Instituto Universitário de Lisboa

Departamento de Ciências e Tecnologias da Informação

Técnicas de bloqueio para operações não autorizadas de UAV Link de Comunicações

António José Borges de Brito

Dissertação submetida como requisito parcial para obtenção do grau de

Mestre em Engenharia de Telecomunicações e Informática

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

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

Outubro, 2018

Resumo

Os drones são formalmente conhecidos como veículos aéreos não tripulados (UAVs) e basicamente são "robots voadores". A presença dos Unmanned Aerial Vehicles (UAVs) está a crescer exponencialmente na comunidade militar e civil. Recentemente os drones estão muito associados ao uso militar e de segurança, sendo usados para espionagem, patrulhamento do espaço aéreo e como armas. Também podem ser utilizados em diversas áreas relacionadas com a vida civil, *e.g.*, na procura e resgate de pessoas, monotorização do tráfego, monotorização do tempo, vídeo vigilância, entre outras áreas.
Como os drones se tornaram cada vez mais desenvolvidos, *i.e.*, com maior capacidade de processamento e inteligência e, por outro lado, com maior procura no mercado, foi necessário desenvolver ações e tecnologia capaz de neutralizar "drones alvo". A esta técnica dá-se o nome de "jammer", que consiste num dispositivo capaz de provocar interferência e anular o controlo de um dado drone no espaço e no tempo. As ligações rádio nos UAVs podem ser alvo de diferentes tipos de jamming, nomeadamente, o link de comunicações, comandos entre o operador e o UAV e receção de sinais de radionavegação.
No âmbito desta dissertação é requerido um foco total na criação e estudo de jammers para a interferência do link de comunicações de drones, recorrendo a uma tecnologia designada por Software Defined Radio (SDR), que é um sistema de comunicação por rádio onde os componentes são implementados em hardware e o controlo das suas funcionalidades por software. Através do estudo de jammers já existentes, foi possível desenvolver jammers específicos durante o trabalho desenvolvido e apresentado nesta dissertação e analisar quais os factores que influenciam a interferência do link de comunicações. Neste sentido, foi utilizado o GNURadio que permitiu a implementação destes sistemas, que em conjunto com a BladeRF serviu para transmitir sinais que permitissem o bloqueio do link de comunicações.
Os resultados dos testes de interferência mostram que é possível o seu bloqueio utilizando diferentes tipos de combinações, com um custo acessível, quando em comparação com outras tecnologias existentes.

Palavras-Chave: drones, jammer, link de comunicações, GNURadio, BladeRF

Abstract

Drones are formally classified as unmanned aerial vehicles (UAVs) and are basically flying robots. The presence of unmanned aerial vehicles (UAVs) is growing exponentially in the military and civilian community. Drones have long been associated with military and security use and are used for espionage, airspace patrolling and weapons. They can also be used in various areas related to civilian life, for example, traffic monitoring, monitoring of time, video surveillance, and other areas.

As drones differentiate themselves more and more developed, that is, with greater processing capacity and intelligence and, on the other hand, with more market demand, the greater the capacity of actions and technologies able to neutralize the "target drones". It is because the jammer is capable of causing interference and void the control of a sound without space and without time. The radio variables in the UAVs may be subject to different types of interference, namely, the communications link, commands between the operator and the UAV and the reception of radio navigation signals.

In the scope of this dissertation it is required to create a set of radio programs for an interactive interface of a radio communication system, using a technology called radio (SDR), which is a radio communication system where the components are implemented in hardware and the control of its functionalities by software. Through the study of already existing jammers, the development of jammers was developed during the work developed and the present one in this dissertation and the analysis of which factors that influence the interference of the communications link. In this sense, it was used the GNURadio that will allow the implementation of these systems, together with the BladeRF service to transmit the signals that allow the blocking of the communications link.

The results of the interference tests showed that it is possible that different forms of use can be used.

