Departamento de Ciências e Tecnologias da Informação

Técnicas de *Jamming* GPS para UAVs Não Autorizados

Renato Branco Ferreira

Dissertação submetida como requisito parcial para obtenção do grau de

Mestre em Engenharia de Telecomunicações e Informática

Orientador:
Doutor Nuno Manuel Branco Souto, Professor Auxiliar,
ISCTE-IUL

Coorientador:
Doutor Pedro Joaquim Amaro Sebastião, Professor Auxiliar,
ISCTE-IUL

Setembro, 2018

Agradecimentos

Na realização da presente dissertação, contei com o apoio direto ou indireto de várias pessoas e instituições às quais estou profundamente grato. Quero deixar expresso os meus agradecimentos:

Ao orientador e coorientador desta dissertação o Professor Doutor Nuno Manuel Branco Souto e o Professor Doutor Pedro Joaquim Amaro Sebastião, respetivamente, pela orientação prestada, esforço, disponibilidade e apoio que sempre demonstraram na investigação e desenvolvimento da dissertação.

Ao Professor Doutor Francisco António Bucho Cercas, por ter disponibilizado o espaço para o desenvolvimento da dissertação, testes em laboratório e algum equipamento para a realização da mesma.

Não poderia deixar de agradecer à minha família por todo o apoio económico, pela força e pelo carinho que sempre me prestaram ao longo de toda a minha vida académica.

Um agradecimento especial para uma pessoa muito importante, a minha namorada, que sempre me apoiou em todos os momentos de mestrado e nas diversas fases desta dissertação. Obrigado por todo o tempo despendido na ajuda da dissertação, com o intuito de sempre melhorar.

A todos os amigos e colegas que auxiliaram na elaboração do presente estudo, pela paciência, atenção e força que prestaram em momentos menos fáceis.

Por fim, queria agradecer ao ISCTE-IUL e ao Instituto de Telecomunicações pelo apoio na investigação e equipamento disponibilizado.

Resumo

Nos últimos tempos, têm sido muitos os relatos de incidentes com drones, especialmente entre estas aeronaves e aviões nas imediações de aeroportos ou aeródromos.

Uma vez que os drones utilizam geralmente sinais de radionavegação para se localizarem, o objetivo desta dissertação passa por implementar técnicas eficazes para *jamming* de sinais GPS. Com o recurso a plataformas SDR (*Software Defined Radio*) pretende-se desenvolver um sinal *jammer* capaz de causar interferência no sistema de navegação GPS, diferente dos já existentes, melhorando a eficiência em termos energéticos, com baixa complexidade na implementação, e sendo ainda reconfigurável de forma a que permita facilmente a adição de novas funcionalidades ou outras frequências. Para o desenvolvimento deste projeto foi utilizado o programa GNURadio e uma placa programável, BladeRF x40 da Nuand.

Ao desenvolver este tema pretendia-se estudar e avaliar num cenário real diferentes técnicas de interferência de forma a selecionar-se a melhor tendo em consideração a eficiência espectral, energética e complexidade. No final, pretendia-se integrar o *jammer* desenvolvido num protótipo de um sistema capaz de bloquear as comunicações entre um drone e a estação/módulo de controlo terrestre neutralizando também a capacidade de operação autónoma do veículo.

O *jammer* eleito com melhor desempenho foi o *Protocol-Aware Jamming*, que usa uma arquitetura semelhante à utilizada pelo emissor do sinal GPS a interferir. Desta forma, o sinal interferente "mistura-se" de forma mais eficaz com o sinal alvo, uma vez que apresentam características semelhantes permitindo destruir a informação deste ou então tornar a sua receção virtualmente impossível de ser realizada no recetor.

Palavras-Chave: GPS*; Jamming*; Radionavegação; SDR; Veículos Aéreos Não Tripulados.

Abstract

Lately, several incidents between drones and planes have been reported in airports and airfields.

Since these drones regularly use radio navigation signals to locate themselves, the purpose of this project is to implement effective techniques for GNSS signals for jamming. Using an SDR platforms (Software Defined Radio) we aim to develop a jammer signal able to interfere with the GPS navigation system, something different of what exists already, creating a new way of efficiency in terms of energy, with low complexity and possibilities to expand, so it can have new features and new frequencies. For this project we will use the GNURadio and a programmable BladeRF x40 platform from Nuand.

Throughout this project, I intend to study and evaluate interference techniques in a real-life scenario and to select the best one, considering the spectral efficiency, energetic and complexity. Our aim is to create a prototype of a device capable of stopping the communications between a drone and communication satellite handy by an operator, and also neutralizing the capacity of autonomous operation of the vehicle.

The best performance jammer chosen was the Protocol-Aware Jamming wich uses a similar architectural to the one used by the GPS signal that we want to interfere. Because of that the interferer signal combine with the most efficient way with the target signal, since they have similar characteristics that allows to destroy his information or to became virtually impossible his reception by the receiver.

Keywords: GPS; Jamming; Radionavigation; SDR; Unmanned Aerial Vehicles.

Conteúdo

Lista de Tabelas

Lista de Figuras

Lista de Siglas

A	Ampere
ADC	*Analog to Digital Converter*
ADF	*Automatic Direction Finder*
AFCS	*Autonomous Flight Control System*
AM	*Amplitude Modulation*
AS	*Anti Spoofing*
ATSC	*Advanced Television System Committee*
AWGN	*Additive White Gaussian Noise*
BB	*Base Band*
BBC	*British Broadcasting Corporation*
BDS	*BeiDou Navigation Satellite System*
BPSK	*Binary Phase-Shift Keying*
C/A	*Coarse Aquisition or Clear Access*
CDMA	*Code Division Multiple Access*
CLP	Controladores Lógicos Programáveis
CW	*Continuous Wave*
D	*Navigation Message*
dB	Decibel
DC	*Direct Current*
DME	*Distance Measuring Equipment*
DoD	*Department of Defense*
DSP	*Digital Signal Processing*
ESA	*European Space Agency*
EUA	Estados Unidos da América
FCC	*Federal Communications Commission*
FFT	*Fast Fourier Transform*
FIR	*Finite Impulse Response*
FM	*Frequency Modulation*
GCS	*Ground Control Station*

GLONASS	*Global'naya Navigatsionnay Sputnikovaya Sistema*
GND	*Ground*
GNSS	*Global Navigation Satellite Systems*
GPIAA	Gabinete de Prevenção e Investigação de Acidentes com Aeronaves
GPIO	*General Purpose Input/Output*
GPL	*General Public License*
GPS	*Global Positioning System*
GSM	*Global System for Mobile*
ICD	*Interface Control Document*
IEEE	*Institute of Electrical and Electronics Engineers*
IMES	*Indoor Messaging System*
IMU	*Inertial Measurement Unit*
ISCTE	Instituto Superior de Ciências do Trabalho e da Empresa
LED	*Light Emitting Diode*
LNA	*Low Noise Amplifier*
LTE	*Long-Term Evolution*
MAC	*Medium Access Control*
NRZ	*Non-Return-to-Zero*
P	*Precise or Protected*
PA	*Power Amplifier*
PN	*Pseudo Random*
PPS	*Precise Positioning Service*
PRN	*Pseudo-Randon-Noise*
PSK	*Phase-Shift Keying*
QZSS	*Quasi-Zenith Satellite System*
RF	Radiofrequência
RSSI	*Received Signal Strength Indication*
RTL	*Register Transfer Level*
RX	*Reception*
SA	*Selective Availability*
SBAS	*Satellite-Based Augmentation System*
SDR	*Software Defined Radio*

SNR	*Signal-to-Noise Ratio*
SPS	*Standard Positioning Service*
SSB	*Single Side Band*
TX	*Transmission*
UE	União Europeia
UHF	*Ultra High Frequency*
USB	*Universal Serial Bus*
UT	*Universal Time*
UTC	*Universal Time Coordinated*
V	Volts
VANT	Veículo Aéreo Não Tripulado
VCO	*Voltage Controlled Oscillator*
VGA	*Variable Gain Amplifier*
VHF	*Very High Frequency*
VOR	*VHF Omnidireccional Range*
W	Watts
WGS	*World Geodetic System*
Wi-Fi	*Wireless Fidelity*
WPMC	*Wireless Personal Multimedia Communications*

Capítulo 1

1. Introdução

1.1 Motivação e Enquadramento

Nos últimos tempos, vários têm sido os relatos de incidentes com drones, especialmente entre estas aeronaves e aviões nas imediações de aeroportos ou aeródromos. Designa-se por drone todo e qualquer tipo de aeronave não tripulada, controlada remotamente ou automaticamente.

De acordo com o Gabinete de Prevenção e Investigação de Acidentes com Aeronaves (GPIAA), em Portugal no decorrer de 2016, foram registados 31 incidentes causados por drones em aeroportos [1]. O incidente mais grave registou-se no Aeroporto Humberto Delgado, em Lisboa a 11 de Dezembro de 2016, quando um drone levou ao cancelamento temporário da descolagem de um avião tendo condicionado também, durante cerca de meia hora, a operação de uma das pistas do aeroporto.

Os acidentes registados já levaram a que o GPIAA realizasse um estudo de segurança com o objetivo de caracterizar um historial de acidentes deste tipo em Portugal e verificar a eficácia do regulamento atual.

Embora exista legislação, muitos pilotos optam por, irresponsavelmente, não cumpri-la, gerando diversos tipos de incidentes e prejudicando a imagem e o trabalho daqueles que diariamente respeitam as regras e fazem dos drones a sua atividade profissional. Não é só em Portugal que estes incidentes têm ocorrido. Este problema tem sido bastante comum noutros estados-membros da União Europeia. De acordo com a BBC (*British Broadcasting Corporation*), a polícia holandesa treinou algumas aves de rapina, como águias, para que estas sejam capazes de perseguir e caçar os aparelhos não tripulados sempre que for necessário [2]. Porém, há grandes hipóteses destes animais ferirem-se com as hélices de carbono do aparelho, por isso, a polícia está a avaliar a necessidade de implementação de alguma proteção adicional. Por sua vez, na Rússia foi apresentada uma nova arma não-destrutiva capaz de resolver o problema em questão. Rex-1 foi a solução apresentada, como emissor de um sinal *jammer* face ao sinal GNSS. A Rex-1 além de cortar a ligação entre o aparelho e o seu controlador, envia sinais para forçar a aterragem, impossibilitando também o sinal GSM (*Global System for Mobile Communications*) e de Wi-Fi na zona, para não permitir nova ligação [3].

Há uma lacuna na atenuação deste problema em Portugal e no Mundo. Esta é a razão pela qual existe uma motivação na procura de uma solução por forma a ajudar a sociedade, atendendo ao facto de poder existir risco de vidas humanas, já para não falar de outros problemas como a invasão de privacidade e a falta de controlo aéreo ou terrestre destes dispositivos.

Jammer é um dispositivo que gera um campo eletromagnético capaz de interferir com a receção de sinais radioelétricos, impedindo, assim, o normal funcionamento do dispositivo (e.g. telemóvel, aparelhos de GPS, radares). Em relação aos drones, estes necessitam de *links* rádio para o envio de telemetria para a estação de controlo, para receção de comandos de voo e frequentemente para transmissão de vídeo. Estes *links* são implementados recorrendo geralmente a rádios dedicados que funcionam em frequências reservadas, ou nas bandas dos 2,4 GHz e 5,8 GHz, ou recorrendo a sistemas como Wi-Fi e redes celulares. Utilizam também sinais de radionavegação por satélite para se localizarem em tempo real. Existem diversos sistemas de navegação e posicionamento por satélite a serem desenvolvidos por diferentes países. O GPS (*Global Positioning System*) foi criado pelos Estados Unidos e foi o primeiro a existir e a ser utilizado, porém não é o único sistema, existe ainda o GALILEO (União Europeia) e o GLONASS (Rússia). Por outro lado existem sistemas que permitem obter localização mas em vez da utilização de satélites, são utilizadas bases terrestres no globo. Alguns dos sistemas que permitem obter uma posição espacial são o ADF (*Automatic Direction Finder*), VOR (*VHF Omnidireccional Range*) e o DME (*Distance Measuring Equipment*). Outro sistema possível de posicionamento é o sistema de navegação inercial, o drone contém um giroscópio e acelerómetro integrado, para determinar a aceleração bem como a direção.

Algumas soluções têm vindo a surgir [4] [5], sendo as mais promissoras as que atuam ao nível da interrupção da ligação que estabelece o controlo e também do sistema de navegação de um UAV [6] [7], uma vez que este tipo de soluções implica o acionamento do modo de segurança dos UAVs, repercutindo-se no pairar do UAV, ou mesmo no aterrar no local onde o mecanismo é acionado. Essas soluções ainda têm várias limitações em relação ao tamanho e à distância máxima sob a qual os veículos podem ser detetados e seguidos, a complexidade/custo do equipamento e as ligações sem fios que podem ser interrompidas.

Com este projeto pretende-se superar as limitações existentes, através do estudo, desenvolvimento e implementação de técnicas efetivas de deteção, localização e neutralização segura, que podem cobrir uma vasta gama de UAVs e integrar estas técnicas num protótipo de sistema.

1.2 Objetivos

Ao desenvolver este tema pretende-se estudar e avaliar técnicas de interferência de sinais de radionavegação recorrendo a métodos que possam focar a interferência em alvos pretendidos e evitar interferências involuntárias nos recetores vizinhos. O projeto é composto por diversas fases: estudar e avaliar diferentes técnicas de interferência bem como métodos de formação de feixes através de plataformas de Rádio Definido por Software (SDR); Implementar e simular o *design* selecionado usando o GNU Radio; Implementar o *jammer* usando uma plataforma de *hardware* SDR; realizar testes experimentais e avaliar os resultados.

O Sistema de Posicionamento Global (GPS) é atualmente o Sistema de Navegação Global por Satélite (GNSS) mais usado e, por este motivo, o trabalho desenvolvido foca-se neste sistema.

O método de investigação baseia-se na análise do comportamento do equipamento de teste em relação à potência recebida no recetor de sinal de GPS. O GPS é um sinal fraco que pode ser facilmente interrompido a partir de um emissor interferente próximo do recetor, sendo esta interferência possível de ser gerada a partir de um equipamento SDR. Este mesmo objetivo deve ser conseguido com o menor recurso energético possível para alcançar a melhor razão de eficiência energética, sem que comprometa sistemas vizinhos. Para isso são criados e testados vários sinais *jammer* recorrendo a técnicas distintas para o mesmo fim, a interferência do sinal de GPS.

Pretende-se que o *jammer* desenvolvido seja diferente dos já existentes, melhorando a eficiência em termos energéticos, necessitando de baixa complexidade na implementação, reconfigurabilidade/ expansibilidade que permite facilmente acrescentar novas funcionalidades ou outras frequência alterando apenas o código carregado para o SDR.

No final, o que se pretende atingir com este trabalho é a integração do *jammer* num modelo protótipo de um sistema capaz de neutralizar a operação não autorizada de um drone.

1.3 Questões de Investigação

Para alcançar os objetivos do tema a desenvolver, existem várias questões que devem ser respondidas no fim do trabalho realizado.

- Ao realizar o *jammer* para as comunicações do drone, existem interferências involuntárias nos recetores vizinhos? Se sim, até que ponto se pode minimizá-las?

- Qual o alcance máximo que o *jammer* consegue interferir, tendo em conta a eficiência energética?

- A resposta do sistema é suficientemente rápida para se poder ter uma solução eficiente?

- Esta solução é capaz de resolver as ameaças dos drones para a sociedade?

1.4 Estrutura e Organização da Dissertação

Esta dissertação está segmentada por 6 capítulos e 2 apêndices. O 1º capítulo um capítulo introdutório que aborda questões relacionadas com a motivação, enquadramento e objetivos no âmbito do projeto. O 2º capítulo, cujo título é Sistemas de Radionavegação para UAVS, explica o funcionamento do sistema GPS e aborda o tema de interferência por radio frequência. Neste capítulo são apresentadas ainda cinco técnicas de interferências, que vão ser exploradas e comparadas nesta dissertação, abordando-as de uma forma teórica. No capítulo 3 é descrito o *software* e *hardware* utilizado e desenvolvido. As técnicas de *jamming* abordadas teoricamente no capítulo 2 são exploradas de forma a serem implementadas na prática. O capítulo 4 consiste na avaliação de resultados. São detalhados a forma como foram feitos os testes práticos e comparadas as diversas técnicas de *jamming*. O 5º capítulo faz referência às principais conclusões e finaliza com um possível trabalho futuro. Por fim o 6º capítulo descreve o desenvolvimento do protótipo final, o dimensionamento de uma antena Yagi e da bateria a implementar para suportar com todo o sistema. Relativamente aos apêndices, estão divididos em A e B, sendo o Apêndice A uma explicação de configurações do equipamento e o Apêndice B o manual de utilizador do protótipo final.

1.5 Contribuições

* Participação na Noite Europeia dos Investigadores – Ciência na Cidade, no dia 28 de setembro de 2018, no Museu Nacional de História Natural e da Ciência da Universidade de Lisboa.

* 2 artigos submetidos para a conferência *Global Wireless Summit* (GWS- 2018) 25 a 28 de novembro de 2018, Chiang Rai, Thailand.

Capítulo 2

2. Sistemas de Radionavegação para UAVS

Neste capítulo há uma visão geral dos sistemas GNSS com foco principal no GPS, uma breve revisão de vários tipos de *jammers* e o impacto que estes têm no recetor GNSS. É relatada ainda a tecnologia SDR utilizada e o *software* utilizado para os testes.

2.1 Veículos Aéreos Não Tripulados

Veículo aéreo não tripulado (VANT), em inglês *unmanned aerial vehicle* (UAV), ou drone é todo e qualquer tipo de aeronave que possa ser controlada nos 3 eixos (rol, yaw e pitch) e que não necessite de pilotos a bordo para ser guiada. Estes tipos de aeronaves são controladas à distância por meios eletrónicos e computacionais, sob a supervisão de humanos, ou mesmo sem a sua intervenção, por meio de controladores lógicos programáveis (CLP).

Além da aeronave, o UAV é também composto por uma estação de controlo no solo, o (*Ground Control Station*) GCS através da qual é possível projetar a missão a ser executada e acompanhar todo o voo remotamente. O UAV possui ainda um recetor GPS acoplado para localização em tempo-real, assim como, uma unidade de navegação inercial. O veículo não aceita comandos de movimento diretamente ligados pelo GPS, recorrendo a uma *Inertial Measurement Unit* (IMU) garantindo uma melhor precisão da posição.

Figura 2.1 – Veículo aéreo não tripulado [8]

A navegação inercial é também utilizada por foguetes, submarinos e navios para determinar coordenadas. Uma unidade de navegação inercial nada mais é que um sistema de navegação que integra as acelerações em Norte/Sul, Este/Oeste por meio de sensores inerciais, determinando a posição. Segue abaixo listada algumas vantagens da navegação inercial [9]:

- Não necessita de informação exterior;
- Não requer emissões ou receções de sinais;
- Imune a interferências.

O piloto automático ou *Autonomous Flight Control System* (AFCS) é um pacote integrado normalmente fornecido pelo fabricante. O AFCS recebe o controlo da estação de solo (GCS) através da telemetria de controlo do sistema que atua de forma autónoma. Em geral consiste em 5 componentes [9]:

- IMU 3 eixos;
- Magnetómetro de 3 eixos;
- GPS;
- Sistema de radio com interface de servo e *safety pilot*;
- Computador de voo. Inclusive algumas já disponíveis para dispositivos móveis como *smartphones*.

2.2 Visão Geral do GNSS

O GNSS - Sistema Global de Navegação por Satélite é a designação para o conjunto de Sistemas de Posicionamento Global.

Principais sistemas que constituem o GNSS:

- GPS – Global Positioning System - EUA, operacional desde 1995;
- GLONASS – GLObal'naya NAvigatsionnaya Sputnikovaya Sistema – Rússia, iniciado em 1982 e completo em 1995;
- GALILEO - da UE da ESA operacional em 2013.

- **Componente espacial – GPS**

- 24 Satélites (+5) dos blocos II, IIA (*Advanced*) e IIR (*Replacement*) distribuídos por 6 órbitas;

- Órbitas aproximadamente circulares com um raio de 26600 km, separadas entre si de 60º em longitude;

- Período orbital de 12 horas siderais (≈11h 58min 26s UTC), que faz com que o nascimento dos satélites se dê cerca de 4 min mais cedo em cada dia;

- Inclinação orbital próxima dos 55º, relativamente ao plano equatorial terrestre.

● Componente espacial – Glonass

- 24 Satélites (+3) distribuídos por 3 órbitas;

- Órbitas aproximadamente circulares com um raio de 25510 km, separadas entre si de 110º em longitude;

- Período orbital de 11h 15 min siderais, o que faz com que o nascimento dos satélites se dê cerca de 50 min mais cedo em cada dia;

- Inclinação orbital próxima dos 64.8º, relativamente ao plano equatorial terrestre;

- Trajeto repete-se ao fim de 8 dias siderais (o satélite seguinte percorre a órbita do satélite anterior).

● Componente espacial – Galileu

- 30 Satélites distribuídos por 3 órbitas;

- Órbitas aproximadamente circulares com um raio de 30000 km, separadas entre si de 120º em longitude;

- Período orbital de 14h 21 min siderais que faz com que o nascimento dos satélites se dê cerca de 2h e 24 min mais tarde em cada dia;

- Inclinação orbital próxima dos 56º, relativamente ao plano equatorial terrestre [10].

Os GNSS (*Global Navigation Satellite Systems*), definidos na página anterior, são capazes de fornecer informações precisas de localização e cronometragem que se encontram em várias aplicações. O uso de GNSS não se limita à navegação pessoal ou automóvel. Podem também ser utilizados para o rastreamento de mercadorias e animais, para localizar comboios, navegar em navios e para aplicações desportivas. Além disso, novas aplicações GNSS estão atualmente em desenvolvimento ou consolidação. Por exemplo, as caixas de GPS podem ser usadas por companhias de seguros para monitorizar o comportamento de um condutor e ajustar o prémio de seguro acordado. O GPS e os GNSS em geral permitem aplicações que exigem a monitorização do comportamento do utilizador. Este tipo de aplicação inevitavelmente introduz problemas de privacidade, uma vez que os GNSS são usados para aglomerar informações sobre os utilizadores. Esta falta de privacidade motiva o desenvolvimento e o uso de dispositivos que podem negar a receção de sinal GNSS [11].

Os sinais GPS atingem um recetor GPS provenientes de uma série de satélites em órbita terrestre permitindo determinar o posicionamento através da trilateração. Trata-se de um método segundo o qual três pontos separados são medidos para calcular uma localização com uma precisão de apenas alguns metros, como mostra a Figura 2.2.

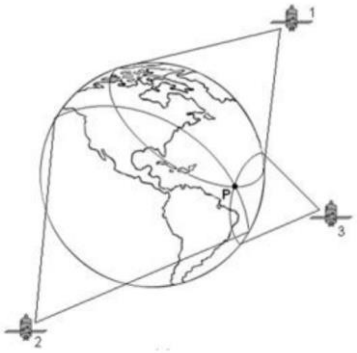

Figura 2.2 – Trilateração [11]

2.2.1 Funcionamento do GPS

O princípio de funcionamento do GPS é bastante simples. Para compreendê-lo recorre-se ao conceito de velocidade média.

A Figura 2.3 representa um carro de fórmula 1 deslocando-se sobre uma trajetória retilínea. O carro parte do ponto S_0 e desloca-se durante um certo tempo até a posição final S.

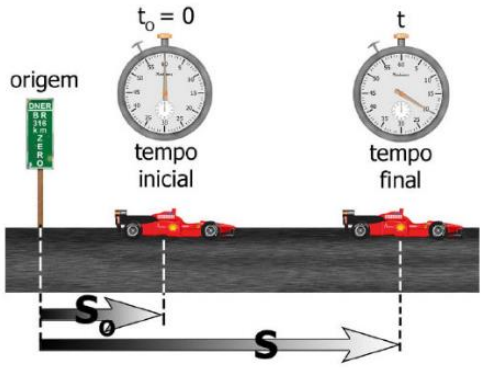

Figura 2.3 - Movimento retilíneo uniforme [11]

Para saber a velocidade do carro no percurso basta medir a distância que ele percorreu e dividi-la pelo tempo (equação 1).

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

Pode-se também utilizar o procedimento contrário, ou seja, sabendo a velocidade com que um objeto se desloca, mede-se o tempo de deslocamento e assim encontra-se a distância percorrida (equação 2). Neste caso, basta isolar o ΔS na equação 1:

$$\Delta S = Vm \times \Delta t \quad (2)$$

No caso do GPS o satélite envia um sinal de rádio para o aparelho recetor com a informação da hora em que o sinal foi enviado. Ao recebê-lo, o aparelho compara a hora de envio com a hora da receção e calcula o tempo de deslocamento [12] [13].

Como o sinal é enviado por uma onda eletromagnética, sabe-se que a sua velocidade é igual à velocidade da luz, ou seja, aproximadamente $3x10^8$m/s. Desta forma, basta aplicar a equação 2 para calcular a distância entre o satélite e o aparelho.

Por exemplo: o tempo calculado pelo aparelho foi de 80ms (0,08s) e a velocidade do sinal é de $3x10^8$m /s. Logo, basta multiplicar estes dois valores para encontrar a distância entre o satélite e o aparelho. Neste caso: 24 000km.

Porém, utilizando apenas um satélite teremos apenas uma distância, ou seja, o aparelho pode estar em qualquer ponto de um círculo de 24 000km de raio, como mostra a Figura 2.4:

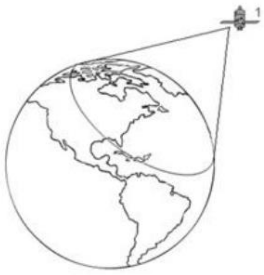

Figura 2.4 - Possíveis localizações usando apenas 1 satélite [11]

Com a utilização de apenas um satélite o aparelho recetor pode estar alocado em toda a circunferência representada na Figura 2.54. Com a contribuição de dois satélites as circunferências intercetam-se e o recetor apenas pode estar localizado em dois pontos (ponto Q ou ponto P). Para obter a localização exata são usados três satélites. O aparelho recetor calcula a distância entre ele e cada um dos três satélites conseguindo saber a sua localização exata.

