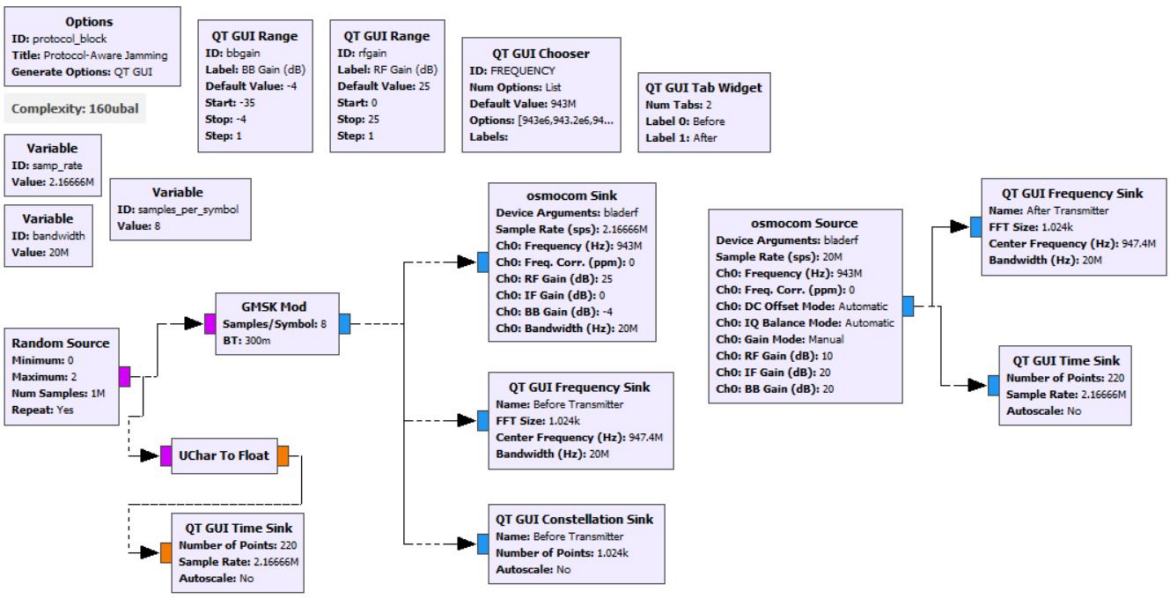


FIGURE 3.18: Protocol-Aware Jamming Flow graph

In order to see the binary sequence created on the Random Source block, represented in figure 3.19, the UChart To Float converter block was used on the QT GUI Time Sink block.

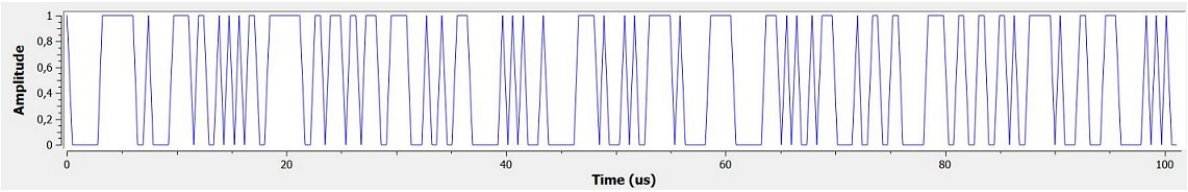


FIGURE 3.19: Binary Sequence created on the Random Source block

In order to see the GMSK modulated signal with AWGN noise received by the osmocom Source block, represented in figure 3.20, the QT GUI Time Sink block was used.

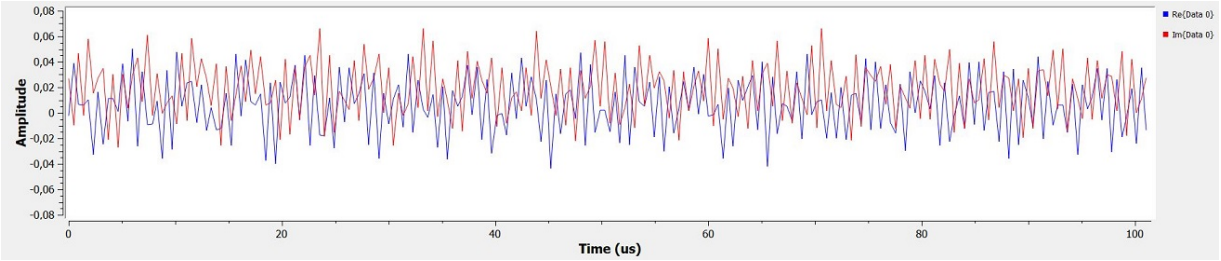


FIGURE 3.20: GMSK modulated signal on the osmocom Source

The GMSK Constellation generated by the QT GUI Constellation Sink block is represented in figure 3.21. The constellation has this circular shape because the GMSK uses CPM.