Keywords: drones, jammer, communications link, GNURadio, BladeRF

Agradecimentos

Primeiramente, gostaria de agradecer ao Professor Pedro Sebastião e ao Professor Nuno Souto, por se terem disponibilizado para serem o meu orientador e o meu co-orientador, respetivamente. Foi um prazer ter trabalhado com os professores, que sempre me ajudaram e encorajaram ao longo deste último ano. O seu conhecimento acerca das diferentes áreas foi fundamental para a conclusão desta dissertação e permitiu o meu o desenvolvimento como aluno.
Quero agradecer ao Instituto de Telecomunicações (IT) e ao ISCTE-IUL, pelo seu suporte financeiro, que permitiu a compra de diverso material necessário para a dissertação e para tornar a mesma ainda mais completa.
Gostaria de agradecer aos colegas com que me cruzei nestes anos, pelo tempo passado com eles a aprender, a estudar e a aproveitar a faculdade. Foram fundamentais para o meu crescimento tanto a nível pessoal como a nível estudantil.
Queria deixar um agradecimento especial aos meus colegas de gabinete, que neste último ano me ajudaram e tornaram ainda mais divertido a realização desta dissertação.
Por último um obrigado à minha família, à minha mãe, ao meu pai, ao meu irmão e aos meus avós, pela sua educação, por me terem suportado nesta etapa e me terem motivado para tentar alcançar sempre os melhores resultados.

Índice

Lista de Figuras

Lista de Acrónimos

ADC Analog to Digital Converter
AUDS Anti-UAV Defense System
BER Bit Error Rate
BPSK Binary Phase-Shift Keying
CDL Common Data Link
CDMA Code-Division Multiplex Access
DAC Digital to Analog Converser
DDC Digital Down Converter
DSP Digital Signal Processor
DSSS Direct-Sequence Spread Spectrum
DUC Digital Up Converter
FFT Fast Fourier Transform
FHSS Frequency-Hopping Spread Spectrum
FPGA Field-Programmable Gate Away
GPP General Purpose Processor
GPS Global Position System
GPU Graphics Processing Unit
GSM Global System for Mobile Communications
IF Intermediate Frequency
IFFT Inverse Fast Fourier Transform
LDPC Low-density parity check code
LO Oscilador Local
LTE Long Term Evolution
LUT Look-Up Table
OFDM Orthogonal-Frequency Division Multiplexing
PN Phase-Noise
QAM Quadrature Amplitude Modulation
QPSK Quadrature Phase-Shift Keying
RC Radio Control
RF Radio Frequency
SDR Software Defined Radio
SNR Signal-Noise Ratio
SRC Sample Rate Conversion
UAS Unmanned Aerial System
UAV Unmanned Aerial Vehicle
UMTS Universal Mobile Telecommunication System

Capítulo 1. Introdução

Neste capítulo são analisados os conceitos que se encontram que suportam os desenvolvimentos apresentados nesta dissertação, qual a motivação para a realização deste trabalho e os objetivos propostos a alcançar.

1.1 Enquadramento do tema

Nas últimas décadas existiu um forte investimento nos Veículos Aéreos Não Tripulados (UAV), ou nos também denominados Sistemas Aéreos Não Tripulados (UASs). Esta tecnologia apresenta uma infinidade de aplicações. Embora este conceito tenha nascido para uso militar, nos últimos anos surgiu um aumento do interesse, tanto para uso académico como para uso civil [1]. Os UAV foram inicialmente desenvolvidos para fornecer apoio militar estratégico, devido à sua capacidade furtiva, eficiência e por puderem ser controlados a partir de um local remoto, reduzindo assim a possibilidade de uma eventual casualidade humana. O uso destes dispositivos por parte de civis vem aumentando devido à diminuição de custos, versatilidade e facilidade de operação. Existem vários tipos de UAV, com características específicas para uma grande variedade de aplicações, tais como: avaliação e manutenção de estruturas de edifícios, operações de busca e salvamento, entre outras. Inicialmente, os UAV eram veículos militares controlados por um piloto com experiência, sem qualquer mecanismo de estabilização ou eletrónico para ajudar o piloto em viagens de longas distâncias. Hoje, a maioria dos sistemas apresentam mecanismos automatizados capazes de fornecer um voo totalmente automático, ou auxiliar o piloto a controlar o veículo sem se preocupar com a estabilização. Esta evolução permitiu às pessoas civis adaptarem-se mais facilmente a esta tecnologia.