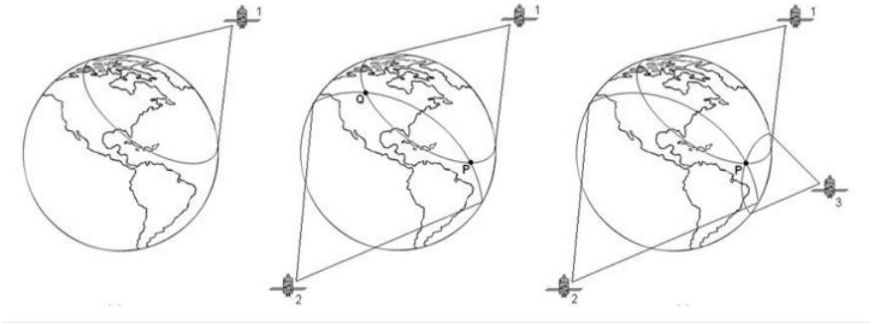

Figura 2.5 - Contribuição de cada satélite na trilateração [11]

Neste caso sabe-se que o aparelho recetor está localizado no ponto P da Figura 2.5. Este processo é chamado de trilateração. Para garantir que os satélites consigam comunicar com o parelho a partir de qualquer lugar na Terra, os 24 satélites orbitam o planeta em 6 planos com 4 satélites cada. Isso faz com que haja sempre pelo menos 4 satélites visíveis em qualquer ponto do planeta [14].

Um sinal é transmitido por cada satélite na direção do planeta Terra. Este sinal é codificado com a "Mensagem de Navegação", que pode ser lida pelos recetores de GPS. A "Mensagem de Navegação" inclui parâmetros de órbita (frequentemente chamados de "efemérides de transmissão"), da qual o recetor pode calcular coordenadas de satélite (X, Y, Z). Estas são coordenadas cartesianas num sistema geocêntrico, conhecido como WGS-84, que tem a origem no centro de massa da Terra, Z eixo apontando para o Pólo Norte, X apontando para o Meridiano Principal (que atravessa Greenwich) e Y em ângulo reto com X e Z. O algoritmo que transforma os parâmetros da órbita em coordenadas WGS-84 é chamado de "Algoritmo Ephemeris", que é definido em Livros de texto GPS (por exemplo, Leick, 1991). Discute-se a "Mensagem de Navegação" em mais detalhes posteriormente. Por enquanto, aborda-se as *pseudoranges.*

O tempo em que o sinal é transmitido do satélite é codificado no sinal, usando o tempo de acordo com um relógio atômico a bordo do satélite. O tempo de receção do sinal é registado pelo recetor usando igualmente um relógio atômico. O recetor mede a diferença nestes tempos (equação 3):

$$pseudorange = (T - T^S) \times \mathrm{c} \tag{3}$$

$T \rightarrow leitura\ conhecida\ do\ relógio\ do\ receptor\ quando\ o\ sinal\ é\ recebido$
$T^S \rightarrow\ leitura\ do\ relógio\ do\ satélite\ quando\ o\ sinal\ foi\ transmitido$
$c \rightarrow velocidade\ da\ luz$

Os recetores registam dados em intervalos regulares e especificados (normalmente a cada 30 segundos, conforme instruído pelo utilizador do recetor). É a leitura do tempo do relógio do recetor T, que é usada para especificar exatamente a amostragem da medição. Portanto, o valor de T em uma época de medição é conhecido exatamente e é gravado no arquivo de dados juntamente com a observação. O que não é conhecido é o tempo real de medição e para uma explicação mais clara é ilustrada a Figura 2.6 [15].

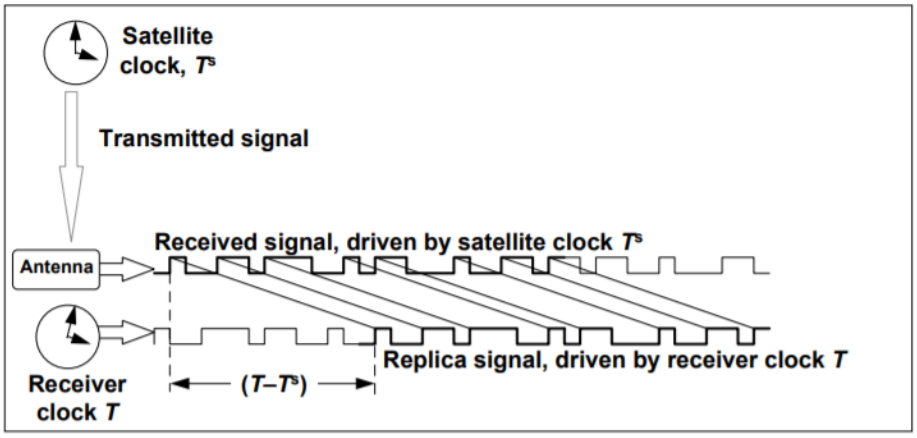

Figura 2.6 - Relógios do satélite e do recetor [15]

A observação modelada pode ser desenvolvida ajustando a hora do relógio T igual ao tempo real de receção t mais uma polarização do *clock* τ, tanto para o recetor (equação 4) como para os relógios de satélite (equação 5):

$$T = t + \tau$$

$$T^S = t^S + \tau^S$$

A substituição dá o *pseudorange* em função do tempo real em que o sinal foi recebido (equação 6):

$$\begin{aligned} \rho^S(t) &= \big((t+\tau) - (t^S + \tau^S)\big)c \\ &= (t - t^S)c + c\tau - c\tau^S \\ &= \rho^S(t, t^S) + c\tau - c\tau^S \end{aligned} \tag{6}$$

$\rho^S(t, t^S)$ representa o intervalo do recetor (no tempo de receção) para o satélite (no tempo de transmissão). Este modelo é simplificado; por exemplo, assume que a velocidade da luz na atmosfera é c, e ignora a teoria da relatividade; mas este modelo simplificado é útil para obter informações sobre os princípios do GPS. Através do recurso do teorema de Pitágoras, pode-se escrever:

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

A Mensagem de Navegação permite calcular a posição do satélite (x^S, y^S, z^S) e o clock do satélite τ^S. Portanto, fica-se com 4 incógnitas, a posição do recetor (x, y, z) e o *clock* do recetor τ.

Se o tempo de receção fosse usado, o erro no intervalo calculado poderia ser de dezenas de metros. Começando com o tempo de receção real, t, o tempo de transmissão pode ser calculado por um algoritmo iterativo conhecido como "a equação do tempo de luz", que pode ser escrito da seguinte maneira:

$$t^S(0) = t = (T - \tau) \tag{8}$$

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

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

$$(. \; . \; .)$$

onde a posição do satélite $\rho^S\,(t, t^S\,)$ é calculado em cada etapa usando os elementos do tipo Kepler da Mensagem de Navegação, e o algoritmo é interrompido quando o intervalo computado converge (ou seja, não muda em mais do que um valor insignificante). Embora métodos mais convergentes tenham sido implementados, o método acima é provavelmente o mais fácil de entender.

Observando o sistema de equações de observação simplificadas a partir de 4 satélites em vista do recetor, pode-se escrever os *pseudoranges* para cada satélite como (equação 9):

$$\rho^1 = ((x^1 - x)^2 + (y^1 - y)^2 + (z^1 - z)^2)^{1/2} + c\tau - c\tau^1 \tag{9}$$
$$\rho^2 = ((x^2 - x)^2 + (y^2 - y)^2 + (z^2 - z)^2)^{1/2} + c\tau - c\tau^2$$
$$\rho^3 = ((x^3 - x)^2 + (y^3 - y)^2 + (z^3 - z)^2)^{1/2} + c\tau - c\tau^3$$
$$\rho^4 = ((x^4 - x)^2 + (y^4 - y)^2 + (z^4 - z)^2)^{1/2} + c\tau - c\tau^4$$

Nota: (Os sobrescritos ao lado das coordenadas do satélite destinam-se a identificar o satélite e não devem ser confundidos com expoentes) [15].

2.2.2 Segmento Espacial

O segmento espacial consiste em 24 satélites distribuídos em 6 planos orbitais igualmente espaçados, com 4 satélites em cada plano numa altitude aproximada de 20200 km. Os planos orbitais são inclinados 55º em relação ao equador e o período orbital é de aproximadamente 12 horas siderais. Dessa forma, a posição dos satélites repete-se a cada 4 minutos antes que a do dia anterior. Essa configuração garante que, no mínimo, 4 satélites GPS sejam visíveis em qualquer local da superfície terrestre a qualquer hora. As Figuras 2.7 e 2.8 ilustram respetivamente, a constelação dos satélites GPS e a distribuição destes em cada um dos planos orbitais [13].

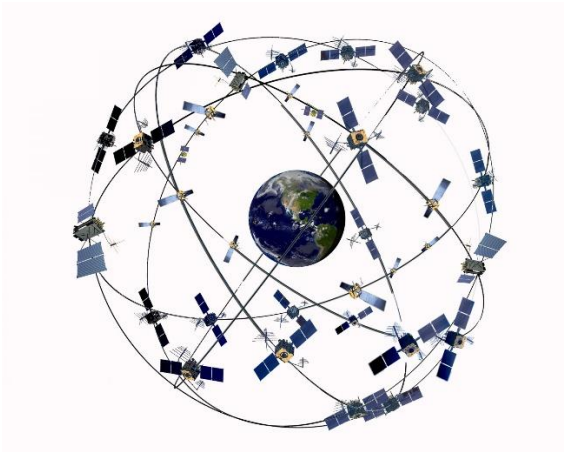

Figura 2.7 - Constelação dos satélites GPS [16]

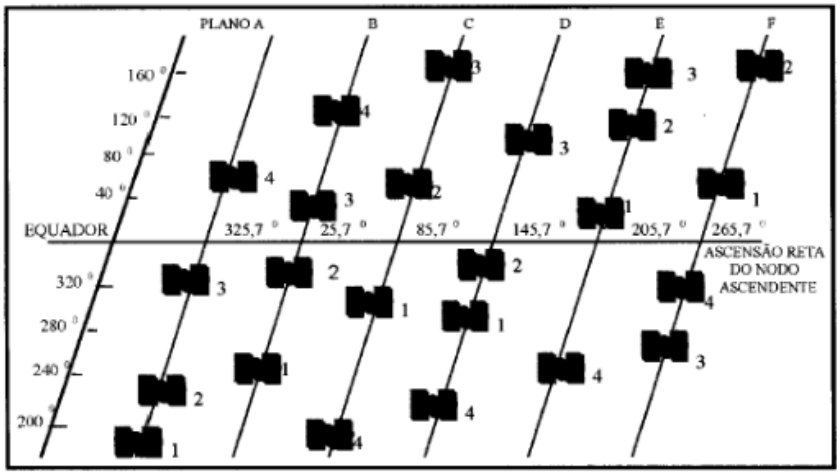

Figura 2.8 - Distribuição dos satélites na constelação final [13]

2.2.3 Características dos Sinais GPS

Cada satélite GPS transmite duas ondas portadoras: L1 e L2. São geradas a partir da frequência fundamental 10.23 MHz, a qual é multiplicada por 154 e 120, respetivamente. Dessa forma, as frequências (L) e os comprimentos de onda (λ) de L1 e L2 são:

Ondas portadoras

- L1 = 10,23 MHz × 154 = 1575, 42 MHz e λ = 19 cm
- L2 = 10,23 MHz × 120 = 1227,60 MHz e λ = 24 cm

Os códigos que formam o PRN (*Pseudo-Random-Noise*) são modelados em fase sobre essas duas portadoras. Esta técnica permite calcular distâncias a partir do tempo de propagação da modelação (Leick, 1995). Um PRN é uma sequência binária de +1 e -1, ou 0 e 1, que parece ter característica aleatória. Como é gerado por um algoritmo pode ser univocamente identificado. Trata-se basicamente dos códigos C/A e P.

O código C/A (*Coarse Acquisition* - fácil aquisição) com comprimento de onda por volta de 300 metros é transmitido a uma razão de 1,023 MHz. É gerado a partir do produto de duas sequências PN (*Pseudo Random* - pseudo aleatória) denominadas G1 e G2, cada uma com períodos de 1.023 bits. O código C/A resultante também consistirá de 1.023 bits, com período de 1ms. Cada satélite transmite um código C/A diferente dentre os 37 definidos no ICD-GPS-200C (Spilker, 1996). Isso poderia causar dificuldades ao recetor GPS ao ter de conseguir distinguir todos os códigos possíveis. No entanto, o código C/A faz parte de uma família de códigos (*Gold Codes*) que têm como característica básica a baixa correlação entre os seus membros. Isso possibilita a rápida distinção dos sinais recebidos, simultaneamente, de vários satélites (Leick, 1995). É modelado somente sobre a onda portadora L1, não é criptografado, embora possa ter uma precisão degradada.

O código P (Precise *or Protected* - preciso ou protegido) tem sido reservado para o uso dos militares americanos e de utilizadores autorizados. É transmitido com uma frequência de 10,23 MHz, o que corresponde a uma sequência de 10,23 milhões de bits por segundo, resultando num comprimento de onda na ordem dos 30 metros. Esse comprimento de onda, menor que o do código C/A, faz com que as medidas resultantes do código P sejam mais precisas. A cada satélite é atribuído um determinado PRN que é modelado nas portadoras L1 e L2. Todos os satélites transmitem na mesma frequência, no entanto, podem ser identificados pelo código exclusivo de cada satélite. Trata-se da técnica denominada CDMA (*Code Division Multiple Access* - divisão do código para múltiplo acesso) (Spilker, 1996), válida tanto para o código C/A como para o código P.

O código D (*Navigation Message*) é responsável pelas informações detalhadas sobre a posição e a rede dos satélites. Esta informação é modulada em 50 bits/s e é chamada de mensagem de navegação. É construído a partir de uma trama de 1.500 bits dividida em 5 subtramas de 300 bits que requerem 6 segundos para transmitir cada um. Existem três componentes importantes na mensagem de navegação. O primeiro contém o estado do satélite, dados e o tempo do GPS, localizados na subtrama 1. O segundo refere-se à subtrama 2 e 3 que, em conjunto, contêm dados que permitem ao recetor calcular a posição do satélite. O terceiro contém a informação e o *status* relativos a todos os satélites na constelação, a sua localização e números PRN. As subtramas 4 e 5 contêm somente 1/25 da mensagem total, o que significa que o recetor deve processar 25 valores para recuperar a mensagem original de 15.000 bits, exigindo 12,5 minutos para recebê-la de um único satélite [17].

Códigos

● C/A (*Coarse Aquisition* ou *Clear Access*) código PRN de 1023 dígitos binários;

● P (*Precise* ou *Protected*) código PRN de 2.34x1014 dígitos binários, sequência de período de 267 dias de duração, divididos em 7 dias, com reinicialização às 0h de domingo;

● D (*Navigation Message*) código PRN de 1500 dígitos binários.

Os sinais GPS resultam da modulação de um código binário PRN (*Pseudo Random Noise* ou Ruído Pseudo-Aleatório).

Tab. 1 – Códigos do sistema GPS

	frequência	modulado em	comp. de onda
P (*Precise*)	f_o = 10.23 MHz	L1* e L2	30 m
C/A (*Coarse Aquisition*)	$f_o/10$ = 1.023 MHz	L1	300 m
D (*Navigation Message*)	50 Hz	L1 e L2	6 km

* modulado em quadratura de fase com o código CA, i.e., separados de 90º em fase

A Mensagem de Navegação (código D) contém o tempo UTC, nº da semana GPS, correção aos relógios dos satélites e outras informações.

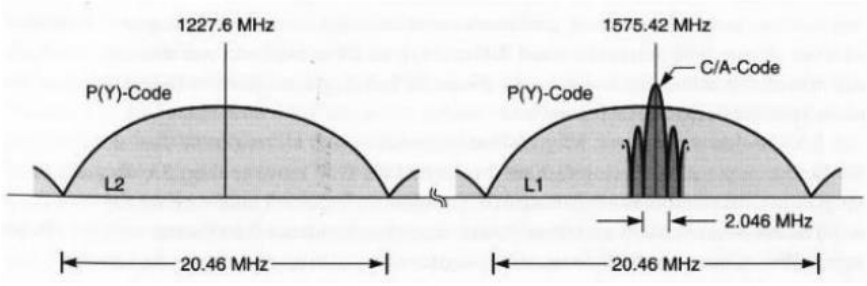

Figura 2.9 - Densidade espectral de potência dos sinais de GPS em L2 e L1 [17]

O código C/A e o código P ambos espalhados são centrados na frequência portadora, com uma largura de banda de 20.46 MHz. Isso permite que a densidade espectral de potência seja reduzida enquanto a potência do sinal for inalterada (Figura 2.9) [18].

2.2.4 Serviço de Posicionamento GPS

Os recetores GPS na Terra podem receber entre 5 e 12 sinais de satélite.

Todos os 24 sinais de satélite L1 podem ocupar a mesma frequência sem interferir uns com os outros, pois cada um deles é propagado por 1 de 37 códigos *Pseudo Random Noise* (PRN) exclusivos com uma largura de banda de 2.046 MHz após serem convertidos e transmitidos.

A propagação do sinal GPS pelo código PRN não só distingue cada sinal dos outros, mas também protege contra interferências.

O DoD (*Department of Defense*) dos EUA proporciona aos utilizadores 2 tipos de serviços de posicionamento: [18]

● **Serviço de posicionamento padrão** (SPS – *Standard Positioning Service*):

- Opera apenas em L1 e é usado na aquisição inicial dos sinais do satélite, através da sintonia do código C/A;

- Este serviço era condicionado até há bem pouco tempo pelo acesso seletivo (SA – *Selective Availability*).

● **Serviço de posicionamento preciso** (PPS – *Precise Positioning Service*):

- Opera em ambas as frequências e usa o código P, permitindo uma maior precisão no posicionamento, sendo essencialmente utilizado para fins militares;

- O acesso a este serviço é controlado através da técnica criptográfica denominada anti-sabotagem (AS – Anti *Spoofing*).

*** Acesso Seletivo** (SA – *Selective Availability*)

O DoD implementou esta técnica para reduzir a precisão da informação GPS (posição, velocidade e tempo), através da introdução de erros pseudoaleatórios no relógio do satélite. O SA foi entretanto removido em 1 Maio de 2000, pelo que atualmente o SPS disponibiliza uma precisão muito semelhante à dada pelo PPS.

*** Anti Sabotagem** (AS – Anti *Spoofing*)

A técnica AS impede que os recetores GPS sejam enganados por sinais falsos e que utilizadores não autorizados façam medições diretas em L2. Em condições de AS, o código P é substituído pelo código Y ao qual apenas podem aceder utilizadores autorizados usando uma chave criptográfica. Esta técnica foi ativada às 0h UT do dia 31 de Janeiro de 1994 e permanece em operação contínua desde essa data, afetando todos os satélites do Bloco II.

Em suma, é possível fazer *spoofing* do serviço de posicionamento padrão, utilizado pelos drones comercias, que operam apenas em L1.

2.2.5 Potência do Sinal GPS

Os sinais GPS são muitos fracos, cerca de 50 W, tendo aproximadamente a mesma potência que os de TV, transmitidos por satélites geoestacionários. A razão pela qual os recetores GPS não necessitam de uma antena de dimensão igual à das parabólicas tem muito a ver com a estrutura dos sinais e a capacidade dos recetores em captá-los. A captação dos sinais GPS está mais concentrada no recetor do que na antena propriamente dita. De qualquer forma, uma antena GPS, geralmente, contém um pré-amplificador de baixo ruído que amplifica o sinal antes de ser processado pelo recetor.

Os sinais GPS sofrem interferências quando passam através da maioria das estruturas. À medida que a antena de satélite difunde o sinal de RF uniformemente sobre a superfície da Terra, a energia transmitida é atenuada. Isso ocorre principalmente devido às perdas de espaço livre, pois a energia transmitida espalha-se espacialmente à medida que viaja até ao utilizador (de acordo com a superfície de uma esfera cujo raio vai aumentando).

O nível mínimo de energia recebida para os utilizadores na Terra é -158,5 dBW para o código C/A em L1 e -160 dBW para o código P em L2 de acordo com as especificações GPS [18].

2.3 Interferência por Radiofrequência

É considerada interferência qualquer sinal de radiofrequência de qualquer fonte indesejada que é recebida por um recetor GNSS. Essa interferência pode resultar em falta de precisão na navegação ou perda completa do sinal no recetor.

2.3.1 *Jamming*

Um *jammer* é um dispositivo com capacidade de interferir com a transmissão de sinais, tais como sinais usados nos sistemas GNSS, sinais de sistemas de comunicações móveis, sinais Wi-Fi e outros sinais.

Existem vários dispositivos de telecomunicações que podem sofrer perturbações devidas a *jammers*. Os principais tipos de *jammers* são [19]:

- *Jammers* de rede móvel;
- *Jammers* de sinal Wi-Fi;
- *Jammers* de GPS;
- *Jammers* de Bluetooth;
- *Jammers* de sinais VHF/UHF;
- *Jammers* de *walkie-talkie*.

Devido ao meio *wireless* ser partilhado, um *jammer* pode facilmente interferir com um canal de comunicações usado por tecnologias de RF. É possível interferir com o canal através de um sinal que ignore os protocolos MAC, ou que interfira com estes mesmos protocolos.

Com o intuito de criar um *jammer* de sinais GPS, recorreu-se a técnicas exploradas em *jamming* de outras tecnologias, podendo estas serem caracterizadas em 5 tipos [20]:

- ***Barrage Jamming*** - É a forma mais simples de interferência e é geralmente definido como um *jammer* que transmite energia semelhante a ruído em toda a porção do espectro ocupado pelo alvo, como representa a Figura 2.10. Essencialmente aumenta o nível de ruído no recetor, dificultando o funcionamento do sistema de comunicação.

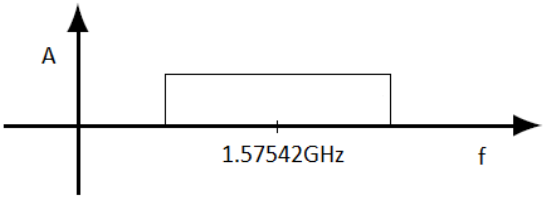

Figura 2.10 - Espectro teórico de Barrage Jamming

- ***Sweep Jamming* –** É uma técnica com um resultado final muito idêntico à *Barrage Jamming*, pois atua em toda a banda de frequência. A diferença entre estas duas técnicas é que a *Sweep Jamming* não emite um sinal estático nem com uma largura de banda de 15.345MHz. Esta técnica é mais eficiente no que diz respeito à densidade espectral de potência uma vez que emite um sinal com baixa largura de banda e faz um varrimento na frequência de modo a percorrer toda a largura de banda do sinal a interferir, como representa a Figura 2.11. Emite portanto um sinal conhecido por *Chirp Signal*.

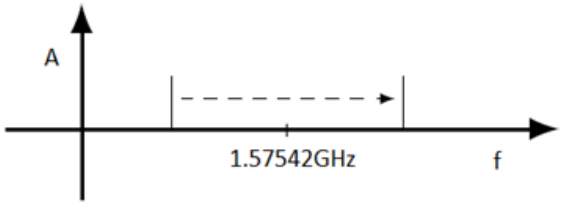

Figura 2.11 - Espectro teórico de Sweep Jamming

- ***Successive Pulses Jamming* –** Geração de impulsos no tempo com baixo *duty cycle*, isto é, pouco tempo a *high* e mais tempo a *low*. Recorrendo a esta técnica obtém-se um empastelamento na frequência da onda portadora utilizando a largura de banda do sinal a interferir, como ilustra a Figura 2.12. O sinal ocupa a banda pretendida com picos em múltiplos da frequência do sinal correspondente à sequência de pulsos.

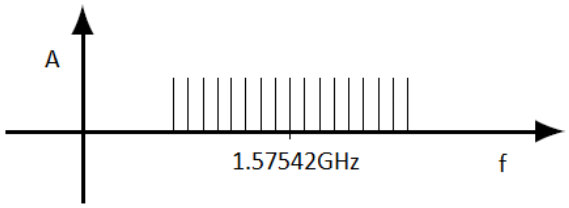

Figura 2.12 - Espectro teórico de Successive Pulses Jamming

- ***Tone Jamming* –** Abordando esta técnica é apenas transmitida uma sinusoide na frequência do GPS ficando apenas a interferência refletida na portadora, frequência central, e não em toda a largura de banda. Utilizando esta técnica toda a energia é aplicada na frequência central da portadora. O espectro é o expresso na Figura 2.13.

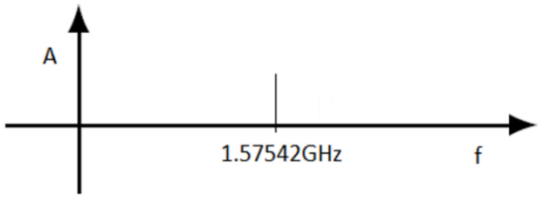

Figura 2.13 - Espectro teórico de Tone Jamming

- ***Protocol-Aware Jamming* -** A última técnica de interferência apresentada é o congestionamento com reconhecimento de protocolo. Durante a construção do sinal de interferência tem-se em conta a modulação do sinal (BPSK), a taxa de dados (sample rate = 1.023MHz) e a largura de banda do canal (15.345MHz). O espectro resultante tem um aspeto muito idêntico à Figura 2.14. Esta técnica é a que resulta num espectro mais próximo do espectro dos sinais GPS.

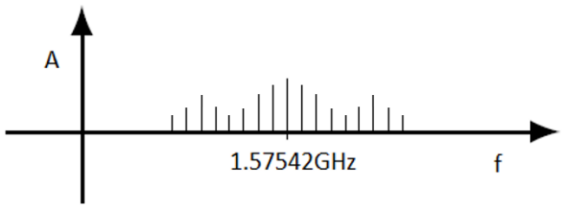

Figura 2.14 - Espectro teórico de Protocol-Aware Jamming

De uma forma geral é prática corrente usar-se para arquitetura do *jammer* uma arquitetura semelhante à utilizada pelo emissor do sinal a interferir. Desta forma, o sinal interferente "mistura-se" com o sinal alvo, uma vez que apresentam propriedades idênticas por forma a destruir a informação deste ou então tornar a sua receção virtualmente impossível de ser realizada no recetor.

Os sistemas GPS utilizam uma transmissão recorrendo à modulação BPSK (*Binary Phase Shift Keying*). Desta forma, o último tipo de *jammer* apresentado, *Protocol-Aware Jamming*, é desenvolvido tendo em conta a modulação BPSK.

Relativamente à modulação PSK pode-se recorrer à codificação de linha NRZ bipolar, facilitando a conceção do emissor. Uma vez que o código de linha bipolar varia entre uma tensão positiva e negativa, obtém-se deste modo a diferença de fase de 180º. O diagrama de blocos que descreve este modulador encontra-se representado na Figura 2.15 [21].