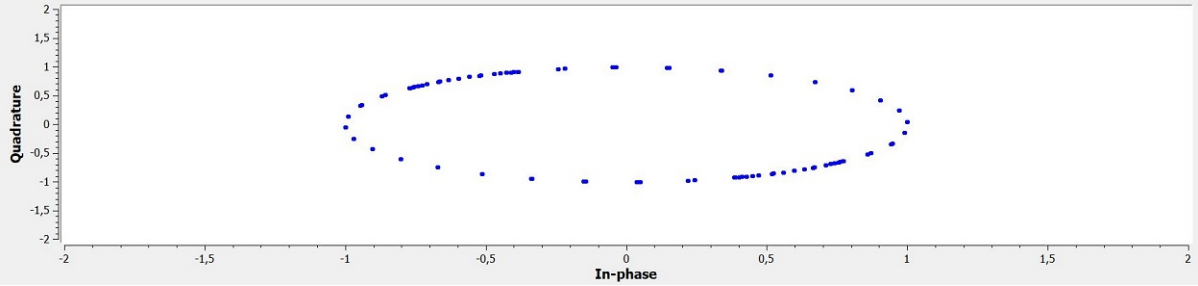


FIGURE 3.21: GMSK Constellation generated by the QT GUI Constellation Sink block

The resulting frequency spectrum received by the osmocom Source block at 949.2 MHz, in a certain period of time, is represented in the figure 3.22, having an average PSD of, approximately, -65 dBW/Hz.

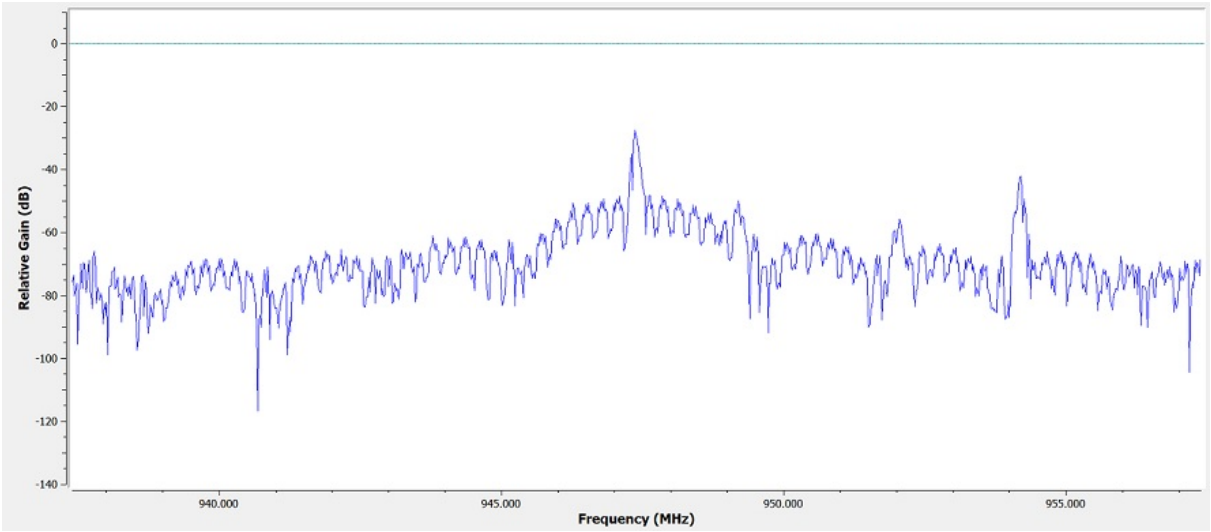


FIGURE 3.22: Protocol-Aware Jamming resulting spectrum at 949.2 MHz

Chapter 4

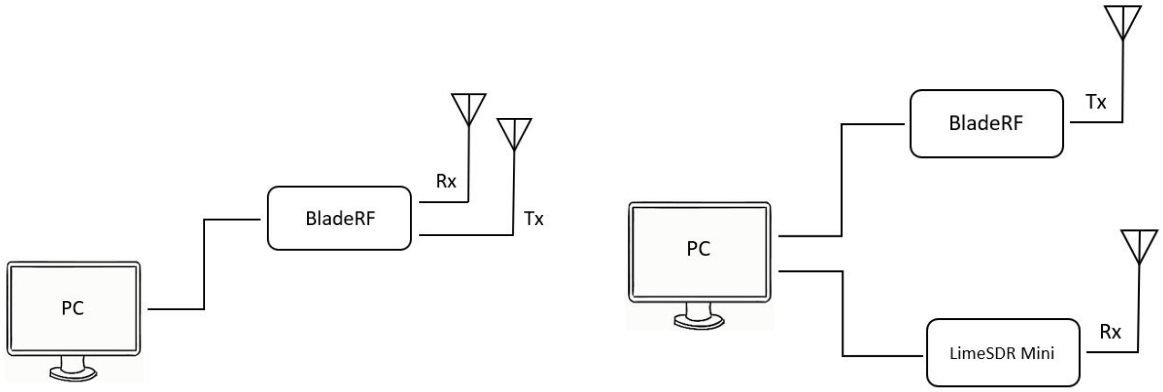
Experiments and Results

In this chapter the performance and behaviour of each jammer implemented on the previous chapter will be studied and analyzed, in terms of energy efficiency and maximum range reached, in order to choose the best jammer to interfere with a GSM signal.