Apesar de os UAV trazerem diversas vantagens, eles também apresentam desvantagens. Como esta tecnologia, relativamente recente e usada por muitas pessoas que não receberam qualquer tipo de treino, as pessoas podem ter dificuldade em perceber que estes aparelhos se não forem manuseados com cuidado conseguem ser perigosos. Em 2016 foram registados 31 incidentes com drones nos aeroportos portugueses. O incidente mais grave ocorreu no Aeroporto Humberto Delgado, 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 [2]. Este género de problemas não acontece apenas em Portugal, mas sim no mundo inteiro [3]. Também existem vários problemas ao nível militar, pois os drones podem transportar explosivos, que podem servir para atacar bases militares, ou até mesmo alvos civis. Neste sentido, houve a necessidade de desenvolver ações e tecnologia com a capacidade de neutralizar "drones clandestinos". Atualmente existem 5 técnicas conhecidas que têm este objetivo: drones anti-drones (são drones que estão equipados com redes, armas ou outros dispositivos); radio jammer (uso do canhão AUDS- sistema de defesa contra UAV); *geofecing* (campo de forças virtual, implementado pelo software associado ao UAV); *drone cannons* (é uma arma que utiliza um radar para interferir com a trajetória do drone, e permite alterar a sua rota utilizando os propulsores do drone) e o raio laser anti-drones (é capaz de destruir os controlos rádio do drone em pleno ar) [4]. Apesar de existirem técnicas com o objetivo de atacar drones é necessário acompanhar o desenvolvimento dos mesmos, criando novas técnicas e evoluindo as antigas de modo a conseguir-se ter técnicas mais eficiente, de menor consumo energético e também de interferência localizada, minimizando os efeitos adversos da interferência com outros sistemas.

1.2 Motivação e objectivos

O trabalho apresentado nesta dissertação de mestrado tem por objetivo estudar e avaliar diferentes tipos de técnicas de jamming utilizando métodos de formação de feixes, que podem ser usados na interferência de drones, evitar interferências involuntárias nos recetores vizinhos e atacar o sistema de comunicação do drone tendo sempre em consideração a redução energética. Para este trabalho irá recorrer-se a uma plataforma de Software Defined Radio (SDR), que é um sistema de comunicação por rádio onde os componentes são geralmente implementados em hardware e o controlo das suas funcionalidades em software.
Para conseguir este objetivo, foram percorridas as seguintes etapas:

- Perceber o conceito de SDR e aprender a usar o GNURadio como uma plataforma de software para implementar diferentes tipos de jammers;
- Estudar as implementações dos diferentes jammers já existentes para SDR no GNURadio, a fim de entender as suas limitações;
- Alterar os jammers encontrados de modo a corrigir as suas limitações e conseguir interferir com o link de comunicações;
- Testar os diferentes tipos de jammers desenvolvidos;
- Analisar, comparar os resultados obtidos para cada jammer e obter conclusões sobre o desempenho de cada jammer;

Este tema de dissertação foi o escolhido, devido ao facto de me possibilitar a aprendizagem de novas plataformas, contribuir para o desenvolvimento futuro da proteção ao uso indevido, e também a forte expansão do mercado de trabalho nesta área.

1.3 Estrutura da dissertação

O capítulo 2 fornece uma visão geral dos conceitos e técnicas que são usados e direcionados para esta tese.
No capítulo 3 é apresentado em detalhe o Hardware e o Software utilizado nesta dissertação, as suas especificações e o seu funcionamento.
No capítulo 4 são apresentados os jammers desenvolvidos no software GNURadio e explicado o seu funcionamento.
O capítulo 5 apresenta a montagem para interferir com o link de comunicações, o alvo do jammers e ainda os testes feitos, recorrendo aos softwares GNURadio e Gqrx.
No capítulo 6 são apresentadas as conclusões que se retiraram com a realização desta tese.

Capítulo 2. Estado de arte

Esta seção fornece uma visão geral dos conceitos e técnicas que são usados e direcionados esta tese.

2.1 Constituição do UAV e da estação terrestre

Na Figura 1 podemos visualizar a constituição do UAV e a estação de controlo terrestre. O UAV é composto por:

- O sistema base que se encontra interligado a todas as outras partes;
- A ligação de comunicações serve para receber e enviar dados entre o UAV e a estação de controlo terrestre;
- Os sensores representam determinadas funcionalidades que podem ser introduzidas no UAV, tais como, GPS e radar;
- O sistema da aeronave que é responsável pela execução dos comandos recebidos, seja através do motor, dos flaps, ou dos estabilizadores.

A estação de controlo terrestre é composta:

- Pelas operações que vão ser enviadas para o drone para serem executadas;
- A ligação de comunicações serve para receber e enviar dados entre a estação de controlo terrestre e o UAV.

Podemos observar que o UAV e a estação terrestre se encontram ligados pela ligação das comunicações, ligação essa que será alvo de jamming na tese de dissertação.