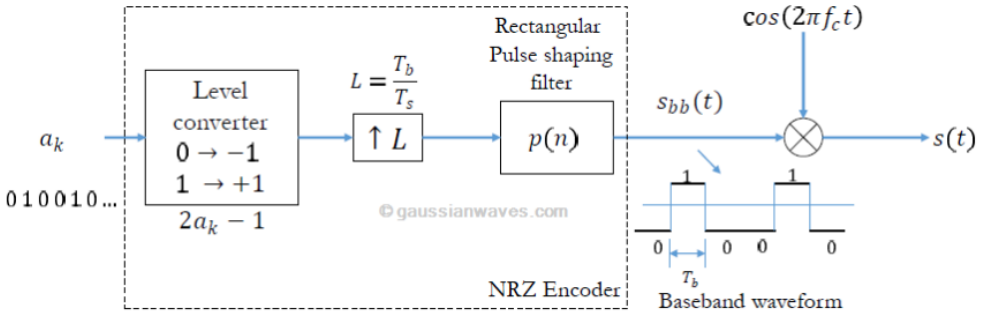

Figura 2.15 - Modulador PSK binário [21]

O sinal PSK resultante desta modulação encontra-se representado na Figura 2.16. Esta modulação é também conhecida como BPSK (*Binary* PSK).

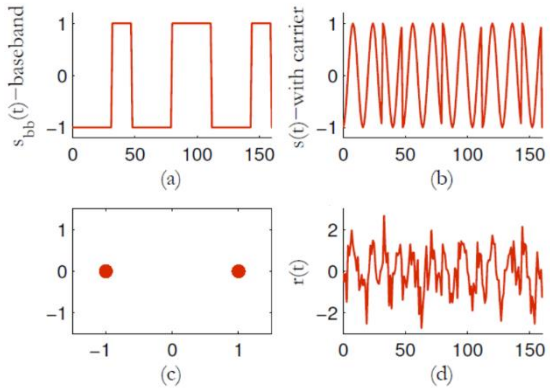

Figura 2.16 - (a) Sinal BPSK de banda base, (b) sinal BPSK transmitido - com portadora, (c) constelação no transmissor e (d) sinal recebido com ruído AWGN [21]

Para esta modulação os valores de amplitude e frequência da portadora são constantes, variando apenas a fase em 180º conforme representado na expressão (10) [22].

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

2.3.2 Principais Componentes de um *Jammer*

Os *jammers* inicialmente foram desenvolvidos para as forças de segurança e para fins militares com o objetivo de serem usados contra criminosos e terroristas. Mais tarde, a utilização deste tipo de dispositivos estendeu-se a aplicações civis nomeadamente para uso por parte de governos como proteção de certas entidades. Os *jammers* para GPS foram inicialmente desenvolvidos com o objetivo de serem utlizados na área militar e em agências de espionagem. Como referenciado anteriormente existem duas frequências de portadoras possíveis que são utilizadas por estes dispositivos, uma para o público em geral (1575,42 MHz) e outra para os militares (1227,6 MHz).

Nos EUA, em Outubro de 2011, a FCC *Enforcement Bureau* efetuou 20 ações contra lojas *online* de venda ilegal de mais de 200 modelos de *jammers* em 12 estados. Foram apreendidos diferentes tipos de *jammers*: *jammers* de Wi-Fi, *jammers* de GPS e ainda *jammers* de outros dispositivos [23].

Os principais módulos que compõem um *jammer* são [24]:

- **Antenas** – Alguns *jammers* menos complexos têm a sua antena no interior do dispositivo, enquanto outros mais sofisticados têm várias antenas na parte exterior do dispositivo, pois assim é possível atingir um maior alcance e bloquear várias bandas de frequência em simultâneo.
- **VCO** – *Voltage Controlled Oscilator*: componente que gera um sinal.
- **Circuito de controlo** – Permite ajustar a frequência a que se vai fazer *broadcast* impondo uma tensão à entrada do VCO.
- **Gerador de ruído** – Pertence ao circuito de controlo. Gera-se neste componente um sinal eletrónico aleatório na frequência onde se pretende fazer o bloqueio de comunicações.
- **Amplificador de RF** – Amplifica o sinal de saída até à potência do sinal rádio necessária para se bloquear comunicações.
- **Bateria** – Alimenta o circuito. A carga depende da complexidade do *jammer*.

Jammers são utlizados na área militar para impedir a localização exata de um determinado objeto como por exemplo, mísseis ou bombas (que tenham incorporados recetores GPS) e de outros (também com recetores GPS) que permitem que tropas possam ser localizadas pelo inimigo. Assim, este dispositivo tanto é útil para ocultar do inimigo a localização de quem o possui, como também para impedir o inimigo de usufruir das funcionalidades de aparelhos com GPS, caso o sinal do *jammer* alcance estes aparelhos do inimigo.

Os *jammers* de GPS têm sido utilizados recentemente por civis que pretendem assegurar a sua própria privacidade. Para isto, utilizam este dispositivo nos seus carros (um dispositivo deste tipo apresenta-se na Figura 2.17). O objetivo de alguns dos utilizadores destes *jammers* é bloquear o recetor GPS da sua viatura de forma a evitar que a sua localização seja detetada por aparelhos com essa capacidade.

Figura 2.17 - Jammer de GPS para ser usado em automóveis [25]

Este aparelho também tem sido utilizado recentemente de forma ilegal para furtos de automóveis que possuam recetores GPS, dado que este *jammer* consegue desativar o localizador de GPS da viatura [25].

O *jammer* abordado nesta dissertação pretende obter a mesma finalidade, com o intuito de interferir na comunicação dos satélites GPS com o drone alvo.

Capítulo 3

3. Implementação de Técnicas de *Jamming*

Este terceiro capítulo consiste no desenvolvimento de diferentes *jammers* em plataformas SDR recorrendo às diversas técnicas exploradas. Tem como finalidade compará-las e analisar qual das técnicas apresenta um melhor desempenho para o objetivo traçado.

3.1 Plataforma SDR

Software Defined Radio é um sistema de radiocomunicação onde os componentes tipicamente implementados em *hardware* (misturadores de frequência, filtros, amplificadores, moduladores/desmoduladores, detetores) são implementadas em *software*, utilizando um computador pessoal ou outros dispositivos de computação embutido [26].

O SDR permite que o recetor faça uma conversão de frequência direta (solução zero-IF, não usa filtro IF) colocando o sinal RF diretamente em banda base [27][28]. Vantagens:

- Melhor seleção de canais devido ao uso de filtros digitais
- Fácil realização de filtros (FIR) com fase linear (menor distorção)
- Arquitetura simples
- Apenas usa um oscilador local

Dispositivos RF não são ideais como em simulação ou como em cálculos teóricos. Em particular, os dispositivos de RF produzem (entre outros) os seguintes efeitos:

- *DC Offset*
- *IQ Imbalance*

3.1.1 DC Offset

Para uma melhor compreensão é apresentado um exemplo de *DC Offset* em um sinal 16 QAM (com algum AWGN adicionado). Neste exemplo, o erro de *DC Offset* é de uma quantidade tal que a diferença de potência no vetor fixo é de -10 dB da potência total no sinal. Observa-se que a mudança pode ser em qualquer magnitude e fase e o fato de não mudar com o tempo torna-a DC. Mesmo que seja 10 dB abaixo da potência total no sinal, aparece significativamente mais alto no espectro, o que pode confundir alguns observadores: isso ocorre porque a energia da forma de onda é distribuída pela largura de banda de modulação, então a potência em cada FFT é menor que a potência no deslocamento DC [29].

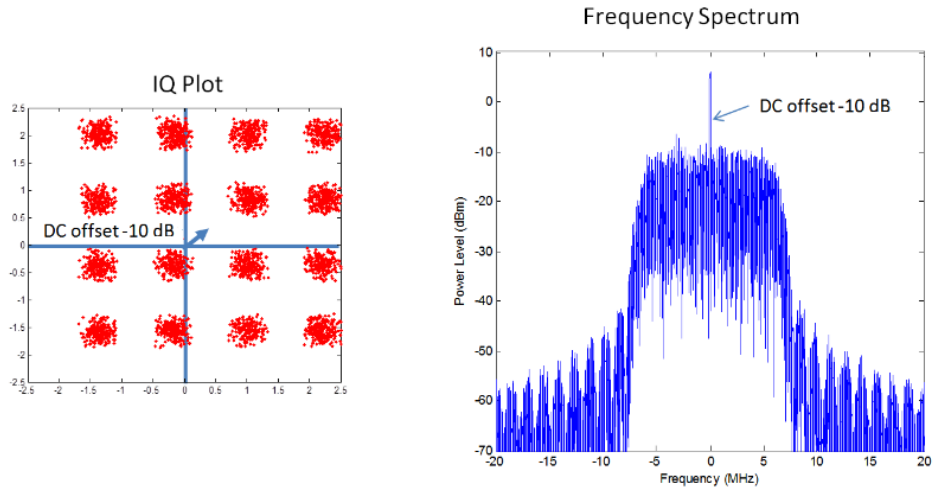

Figura 3.1 - Exemplo de DC Offset em um sinal 16 QAM [29]

Abaixo está uma abordagem simples para eliminar o deslocamento DC. Este filtro de segunda ordem, onde a constante de ganho α controla a largura de banda, ficando mais estreita à medida que α se aproxima de 1.

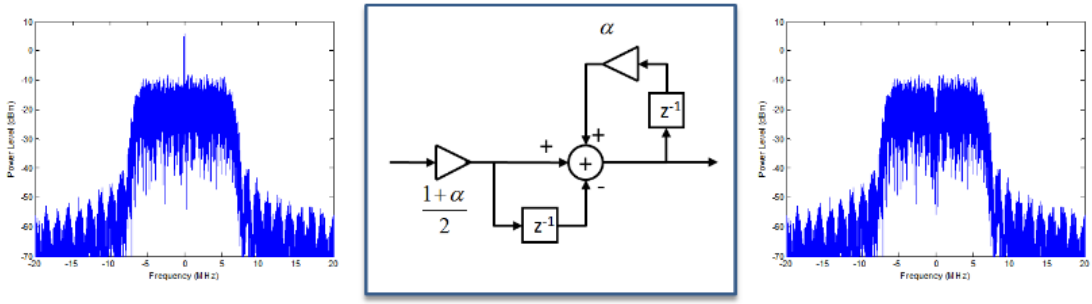

Figura 3.2 - Filtragem do erro DC Offset [29]

Na Figura 3.2, mais à esquerda está representado o espectro de um sinal 16 QAM, que com a filtragem representada no centro da imagem, resulta num espectro apresentado à direita onde o erro de *DC Offset* já não existe.

3.1.2 *IQ Imbalance*

O *IQ Imbalance* é um problema de limitação de desempenho no projeto de recetores de conversão direta, também conhecidos como frequência intermediária zero.

Como exemplo de *IQ Imbalance*, é demonstrado no mesmo sinal 16 QAM na Figura 3.3, como pode resultar em um desequilíbrio de amplitude ou desequilíbrio de fase ou ambos. Com o desequilíbrio de amplitude, a escala de um eixo é alterada com outro, com desequilíbrio de fase, o eixo não se encontra em quadratura perfeita [30].

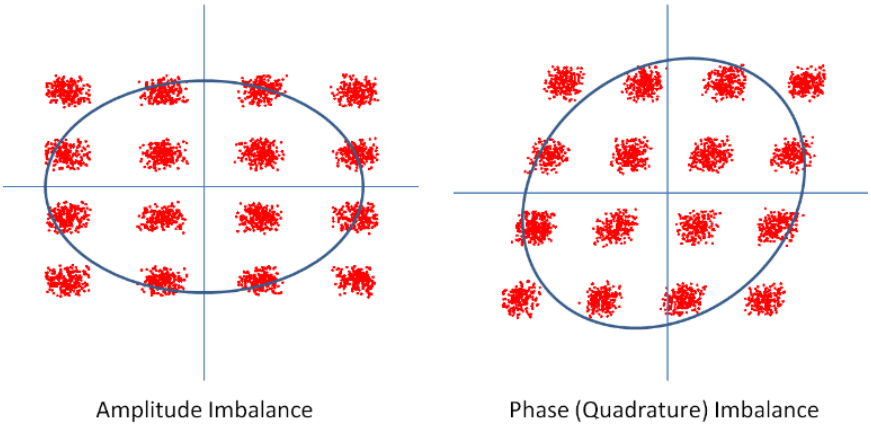

Figura 3.3 – IQ Imbalance num sinal 16 QAM [30]

A correção para o *IQ Imbalance* é feita como na Figura 3.4, com um fator de ganho α mostrado para o desequilíbrio de amplitude e um fator de ganho β mostrado para o desequilíbrio de quadratura.

α = correção de amplitude, tipicamente $0.9 < \alpha < 1.1$ (normalizado a 1)

β = correção de fase (quadratura), tipicamente $-0.1 < \beta < 0.1$ (normalizado a 1)

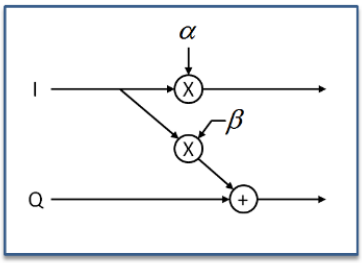

Figura 3.4 - Correção IQ Imbalance [30]

3.2 *Hardware* e *Software* Utilizados

Os sinais *jammers* foram desenvolvidos e modulados com recurso ao *software* GNURadio e Python IDLE. Para a transmissão dos sinais desenvolvidos utilizou-se a plataforma de SDR, BladeRF, pois as suas especificações permitem alcançar o objetivo.

3.2.1 *Hardware*

O principal *hardware* utilizado é uma BladeRF x40 e um amplificador xb 300, ambos da Nuand. A placa BladeRF x40 é um aparelho com USB 3.0 para utilização como "*Software Defined Radio*". A BladeRF pode ser configurada para funcionamento como um modem de RF, GSM ou LTE picocell. Pode ainda ser configurada como um recetor de GPS, um transmissor ATSC ou uma combinação de bluetooth / cliente Wi-Fi, sem qualquer necessidade de expansão [31].

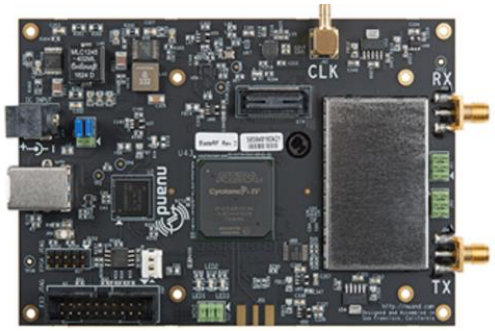

Figura 3.5 - BladeRF x40

Uma descrição mais detalhada da arquitetura de *hardware* da BladeRF é mostrada na Figura 3.6.

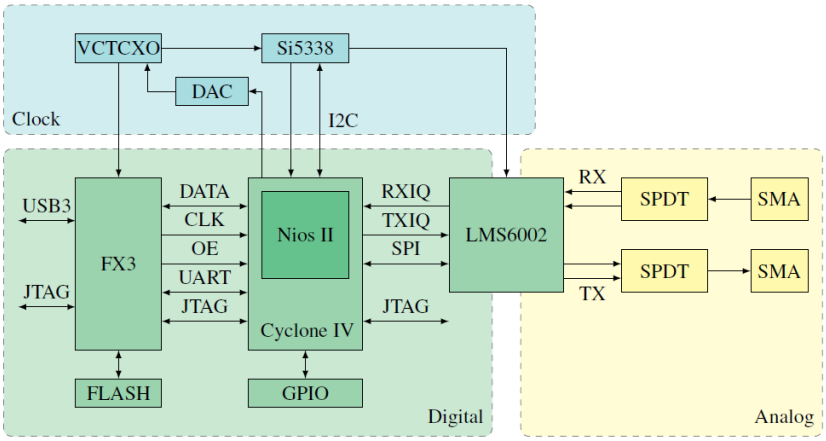

Figura 3.6 - Diagrama de blocos da placa BladeRF [31]

A BladeRF possui caminhos separados para receber e transmitir sinais de RF e pode fazê-lo no modo bidirecional. Tanto a conversão analógica para digital como a conversão digital para analógica são realizadas pelo chip LMS6002D. É um transcetor RF de chip único, abrangendo a faixa de frequência de 0,3 GHz a 3,8 GHz e tem até 28 MHz de largura de banda instantânea [32]. A largura de banda de modulação programável varia com os seguintes valores: 1,5 1,75 2,5 2,75 3 3,84 5 5,5 6 7 8,75 10 12 14 20 e 28 MHz. Os sinais GPS têm uma largura de banda de 15.345 MHz, valor compreendido entre os 14 e 20 MHz disponíveis pela BladeRF. Para os *jammers* desenvolvidos optou-se pelos sinais com 14 MHz de largura de banda, uma vez que com 20 MHz seria um desperdício de potência pois 5 MHz seriam desnecessários.

Figura 3.7 - Amplificador xb300

Quanto ao amplificador xb300 (Figura 3.7) também desenvolvido pela Nuand, analisando apenas a parte de transmissão, o ganho é de 20dB para uma frequência de 2.45GHz com uma largura de banda de 100MHz e o máximo de potência de saída é de +25dBm. Contém um ADC (*analog to digital converter*) de alta resolução para medir a potência de saída de PA (Power Amplifier). É aconselhado uma fonte de alimentação dedicada para a amplificação.

Uma descrição mais detalhada da arquitetura de *hardware* do amplificador xb300 é mostrada na Figura 3.8. Para o caso de estudo não é utilizado o LNA (*Low Noise Amplifier*), uma vez que o amplificador é usado apenas para a transmissão.

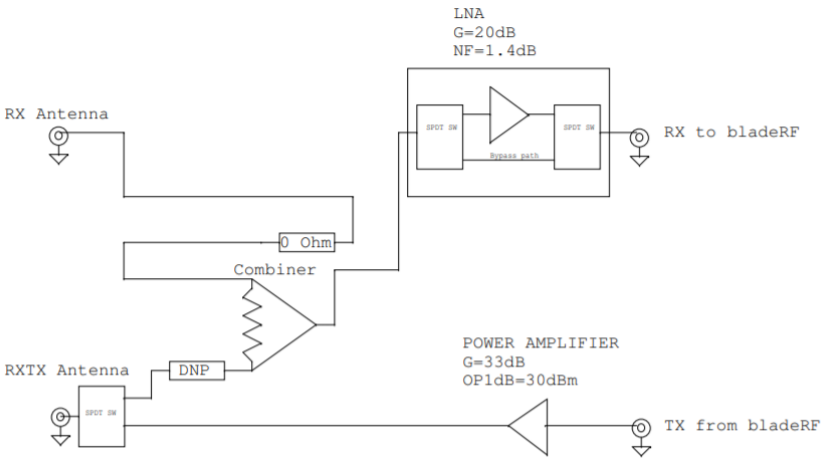

Figura 3.8 - Diagrama de blocos do amplificador xb300 [32]

Para uma análise de espectro *plug and play*, isto é, sem ser necessário demasiadas configurações e sem ter de desenvolver nenhum tipo de *software*, utilizou-se o RTL SDR com o SDR Sharp como interface.

O RTL SDR usa o *chipset* R820T2 para um melhor desempenho. Este SDR com conexão USB 2.0 pode ser usado em frequências compreendidas entre 25 MHz a 1800 MHz, com uma largura de banda máxima de 2.5 MHz. Permite a receção de AM, CW, FM, SSB para Radio Amador, rádio de transmissão e outras frequências (incluindo radar / rastreamento). O processamento é feito pelo computador ao qual está conectado. Para uma análise de espectro utiliza-se o SDR 820T2 representado na Figura 3.9.

Figura 3.9 - SDR 820T2

Como recetor de GPS utilizou-se o módulo u-blox EVK-M8T. Este recetor simula o recetor GPS do drone que se pretende afetar, O u-blox EVK-M8T é um recetor de sinais GNSS bastante interativo e de fácil utilização. A interface USB integrada serve de fonte de

alimentação e de transferência de dados. O *hardware* que compõe o recetor GPS é apresentado pela Figura 3.10.

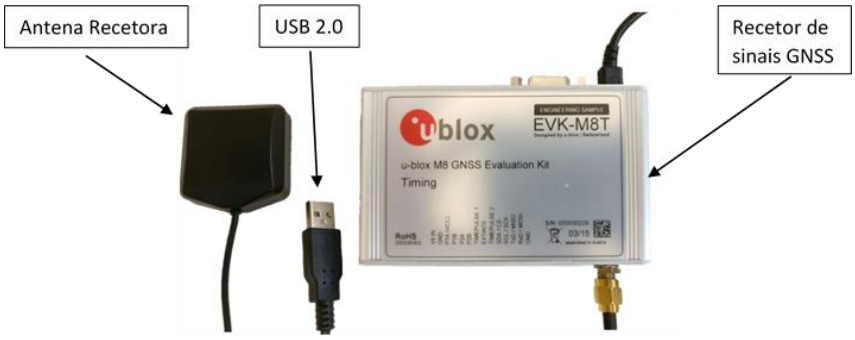

Figura 3.10 - Hardware que constituí o Ublox

Para realizar o protótipo e criar um produto móvel e leve, podendo ser manuseável por um operador, o processamento dos sinais foi desenhado para poder ser feito por um Raspberry Pi 3 (Figura 3.11). O Raspberry Pi 3 *model* B contém um processador 1.2GHz 64-bit quad-core ARMv8 CPU, 1 GB de RAM e Bluetooth 4.1. Conectados ao Raspberry Pi estão vários sensores e LEDs indicativos, que serão descritos no Anexo B.

Figura 3.11 - Raspberry Pi 3 model B

3.2.2 *Software*

Uma das ferramentas de desenvolvimento de *software* para implementação do SDR é o GNU Radio, licenciado pela GPL (*General Public License*). O GNU Radio é muito utilizado por ser uma biblioteca de *software* aberta operando com processamento de sinais digitais e fluxo de dados. Os blocos de processamento de sinais digitais são escritos na linguagem C++ e a linguagem Phython é utilizada para criar uma rede interligando os blocos entre si. Para uma interface mais apelativa para o programador a programação pode realizada por blocos, usando o *GNU Radio Companion* (GRC), como é possível verificar na Figura 3.12 [33].

Para conseguir programar algumas técnicas de *jamming* abordadas ao longo da dissertação foi necessário recorrer a programação em linguagem Python.

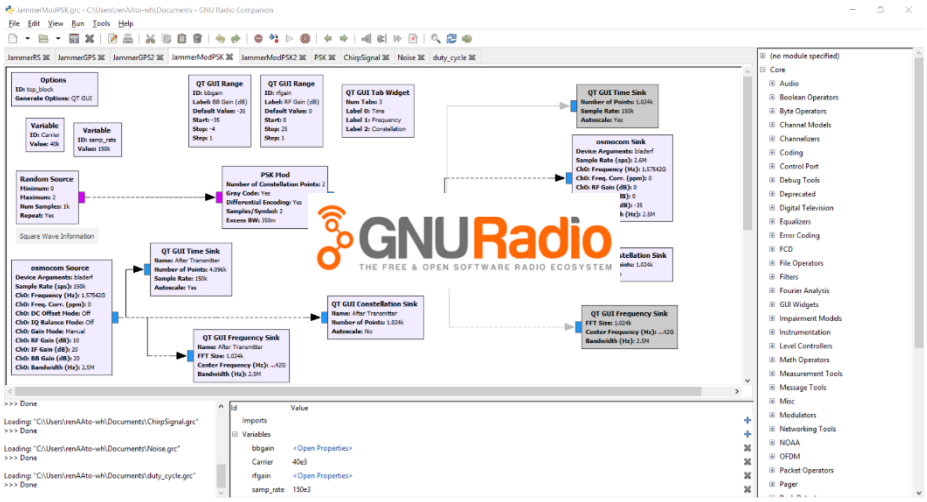

Figura 3.12 - Interface GNU Radio

Para permitir detetar mais facilmente se existe algum problema de programação/configuração no transmissor (*jammer* desenvolvido) e não no recetor, utilizou-se uma plataforma já criada, o SDR Sharp.

O SDR Sharp é uma aplicação para DSP (*Digital Signal Processing*), *open source* e de fácil configuração. O principal objetivo é oferecer uma simples aplicação de técnicas de DSP. A interface do SDR Sharp está espelhada na Figura 3.13.

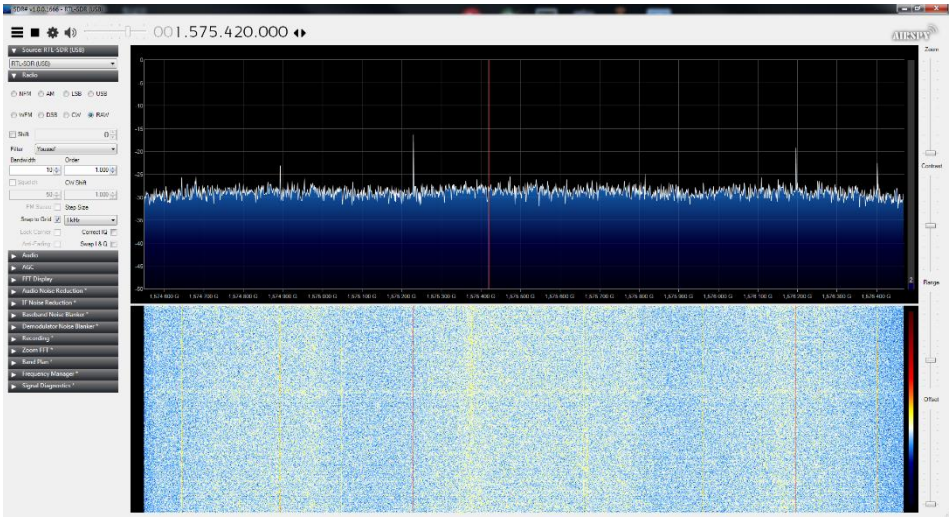

Figura 3.13 - Interface SDR Sharp

O *software* U-Center é uma ferramenta poderosa para avaliação, análise de desempenho e configuração de recetores GNSS da u-blox. Os recetores GNSS da u-blox podem ser configurados utilizando o *software* de avaliação U-Center (Figura 3.14).

Esta ferramenta foi utilizada tanto para testes em ambiente controlado como em ambiente real.