4.1 Jammer Configuration

As already mentioned, a NOS smartphone Android was used as a GSM target, with the 2G mode activated only, working with GSM900. In order to monitor and analyze the signal strength values received by the smartphone, an Android app called "NetMonitor Cell Signal Logging" was used, explained in more detail in the section 3.2.

In order to visualize the signal received by the BladeRF when the transmission frequency is fixed, the osmocom Source block is used in each GRC scheme of every jamming technique implemented in chapter 3, having only the BladeRF as a SDR hardware, as presented in figure 4.1a. When the signal created performs the frequency hops across the defined bandwidth, it is not possible to see the spectrum through the GRC since the python file was modified in order to change the transmission frequency automatically. Therefore, the LimeSDR Mini was used as a receptor in those cases, as represented in figure 4.1b, in combination with the CubicSDR platform in order to observe the signal hops.



(A) Assembly Scheme with BladeRF only

(B) Assembly Scheme with BladeRF and LimeSDR Mini

FIGURE 4.1: Assembly Schemes

4.2 Evaluation Tests

Having the two TX maximum gain values of the BladeRF, which means, the BB gain (TXVGA1) at -4 dB and the RF gain (TXVGA2) at 25 dB, the average PSD values, already mentioned on each technique implemented on chapter 3, are gathered on table 4.1.

Jamming Technique	**Average PSD**
Barrage Jamming	-60 dBW/Hz
Tone Jamming	-85 dBW/Hz
Sweep Jamming	-90 dBW/Hz
Protocol-Aware Jamming	-65 dBW/Hz

TABLE 4.1: PSD values for each jamming technique implemented

Based on the previous table, it is possible to verify that the weakest signals are from the Tone Jamming and the Sweep Jamming, which makes sense since these two techniques are similar.

The Sweep Jamming was implemented with a sample rate bigger than the Tone Jamming, which could lead to a higher value of PSD, although this is not what happens because, opposite to the Tone Jamming, the Sweep Jamming operates across all the bandwidth, focusing all its power in each frequency hop made, reducing its power.

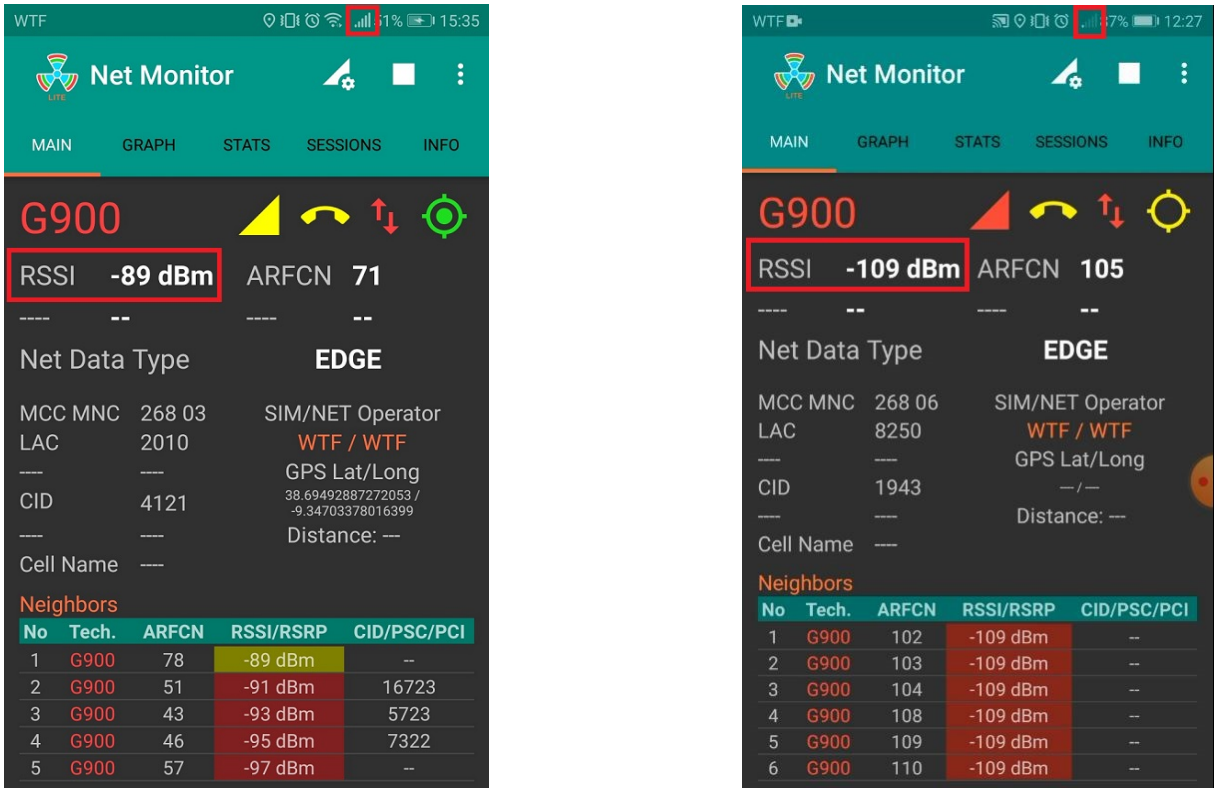
The Barrage Jamming and the Protocol-Aware Jamming are considered the jammers with higher PSD since the first one applies noise on the center channel, performing in all the studied bandwidth, not having the need of reproducing the frequency hops of the GSM standard. On the other hand, the Protocol-Aware Jamming used the lowest sample rate of all the jammers implemented, but also it is the only one capable of transmitting the most similar signal to the GSM signal.