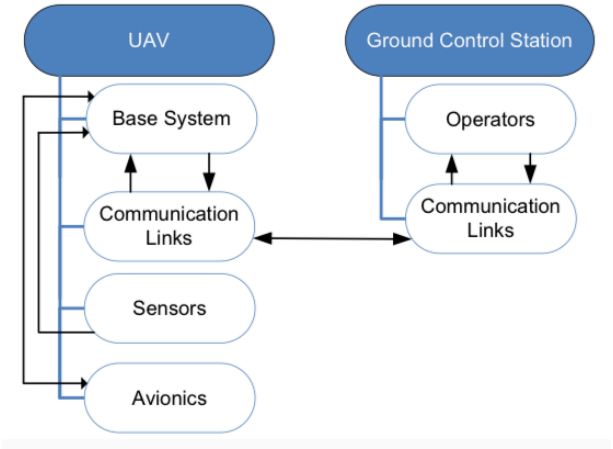

Figura 1-Informação entre os componentes do UAV e a estação terrestre [5]

O link de comunicações num UAV consiste num transmissor de RF e um recetor, uma antena. Para os UAV, os links de dados têm duas funções importantes: (1) *Uplinks* da estação terrestre e/ou um satélite para enviar dados de controlo para o UAV (2) *Downlinks* do UAV para enviar dados dos sensores integrados e do sistema de telemetria para a estação terrestre. Os esforços para padronizar os links de dados resultaram no uso do link de dados comuns (CDL), geralmente um link de dados de banda larga, quando usado pelo UAV normalmente é resistente ao bloqueio e seguro. Esses links ligam a estação terrestre com o UAV através de links diretos, ponto-a-ponto ou usam comunicações por satélite (SATCOM) [6].

2.2 Software Defined Radio

O termo “Software Defined Radio (SDR)” foi criado em 1991 por Joseph Mitola III [7]. A organização IEEE, definiu SDR como um conjunto de sistemas rádio onde grande parte das suas funções são definidas através de um software [8]. O SDR é composto por duas tecnologias: rádio digital e software de computador. Graças aos rádios digitais, grande parte do processamento é realizado no domínio digital, mantendo-o mais próximo do front-end de RF. Componentes que geralmente são implementados em hardware (por exemplo, amplificadores, filtros, modeladores, etc.) são implementados pelo meio do software ou hardware programável [9].

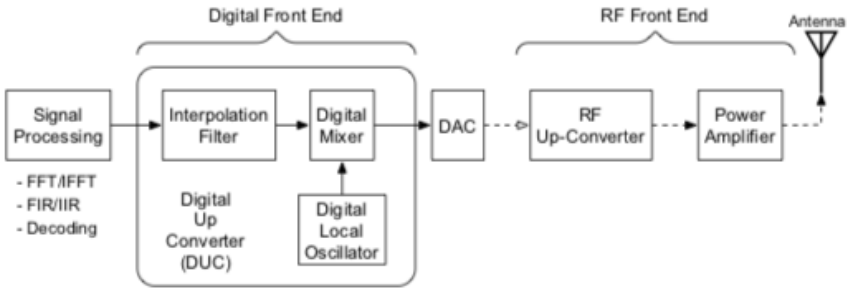

Figura 2-Arquitetura básica do SDR vista do lado do transmissor [10]

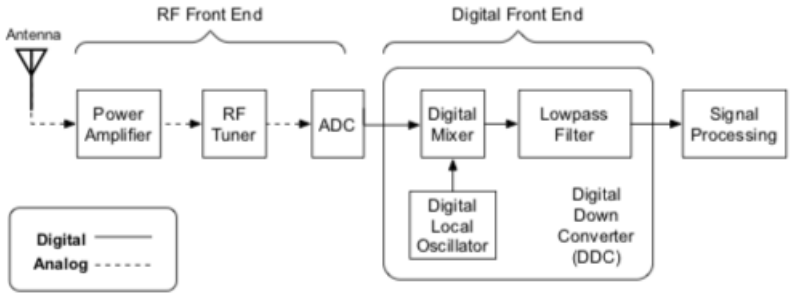

Figura 3-Arquitetura básica do SDR vista do lado do recetor [10]

Como é possível visualizar na Figura 2. e Figura 3, um típico SDR apresenta as seguintes componentes: uma antena, RF Frontal Analógico, Frontal Digital e Processamento de Sinal.
1) Antena: as plataformas SDR geralmente necessitam de várias antenas para cobrir uma ampla gama de bandas de frequências [11]. As antenas são muitas vezes referidas como "inteligentes" devido à sua capacidade de escolher uma banda de frequências e adaptar-se ao rastreamento móvel ou ao cancelamento de interferências [12], [13].
2) RF Front End: Este é um circuito RF cuja principal função é transmitir e receber o sinal em várias frequências. Outra função é mudar o sinal para / da Frequência Intermediária (IF). O processo de operação é dividido em dois, dependendo da direção do sinal (ou seja, modo Tx ou Rx):