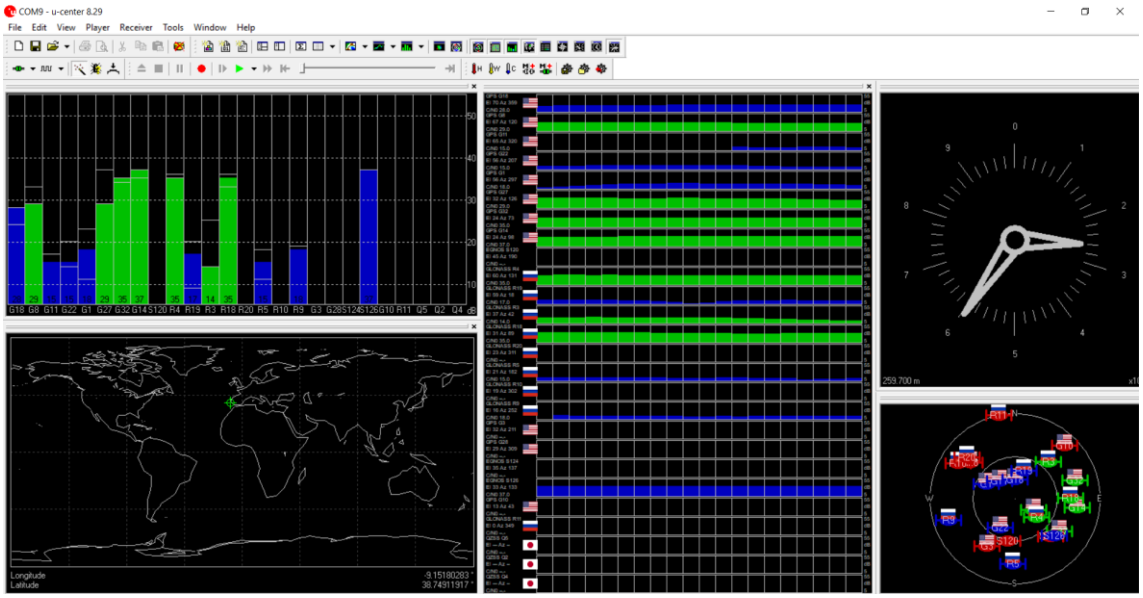

Figura 3.14 - Interface U-Center

3.3 Várias Técnicas de *Jamming*

O *jamming* de sinal GPS é possível recorrendo a várias técnicas introduzidas brevemente no capítulo 2. Apresentam-se em seguida os detalhes relativos à implementação das cinco técnicas diferentes de interferir com o sinal GPS.

3.3.1 *Barrage Jamming*

O *Barrage Jamming*, recorrendo a informação teórica, é o melhor *jammer* que se pode fazer na ausência de qualquer conhecimento do sinal alvo [34]. O bloqueio completo de redes sem fio pode ser realizado através da geração de um ruído contínuo com potência acima do que o sistema suporta. O lado negativo desta abordagem é a alta energia despendida, o que contribui para uma baixa eficiência energética, e o facto de não ser possível selecionar quais os sinais que se pretende afetar na banda RF utilizada. Ao aplicar esta técnica para bloqueio de sinal GPS, esta última restrição não é um entrave, uma vez que o que se pretende afetar é a totalidade da banda de frequência do GPS.

A construção do sinal a transmitir é representada na Figura 3.15 onde é gerado ruído do tipo Gaussiano, através do bloco *Noise Source*, e transmitido em toda a largura de banda do sinal GPS da banda L1, com uma frequência central de 1.57542 GHz e uma largura de banda de 14 MHz, recorrendo ao bloco *Osmocom Sink*, responsável pela transmissão. O sample rate é o programado com o máximo permitido pelo processamento, 8 MHz, sendo que a BladeRF consegue no seu máximo 40 MHz.

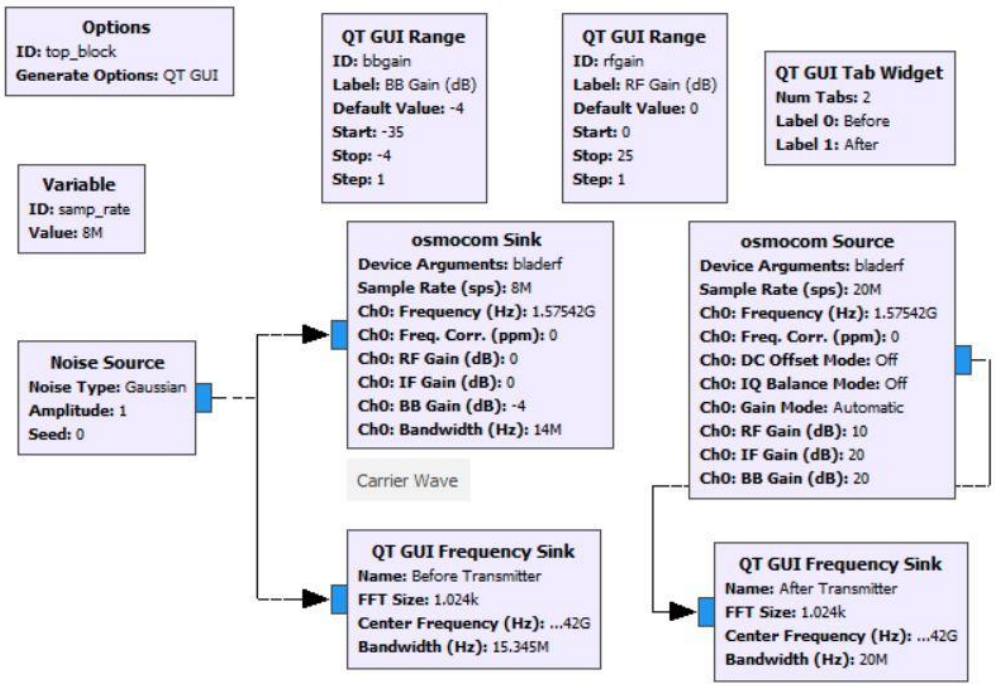

Figura 3.15- Programação GNU Radio do Barrage Jamming

Recorrendo ao bloco *osmocom Source*, bloco responsável pela receção da BladeRF, consegue-se analisar o sinal interligando esse mesmo bloco ao *QT GUI Frenquency Sink* para se poder representar o espectro do sinal transmitido (Figura 3.16).

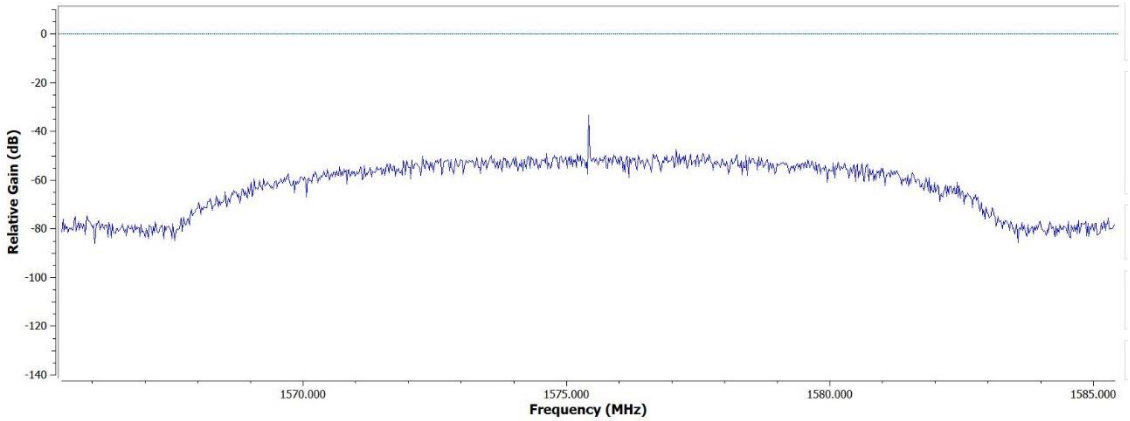

Figura 3.16 - Espectro resultante do Barrage Jamming

O resultado no espectro está de acordo com a teoria, tendo este sinal uma largura de banda de 14 MHz e uma densidade espectral de potência média de -60 dBW/Hz. Na frequência central existe um pico máximo devido ao problema, já anteriormente indicado, do DC Offset. Este problema reside em todas as técnicas apresentadas seguidamente.

3.3.2 *Sweep Jamming*

Para a realização da técnica *Sweep Jamming* é necessário criar um *Chirp Signal*, um sinal que aumenta ou diminui a sua frequência no tempo. O resultado ao nível de espetro é o varrimento de uma gama de frequências. O GNU Radio não permite uma aplicação direta para o desenvolvimento deste tipo de sinal. A solução foi criar um sinal cuja frequência de transmissão varia em tempo real através de um *slider*. Para um sistema mais autónomo e porque a utilização do *slider* produz atrasos, isto é, uma variação de frequências muito lenta, foi portanto exportado o código Python e modificado para realizar este mesmo efeito automaticamente e de uma forma mais dinâmica, programando linguagem Python.

A construção do sinal a transmitir é representada na Figura 3.17, onde é gerado uma sinusoide, através do bloco *Signal Source*, e é transmitida com uma largura de banda mínima suportada pela BladeRF, 1.5 MHz. Sabendo que a largura de banda do sinal GPS é de 15.345 MHz, são calculados os limites do *slider* (varia entre os 1.5678 GHz e 1.5831 GHz, com saltos de 10 kHz) como é demonstrado seguidamente pelas equações (11) e (12). O sample rate é o programado com máximo permitido pelo processamento, 8 MHz, sendo que a BladeRF consegue no seu máximo 40 MHz.

$$f_{min} = fc - \frac{LB}{2} = 1.57542 \times 10^9 - \frac{15.345 \times 10^6}{2} = 1.5678\ GHz \qquad (11)$$

$$f_{máx} = fc + \frac{LB}{2} = 1.57542 \times 10^9 + \frac{15.345 \times 10^6}{2} = 1.5831\ GHz \qquad (12)$$

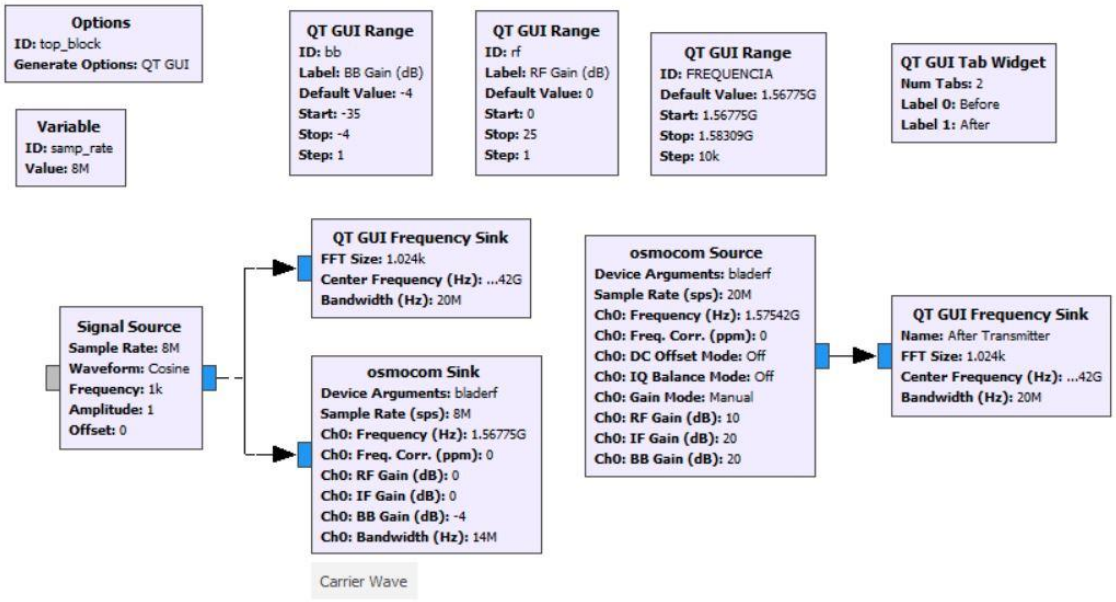

Figura 3.17 - Programação GNU Radio do Sweep Jamming

O resultado no espetro da frequência num ponto estático do *slider* está representado na Figura 3.18.

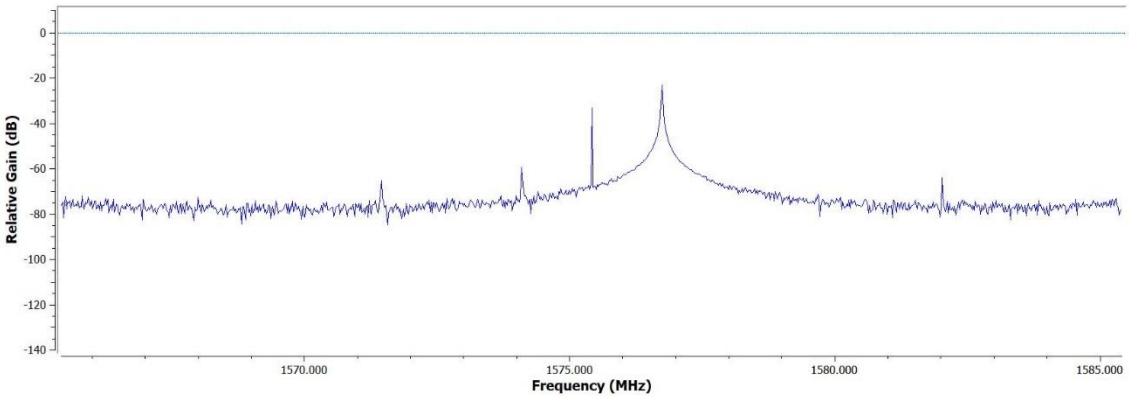

Figura 3.18 - Espectro resultante do Sweep Jamming

O espectro apresentado na Figura 3.18 é apenas um instante no tempo do espectro real, pois o varrimento de frequência é demasiado rápido para ser notado a olho nu. Com este rápido varrimento poder-se concluir que o sinal tem uma densidade espectral de potência média de -50 dBW/Hz e uma largura de banda de 15.3 MHz (sabendo que na realidade o sinal apenas tem 1.5 MHz de largura de banda).

Durante a realização de testes desta técnica identificou-se um problema. Devido à alteração da frequência a transmitir no bloco *osmocom Sink*, este introduz um atraso fazendo com que o *jammer* perca eficiência. A solução encontrada passa por permutar a frequência da sinusoide a transmitir (bloco *Signal Source*), ao invés de alterar a frequência da portadora (bloco *osmocom Sink*), como demonstra a Figura 3.19.

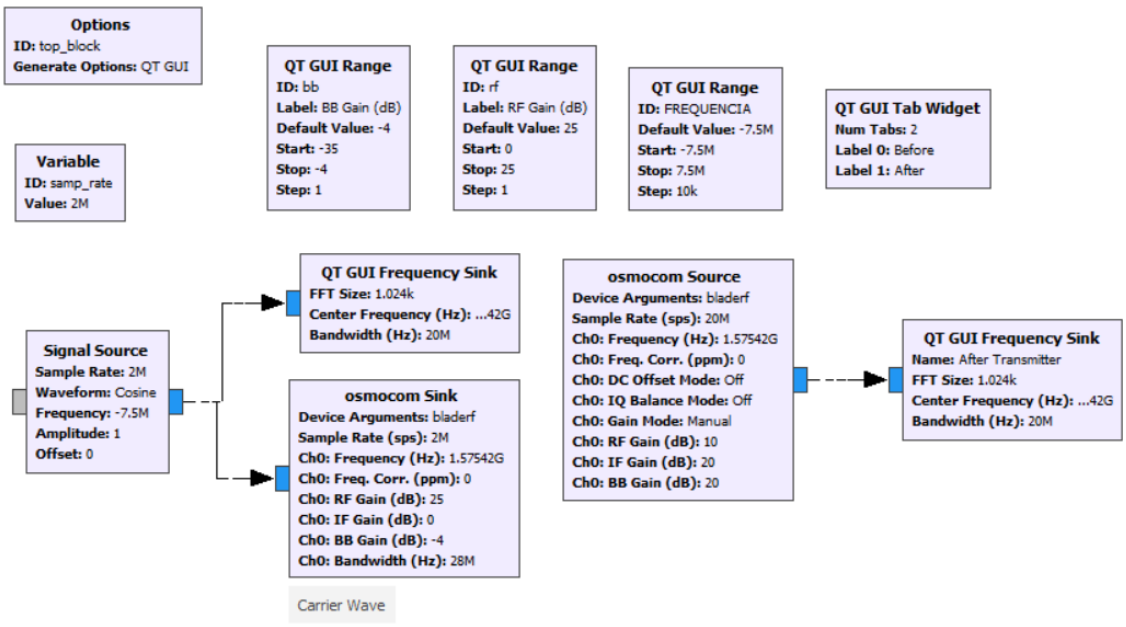

Figura 3.19 - Programação GNU Radio do Sweep Jamming 2

A frequência central permanece fixa, 1575.42 MHz, enquanto a sinusoide varia entre os -7.5 MHz e os 7.5 MHz da frequência central, ficando este *jammer* com uma ocupação de 15 MHz de largura de banda.

O resultado do espectro do recetor encontra-se na Figura 3.20, onde existe um varrimento no espectro, embora a figura apenas represente um instante em que a frequência do bloco *Signal Source* é de -5.42 MHz ficando com o resultado de 1570 MHz.

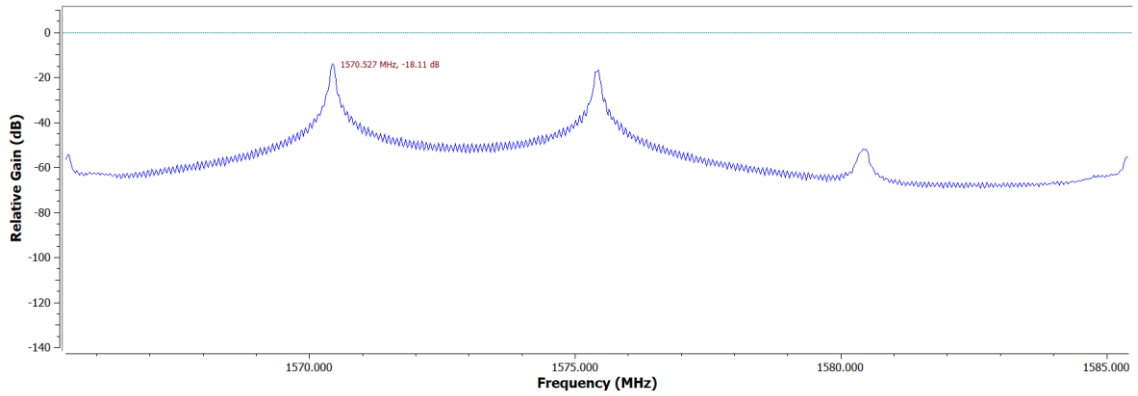

Figura 3.20 - Espectro resultante do Sweep Jamming 2

Através desta solução é possível resolver uma limitação de *hardware* que não permitia a implementação eficiente do *Chirp Signal*. As diferenças entre o problema identificado e a solução apresentada podem ser observadas através do SDR Sharp com um espetro do tipo *waterfall*. Na Figura 3.21 é expresso o problema identificado e na Figura 3.22 a solução apresentada.

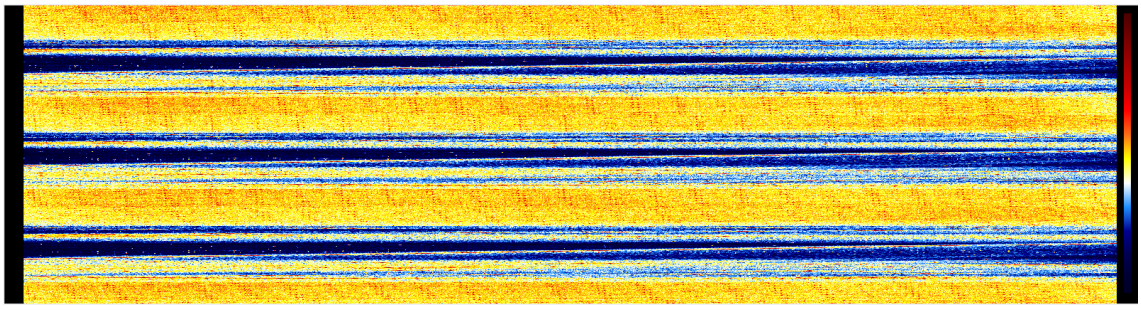

Figura 3.21 - Espectro waterfall Sweep Jamming

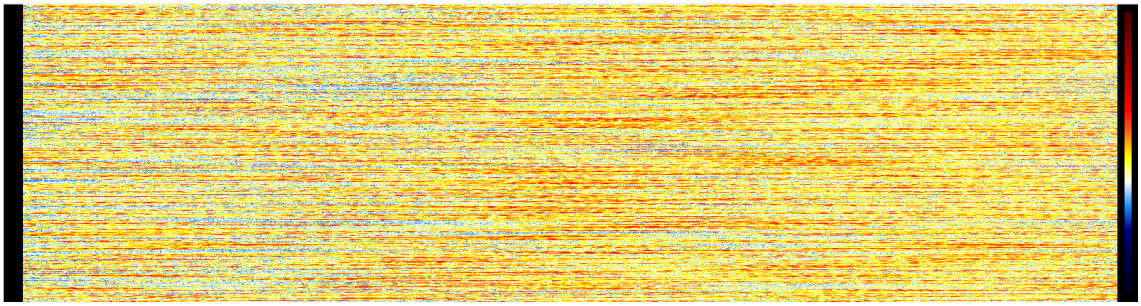

Figura 3.22 - Espectro waterfall Sweep Jamming 2

Na Figura 3.21 é notório o espaço de tempo em que a BladeRF não está a transmitir, representado a cor azul. Enquanto que na solução apresentada na Figura 3.22 o mesmo não acontece e entende-se que a BladeRF está constantemente em transmissão. A análise deste tipo concreto de espectro (*waterfall*) é analisado na frequencia portadora, 1575.42 MHz para ambos os casos.

3.3.3 *Successive Pulses Jamming*

Esta técnica consiste em enviar um sinal com impulsos no tempo com baixo *duty cycle*, na frequência do sinal GPS 1.57542 GHz, ocupando toda a sua largura de banda, 14 MHz, que resulta no esquema desenhado na Figura 3.23. O sample rate é o programado com máximo permitido pelo processamento 8 MHz, sendo que a BladeRF consegue no seu máximo 40 MHz.

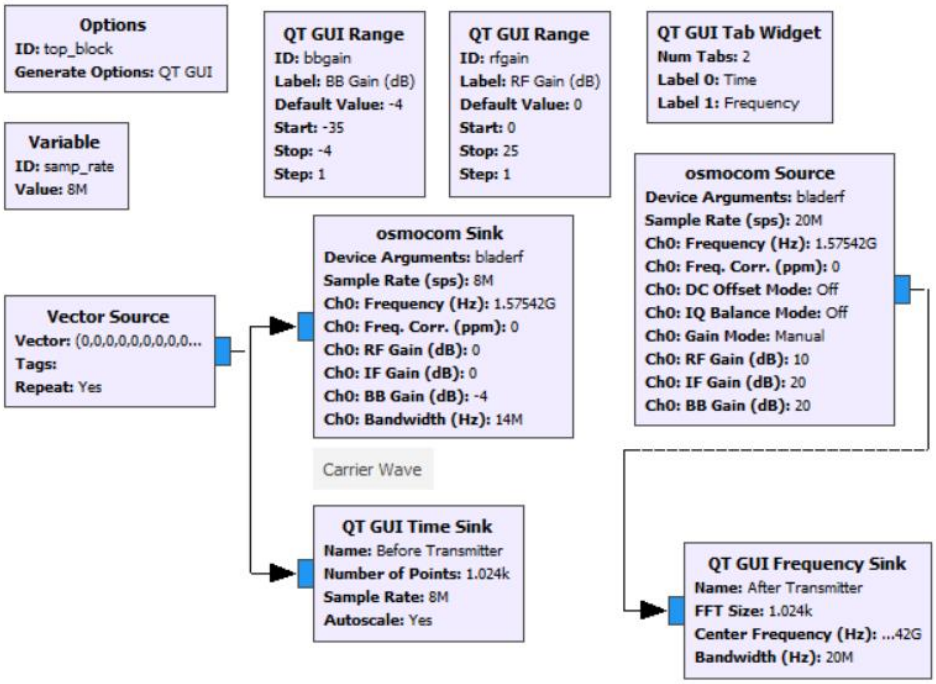

Figura 3.23 - Programação GNU Radio do Successive Pulses Jamming

Para se conseguir gerar um sinal com baixo *duty cycle* no tempo, emite-se um vetor com a seguinte configuração: [0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1], através do bloco *Vector Source*, podendo-se afirmar que o *duty cycle* deste sinal é de 2%, como se pode verificar na Figura 3.24.

O resultado do espectro no recetor é o apresentado na Figura 3.25.

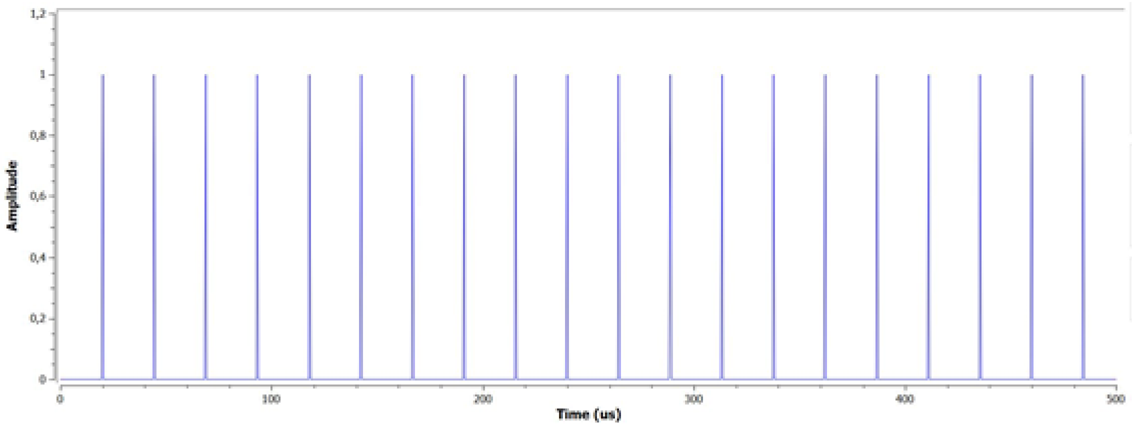

Figura 3.24 - Impulsos no tempo com baixo duty cycle

Impulsos com periocidade de cerca de 24 us e de amplitude 1.

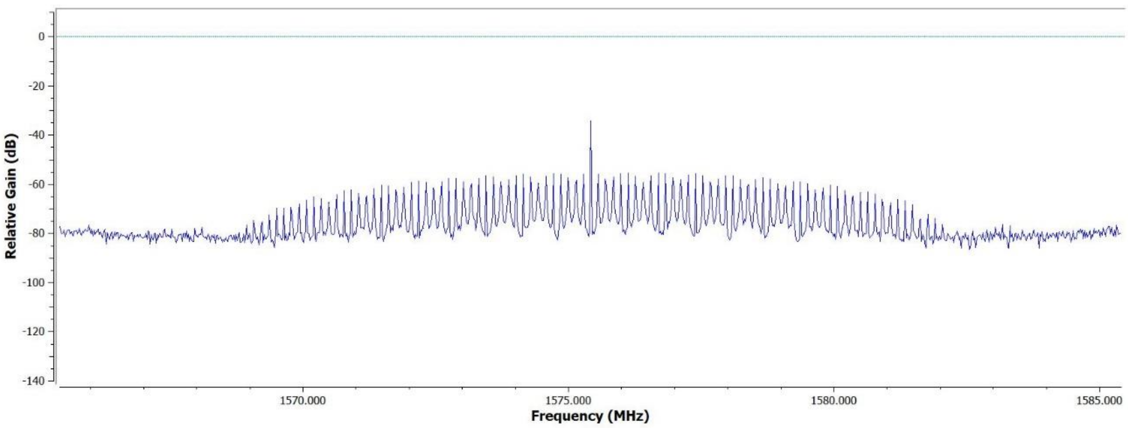

Figura 3.25 - Espectro resultante do Successive Pulses Jamming

Apesar do resultado do *Successive Pulse Jamming* ocupar toda a largura de banda do sinal GPS, não o faz uniformemente como é possível verificar na Figura 3.25, o que poderá diminuir a sua eficiência como *jammer*. A densidade espectral de potência média é de cerca de -70 dBW/Hz, valor um pouco inferior aos restantes.