One of the techniques that can be excluded automatically is the Tone Jamming. This jammer applies all its power into a single frequency, nevertheless the GSM technology uses the FHSS systems, which means that every transmitter and receiver use, for a period of time, a certain channel with a constant carrier frequency and then hop to another channel with a different frequency. Therefore, the Tone Jamming is not a viable technique for the GSM standard because it only transmits in a certain frequency, not being able to follow the channel variations made, along the bandwidth, by a FHSS system like GSM. This statement has been already proven by others studies such as [69].

Thereby, the remaining three jammers were tested, with the BladeRF maximum TX gains and with only the smartphone 2G mode on, in two environments:

- Environment 1: in a place with good coverage;
- Environment 2: In a place with bad coverage.

To have an idea of the signal strength levels received by the smartphone in each environment, with no jammer working, the figures 4.2a and 4.2b represent screenshots of the NetMonitor App with those values expressed by the RSSI indicator, in dBm.



(A) Environment 1 (B) Environment 2

FIGURE 4.2: Signal Strength Levels of each Environment

In each environment, the jammers where tested near the smartphone, and then with a distance of 3m and 6m, as represented in figure 4.3. For distances above 6m, the jammers were unable to block the signal from the base station.

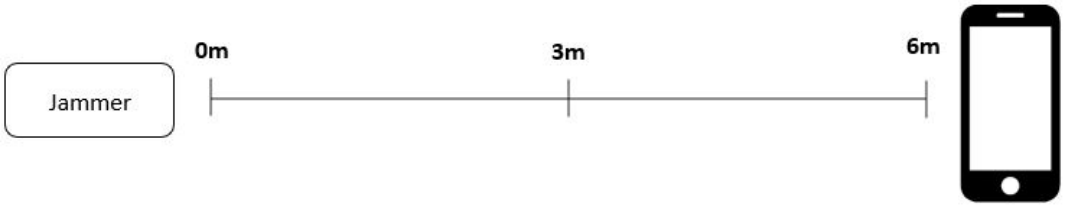


FIGURE 4.3: Distance tested between the jammer and the smartphone

The Barrage Jamming was capable of disrupting completely the mobile network on the first environment, only when near to the smartphone, while in the second environment it was capable at all distances.

The Sweep Jamming and the Protocol-Aware Jamming were able to only work in the second environment, blocking the mobile signal at all studied distances.

There is a common behaviour between all the jammers in the the second environment: they lost effectiveness as they moved away from the intended target.

When the mobile network is totally interrupted on the second environment, the smartphone reaches its minimum operating levels, and those values are indicated in the table 4.2.

	0m	**3m**	**6m**
Barrage Jamming	- 335 dBm	- 319 dBm	- 315 dBm
Sweep Jamming	- 341 dBm	- 337 dBm	- 317 dBm
Protocol-Aware Jamming	-337 dBm	- 327 dBm	- 321 dBm

TABLE 4.2: Signal Strength on the GSM receptor - Jammers tests

4.3 Results Analysis

Before analyzing the results, it is important to refer the reason why these tests were chosen. First of all, the first environment is usually the most common scenario on places with higher population density, providing a good coverage for the smartphone which means that it is possible to have the smartphone near a base station. As already mentioned, the only technique capable of completely disrupting the smartphone on the first environment was the Barrage Jamming, only when there was no range. Having these inconclusive results on this environment showed the liability of the BladeRF's low transmission power. In order to overcome this limitation, there were three possibilities:

- Increase BladeRF's transmission power through amplification;
- Use an antenna with a higher gain for transmission;
- Reduce the signal strength received by the smartphone from its base station.

Therefore, the amplification power methods, available on the BladeRF, were already being used by having the BladeRF TX gains, TXVGA1 and TXVGA2, with their maximum values, and there was no external amplification resource available for the BladeRF. Similarly, there was no available antenna with a higher transmission gain to use.