- No caminho de transmissão, as amostras digitais são convertidas num sinal analógico pelo Conversor Digital-para-Analógico (DAC), que por sua vez alimenta o Front End RF. Este sinal analógico é misturado com uma frequência de RF predefinida, modulada e depois transmitida.
- No caminho de receção, a antena captura o sinal de RF. A entrada da antena é ligada ao RF Front End usando um circuito correspondente para garantir uma transferência de potência de sinal ideal. Em seguida, passa através de um amplificador de baixo ruído (LNA), que se encontra próximo da antena, para amplificar os sinais fracos e minimizar o nível de ruído. Este sinal amplificado, com um sinal do Oscilador Local (LO), é alimentado pelo mixer para convertê-lo para o IF [14].

3) Digital Front End: O Digital Front End tem duas funções principais [15]:

- Sample Rate Conversion (SRC), que é uma funcionalidade para converter a amostras de uma taxa para outra. Isso é necessário, pois as duas partes da comunicação devem estar sincronizadas.
- Canalização, que inclui conversão up/down no lado do transmissor e do recetor, respetivamente. Também inclui filtragem de canais, onde os canais divididos por frequência são extraídos. Exemplos incluem interpolação e filtros passa-baixo, como pode ser observado nas Figura 2 e 3.

As seguintes tarefas são executadas no front end digital:

- No lado de transmissão (Figura 2), o conversor digital ascendente (DUC) converte o sinal de banda base para IF. O DAC que está conectado ao DUC, então, converte as amostras IF digitais em um sinal IF analógico. Posteriormente, o conversor up RF converte o sinal IF analógico em frequências RF.
- No lado de receção (Figura 3), o ADC converte o sinal IF em amostras digitais. Essas amostras são subsequentemente alimentadas no próximo bloco, que é o Digital Down Converter (DDC). O DDC inclui um mixer digital e um oscilador controlado numericamente. O DDC extrai o sinal digital de banda-base do ADC e, depois de processado pelo Digital Front End, esse sinal de banda-base digital é encaminhado para um bloco de processamento de sinal digital de alta velocidade [16].

5) Processamento de Sinais: operações de processamento de sinais, tais como codificação/descodificação, modulação/desmodulação, são realizadas neste bloco. Codificação para o canal serve como um código de correção de erros. Especificamente, o sinal codificado inclui redundância que é utilizada pelo descodificador do recetor para reconstruir o sinal original a partir do sinal recebido corrompido. Exemplos de códigos de correção de erro incluem códigos de convolução, códigos turbo e verificação de paridade de baixa densidade (LDPC) [17]. O descodificador constitui a parte mais intensivamente computacional do bloco de Processamento de Sinal, devido à transferência de dados e esquemas de memória [18]. A segunda parte que é considerada altamente complexa e cara (em termos de área e potência) é a Transformada Rápida de Fourier (FFT) e a Inversa FFT (IFFT), como parte da fase de modulação [19].

O bloco de processamento de sinal também é chamado de bloco de processamento de banda base. Ao falar de SDR, o bloco de banda base está no centro da discussão, pois compõe a maior parte do domínio digital da implementação. Essa implementação é executada sobre um circuito de hardware que é capaz de processar sinais com eficiência. Exemplos incluem ASICs, FPGAs, DSPs, GPPs e GPUs. A segunda parte da implementação é o software, que fornece a funcionalidade e abstrações de alto nível para executar operações de processamento de sinal.

Em termos de software para o desenvolvimento de aplicações SDR, o GNURadio é uma das ferramentas mais populares. O GNURadio é um software gratuito e de código aberto que fornece blocos de processamento de sinal para implementar programas rádio. O que torna esta tecnologia mais usada em detrimento de outros, é devido ao facto de ser possível mover blocos ao longo da cadeia de processamento. Como move grandes quantidades de memória armazenadas nos blocos, em vez de amostra por amostra, permite que seja mais fácil e eficiente, portanto adequado ao processamento de sinal em tempo real [9].

2.3 Plataformas de SDR

Em relação ao hardware, os jammers mais caros disponíveis no mercado permitem apenas interferir com uma frequência configurada específica. Não é possível analisar essa frequência específica nem configurar o equipamento para uma frequência diferente, o que torna seu uso limitado, não apenas pela sua configuração, mas também pela sua única frequência de operação.
Um equipamento SDR é definido, em geral, como um com uma ampla gama de frequências e sem foco em qualquer frequência específica. Com o aparecimento de equipamentos SDR todos os anos, é necessário escolher qual o equipamento que irá ser utilizado na elaboração da tese de dissertação. A partir da análise de vários SDRs de acordo com o custo, a faixa de frequência, a resolução do ADC e a capacidade de transmitir ou receber sinais, a escolha recai entre três equipamentos: a BladeRF, a HackRF One e o USRP B200/B210, que são representados na Figura 4, Figura 5 e Figura 6 respetivamente.