3.3.4 *Tone Jamming*

O modelo de *Tone Jamming* desenvolvido é mostrado na Figura 3.26. É gerado uma sinusoide (bloco *Signal Source*) e transmitida na frequência central do GPS, 1.57542GHz.

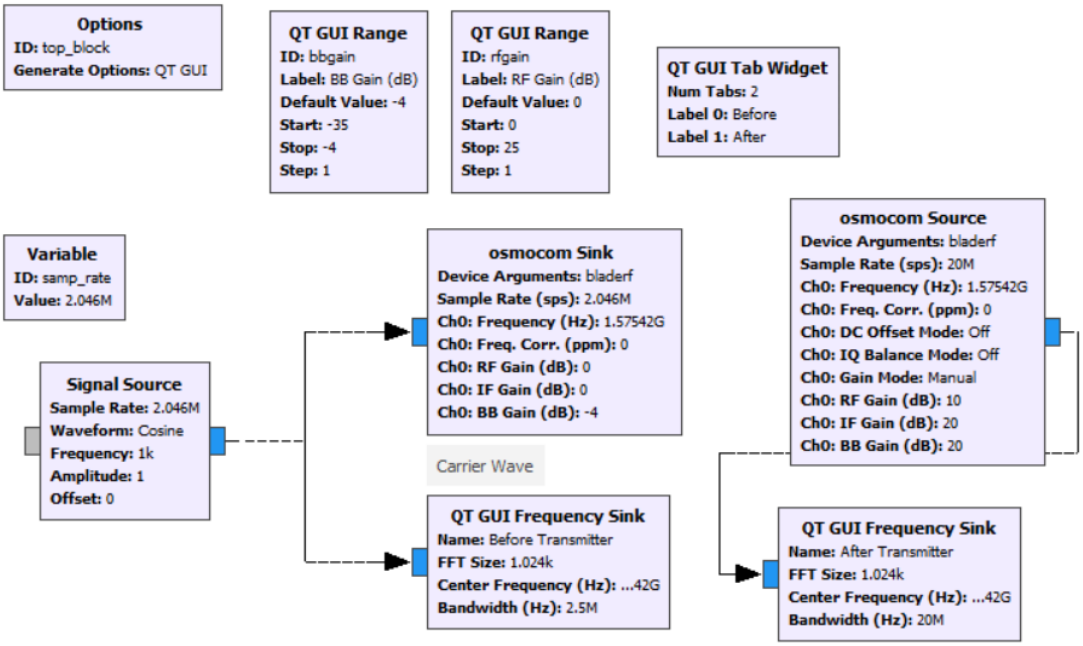

Figura 3.26 - Programação GNU Radio Tone Jamming

Os resultados da interferência são mostrados na Figura 3.27. Embora o sinal seja eficiente para interferir com o sistema é certo que não ocupa toda a banda do sinal GPS, sendo isso uma das possíveis desvantagens, principalmente porque o sinal GPS é *Spread Spectrum*. A densidade espectral de potência média é de -50 dBW/Hz.

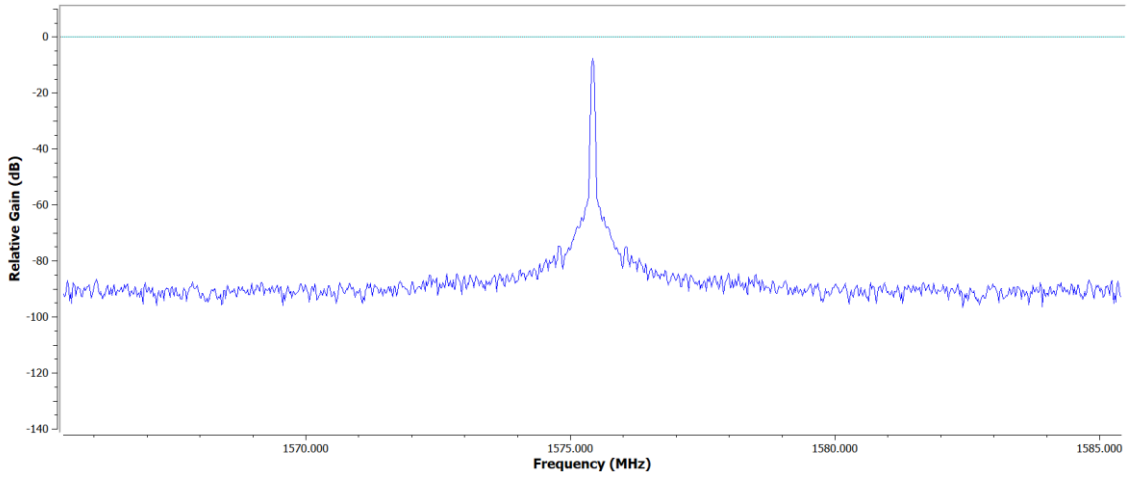

Figura 3.27 - Espectro resultante do Tone Jamming

3.3.5 *Protocol-Aware Jamming*

A viabilidade do uso de *jammers* com reconhecimento de protocolo tem sido estudada principalmente em sistemas de comunicação de rede local sem fio baseados em IEEE 802.11. Concluiu-se que estes podem atingir interferência com requisitos de energia muito baixos e baixa probabilidade de deteção do protocolo [35] [36]. Os *jammers* com o reconhecimento de protocolo evitam também a interferência em outros sistemas de comunicação que operam na mesma banda de RF.

A composição do sinal a transmitir é representada na Figura 3.28 começando por criar uma fonte aleatória de bits, 0s e 1s, que são convertidos em *float*, aplicando o bloco *UChart To Float*. Para se poder mapear esses 0s e 1s para -1s e 1s, respetivamente, multiplica-se por 2 e seguidamente adiciona-se -1 $([0\ 1] \times 2) - 1 = [0\ 2] - 1 = [-1\ 1]$.

Só é possível transmitir o sinal se este for convertido para complexo, uma vez que o bloco *osmocom Sink* apenas recebe um complexo, sendo este o bloco responsável pela transmissão de sinais da BladeRF. Na parte real consta o sinal modulado e a parte imaginária é nula, adicionado portanto a constante 0, pois o sinal GPS L1 não é representado com sinal em quadratura. O *sample rate* é o programado com 1.023MHz, como o sinal GPS.

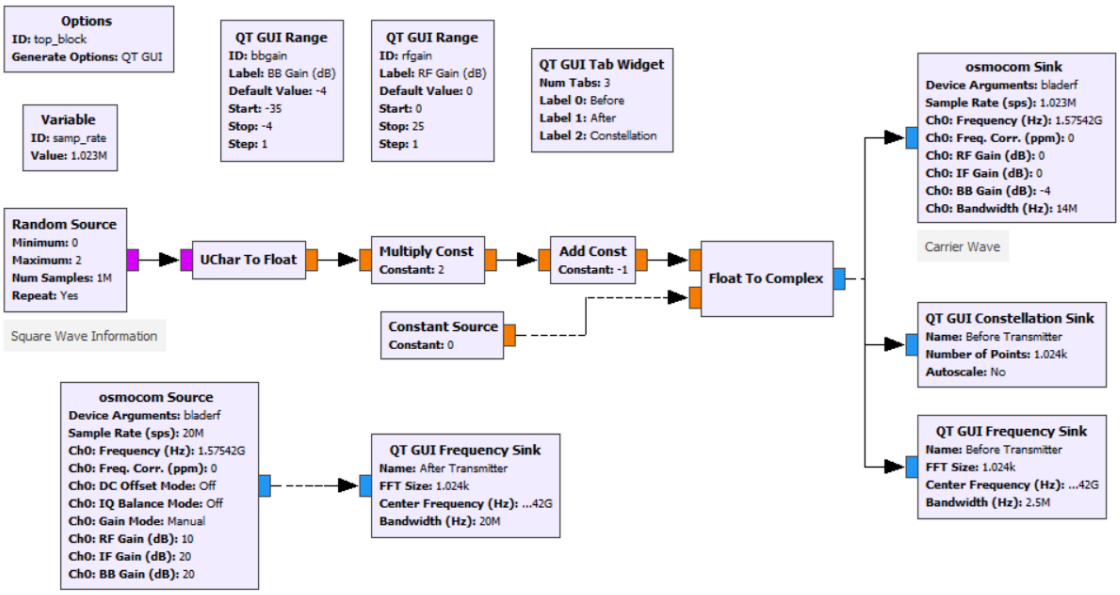

Figura 3.28 - Programação GNU Radio do Protocol-Aware Jamming

Na Figura 3.29 é possível observar o comportamento da fonte de bits aleatória de 0s e 1s, (Figura 3.29 a)) depois das operações para os 0s e 1s corresponderem a -1s e 1s respetivamente representados na Figura 3.29 b).

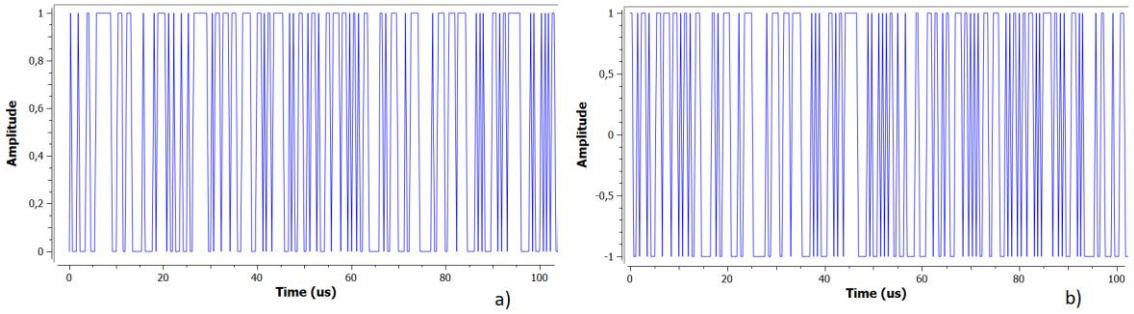

Figura 3.29 - a) Random Source [0 1] b) Random Source [-1 1]

O resultado da onda modulada em BPSK na receção é a demonstrada na Figura 3.30, sinal *jammer* recebido com ruído AWGN.

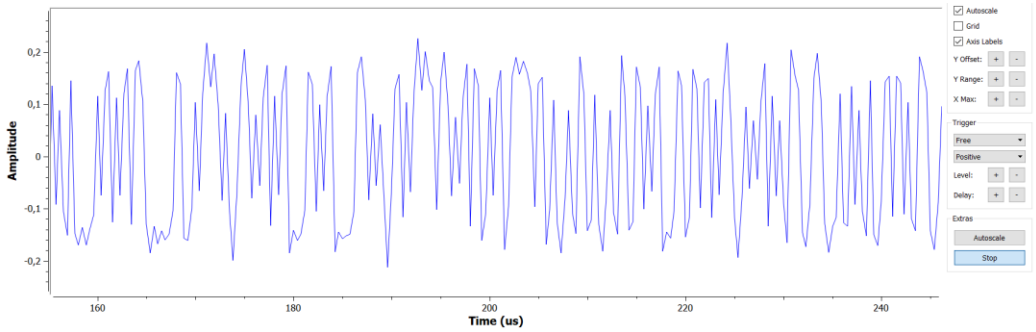

Figura 3.30 - Receção do Protocol-Aware Jamming no tempo

A constelação digital BPSK é expressa através do bloco *QT GUI Constellation Sink* e representada na Figura 3.31.

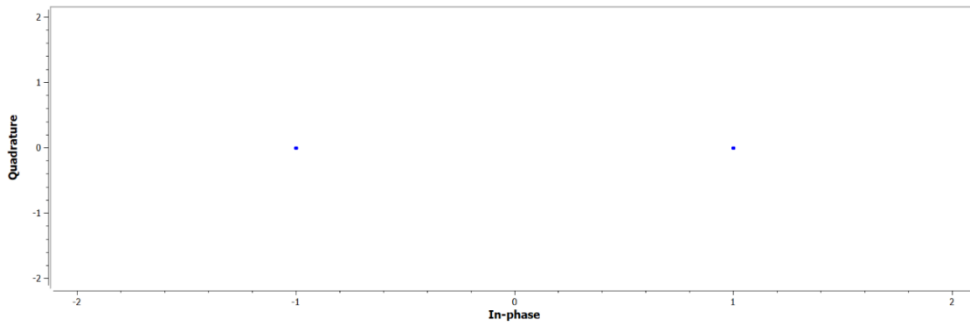

Figura 3.31 - Constelação BPSK

O resultado no espetro da frequência depois de recebido consta na Figura 3.32. A densidade espectral de potência média é de -60 dBW/Hz.

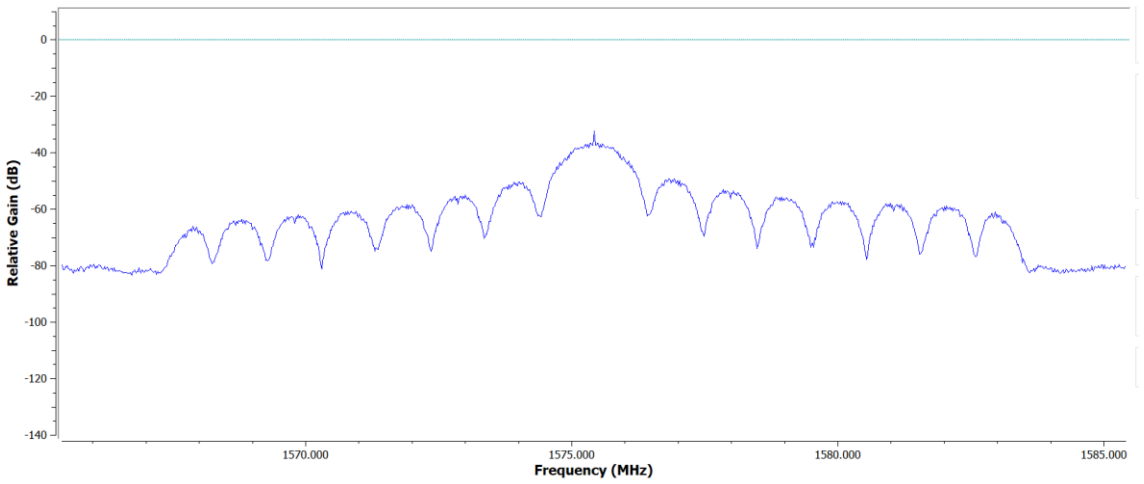

Figura 3.32 - Espetro resultante do Protocol-Aware Jamming

Outra solução para este tipo de *jammer* é recorrer a um simulador de sinais de GPS e utilizar uma mensagem com uma localização inexistente. O simulador usado é o GPS-SDR-SIM que gera fluxos de dados de sinal de banda base de GPS, que podem ser convertidos em RF usando plataformas de rádio definidas por *software* (SDR) como ADALM-Pluto, BladeRF, HackRF e USRP.

A mensagem é criada através de um ficheiro .txt e é baseada em outras mensagens criadas pelo simulador sendo depois adaptada à situação em causa. Exemplo de uma linha da mensagem .txt:

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

De assinalar que os dígitos sublinhados são as coordenadas de um ponto que não existe no planeta Terra e portanto com isso consegue-se baralhar o recetor GPS, traduzindo-se num sinal *jammer* GPS.

O espectro resultante encontra-se na Figura 3.33, onde se pode verificar que é bastante semelhante ao anteriormente criado (Figura 3.32). A densidade espectral de potência média é um pouco inferior a -60 dBW/Hz.

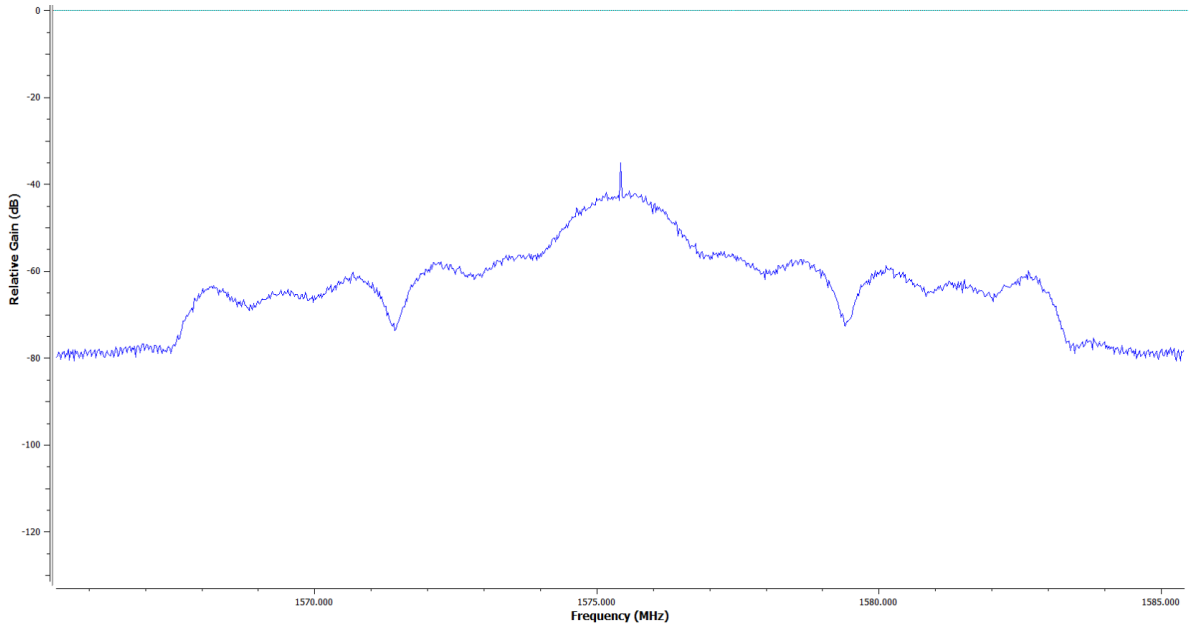

Figura 3.33 - Espetro resultante do Protocol-Aware Jamming 2

O espectro resultante da primeira abordagem (Figura 3.32) origina um espectro mais semelhante ao espectro teórico do GPS representado na Figura 4.8.

Capítulo 4

4. Avaliação Experimental dos *Jammers*

Este quarto capítulo consiste na avaliação experimental das técnicas abordadas no capítulo 3. Pretende-se avaliar o comportamento de cada técnica e concluir qual o melhor sinal a transmitir, para interferir com o sinal GPS, tendo em conta a eficiência energética e a efetividade do *jamming* do ponto de vista do alcance máximo conseguido.

4.1 Recetor GPS

A u-blox disponibiliza o *software* U-Center para a visualização dos dados em tempo real, como demonstra a Figura 4.1.

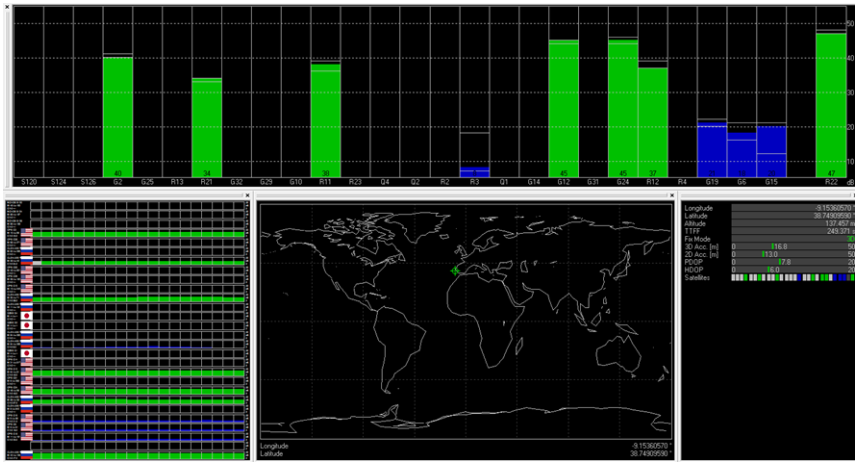

Figura 4.1 - U-Center Interface

Através desta ferramenta é possível saber quais os satélites que estão a ser detetados pelo recetor, a sua localização, bem como a qualidade do sinal GPS.

4.2 Configuração do *Jammer*

Para se perceber qual o melhor sinal *jammer* do sinal GPS, tendo em conta a densidade espectral de potência, realizam-se vários testes com recurso às técnicas abordadas anteriormente e com distância distintas.

Para analisar a densidade espectral de potência dos vários tipos de *jammers*, é conectado à BladeRF a antena recetora para uma análise do espetro no GNU Radio com a seguinte configuração demonstrada na Figura 4.2. Só é permitido esta configuração devido à BladeRF ser um transcetor.

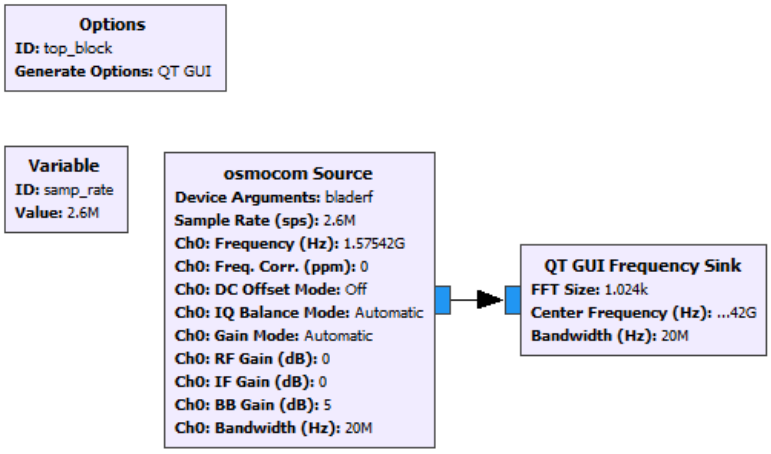

Figura 4.2 - Análise espectral GNU Radio

A Figura 4.3 representa a configuração do *jammer* criado. A alimentação da BladeRF é através do USB do computador.

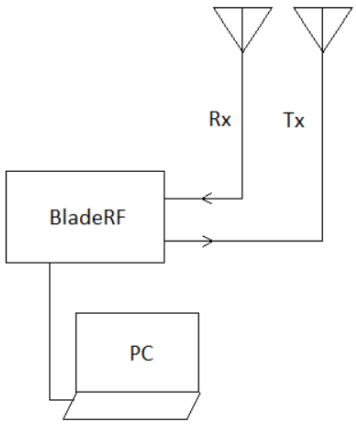

Figura 4.3 - Diagrama de blocos do emissor (jammer)

A BladeRF possui *Variable Gain Amplifier* (VGA) no módulo de transmissão, TXVGA1 para BB (*Base Band*) Gain e TXVGA2 para RF (*Radio Frequency*) Gain. Para uma explicação mais clara é apresentado o diagrama de blocos do LMS6002D.

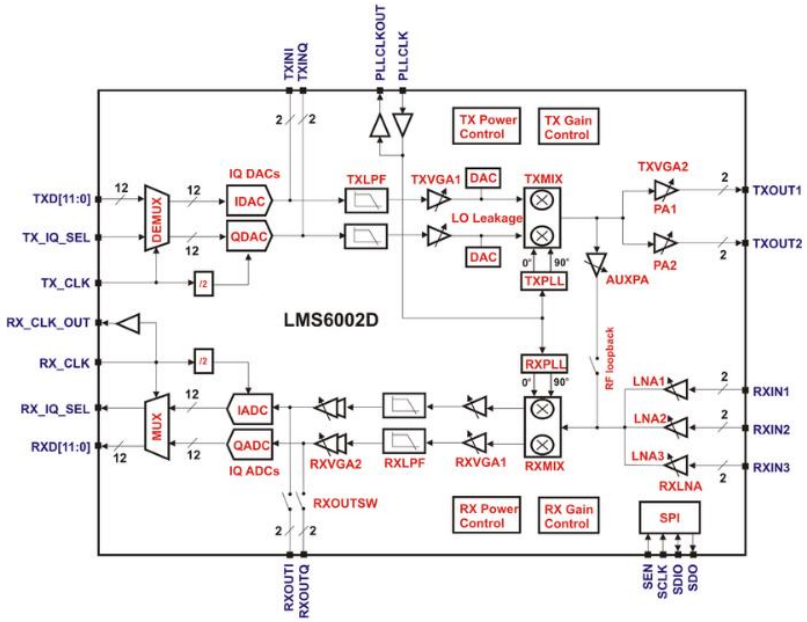

Figura 4.4 - Diagrama de blocos do LMS6002D [37]

Geralmente, o TXVGA1 deve ser aumentado antes do TXVGA2. *Sliders* para estes parâmetros foram fornecidos na GUI, através do bloco *QT GUI Range*.

Analisando a densidade espectral de potência das 4 técnicas apresentadas para *jamming* do sinal GPS, com os ganhos TXVGA1 e TXVGA2 no máximo, -4 dB e 25 dB respetivamente, é possível apresentar a tabela 1. A densidade espectral de potência apresentada na tabela 1 é referente à potência máxima, isto é, na frequência central (1575.42MHz).

Tab. 2 - Densidade espectral de potência dos vários jammers

	Densidade Espectral de Potência Máxima Medida	Densidade Espectral de Potência Média
Barrage *Jamming*	-28 dBW/Hz	-60 dBW/Hz
Sweep Jamming	-8 dBW/Hz	-50 dBW/Hz
Successive Pulses Jamming	-24 dBW/Hz	-70 dBW/Hz
Tone Jamming	2 dBW/Hz	-50 dBW/Hz
Protocol-Aware Jamming	-14 dBW/Hz	-60 dBW/Hz

O resultado das potências medidas vão ao encontro com a parte teórica, em que os sinais mais fracos são os de *Barrage Jamming* e *Successive Pulses Jamming*, devido a usarem todas a gama de frequência do GPS, isto é 14 MHz disponíveis pela BladeRF. O facto do *Successive*

Pulses Jamming corresponder a um valor um pouco superior ao do *Barrage Jamming* deve-se a que, mesmo ocupando os 14 MHz, não o faz de forma uniforme. Embora o *Protocol-Aware Jamming* use também os 14 MHz de largura de banda contém um sample rate mais baixo que os referidos anteriormente, sendo que assim concentra mais energia na frequência central, por essa razão conseguir obter densidade espectral de potência mais elevada. O *Tone Jamming* é o que apresenta uma densidade de potência elevada concentrada numa zona pequena do espectro. O *Sweep Jamming* na teoria, deveria obter valores iguais ao *Tone Jamming*, uma vez que são exatamente iguais, embora o *Sweep Jamming* faça o varrimento na frequência. Isso não se verifica devido ao efeito de erro de *DC Offset*.