For the reasons already mentioned above, the third approach was chosen, and the second environment emerged.

Taking into account the table 4.2, an analysis can be made related to the efficiency of each jammer, by significantly reduce the signal strength received by the smartphone from its base station, based on the three studied distances:

- When the distance was 6m, the most efficient jamming technique was the Protocol-Aware Jamming;
- When there was no distance and a distance up to 3m, the most efficient jamming technique was the Sweep Jamming.

At this moment, the two jamming techniques that have shown a better performance are the Sweep Jamming and the Barrage Jamming. On one hand, the Barrage Jamming was the only one capable of working on the first environment, but considering the average PSD levels presented on the table 4.1, it was the jammer more costly in terms of energy. In contrast, the Sweep Jamming was the more energy-efficient jammer, showing the best performance on environment 2, based on table 4.2, on blocking the signal target decreasing it to its lowest levels.

In conclusion, considering the importance proposed on this dissertation of having a energy efficiency mechanism, it is possible to conclude that better reaches the objectives' goals is the Sweep Jamming.

Chapter 5

Conclusion and Future Work

The main goal of this dissertation was the development of a jammer capable of blocking the communication of a GSM signal, in order to contribute to the neutralization of UAVs in unauthorized areas. Through the use of SDR technology, this objective was successfully accomplished. The jammer which showed the best results in terms of energy-efficiency and range was the Sweep Jamming. This jammer generates a chirp signal, which is swept in time, across the entire studied bandwidth.

5.1 Main Conclusions

Between all the tested techniques, the one which achieved the best result was the Sweep Jamming, in terms of energy-efficiency, showing a maximum operation range of 6m. The SDR hardware showed some limitations on this specific scenario, regarding its transmission power which was low compared to the power levels used by GSM.

In chapter 1, a set of questions was raised in order to find answers for them through the development of this dissertation.

The first question was related to the existence of unintentional interference with neighbouring receivers while performing the jamming. The answer for this question is yes, it is possible to have unintentional interference with neighbouring receivers since all the devices within the action range of the jammer are affected. In order to minimize this behaviour, a directional antenna must be used, since with those, there is a higher concentration of radiated power in a certain direction of space.

One of the most important questions was about the jammer energy efficiency and its maximum range. Through the tests made and analyzed on chapter 4, it was possible to have a maximum operation range of 6m, where the target GSM receptor had its communication system completely blocked, with also a low power spent for this effect. This range value could be increased through the usage of an amplifier adapted to the transmission frequency combined with an higher gain antenna.

The third question concerns the system's response, which has to be reasonably quick to be considered an effective solution. The hardware used in this work showed some limitations due to the existing high power values of the GSM technology, highlighting even more the robustness of the 2G technology. Therefore, this study can contribute to the continuity of the development of a quick approach for the GSM jamming but it cannot be considered yet a final effective solution by itself.

Finally, the ending question pretends to know if the solution found is capable of combating the imminent risks of drones at a social level. Taking into account this main problem, the jammer considered as the most effective, will be able to contribute to the drones threat on airspace when allied to mechanisms of signal amplification and specialized systems already prepared for other technologies in order to allow the mitigation of UAVs on unauthorized areas, such as the prototype used on [56].

5.2 Challenges and Future Work

On this dissertation, some challenges were faced with the software used due to the fact that, the SDR technology is a relatively new technology and an open-source platform, which means there is not enough official documentation and most of the information is scattered around the internet, since the development of this technology is made by the contribution of many users and enthusiasts on the subject, making the learning process slower.

Another difficulty found was the limitation inherent to the hardware that prevented of obtaining results on environments with higher coverage, which are the most usual scenarios on highly population areas. This limitation could be overcomed by using an amplification mechanism adapted to the transmission frequency combined with a more directive antenna.

With all these challenges ahead, a deep research for the creation of solutions was necessary, having dedicated a lot of effort in order to achieve satisfactory results. Thereby, this dissertation was a challenge both personally and academically.

As future work, the jammer developed on this dissertation could be improved by first, applying an amplification mechanism combined with a more directive antenna, as explain previously, in order to be used in a GSM environment with a higher coverage, increasing the jammer signal strength to a more similar level of a GSM signal and, consequently its range.

Then, after the jammer is improved in terms of power, it is ready to be explored its use to jam any unmanned vehicles, either in ground or air space.

In the case of following the ground space path, there is a way for this jammer to contribute directly on the specific mitigation of the UAVs on unauthorized areas, which is by incorporating it on a specialized prototype capable of safeguarding the intrusion of UAVs in restricted areas, analyzed and used on [56], which is already prepared for the jamming and spoofing of other technologies such as the GPS.

Considering the prototype mentioned above and using the SDR technology as well, there is another interesting possibility of improving it, which is by incorporating jammers of other mobile cellular networks technologies generations such as 2.5G, 3G or even 4G. This could be a good form of following the new technologies integrated on drones.