Figura 4-BladeRF [20]

Figura 5-HackRF One [21]

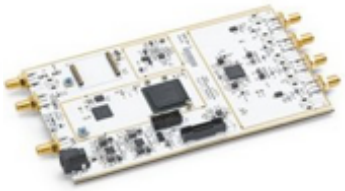

Figura 6-Figura 6-USRPB200/B210 [22]

A BladeRF é uma plataforma SDR onde existem duas versões que custam cerca de 355 euros e 550 euros, pode operar em full duplex, o que significa que pode receber e transmitir simultaneamente. Ela tem uma faixa de frequência (300 MHz a 3,8 GHz) e uma resolução (ADC) de 12 bits, que faz dele um receptor melhor do que a HackRF, mas perde as frequências abaixo de 300 MHz, que podem ser recebidas com um transformador por um custo extra.
A HackRF One é o mais barato dos três e é um dos primeiros SDRs de baixo custo que surgiram no mercado, cujo preço é de cerca de 250 euros. É capaz de receber e também transmitir. É uma plataforma half duplex que significa que é necessário alternar entre modos por comando. As suas principais vantagens são os seus recursos de transmissão, ampla largura de banda e uma ampla faixa de frequência maior (1 MHz a 6 GHz) em comparação com a BladeRF. A única desvantagem é a sua pequena resolução de 8 bits e o pobre design de RF que afeta o desempenho de sinal-ruído (SNR).
O USRP B200 / B210 é o mais dispendioso dos três, já que também existem duas versões que custam cerca de 570 euros e 930 euros. É considerado um SDR avançado voltado mais para o mercado profissional e de pesquisa. Tem a possibilidade de transmitir e receber em full duplex com dois sinais ao mesmo tempo e tem a mesma resolução ADC que a BladeRF. Tem maior largura de banda do que o BladeRF (70 MHz a 6 GHz), não suportando frequências inferiores a 70 MHz.

A plataforma escolhida para a realização desta tese de dissertação, foi a BladeRF, uma vez que para desenvolver jammers do link de comunicações basta que o SDR consiga interferir com as frequências na ordem dos 2.4GHz. Também é importante que consiga funcionar em modo full duplex, conseguindo assim tanto transmitir, como receber sinais. De entre estas três plataforma a BladeRF cumpre os requisitos e consegue ser mais barata que o USRP. A BladeRF irá ser analisada em pormenor mais à frente.

2.4 Espalhamento do espectro

Os drones, comercialmente disponíveis utilizam técnicas de espalhamento espectral para reduzir a interferência de ruído e a interferência com outros drones que se podem encontrar a operar nas proximidades. O desenvolvimento deste tipo de técnicas ocorreu na década de 1940, para aumentar a resistência ao bloqueio e também para impedir a deteção [23]. Só é possível conseguir aumentar a resistência ao bloqueio e prevenir a deteção, com a transmissão de um sinal que ocupa a largura de banda superior à largura de banda mínima para a transmissão de dados (Figura 7) [24]. As técnicas de espalhamento do espectro que serão analisadas, são: Direct-Sequence Spread Spectrum e Frequency-Hopping Spread Spectrum.

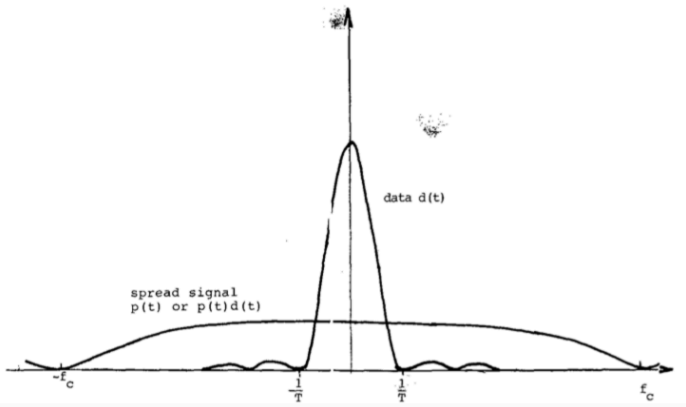

Figura 7-Potência do espectro do sinal e do espalhamento do espectro [25]