4.3 Configuração do GPS Falso

Para assegurar que as condições dos vários testes são as mesmas, optou-se por não se utilizar os sinais de GPS reais, porém emitir um sinal de GPS falso. Isto para garantir que a intensidade e qualidade de receção é a mesma, visto que ao longo do dia estes dois fatores alteram-se usando os sinais de GPS reais, devido às orbitas dos satélites. Algumas configurações de equipamento estão expressas no Apêndice A.

A Figura 4.5 representa o formato do recetor GPS, bem como a emissão do sinal GPS falso.

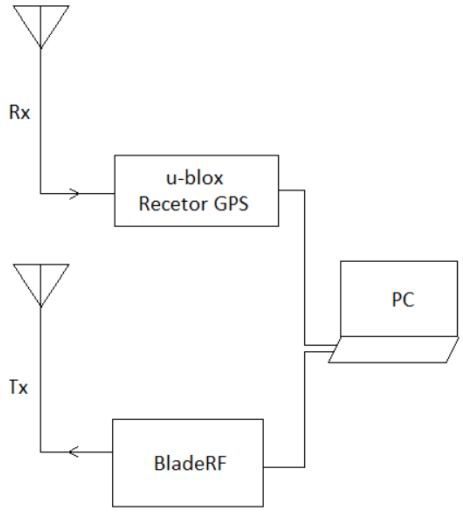

Figura 4.5 - Diagrama de blocos do recetor juntamente com o GPS falso

Através de um ficheiro efemérides de transmissão GPS especifica-se a constelação de satélites GPS a usar. As efemérides contêm informações referentes à posição e ao erro do relógio dos satélites necessários no posicionamento.

A emissão do sinal de GPS falso foi baseada no software GPS-SDR-SIM disponível no github no seguinte endereço: https://github.com/osqzss/gps-sdr-sim.

Para criar o ficheiro de localização estática, escolheu-se um ponto de localização que nada tem a ver com a localização real (Brasil). A interface de linha de comandos BladeRF requer pares de I/Q armazenados como inteiros de 16 bits, que é o que se encontra por predefinição.

Na Figura 4.6 estão demonstradas as diversas opções de configuração do GPS-SDR-SIM, podendo criar ficheiros .txt de localização estática ou dinâmica.

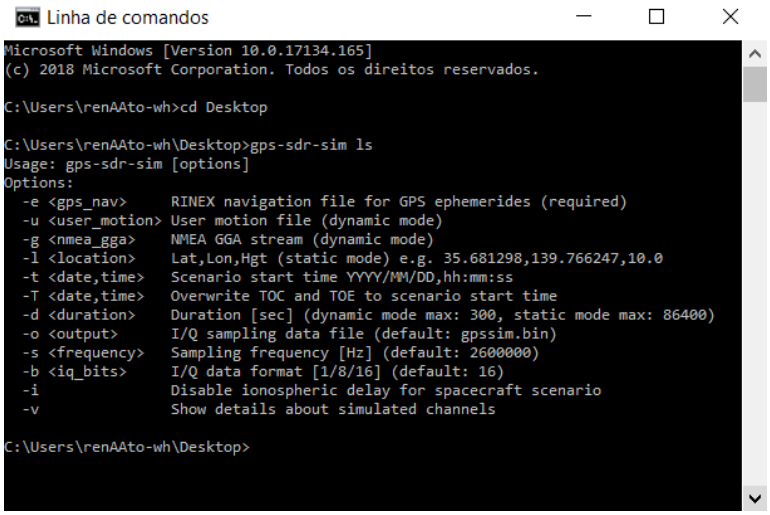

Figura 4.6 - Opções de configuração do GPS-SDR-SIM

Através da linha de comandos na diretoria onde se encontram os ficheiros brdc3540.14n (efemérides de satélite GPS, mensagens de 20 de dezembro de 2014) e GPS-SDR-SIM, executam-se os códigos seguindo as opções da Figura 4.6.

```
> gps-sdr-sim.exe -e brdc3540.14n –l -5.438965,-64.843601,10.0
```

O ficheiro de sinal GPS simulado, chamado "gpssim.bin", pode ser carregado na BladeRF para transmissão. A transmissão do sinal de GPS falso é feita com as seguintes configurações na aplicação BladeRF CLI ou na linha de comandos acedendo por:

```
> bladerf-cli –i
```

```
> set frequency tx 1575.42M
> set samplerate 2.6M
> set bandwidth 14M
> set txvga1 -35
> cal lms
> cal dc tx
> tx config file=C:\Users\renato\Desktop\gpssim.bin format=bin
> tx start
```

A BladeRF requer uma taxa de amostragem de 2,6 MHz e o tempo máximo *de* duração da simulação é definido por USER_MOTION_SIZE para evitar que o arquivo de saída fique com um tamanho demasiado grande. Através dos comandos: **>cal lms; >cal dc tx;** a BladeRF realiza a calibração automática de *DC Offset* e *IQ Imbalance.*

O resultado no recetor consta na Figura 4.7, com o *spoofing* do sinal GPS.

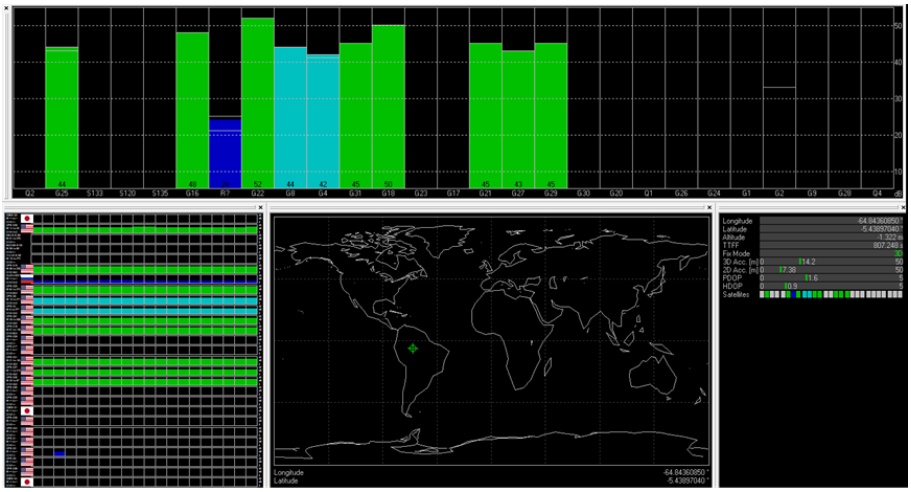

Figura 4.7 - Spoofing do sinal GPS

É importante emitir o sinal de GPS simulado a uma potência credível, tendo em conta a potência recebida por um sinal de GPS real. Para isso recorreu-se a algumas equações.

O processo começa com o sinal GNSS propagando-se pelo espaço até incidir na antena recetora GNSS do utilizador. A potência recebida é extremamente fraca, correspondendo a uma potência de sinal garantida de -160 dBW no caso do Sistema de Posicionamento Global (GPS) e tem uma frequência de portadora de 1575,42MHz. Considerando uma largura de banda de 2 MHz (a largura de banda aproximada *null-to-null* do sinal de código GPS C/A), a potência do sinal GPS recebido é realmente inferior à potência de ruído térmico, conforme definido pela equação (13) com uma ilustração simplificada na Figura 4.8 [38].

$$P_{Ruído\ Térmico} = k_B.T.\Delta f \ \ (W) \tag{13}$$

$k_B \rightarrow constante\ de\ Boltzmann\ em\ joules\ por\ kelvin$
$T \rightarrow \ temperatura\ absoluta\ da\ resistência\ em\ kelvins$
$\Delta f \rightarrow largura\ de\ banda\ em\ hertz\ sobre\ a\ qual\ o\ ruído\ é\ medido$

Cálculo do ruído térmico expresso na equação (14):

$$P_{Ruído\ Térmico} = 1.38 \times 10^{-23} \times 290 \times 2 \times 10^{6} = 8 \times 10^{-15}\ W \tag{14}$$

Ruído térmico em dB e dBm definido na equação (15):

$$P_{Ruído\ Térmico} = 10\log(8 \times 10^{-15}) = -140.97dBW = -110.97dBm \quad (15)$$

Sabendo que as potências de emissão dos satélites de GPS são entre 20 W a 50 W, com uma antena de transmissão com ganho de 12 dB [39] e que os satélites se localizam a 20 200 km de altura (90° de elevação), calcula-se a potência máxima recebida na superfície terrestre recorrendo à equação (16), perdas em espaço livre:

Modelo de perdas em espaço livre:

$$L_{fs} = \frac{(4\pi)^2 d^2}{\lambda^2} = \frac{(4\pi)^2 d^2}{\left(\frac{c}{f}\right)^2} \quad (16)$$

$c \rightarrow velocidade\ da\ luz$
$k_B \rightarrow frequência\ do\ sinal$
$d \rightarrow distância\ em\ metros$

Cálculo das perdas em espaço livre expresso na equação (17):

$$L_{fs} = \frac{(4\pi)^2 \times (20\ 200 \times 10^3)^2}{\left(\frac{3 \times 10^8}{1.57542 \times 10^9}\right)^2} = 1.78 \times 10^{18} \quad (17)$$

Representação das perdas em dB através da equação (18):

$$L_{dB} = 10\log_{10}(L) = 10\log_{10}(1.78 \times 10^{18}) = 182.5\ dB \quad (18)$$

Representação da potência máxima emitida pelo satélite GPS em dBW, equação (19):

$$P_{TXmax}\ (dB) = 10\log_{10}(50) = 17\ dBW \quad (19)$$

Considerando a potência transmitida e tendo em conta as perdas em espaço livre calculadas anteriormente, pode-se obter facilmente a potência recebida recorrendo as equações (20):

$$P_{Rx} = P_{Tx} + G_{Tx} - L_{fs} = 17 + 12 - 182.5 = -153.5\ dBW = -123.5dBm \quad (20)$$

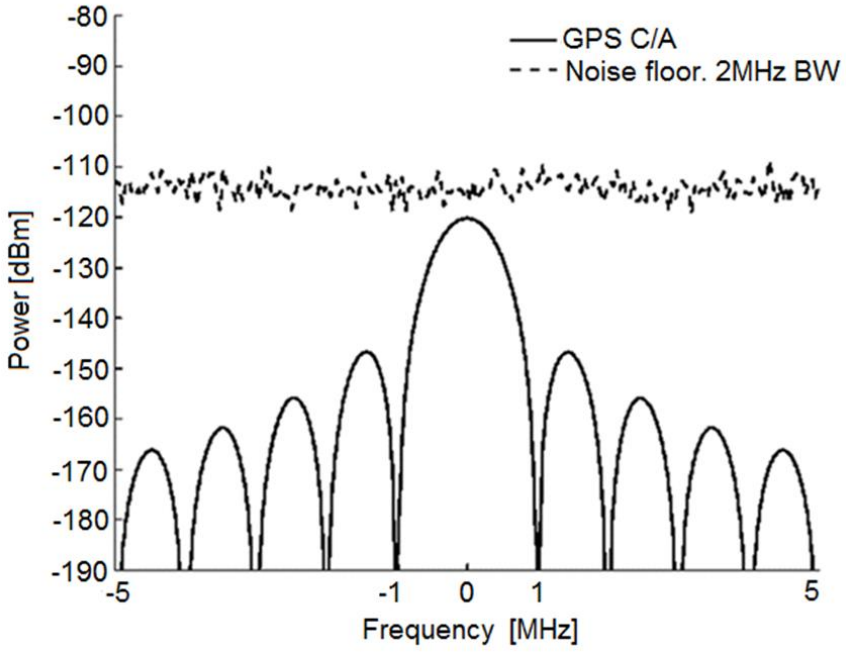

Figura 4.8- Espectro do sinal de GPS e da potência de ruído térmico.

A BladeRF com um ganho $TxVGA1 = -4\ dB$ e $RxVGA1_{min} = 5\ dB$ resulta num sinal de GPS falso com -122 dB de potência, medido com a BladeRF sem qualquer tipo de filtragem. Para que o sinal tenha uma potência de -153.5 dBW são necessários ajustes.

Desprezando os ganhos VGA1 da emissão e da receção, -122 - (-4) - 5 = -123 dB. Consegue-se ainda recorrer ao ajuste do ganho de TxVGA1 para -35 dB, perdendo 31 dB face ao caso anterior (-4 - 31 = -35 dB). Concluindo e somando a perda de 31 dB face ao ajuste do ganho TxVGA1, -122 - 31 = -153 dB. Em suma o recetor GPS e o transmissor de GPS falso têm de estar localizados próximo um do outro e com uma configuração de TxVGA1= -35 dB, para poder-se ter uma potência de sinal recebida próxima da potência de sinal recebida num caso real. Todos estes cálculos são necessários, uma vez que o equipamento não consegue medir densidade espectral de potência inferior à do ruído térmico.

4.4 Discussão dos Resultados

As cinco técnicas apresentadas acarretam consigo vantagens e desvantagens. Seguidamente são apresentadas essas mesmas vantagens de cada técnica bem como possíveis desvantagens, consideradas antes da realização dos testes em ambiente real.

O *Barrage Jamming* tem como principal vantagem o empastelamento de toda a banda do sinal GPS. O grande problema é o recurso energético, pois a densidade espectral de potência não é muito elevada uma vez que a potência distribui-se pela largura de banda de 15.345 MHz.

A grande vantagem do *Sweep Jamming* é conseguir uma densidade espectral de potência muito superior ao *Barrage Jamming*, recorrendo a um sinal com uma largura de banda inferior. Como a largura de banda do sinal é menor a potência do sinal não se dispersa e concentra-se mais na frequência central do sinal, sendo esta variável. Esta técnica recorre a um varrimento de frequências para que seja possível preencher toda a largura de banda do sinal GPS. A desvantagem poderá ser a nível de *hardware* pois é necessário equipamento que consiga realizar um varrimento de frequências suficientemente rápido para que esta técnica tenha sucesso.

A vantagem do sinal *Successive Pulses Jamming* é obter valores de densidade espectral de potência superior que o *Barrage Jamming*, pois embora ocupe toda a largura de banda do sinal GPS não o faz de forma uniforme. O facto de existir espaçamento de *jamming* entre frequências ao longo de toda a banda do sinal GPS é uma desvantagem uma vez que o recetor pode conseguir recuperar o sinal de GPS.

O *Tone Jamming* apenas emite uma sinusoide na frequência central, mas na prática não é isso que acontece, pois o chip LimeMicro LMS6002D, responsável pela emissão na BladeRF tem uma largura de banda de emissão mínima de 1.5 MHz. Os sinais de GPS ao terem uma largura de banda superior à do *jammer* será espectável que a técnica não seja das mais eficientes. A grande vantagem é concentrar toda a sua energia na frequência portadora dos sinais GPS.

Por fim, o *Protocol-Aware Jamming* (considerando o sinal aleatório BPSK criado com recurso ao GNU Radio) tem um resultado muito idêntico ao do *Barrage Jamming*, embora este não consista em emitir ruído propriamente dito, mas sim bits aleatórios modulados em BPSK para poder confundir o recetor. Configurando o *sample rate* idêntico ao do GPS, torna o espectro do *Protocol-Aware Jamming* muito idêntico ao do GPS, rentabilizando a densidade espectral de potência utilizada.

Numa primeira fase manteve-se uma distância fixa de 5 metros e variou-se os ganhos de transmissão para se perceber quais os *jammers* com maior potencial. Os *jammers* que

conseguirem bloquear o sinal do GPS falso com valores de ganhos inferiores serão, à priori, aqueles com melhor desempenho. Os resultados dos testes recorrendo ao GPS falso são apresentados graficamente na Figura 4.9. Analisando o gráfico percebe-se que o *Barrage Jamming*, *Sweep Jamming* e o *Protocol-Aware Jamming* são os que têm mais potencial.

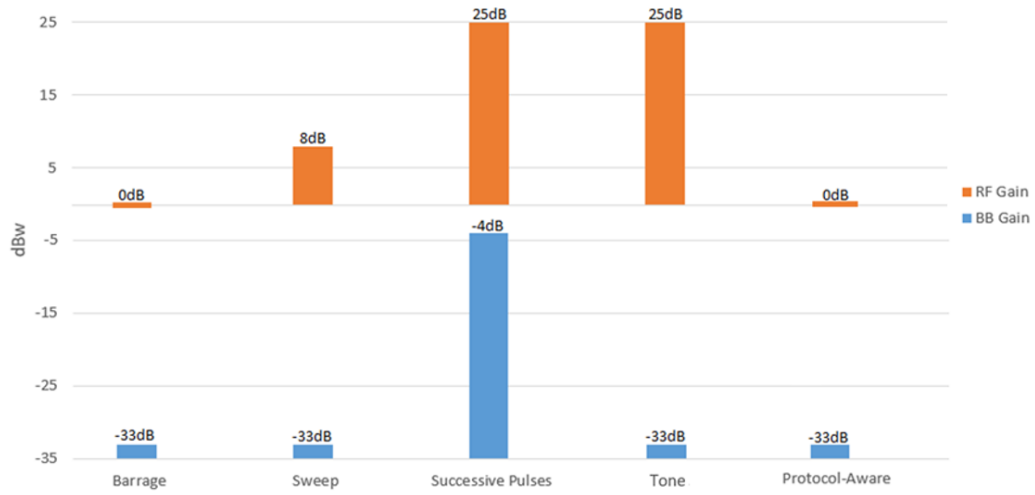

Figura 4.9 - Ganhos de transmissão mínimos para uma distância de 5 metros

Na etapa seguinte realizou-se testes de alcance máximo de cada um dos *jammers* estudados em ambiente controlado (tabela 3), para garantir que os resultados são coerentes com os expressos na Figura 4.9.

Tab. 3 - Alcance máximo dos vários jammers em ambiente controlado

	5 metros	10 metros	15 metros	20 metros	25 metros
Barrage Jamming	√	√	√	√	√
Sweep Jamming	√	√	√	√	√
Successive Pulses Jamming	√	X	X	X	X
Tone Jamming	√	√	√	√	X
Protocol-Aware Jamming	√	√	√	√	√

Nota: √ →recetor GPS sem localização X → recetor GPS com localização

Com base nos resultados obtidos, não se pode ainda chegar a uma conclusão final, embora os *jammer* com melhor desempenho sejam o *Barrage Jamming*, o *Sweep Jamming* e o *Protocol-Aware Jamming*. Resultados que vão ao encontro dos obtidos no primeiro teste, com uma distância fixa.

4.5 Testes em Ambiente Real

Uma vez realizados os testes em ambiente controlado, concretiza-se em ambiente real, deixando de utilizar um sinal GPS falso e efetuando os testes com os sinais reais de GPS.

Através dos resultados em ambiente controlado, o *Barrage Jamming* é utilizado como o *jammer* base para comparação com os restantes. Os testes consistem em avaliar a distância máxima que o *Barrage Jamming* consegue interferir em ambiente real e com isso colocar o recetor fora da zona de alcance como demonstra a Figura 4.10. A BladeRF foi alimentada por USB 3.0, com ganhos de TxVGA1 = -4 dB e TxVGA2 = 25 dB.

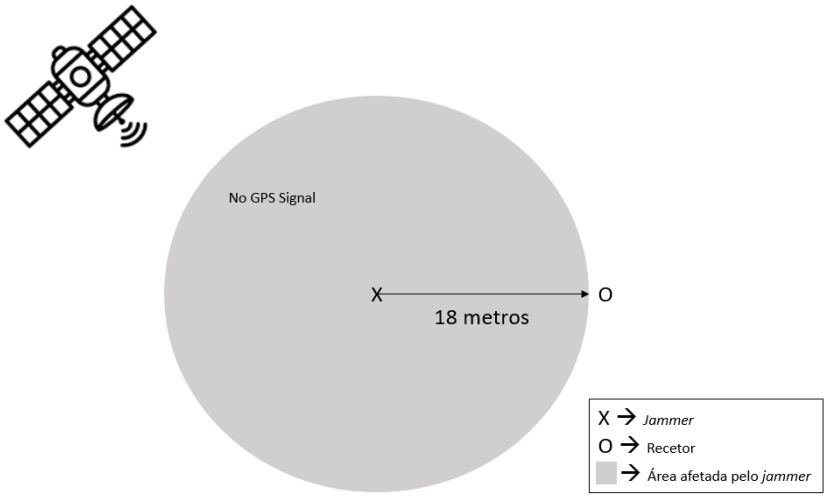

Figura 4.10 - Teste em ambiente real

Avaliando os *jammers* que, com a configuração da Figura 4.10, conseguem interferir com o recetor, pode-se concluir que o seu alcance é superior ao do *Barrage Jamming*.

O *Successive Pulses Jamming* como seria de esperar depois dos resultados em ambiente controlado, não conseguiu interferir com o recetor. O facto de existir espaçamento de interferência em toda a largura de banda do GPS faz com que esta técnica seja pouco eficiente, pois o recetor consegue a pouca distância do *jammer* recuperar a localização.

O *Tone Jammer* consegue interferir com o recetor baixando todos os níveis de potência dos satélites mas ainda assim, não consegue manter a não localização. Existem espaços de tempo em que o recetor consegue manter a localização e espaços de tempo em que não existe localização. Como relatado na parte teórica, esta técnica não ocupa uniformemente toda a largura de banda do GPS.

Por sua vez o *Sweep Jamming* e o *Protocol-Aware Jamming* conseguem bloquear os sinais GPS no recetor, pelo que são técnicas mais eficientes comparativamente ao *Barrage Jamming*.

Com base nestes resultados estas duas técnicas merecem uma análise mais pormenorizada e detalhada. Ambos conseguem com que o recetor deixe de conseguir a localização, embora a análise de potências de sinais dos satélites GPS no recetor sejam diferentes, como é possível observar na Figura 4.11 e Figura 4.12.

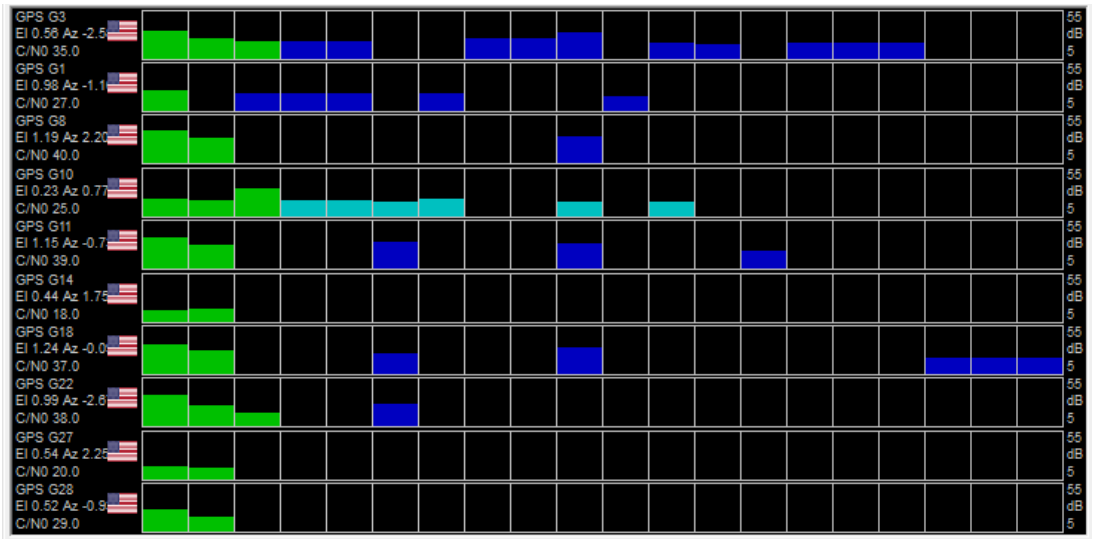

Figura 4.11 - Potência dos sinais de satélites GPS com o Sweep Jamming

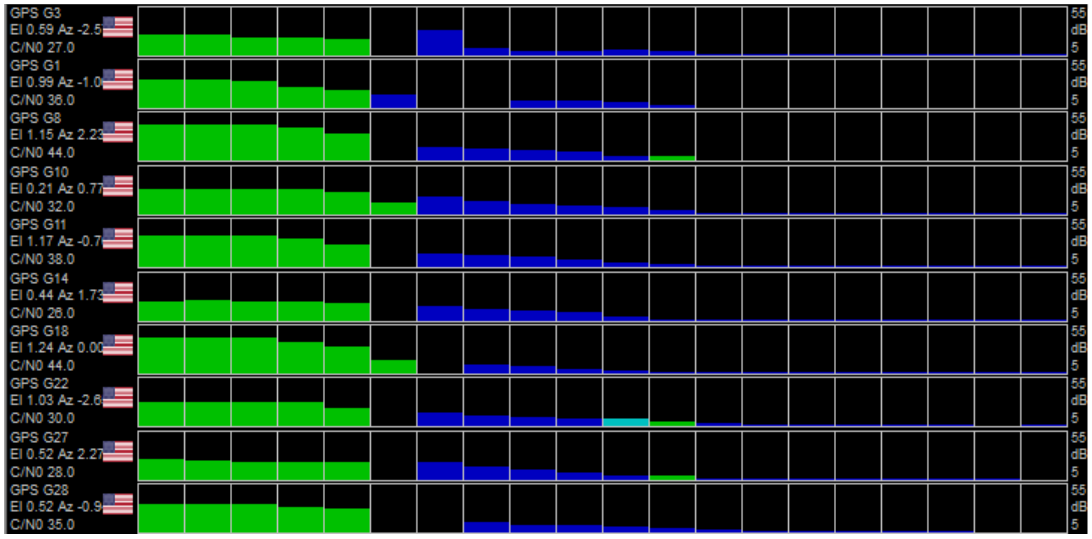

Figura 4.12 - Potência dos sinais de satélites GPS com o Protocol-Aware Jamming

Os gráficos apresentados em ambas as figuras relacionam o nível de potência recebida (eixo vertical) e os instantes de tempo no eixo horizontal, sendo o mais antigo representado à esquerda e o atual à direita.

É possível observar que com o *Sweep Jamming* os satélites nunca perdem a totalidade de potência nos diversos instantes, enquanto que no *Protocol-Aware Jamming* assim que o *jammer* é acionado as potências dos satélites vão diminuindo gradualmente nos vários instantes de tempo até perderem na totalidade a receção de qualquer satélite.