Finally, this dissertation came to reaffirm the robustness of the mobile cellular systems, proving that the investment and study are relevant in these technologies in order to find new vulnerabilities and, consequently develop and implement mitigation systems to eliminate them.

Bibliography

[1] Technopedia, *Unmanned Aircraft Systems: UAV Design, Development and Deployment*. Chippenham, UK: Wiley, A John Wiley Sons, Ltd, Publication, 2010.

[2] M. Scherer, *Development and Implementation of an Unmanned Aerial Vehicle with Stereoscopic Cameras Controlled via a Virtual Reality Head-Mounted Display*. Master's thesis, Frankfurt University of Applied Sciences, 2015.

[3] A. Tahira, J. Böling, M.-H. Haghbayan, H. T. Toivonen, and J. Plosila, "Swarms of unmanned aerial vehicles - a survey," *Journal of Industrial Information Integration*, 2019.

[4] "Fixed Wing UAV." `http://www.your-flying-camera-drone.com/fixedwingdrone.html`. [Online] Accessed: November 2019.

[5] "Multi-rotor UAV." `https://static.fnac-static.com/multimedia/Images/PT/NR/73/02/0f/983667/1540-1/tsp20161111142256/Drone-DJI-Mavic-Pro-4K.jpg`. [Online] Accessed: November 2019.

[6] G. V. Hristov, P. Z. Zahariev, and I. H. Beloev, "A review of the characteristics of modern unmanned aerial vehicles," *Acta Technologica Agriculturae*, vol. 19, no. 2, pp. 33–38, 2016.

[7] İsmet Çuhadar and M. Dursun, "Unmanned air vehicle system's data links," *Journal of Automation and Control Engineering*, vol. 4, no. 3, 2016.

[8] J. A. Kakar, *UAV Communications: Spectral Requirements, MAV and SUAV Channel Modeling, OFDM Waveform Parameters, Performance and Spectrum Management*. Master's thesis, Faculty of the Virginia Polytechnic Institute and State University, 2015.

[9] A. S. L. Raimundo, *Autonomous Obstacle Collision Avoidance System for UAVs in Rescue Operations*. Master's thesis, ISCTE-IUL, 2016.

[10] "Mission Planner App." https://conservationdrones.org/mission-planne/. [Online] Accessed: November 2019.

[11] A. Koubâa, A. Allouch, M. Alajlan, Y. Javed, A. Belghith, and M. Khalgui, "Micro air vehicle link (mavlink) in a nutshell: A survey," *CISTER - Research Centre in Real-time Embedded Computing Systems*, vol. 4, 2019.

[12] "MAVLink protocol." https://erlerobotics.gitbooks.io/erle-robotics-erle-brain-a-linux-brain-for-drones/en/mavlink/mavlink.html. [Online] Accessed: November 2019.

[13] J. J. O. Pires, *Sistemas e Redes de Telecomunicações*. 2006.

[14] P. Queluz and F. Pereira, "Introdução às comunicações móveis." https://fenix.tecnico.ulisboa.pt/downloadFile/3779571261375/ST_Moveis_06_07.pdf. [Online] Accessed: December 2019.

[15] J. H. Schiller, *Mobile Communications*. Harlow, UK: Pearson Education Limited, 2003.

[16] M. Tolstrup, *Indoor Radio Planning: A Practical Guide for GSM, DCS, UMTS and HSPA*. Chippenham, UK: Wiley, A John Wiley Sons, Ltd, Publication, 2008.

[17] S. C. Horng and S. S. Lin, "7-cell reuse cluster system." https://www.researchgate.net/figure/cell-reuse-cluster-system_fig1_277579389, 2015. [Online] Accessed: January 2020.

[18] L. M. Correia, "Sistemas de Comunicações Móveis." https://fenix.tecnico.ulisboa.pt/downloadFile/3779571243381/01_Introduca.pdf. [Online] Accessed: December 2019.

[19] N. dos Santos, "5g: afinal, quando será lançada esta nova geração de rede móvel?." https://www.comparaja.pt/blog/5g-quando-sera-lancada. [Online] Accessed: December 2019.

[20] T. I. E. Consortium, "Global system for mobile communication (gsm)," pp. 1–19, 1997.

[21] N. dos Santos, "Global system for mobile communications (gsm)." https://www.techopedia.com/definition/5062/global-system-for-mobile-communications-gsm. [Online] Accessed: December 2019.

[22] I. ul Haq, Z. U. Rahman, S. Ali, and E. M. Faisal, "Gsm technology: Architecture, security and future challenges," *International Journal of Science Engineering and Advance Technology*, vol. 5, no. 1, pp. 1–6, 2017.

[23] G. T. Insight, "Gsm (global system for mobile communications)." http://www.mobilecomms-technology.com/projects/gsm/. [Online] Accessed: December 2019.