2.4.1 Processamento do ganho

Os sistemas de comunicação que utilizam o espalhamento do espectro beneficiam da maior largura de banda ocupado pelo sinal modulado em comparação com o sinal de dados. Esse aumento de largura de banda, que é característica do aumento de resistência do sistema de comunicação à interferência, é geralmente referida como ganho de processamento [26]. O ganho de processamento (Gp) (Equação 1) de um sistema de comunicação por espalhamento espectral é definido pela razão entre a largura de banda do sinal modulado e a largura de banda. O princípio subjacente ao ganho de processamento é que, ao distribuir um sinal de dados de banda relativamente estreita numa faixa mais ampla, força um jammer com uma quantidade fixa de potência total a espalhar essa potência fixa sobre toda a largura de banda, induzindo assim um pouco de interferência em cada subseção, ou então coloca toda a potência numa pequena subseção, deixando o restante da banda livre de interferências [24].

$$Gp = \frac{Bss}{Bd} \tag{1}$$

A interferência que podia ser anulada com sucesso teoricamente devia ser igual ao ganho de processamento, mas não é verdadeiramente assim. O nível de interferência que um sistema é capaz de aceitar e ainda manter um nível especificado de desempenho é chamado de margem de interferência e, para sistemas de espectro expandido de sequência direta e salto de frequência com ganho de processamento idêntico, as margens de interferência são bem diferentes. O ganho de processamento de um sistema será sempre maior que sua margem de congestionamento.
A margem de interferência é definida como na Equação 2, onde Gp é o ganho de processamento [dB], Lsystem representa as perdas do sistema [dB] e SNRmin [dB] é a relação sinal-ruído de saída (SNR) mínima requerida. A perda de implementação do sistema é uma consequência da

sincronização imperfeita no recetor, correlação imperfeita da forma de onda recebida e da sequência de dispersão e assim por diante. Todos os sinais modulados requerem um SNR de saída mínimo para realizar um determinado nível [28].

$$Mj = Gp - [Lsystem + SNRmin] \quad (2)$$

2.4.2 Direct-Sequence Spread Spectrum

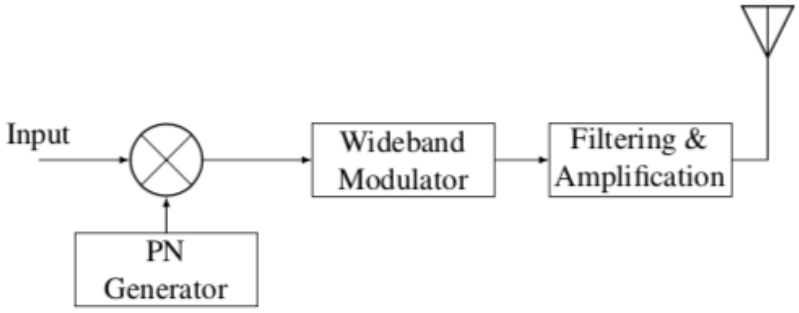

Figura 8-Transmissor de sinais DSSS[28]

Nos sistemas de comunicação DSSS, o sinal de dados é multiplicado por um código PN (Figura 8), que possui uma taxa maior que o sinal de dados. Um sinal mais rápido resulta numa maior largura de espectro e o sinal resultante da multiplicação tem a mesma largura de banda que o sinal PN usado para codificação [26]. Para sistemas de comunicação DSSS, o ganho de processamento (Equação 3) é definido pela razão entre a largura de banda do sinal PN e a largura de banda do sinal de dados, isto corresponde à razão do tempo dos bits do PN por o tempo de bits dos dados [27].

$$Gp = \frac{Bss}{Bd} = \frac{Tb}{Tc} = Nc \quad (3)$$

A margem de interferência de um sistema DSSS é, pelo menos, a diferença entre o ganho de processamento e o SNR mínimo na saída e diminuída ainda mais pelas possíveis perdas de implementação no sistema DSSS.