Em suma, considera-se que o *Protocol-Aware Jamming* é o *jammer* mais viável em termos de alcance face aos restantes. O *Sweep Jamming* é uma solução muito interessante, mas o equipamento pode limitar a eficiência da técnica abordada. Se o *hardware* não possibilitar um varrimento de frequências suficiente rápido para que o recetor não seja capaz de receber sinais GPS, não se consegue garantir uma total eficiência.

Capítulo 5

5. Protótipo

A última etapa do trabalho passava por construir um protótipo final de um sistema anti-UAV o qual deveria ser móvel e manuseável por um operador. Com a eleição do *jammer* mais eficiente é possível criar um aparelho do género de uma "arma" não destrutiva para bloquear voos de drones não autorizados em determinadas áreas.

Para que o protótipo fique com funcionalidades mais abrangentes foram integradas várias tecnologias desenvolvidas por dissertações de outros alunos, nomeadamente o *spoofing* do sinal GPS, para se poder ganhar o controlo do drone e desviá-lo para zonas seguras e também o *jamming* do sinal RF do telecomando do drone para o caso de estar a operar através de comandos diretos de um utilizador e modo de voo autónomo com utilização de GPS.

Com a integração do conjunto de tecnologias desenvolvidas é possível proteger a intrusão de drones, terrestres, aéreos e aquáticos em zonas restritas como aeroportos, áreas militares, condomínios e situações pontuais de eventos públicos e zonas que é necessário garantir a segurança. Tratando-se de um sistema móvel, consegue-se assim uma boa flexibilidade quanto aos locais a proteger, não necessitando de uma demorada instalação no local.

5.1 Componente Eletrónica

Para desenvolver o aparelho foi necessário substituir o processamento do computador por algo mais pequeno e leve. A escolha trata-se de um Raspberry Pi 3 com alto poder de computação e que serve na perfeição para atender à meta traçada.

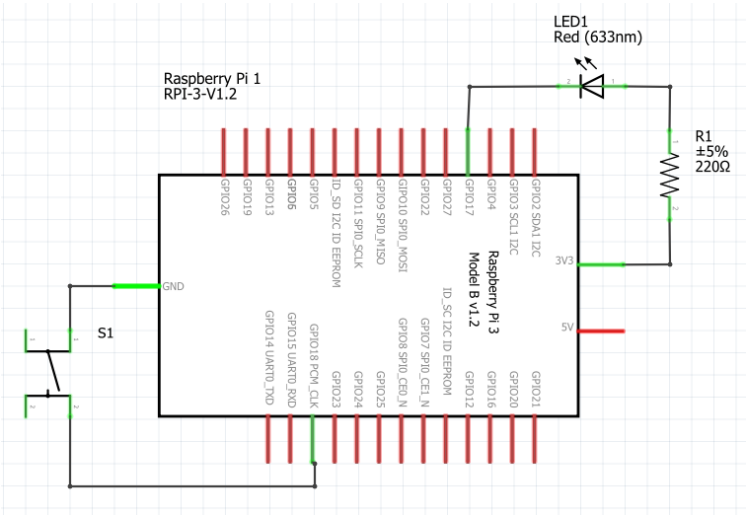

Figura 5.1 - Esquema do gatilho e LED no Raspberry Pi 3

O esquema de ligação dos componentes com o Raspberry Pi 3 é representado pela Figura 5.1. É utilizado um botão de pressão, com a função de gatilho, que quando pressionado inicia a transmissão do *jammer*. Para abortar a transmissão, basta o utilizador deixar de premir o botão. O LED serve apenas de indicação. Aceso para quando está a ser emitido o sinal *jammer* e apagado quando não existe transmissão.

O botão de pressão está conectado entre o GND e o GPIO18, enquanto o LED encontra-se entre os 3.3V e o GPIO17, contendo uma resistência de 330Ω em série para proteção.

5.2 Componente de *Software*

Em termos de *software*, para que o Raspberry Pi 3 arranque automaticamente para o código Python que contém o ficheiro de controlo do botão de pressão, é necessário acrescentar o comando Python *nomedoficheiro.py* no fim do código do ficheiro *bashrc*, ficheiro responsável pelo arranque do sistema operativo Linux, versão Ubunto Mate. Pode-se modificar o código recorrendo ao comando *sudo nano .bashrc*.

Para que não exista login ao arrancar, é necessário acrescentar o seguinte: *autologin-user:username* no ficheiro *60-lightdm-gtk-greeter.conf* disponível na diretoria */usr/share/lightdm/lightdm.conf.d.*

Ilustra-se um pequeno diagrama, representado na Figura 5.2, para melhor explicação do funcionamento do aparelho.

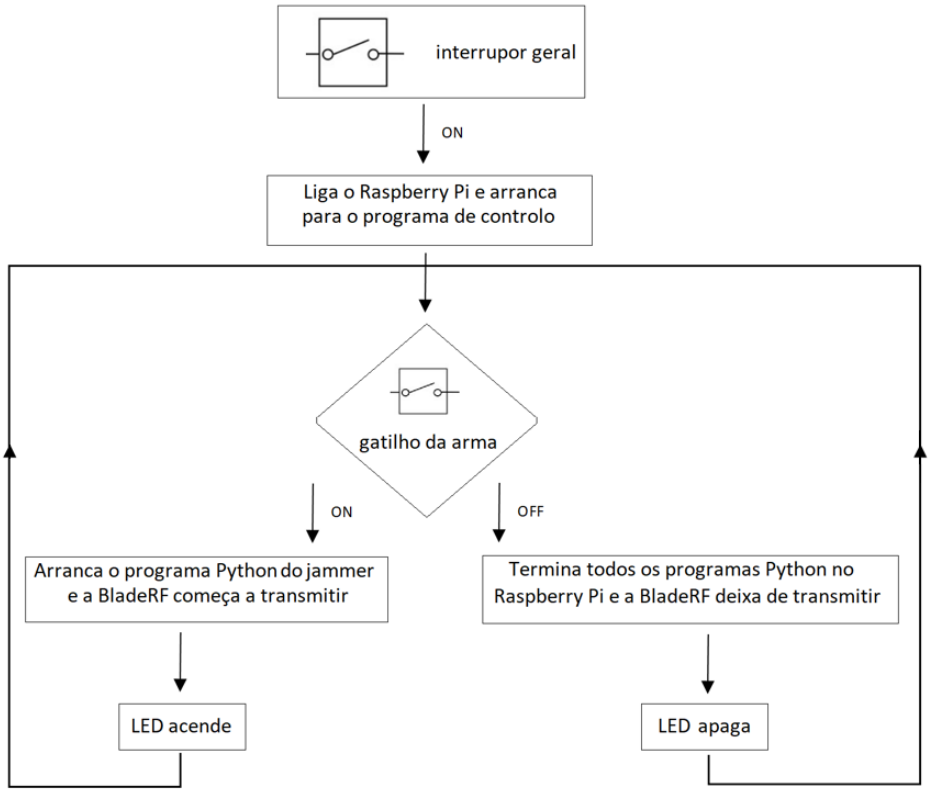

Figura 5.2 - Diagrama de funcionamento

5.3 Dimensionamento da Antena Yagi

Para conseguir-se minimizar a interferência com recetores GPS indesejados existiu a necessidade e importância de implementar uma antena diretiva. Com um feixe de transmissão menor consegue-se direcionar o sinal *jammer* a transmitir e com isso aumentar a potência desse mesmo sinal em determinado sentido e direção.

A antena Yagi é uma antena de grande potência que pode ser usada tanto para transmitir sinais em distâncias relativamente grandes, como para captar sinais fracos. Nas redes *wireless* as antenas Yagi são as que oferecem um maior alcance, mas em compensação são capazes de cobrir apenas uma pequena área para onde são apontadas.

Para o dimensionamento da antena Yagi é utilizado um simulador *Yagi Calculator - VK5DJ* desenvolvido por John Drew [40]. O *Yagi Calculator - VK5DJ* é um programa cuja finalidade é produzir dimensões para uma antena Yagi de estilo DL6WU. Está desenhado para frequências compreendidas entre os 144MHz e 2,4GHz. O modelo Yagi DL6WU é considerado como sendo fácil de construir e com resultados bastante positivos. Os parâmetros introduzidos para o dimensionamento da antena estão expressos na Figura 5.3.

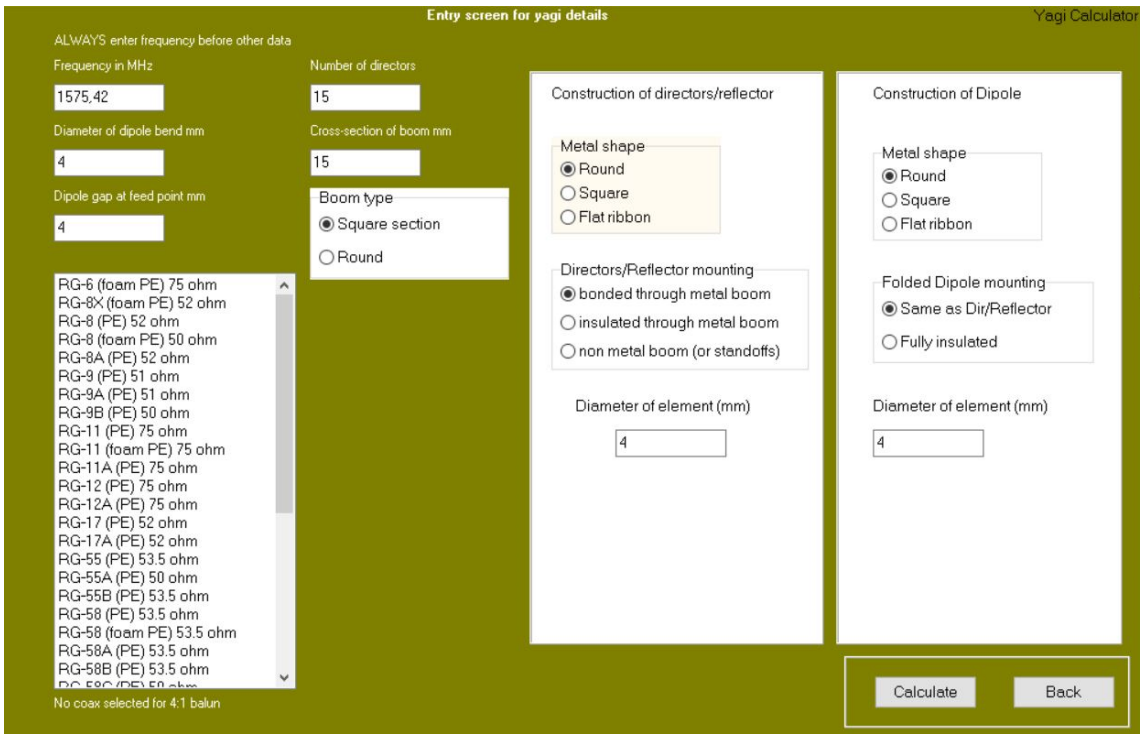

Figura 5.3 - Parâmetros introduzidos no simulador Yagi Calculator - VK5DJ

Para uma frequência de 1575.42 MHz e com recomendação do simulador em utilizar 8 diretores no mínimo, os resultados das dimensões da antena são expressos na Figura 5.4.

VK5DJ's YAGI CALCULATOR

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

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

RADIATOR
Single dipole 87,0 mm tip to tip, spaced 38 mm from reflector at boom posn 68 mm (IT = 36,0 mm)
Folded dipole 100,8 mm tip to tip, spaced 38 mm from reflector at boom posn 68 mm (IT = 43,0 mm)

DIRECTORS

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

Figura 5.4 - Resultados do dimensionamento da antena Yagi

Através dos resultados do simulador é possível representar um esboço da antena Yagi (Figura 5.5), com 15 diretores aumentando o ganho da antena.

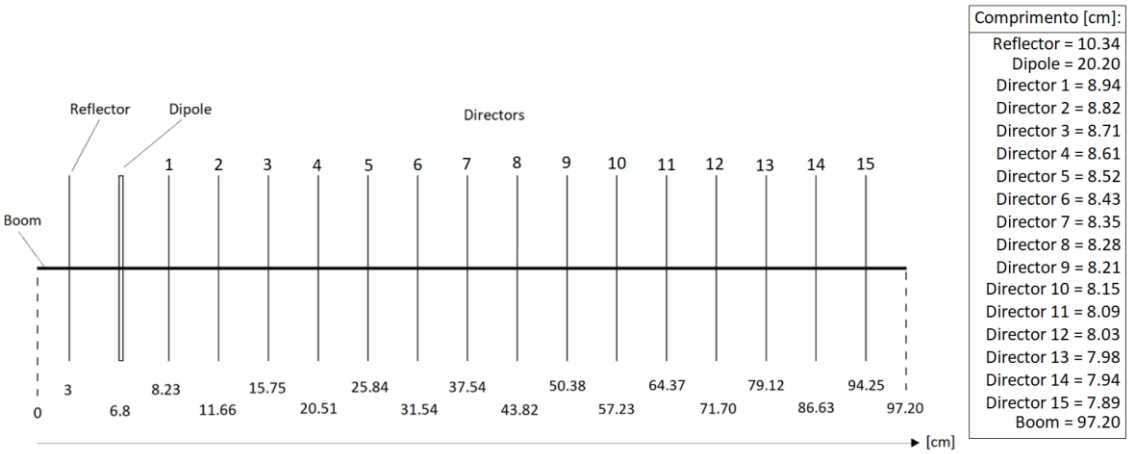

Figura 5.5 - Esboço da antena Yagi

O simulador apresenta também nos seus resultados as dimensões do *folded dipole* (Figura 5.6)

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

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

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

The beam's estimated 3dB beamwidth is 30 deg

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

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

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

Figura 5.6 - Resultados das dimensões do folded dipole

Através dos resultados do simulador (Figura 5.6) é possível representar um esboço das dimensões do *folded dipole* na Figura 5.7.

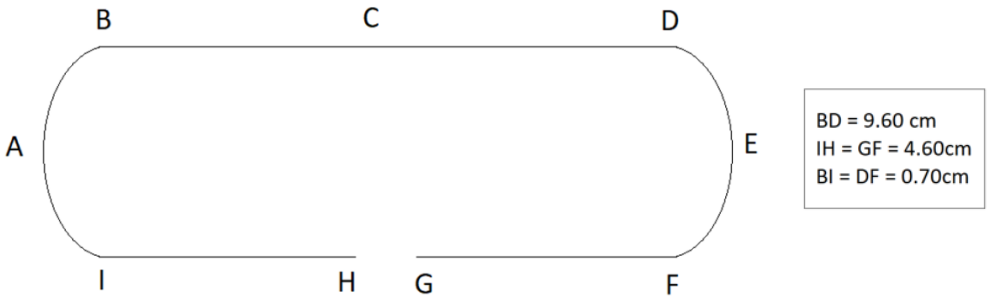

Figura 5.7 - Esboço do folded dipole

O simulador calcula também o ganho da antena, sendo que neste caso prevê-se um ganho de 14.8 dB e aproximadamente 29° de largura de feixe para ambos os planos (vertical e horizontal).

O resultado final da construção da antena Yagi artesanal, respeitando os resultados obtidos pelo simulador, está expresso na Figura 5.8.

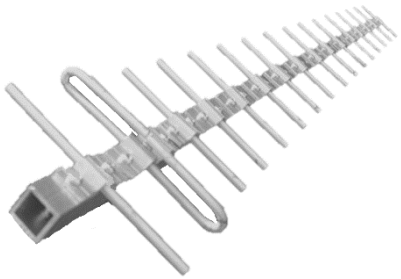

Figura 5.8 - Antena Yagi artesanal

Foram feitos os diagramas de radiação da antena Yagi artesanal, nos planos XY (Figura 5.9) e YZ (Figura 5.10). A densidade de potência espectral foi medida com o RTL SDR 820T2 com espaçamento de 5 graus. Em ambas as figuras, as linhas a azul foram os resultados medidos, e com a linha vermelha traçou-se uma aproximação desses resultados.

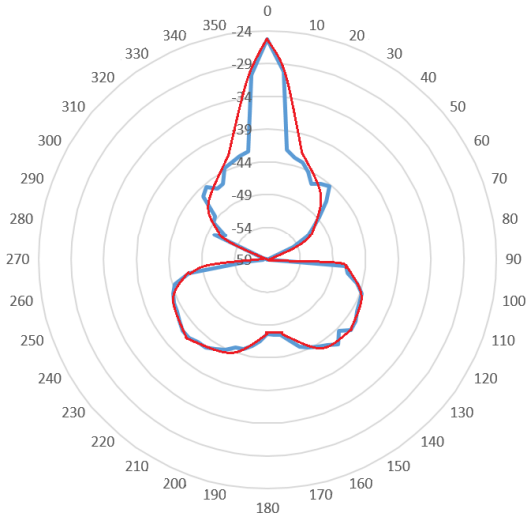

Figura 5.9 - Diagrama de radiação plano XY

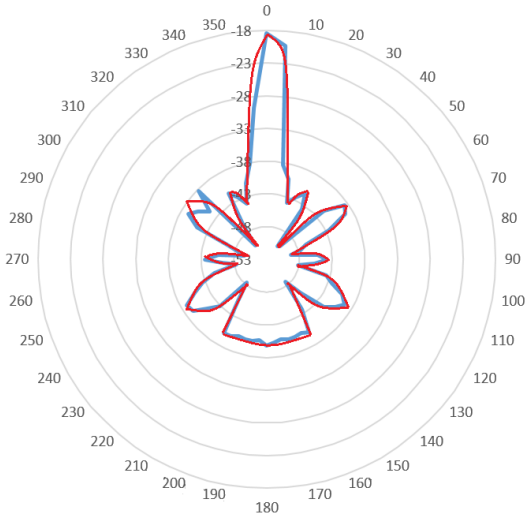

Figura 5.10 - Diagrama de radiação plano YZ

As condições onde foram realizados as medições para desenhar os diagramas não foram as melhores. Para que os resultados fossem mais assertivos as medições deveriam ter sido feitas numa câmara anecoica para evitar reflexões que influenciam os resultados pretendidos.

A distância angular entre os pontos com metade da potência é definida como a largura do feixe. A metade da potência expressa em decibéis é -3 dB da potência máxima. Então, a largura de feixe em meia potência é algumas vezes chamada de largura de feixe de 3 dB [41]. A largura de feixe está assinalada a verde em ambos os planos XY (Figura 5.12) e YZ (Figura 5.11), correspondendo uma largura de feixe de cerca 5 graus para ambos os casos.

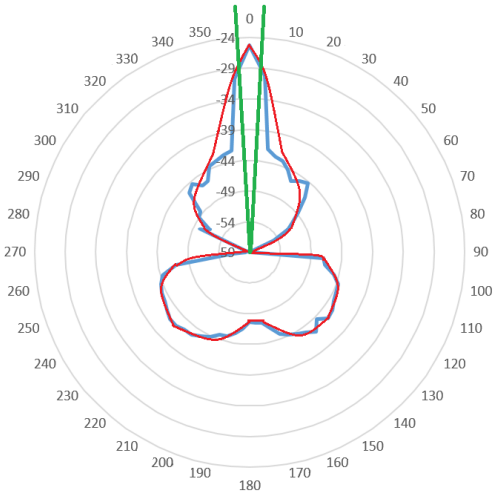

Figura 5.11 - Largura de feixe plano XY

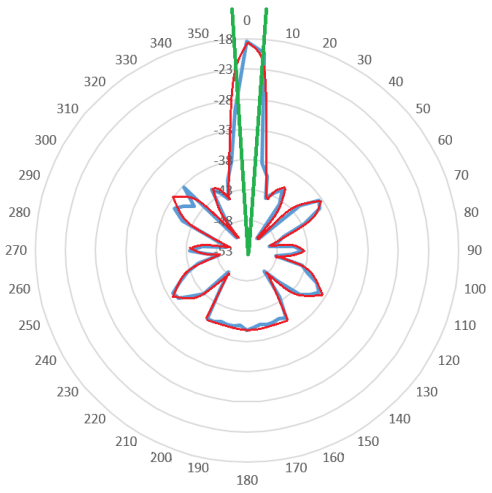

Figura 5.12 - Largura de feixe plano YZ

Para calcular o ganho da antena é necessário recorrer ao modelo de propagação em espaço livre (equação 21), uma vez que os diagramas de radiação apresentados são referentes às potências recebidas.

$$P_{RX} = P_{TX}\left(\frac{c}{4\pi df}\right)^2 G_{TX}G_{RX} \tag{21}$$

$P_{RX} \rightarrow potência\ recebida$
$P_{TX} \rightarrow\ potência\ transmitida$
$c \rightarrow velocidade\ de\ propagação\ da\ luz$
$d \rightarrow distância\ entre\ o\ emissor\ e\ recetor$

$f \rightarrow\ frequência\ da\ portadora$
$G_{TX} \rightarrow ganho\ da\ antena\ de\ transmissão$
$G_{RX} \rightarrow ganho\ da\ antena\ de\ receção$

Como P_{RX} deveria ser igual em ambos os planos, para efeitos de cálculos é feita uma média dos 2 valores medidos, sendo P_{RX} = -21.5 dBW.

$$G_{TX} = \frac{P_{RX}}{P_{TX}\left(\frac{c}{4\pi df}\right)^2 G_{RX}} = \frac{10^{\frac{-21.5}{10}}}{10^{\frac{-3}{10}} \times \left(\frac{3\times 10^8}{4\pi \times 1.10 \times 1.57542 \times 10^9}\right)^2 \times 1} = 74.43\ W \tag{22}$$

Conversão do ganho de transmissão para dBW:

$$G_{TX}(dB) = 10\log(74.43) = 18.72\ dBW \tag{23}$$

O sinal emitido através do GNU Radio para medição dos valores, tinha um ganho de -4dB de transmissão, portanto o ganho real da antena é:

$$G_{Antena}(dB) = G_{TX}(dB) + G_{TX\ GNU\ Radio} = 18.72 + (-4) = 14.72\ dBW \quad (24)$$

Na tabela 4, pode-se comparar os valores resultantes do simulador com os valores medidos.

Tab. 4 - Comparação dos valores simulados com os obtidos

	Largura de feixe a meia potência	Ganho da antena
Valores do Simulador	29 graus	14.8 dBW
Valores Reais	5 graus	14.72 dBW

Os resultados obtidos através do simulador, comparados aos valores reais, são ligeiramente diferentes em relação à largura de feixe a meia potência, que se traduz na diretividade da antena, obtendo-se uma antena mais diretiva do que o esperado. Relativamente ao ganho da antena, está bastante próximo do esperado. Os valores podem discrepar devido às condições das medições não serem as perfeitas.

5.4 Dimensionamento da Estrutura

O dimensionamento do aparelho é baseado no formato de uma arma, tornam-se num dispositivo móvel e de fácil manuseamento. É utilizado o programa *Autocad Inventor Student* para projetar a ideia, como demonstrado na Figura 5.13.

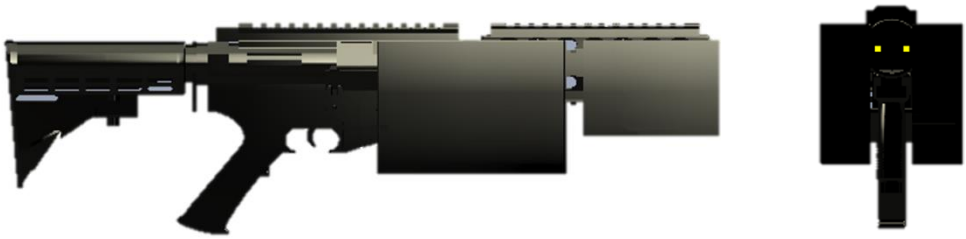

Figura 5.13 – Estrutura do protótipo com perspetiva lateral e frontal

A estrutura apresenta quatro caixas (duas de cada lado), para colocação de duas BladeRF, Arduíno e Raspberry Pi. Na coronha da arma, são alocadas as respetivas baterias para a alimentação de todo o sistema. O gatilho é substituído por botões *switches* responsáveis pela inicialização da transmissão. Ao longo da estrutura são ainda alojados vários sensores, bem como outros botões e LEDs para uma interação com o sistema. Por fim, na ponta da arma é aparafusada a antena desenvolvida. Mais detalhes sobre o protótipo estão referido no Apêndice B.

O resultado final do protótipo encontra-se na Figura 5.14. A antena Yagi artesanal é fixada na ponta da arma.

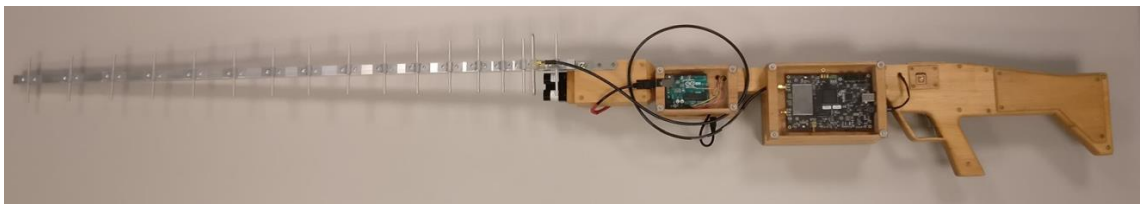

Figura 5.14 - Resultado final do protótipo

5.5 Dimensionamento da Bateria

É realizado previamente um dimensionamento da bateria a implementar.

Tendo em conta que Raspberry Pi 3, Arduíno Uno e BladeRF trabalham com uma tensão de cerca de 5V, a bateria tem essa mesma tensão, faltando apurar qual a sua amperagem.

A Blade RF tem um consumo máximo de 3.644 Watts e considera-se o pior caso para este dimensionamento:

$$\frac{W}{V} = A \Leftrightarrow \frac{3.644}{5} = 0.73\ A \tag{25}$$

A Blade RF + xb 300 com o Tx ON e Rx OFF tem um consumo de 8.584 Watts, consumos disponíveis pelo *site* oficial da Nuand:

$$\frac{8.584}{5} = 1.72\ A \tag{26}$$

O Arduíno Uno tem um consumo de 250mW:

$$\frac{250 \times 10^{-3}}{5} = 50mA \tag{27}$$

O Raspberry Pi 3 tem um consumo de 1.2W:

$$\frac{1.2}{5} = 240mA \tag{28}$$

Ainda não existindo um amplificador de referência para a amplificação do sinal *jammer* e *spoofing*, relativamente ao GPS, utiliza-se um valor médio de 1A como referência.

Total de amperes em consumo instantâneo:

$$0.73 + 1.72 + 50 \times 10^{-3} + 240 \times 10^{-3} + 1 = 3.74\ A \tag{29}$$

Admitindo que um soldado tem um turno de 8 horas, pretende-se que a bateria tenha capacidade para alimentar o sistema em cerca de 20 % do tempo do turno (1.6 horas). A bateria é colocada de maneira a ser fácil a sua troca por outra, assim que estiver descarregada.

$$horas\ de\ autonomia\ \times consumo = \frac{amperes}{hora} \Leftrightarrow 1.6\ \times 3.74 \approx\ 6\ Ah \tag{30}$$

Concluindo, a bateria deve ser de 5V com 6Ah para suportar o sistema. É de referir que este dimensionamento de bateira está um pouco simplificado, serve apenas para ter uma noção da bateria a implementar no sistema.