[24] A. de Sousa Silvério, *Propagation model for cellular mobile networks used in UAVs communications environments*. Master's thesis, ISCTE-IUL, 2017.

[25] J. Scourias, "Overview of the global system for mobile communications," tech. rep., 1995.

[26] electronicsnotes, "Gsm network architecture." https://www.electronics-notes.com/articles/connectivity/2g-gsm/network-architecture.php. [Online] Accessed: November 2020.

[27] L. Frenzel, *Electronics Explained - The New Systems Approach to Learning Electronics*. Oxford, UK: Elsevier Inc, 2010.

[28] M. Sauter, *From GSM to LTE: An Introducion to Mobile Networks and Mobile Broadband*. Chippenham, UK: Wiley, A John Wiley Sons, Ltd, Publication, 2011.

[29] "Electronics notes." https://www.electronics-notes.com/articles/radio/modulation/what-is-gmsk-gaussian-minimum-shift-keying.php. [Online] Accessed: March 2020.

[30] M. Barnela, "Digital modulation schemes employed in wireless communication: A literature review," *International Journal of Wired and Wireless Communications*, vol. 2, no. 2, 2014.

[31] T. Turletti, "Gmsk in a nutshell," *Telemedia Networks and Systems Group*, 1996.

[32] S.Neeraja and G. Rao, "A comparative study on handoff algorithms for gsm and cdma cellular networks," *International Journal of Electrical and Computer Engineering*, vol. 7, no. 3, pp. 1219—-1227, 2017.

[33] S.A.Mawjoud and H.A.Al-Tayyar, "Investigation of handoff algorithms for gsm mobile cellular networks," *Al-Rafidain Engineering Journal*, vol. 18, no. 4, 2010.

[34] N. Ekiz, T. Salih, S. Küçüköner, and K. Fidanboylu, "An overview of handoff techniques in cellular networks," *World Academy of Science, Engineering and Technology*, vol. 6, 2007.

[35] A. Graham, *Communications, Radar and Electronic Warfare*. West Sussex, UK: Wiley, A John Wiley Sons, Ltd, Publication, 2011.

[36] P.Naresh, P. R. Babu, and K.Satyaswathi, "Mobile phone signal jammer for gsm, cdma with pre-scheduled time duration using arm7," *International Journal of Science, Engineering and Technology Research (IJSETR)*, vol. 2, no. 9, 2013.

[37] F. V. Correia, *Jammers para FSK e BPSK Engenharia Electrotécnica e de Computadores*. Master's thesis, Instituto Superior Técnico - IST, 2014.

[38] K. Grover, A. Lim, and Q. Yang, "Jamming and anti-jamming techniques in wireless networks: A survey," *International Journal of Ad Hoc and Ubiquitous Computing*, 2014.

[39] "How cell phone jammers work." `https://electronics.howstuffworks.com/cell-phone-jammer3.htm`. [Online] Accessed: April 2020.

[40] T. F. Collins, R. Getz, D. Pu, and A. M. Wyglinski, *Software-Dened Radio for Engineers*. Artech House Publishers, 2018.

[41] J. R. Machado-Fernández, "Software defined radio: Basic principles and applications," *Revista Facultad de Ingeniería (Fac. Ing.)*, vol. 24, no. 38, pp. 79–96, 2015.

[42] E. Grayver, *Implementing Software Dened Radio*. Springer, 2013.

[43] banggood, "Hackrf one 1mhz a 6ghz usb software de fonte aberta plataforma de rádio placa de desenvolvimento sdr rtl recepção de sinais." https://www.banggood.com/pt/HackRF-One-1MHz-to-6GHz-USB-Open-Source-Software-Radio-Platform-SDR-RTL-Development-Board-Reception-of-Signals-p-1545357.html?gpla=1&gmcCountry=PT&currency=EUR&createTmp=1&utm_source=googleshopping&utm_medium=cpc_bgcs&utm_content=lijing&utm_campaign=ssc-pt-1-all-0911-re0323&ad_id=381916462714&gclid=EAIaIQobChMIuu7A7cG56QIVjrLVCh02UAewEAQYASABEgKOhfD_BwE&cur_warehouse=UK. [Online] Accessed: May 2020.

[44] R. Baguley, "Bladerf 2.0 micro is smaller, more powerful." https://hackaday.com/2018/08/30/bladerf-2-0-micro-is-smaller-more-powerful/, 2018. [Online] Accessed: May 2020.

[45] M. Ossmann and D. Spill, "Hackrf one." https://github.com/mossmann/hackrf/wiki/HackRF-One, 2017. [Online] Accessed: May 2020.

[46] Kickstarter, "bladerf - usb 3.0 software defined radio." https://www.kickstarter.com/projects/1085541682/bladerf-usb-30-software-defined-radio, 2015. [Online] Accessed: May 2020.

[47] nuand, "bladerf usb 3.0 software defined radio," tech. rep.