Capítulo 6

6. Conclusões e Trabalho Futuro

Ao desenvolver este trabalho pretendia-se que o resultado final fosse a implementação de um protótipo de um sistema para neutralização de drones, aglomerando várias tecnologias, para que todo o estudo em causa pudesse ser posto em prática. Esse objetivo foi concluído com sucesso, não esquecendo o objetivo principal, o de desenvolver através do uso de uma plataforma SDR um *jammer* o mais eficiente possível.

O *jammer* eleito com melhor desempenho foi o *Protocol-Aware Jamming*, que usa uma arquitetura semelhante à utilizada pelo emissor do sinal GPS a interferir. Desta forma, o sinal interferente "mistura-se" com o sinal alvo, uma vez que apresentam propriedades idênticas por forma a destruir a informação deste ou então tornar a sua receção virtualmente impossível de ser realizada no recetor.

6.1 Respostas às Questões de Investigação

No capítulo 1 são colocadas algumas questões sendo um dos objetivos desta dissertação encontrar respostas para as mesmas.

Primeira pergunta "Ao realizar o *jammer* para as comunicações do drone, existem interferências involuntárias nos recetores vizinhos? Se sim, até que ponto se pode minimizá-las?". Com a transmissão do *jammer* é afetado o sinal GPS em todos os dispositivos recetores que estejam dentro do raio de alcance do *jammer*. Este problema é atenuado recorrendo-se a uma antena direcional, onde o raio de ação do *jammer* é diminuído, aumentado o seu ganho de transmissão.

Relativamente à segunda questão, "Qual o alcance máximo que o *jammer* consegue interferir, tendo em conta a eficiência energética?". Ao nível de *software* é apresentada nesta mesma dissertação, tendo em conta os resultados obtidos, qual a técnica de *jamming* com um alcance maior. A contribuição de *hardware* é claramente um ponto influenciador nesta questão. Com a aplicação de uma antena direcional e de um amplificador adaptado à frequência de transmissão é possível aumentar o ganho de transmissão que consequentemente aumenta o alcance máximo do *jammer*.

Terceira pergunta, "A resposta do sistema é suficientemente rápida para se poder ter uma solução eficiente?". Esta questão vai ao encontro de possíveis limitações existentes com o *hardware*, embora para este caso não haja qualquer implicação.

Para finalizar, a quarta e última pergunta, " Esta solução é capaz de resolver as ameaças dos drones para a sociedade?". Esta solução, acompanhando aquilo que foi projetado como protótipo final e completada com outras tecnologias, é uma solução bastante eficiente para o problema causado pelos drones nomeadamente no que diz respeito à segurança e privacidade pessoal ou coletiva.

6.2 Dificuldades e Trabalho Futuro

O projeto ao ser desenvolvido numa plataforma em que o autor não tinha interagido anteriormente, tornou-se bastante atrativo e enriquecedor. Informação de desenvolvimento disponível com a plataforma SDR ainda é escassa, sendo que foi necessário a interação *online* com outros investigadores para que o crescimento e os primeiros passos fossem desenvolvidos. Os vídeos do autor Michael Ossmann foram uma grande ajuda para a inicialização à plataforma. Este projeto requereu de muita força de vontade e dedicação pessoal para que fosse possível atingir os objetivos traçados. Futuramente, o interessante seria explorar estas mesmas questões mas para sistemas de posicionamento diferentes, nomeadamente o Glonass e o Galileu. Recorrendo às técnicas abordadas poder-se-ia concluir se, mudando o sistema de posicionamento, os resultados permanecem os mesmos ou se serão diferentes. Para a realização desse trabalho futuro, o recetor GNSS utilizado nesta dissertação não permite a receção de sinais do sistema de posicionamento Galileu, sendo necessária a aquisição de uma versão de *hardware* mais recente para esse efeito. Poderia ainda ser desenvolvido um sistema para correção dos erros de *DC Offset* e *IQ Imbalance* provocados pelas plataformas SDR. Salienta-se ainda que os aspetos científicos que estão na base do desenvolvimento destas tecnologias são fundamentais para o sucesso deste projeto, uma vez que existem funcionalidades que são necessárias desenvolver para novos sistemas de controlo que irão integrar os futuros drones.

Referências

[1] P. Pinto, "Portugal: 31 incidentes com drones nos aeroportos", [Online]. Available: https://pplware.sapo.pt/informacao/portugal-31-incidentes-drones-nos-aeroportos/. [Accessed: 11-Jan-2018].

[2] BBC News Brasil, "Polícia holandesa treina águias para capturar drones em pleno voo", Fev. 2016 [Online]. Available: https://www.bbc.com/portuguese/noticias/2016/02/ 160202_drone_aguia_tg. [Accessed: 11-Jan-2018].

[3] N. Litôvkin, "Kalashnikov lança nova arma que combate drones", August 2017 [Online]. Available: https://br.rbth.com/defesa/2017/08/29/kalashnikov-lanca-nova-arma-que-combate -drones_830472. [Accessed: 11-Jan-2018].

[4] D. Eshel and J. M. Doyle. (2015, November) 'UAV Killers Gain Role Against Growing Threat', Aviation Week. [Online]. Available: http://aviationweek.com/defense/ uav-killers-gain-role-against-growing-threat.

[5] G. Warwick. (2016, February) 'Counter-UAS Special Report: The Countermeasures Options', Aviation Week. [Online]. Available: http://aviationweek .com/technology/counter-uas-special-report-countermeasuresoptions.

[6] G. Warwick. (2015, December) "Countering Unmanned Defense & Space Technologies To Watch In 2016", Aviation Week. [Online]. Available: http://aviationweek.com/defense/defense-space-technologieswatch-2016-0.

[7] S. Khandelwal. (2015, October) 'First Ever Anti-Drone Weapon that Shoots Down UAVs with Radio Waves', The Hacker News. [Online]. Available: http://thehackernews.com/2015/10/drone-defender-gun.html.

[8] F. Corrigan. (2018, August) "Drone Gyro Stabilization, IMU And Flight Controllers Explained". [Online]. Available: https://www.dronezon.com/learn-about-drones-quadcopters/ three-and-six-axis-gyro-stabilized-drones/.

[9] X. Wang, J. Guo, N. Cui. "Adaptive extended Kalman filtering applied to low-cost MEMS IMU/GPS integration for UAV". International Conference on Mechatronics and Automation, 2009.

[10] Faculdade de ciências da universidade de lisboa - DEGGE- hidrografia, "GNSS and Earth Observation: recent results and challenges",2013.

[11] S. Pullen and G. Gao, "GNSS jamming in the name of privacy," Inside GNSS, pp. 34–43, March/April 2012.

[12] W. Hoffmann, B.H. Lichtenegger and J. Collins, GPS: Theory and Practice (Springer-Verlag, New York, 1994), 3ª ed.

[13] J. Monico, Posicionamento Pelo GNSS: Descrição, Fundamentos e Aplicações (Unesp, São Paulo, 2008).

[14] Parque Newton Freire Maia, "A tecnologia GPS - Parte II" [Online]. Available: http://parquedaciencia.blogspot.pt/2013/08/a-tecnologia-gps-parte-ii.html. [Accessed: 12-Dez-2017].

[15] G. Blewitt, "Basics of the GPS Technique: Observation Equations" [Online]. Available: http://www.nbmg.unr.edu/staff/pdfs/blewitt%20basics%20of%20gps.pdf. [Accessed: 21-Set-2018].

[16] E. Frazier, "GPS Turns 40" [Online]. Available: http://www.frazeology.com/gps-turns-40/. [Accessed: 22-Set-2018].

[17] R. Bingley, Handouts Satellite Based Positioning (H24VST). University of Nottingham, 2013.

[18] P. Misra and P. Enge, Global Positioning System: Signals, Measurements and Performance. Lincoln, Massachusetts: Ganga-Jamuna Press, 2010.

[19] Graham, A. Communications, Radar and Electronic Warfare. s.l. : John WIley & Som Ltd, 2011.

[20] K. Pärlin, "Jamming of Spread Spectrum Communications used in UAV Remote Control Systems", 2017.

[21] Sklar, B. Digital Communications: Fundamentals and Applications. s.l. : Prentice Hall, 2001.

[22] Lloyd N. Trefethen, David Bau III, Numerical linear algebra, Philadelphia: Society for Industrial and Applied Mathematics, ISBN 978-0-89871-361-9, pp.56.

[23] Federal Communications Commission, Website Notices [Online]. Available: http://www.fcc.gov [Accessed: 12-Dez-2017].

[24] Cell Phone Jammer, jammer berkulitas [Online]. Available: www.signaljammerblockers.com [Accessed: 8-Dez-2017].

[25] Tech-Faq, GPS Jammer [Online]. Available: http://www.tech-faq.com/gps-jammer.html [Accessed: 8-Dez-2017].

[26] J. Lehnert, W. Stark, D. Borth, (2017, August). "Telecommunication" [Online]. Available: https://www.britannica.com/technology/telecommunication/Modulation [Accessed: 24-Set-2018].

[27] P. Kenington, "RF and Baseband Techniques for Software Defined Radio", Artech House, 2005.

[28] T. Rouphael, "RF and Digital Signal Processing for Software-Defined Radio", Newnes, 2009.

[29] G. Benmouyal (Apr, 1995) "Removal of DC-offset in current waveforms using digital mimic filtering".

[30] D. Boschen (Dec, 2012) "IQ Imbalance" Available: https://dsp.stackexchange.com /questions/28678/iq-imbalance-amplitude [Accessed: 24-Set-2018].

[31] HJFR-INFO, BladeRF X40 [Online]. Available: https://www.hjfr-info.pt/produto/ bladerf-x40/. [Accessed: 5-Jan-2018].

[32] Lime Microsystems. LMS6002D: Multi-band Multi-standard Transceiver with Integrated Dual DACs and ADCs. [Online]. Available: http://www.limemicro.com/download/ LMS6002Dr2-DataSheet-1.2r0.pdf.

[33] Joeldo Pantoja Oliveira, Jeferson Breno Negrão Leite, Aldebaro Barreto da Rocha Klautau Jr, "Uso de Software Livre no Ensino de Telecomunicações", *XL Congresso Brasileiro de Educação em Engenharia*, p. 1–11, set. 2012.

[34] Tamer Basar. The gaussian test channel with an intelligent jammer. IEEE Transactions on Information Theory, 29(1):152–157, January 1983.

[35] Abid Hussain, Nazar A Saqib, Usman Qamar, Muhammad Zia, and Hassan Mahmood. Protocol-aware radio frequency jamming in Wi-Fi and commercial wireless networks. Journal of communications and networks, 16(4):397–406, 2014.

[36] David Thuente and Mithun Acharya. Intelligent jamming in wireless networks with applications to 802.11 b and other networks. In Proc. of MILCOM, volume 6, page 100, 2006.

[37] MyRiad RF, "LimeMicro:LMS6002D Datasheet" [Online]. Available: https://wiki.myriadrf.org/LimeMicro:LMS6002D_Datasheet [Accessed: 23-Set-2018].

[38] what-when-how - In Depth Tutorials and Information, "GNSS Antennas and Front Ends (GPS and Galileo Receiver) Part 1" [Online]. Available: http://what-when-how.com/a-software-defined-gps-and-galileo-receiver/gnss-antennas-and-front-ends-gps-and-galileo-receiver-part-1/. [Accessed: 14-Julho-2018].

[39] Global Position System Low Noise Amplifier. GPS, LNA, Sensitivity, Jamming, Cohabitation, TTFF. NXP founded by Philips. Date of release: May 2009.

[40] J. Drew, "Yagi Calculator DL6WU" Download Version 2.6.18 - May 2016 [Online]. Available: http://www.vk5dj.com/yagi.html [Accessed: 10-Aug-2018].

[41] M. Vieira, "Glossário sobre antenas", janeiro 2010. [Online]. Available: https://wirelesspt.net/wiki/Gloss%C3%A1rio_sobre_antenas [Accessed: 29-Set-2018].

Configuração de Equipamento

Apêndice A

- GNU Radio

O *software* GNURadio é um software *open source* e foi desenvolvido para ser utlizado em sistema operativo Linux. Para se poder operar em sistema operativo Windows recorreu-se a um *software* que faz essa adaptação, o programa PhotosSDR, disponível no github no seguinte endereço: https://github.com/pothosware/PothosSDR/wiki/GNURadio.

- BladeRF

Com a instalação do PhotosSDR, onde inclui o programa GNURadio, é necessário reconhecer as *drivers* da BladeRF disponíveis da Nuand. Através do *software* Zadig substitui-se a Driver WinUSB pela libusb-win32, para que a BladeRF seja reconhecida no GNURadio.

Depois de tudo configurado entre a BladeRF e o GNURadio já é possível delinear vários sinais *jammers*, em sistema operativo Windows, recorrendo a várias técnicas de *jamming* estudadas.

- Recetor GPS

A Figura A.1 representa uma tabela que está disponível no manual de utilizador do u-blox com o esquema de codificação das cores para visualizações gráficas do U-Center.

	Color	Meaning
+	Yellow	Current value
+	Orange	Valid 3D navigation fix + Dead Reckoning
+	Green	Valid 3D navigation fix
+	Cyan	Valid 2D navigation fix
+	Magenta	Dead Reckoning fix
+	Blue	Degraded navigation fix
+	Red	No or invalid navigation fix

Figura A.1 - Esquema de codificação por cores para visualizações gráficas

Com a transmissão de um sinal *jammer*, o recetor deixa de receber os sinais dos satélites e como consequência, perde a localização. O ponto no mapa-mundo deixa de ser verde, e passa a ser vermelho, como pode ser verificado na Figura A.2.

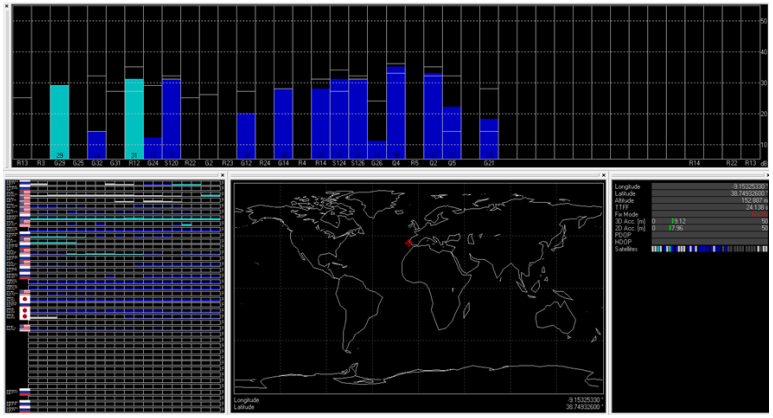

Figura A.2 - Perda da localização no recetor

A ferramenta U-Center analisa não só os sinais GPS como também, SBAS, BeiDou, IMES, QZSS e GLONASS. Acedendo às configurações é possível ativar apenas os sinais GPS, desprezando os restantes como se verifica na Figura A.3.

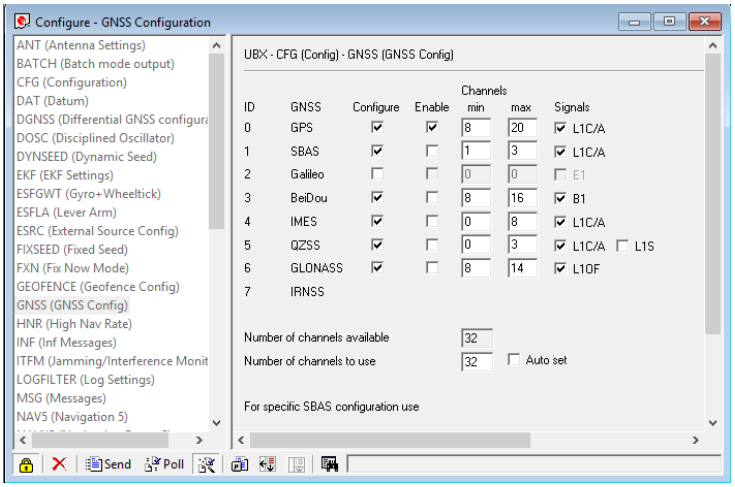

Figura A.3 - GNSS Configuration

Manual de Utilizador

Apêndice B

A estrutura do produto é em madeira, sendo as tampas para as plataformas BladeRF, Arduíno e Raspberry Pi em acrílico. A antena é toda constituída em alumínio. Todo o equipamento é desmontável e leve facilitando o seu transporte e manuseamento. É um produto projetado para ser bastante versátil, para se no futuro for necessário adaptações ou acréscimo de tecnologia.

1º Passo

- Ligar o botão 1 para a posição ON, alimentando o sistema (LED Vermelho acende);

2º Passo

- Calibrar os sensores, até o LED Verde acender;

3º Passo

- Escolher o modo de transmissão *jamming* através do botão 2;

4º Passo

- Apontar para o drone alvo e premir ambos os gatilhos (1 e 2) para inicializar o *jamming* do controlo remoto e do sistema de posicionamento GPS (LEDs piscam);

5º Passo

- Uma vez o drone imobilizado, trocar o botão 2 para o modo de funcionamento de *spoofing*;

6º Passo

- Selecionar o modo de *spoofing* a transmitir através do botão 3 (este modo dever ser previamente selecionado para não existir atrasos no processo);

7º Passo

- Pressionar o Gatilho 1 para inicializar a transmissão de *spoofing*, mantendo o drone alvo em mira;

8º Passo

- Assim que o drone esteja numa área segura a transmissão de *spoofing* deixa de ser necessária e pode deixar de premir o Gatilho (LEDs deixam de piscar).

Aviso: Este dispositivo deve ser utlizado por entidades competentes e/ou pessoas formadas e conscientes dos perigos que acarretam a sua utilização. Boas práticas de utilização devem ser toleradas e postas em causa, pertencendo ao utilizador fazer uso do equipamento com um objetivo adequado e consciente.

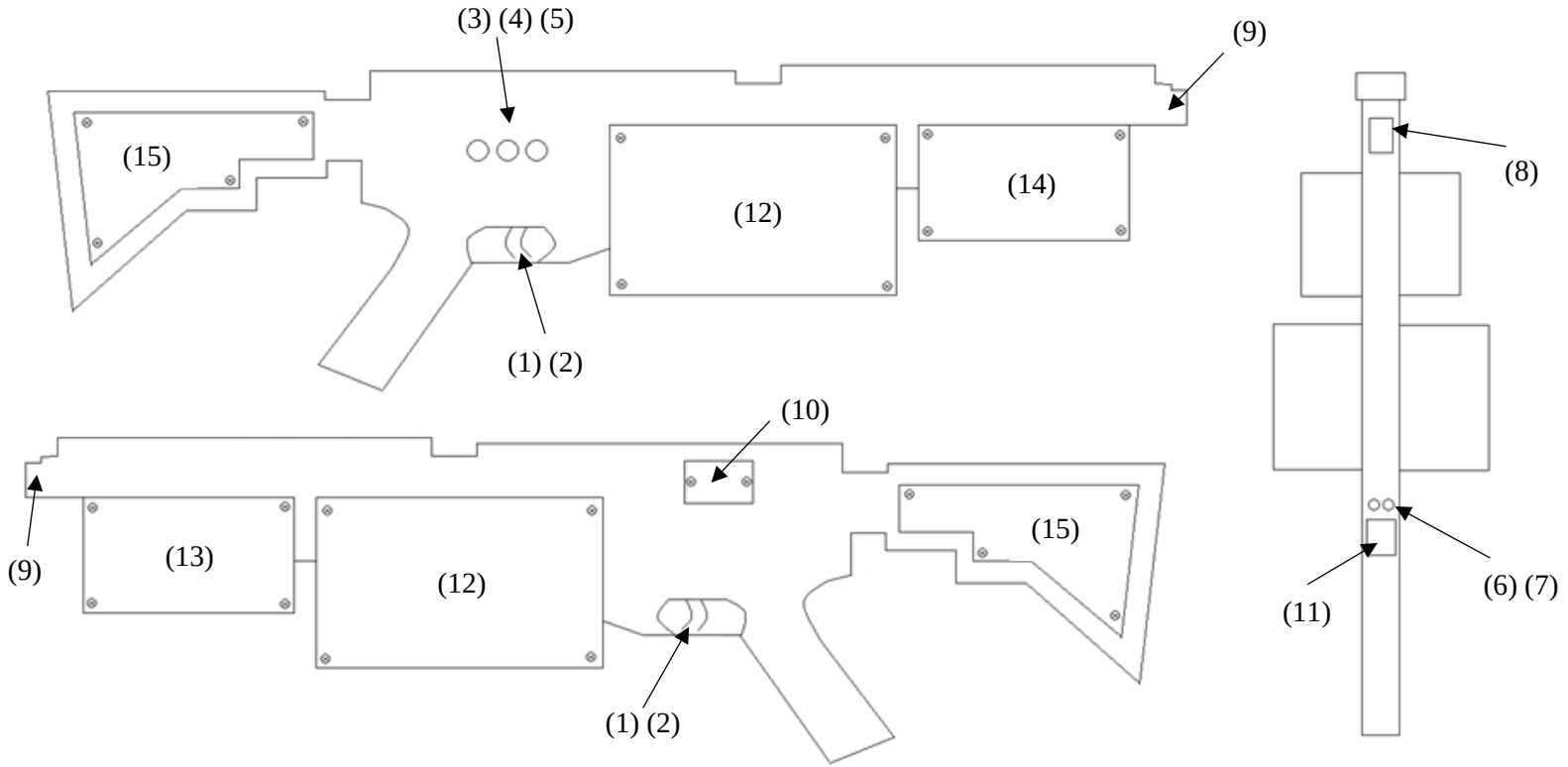

Figura B.1 - Esquema de localização dos elementos no protótipo

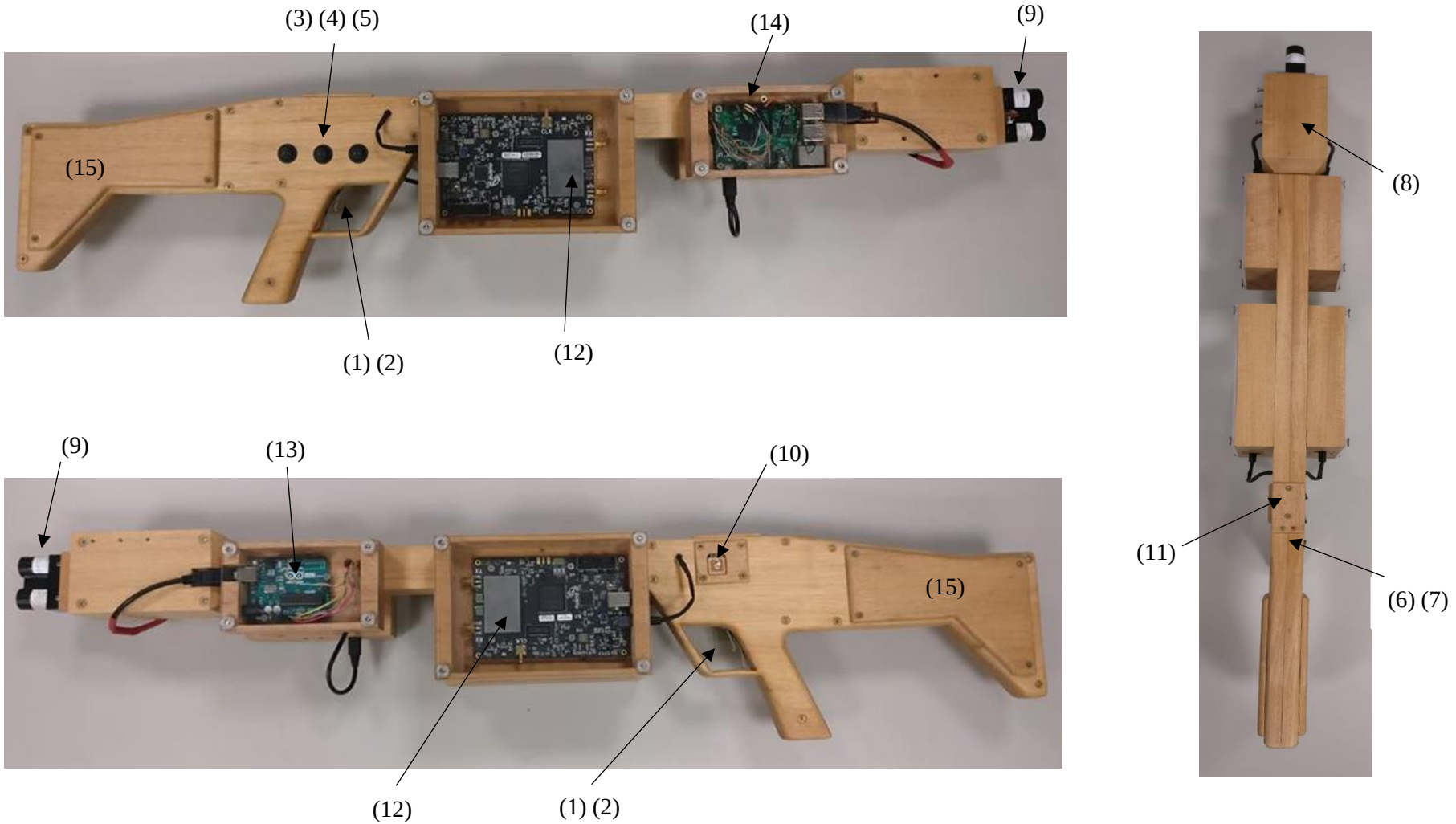

Figura B.2 - Localização dos elementos no protótipo

Tab. 5 - Lista dos Elementos Constituintes do Protótipo

Botões		
(1)	Gatilho 1	Transmissão de *jamming*/*spoofing* de GPS
(2)	Gatilho 2	Transmissão de *jamming* do controlo remoto
(3)	Botão 1	Botão ON/OFF de todo o sistema
(4)	Botão 2	Botão de seleção entre *jamming* ou *spoofing*
(5)	Botão 3	Botão de seleção entre técnicas de *spoofing*
LEDS		
(6)	LED Vermelho	LED *Standby*
(7)	LED Verde	LED indicativo de calibração dos sensores
Sensores		
(8)	Sensor MPU6050	Sensor de inclinação
(9)	Sensor LIDAR-Lite v3	Sensor ótico para medição de distâncias
(10)	Ublox-Max-7Q	Sensor de localização GPS
(11)	LSM303D	Sensor magnetómetro (Bússola)
Plataformas		
(12)	BladeRF	Plataforma SDR
(13)	Arduíno	Microcontrolador
(14)	Raspberry Pi	Microprocessador
Alimentação		
(15)	Bateria	Fonte de alimentação do sistema