[48] G. R. project, "About gnu radio." https://www.gnuradio.org/about/, 2020. [Online] Accessed: May 2020.

[49] S. Sriram, G. Srivatsa, G. R, and S. K. P, "Plug-ins for gnu radio companion," *International Journal of Computer Applications*, vol. 52, no. 16, 2012.

[50] M. Gummineni and T. R. Polipalli, "Cognitive radio-modulation and demodulation," *Recent Trends in Communication Networks*, 2019.

[51] P.Naresh, P. Babu, and K.Satyaswathi, "Mobile phone signal jammer for gsm, cdma with pre-scheduled time duration using arm7," *International Journal of Science, Engineering and Technology Research (IJSETR)*, vol. 2, no. 9, pp. 1781—-1784, 2013.

[52] N.K.Mishra, "Development of gsm — 900 mobile jammer: An approach to overcome existing limitation of jammer," *Fifth International Conference on Wireless Communication and Sensor Networks (WCSN)*, pp. 1—-4, 2009.

[53] J. Farlik, M. Kratky, and J. Casar, "Detectability and jamming of small uavs by commercially available low-cost means," *International Conference on Communications (COMM)*, pp. 327–330, 2016.

[54] G.-M. Nam, G.-H. Lee, J.-S. Lee, H.-B. Kil, and E.-R. Jeong, "Reactive jamming for commercial drones," *International Journal of Engineering Technology*, pp. 100–103, 2018.

[55] J. A. D. García, "Software defined radio for wi-fi jamming." `https://www.researchgate.net/publication/301850218_Software_Defined_Radio_for_Wi-Fi_Jamming`, 2016. [Online] Accessed: May 2020.

[56] R. B. Ferreira, *Técnicas de Jamming GPS para UAVs Não Autorizados*. Master's thesis, ISCTE-IUL, 2018.

[57] RoboSavvy, "bladerf x40." `https://robosavvy.com/store/bladerf-x40.html`. [Online] Accessed: June 2020.

[58] L. microsystems, "Lms6002d - multi-band multi-standard transceiver with integrated dual dacs and adcs," tech. rep., 2012.

[59] R. Tucker, "Gnuradio osmosdr device string options." `https://github.com/Nuand/bladeRF/wiki/Gnuradio-OsmoSDR-device-string-options`. [Online] Accessed: July 2020.

[60] L. Microsystems, "Limesdr mini." `https://limemicro.com/products/boards/limesdr-mini/`. [Online] Accessed: August 2020.

[61] Myriad-RF, "Limesdr-mini." `https://wiki.myriadrf.org/LimeSDR-Mini`. [Online] Accessed: August 2020.

[62] M. Claussen, "Review: Lime sdr mini." `https://www.elektormagazine.com/news/review-lime-sdr-mini`. [Online] Accessed: August 2020.

[63] Seeed, "Omnidirectional 4g/lte sma antenna." https://www.seeedstudio.com/RF-4GHz-SMA-Antenna-up-to-5dBi-p-2426.html. [Online] Accessed: July 2020.

[64] Taoglas, "Apex tg.30 4g/3g/2g terminal antenna, sma (m) ra." https://www.taoglas.com/product/apex-tg-30-2g3g4g-terminal-antenna-ra-sma-m/. [Online] Accessed: July 2020.

[65] SolidSignal, "Taoglas apex 46 lte ultra wideband antenna (tg-30-8112)." https://www.solidsignal.com/pview.asp?mc=&p=TG-30-8112&d=Taoglas-Apex-46-LTE-Ultra-Wideband-Antenna-(TG308112)&c=&sku=729198314835. [Online] Accessed: July 2020.

[66] CubicSDR, "Cubicsdr - introduction." https://cubicsdr.readthedocs.io/en/latest/introduction.html#what-is-cubicsdr. [Online] Accessed: August 2020.

[67] CubicSDR, "Cubicsdr - cross-platform and open-source software-defined radio application." https://cubicsdr.com/. [Online] Accessed: August 2020.

[68] A. A. N. de Comunicações, "Serviço de comunicações eletrónicas terrestres - frequências." https://www.anacom.pt/render.jsp?categoryId=382989. [Online] Accessed: July 2020.

[69] R. Poisel, *Modern Communications Jamming Principles and Techniques*. Norwood, Massachusetts, EUA: Artech House Publishers, 2011.

[70] K. Pärlin, *Jamming of Spread Spectrum Communications used in UAV Remote Control Systems*. Master's thesis, Tallinn University of Technology, 2017.

[71] A. Hussain, N. A. Saqib, U. Qamar, and M. Zia, "Protocol-aware radio frequency jamming in wi-fi and commercial wireless networks," *Journal of Communications and Networks*, vol. 16, no. 4, pp. 397–406, 2014.

[72] D. J. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11b and other networks," *MILCOM'06: Proceedings of the 2006 IEEE conference on Military communications*, pp. 1075–1081, 2006.