2.4.3 Frequency-Hopping Spread Spectrum

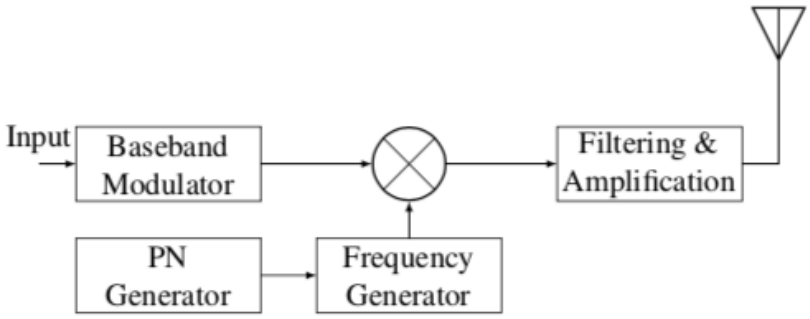

Figura 9-Transmissor de sinais FHSS[28]

Nos sistemas de comunicação FHSS, o sinal de dados é modulado num sinal de portadora e a frequência do sinal da portadora é alterada periodicamente (Figura 9), o que ajuda o sistema a evitar interferência de banda estreita [29]. O FHSS é dividido em salto de frequência rápida e salto de frequência lenta com base na quantidade de bits de dados enviados por salto de frequência. Para ambos os tipos de sistemas de comunicação FHSS, o ganho de processamento (Equação 4) é definido pela relação entre a largura de banda total de todos os canais e a largura de banda de um único canal [27], ou seja, o número de canais Nc com largura Bd em Bss.

$$Gp = \frac{Bss}{Bd} = Nc \tag{4}$$

A margem de bloqueio para sistemas FHSS não está claramente definida, porque nos sistemas FHSS a interferência com a desmodulação ocorre somente quando o interferente está dentro do canal atual. A interferência num canal, não têm efeito sobre os outros canais, desde que os filtros de canal tenham seletividade suficiente. A taxa de transferência de um sistema FHSS vai para zero somente quando o sinal de interferência estiver presente em todos os canais. Isso difere do DSSS, em que um único interferente com energia suficiente pode reduzir a taxa de transferência para zero [30].

2.5 Code-Division Multiple Access

O CDMA é um método de acesso de canal utilizado por várias tecnologias de comunicações por rádio [31]. Esta técnica é um exemplo de acesso múltiplo, pois permite que vários utilizadores partilhem uma faixa de frequências. Para permitir isso sem a interferência de utilizadores, esta tecnologia utiliza o espalhamento espectral e um esquema de codificação especial (onde cada transmissor recebe um código) [31].
Esta técnica espalha a largura de banda dos dados uniformemente pela mesma potência transmitida. Um código de dispersão é um código pseudoaleatório que possui uma função estreita de ambiguidade, ao contrário de outros códigos de pulso estreitos. No CDMA, um código gerado localmente é executado numa taxa muito maior do que os dados a serem transmitidos. Os dados para transmissão são combinados por XOR bit a bit (OR exclusivo) com o código mais rápido. A Figura 10 mostra como um sinal de espectro espalhado é gerado. A divisão do *Tb* pelo *Tc* representa o ganho de processamento e determina o número máximo de utilizadores que podem utilizar simultaneamente a estação base.

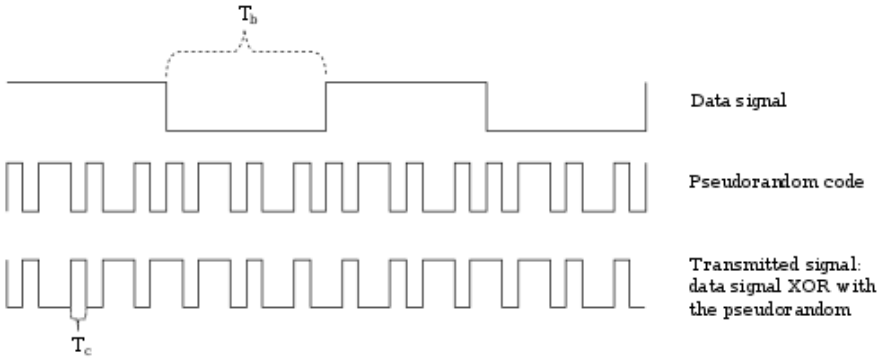

Figura 10-Funcionamento do CDMA [32]

Cada utilizador de um sistema CDMA usa um código diferente para modular o seu sinal. A escolha dos códigos usados para modular o sinal é muito importante no desempenho dos sistemas CDMA [32]. O melhor desempenho ocorre quando há uma boa separação entre o sinal de um utilizador desejado e os sinais de outros utilizadores. A separação dos sinais é feita correlacionando o sinal recebido com o código gerado localmente do utilizador desejado. Se o sinal corresponder ao código do utilizador desejado, a função de correlação será alta e o sistema poderá extrair esse sinal. Se o código do utilizador desejado não tem nada em comum com o sinal, a correlação deve ser o mais próxima possível de zero (eliminando assim o sinal); isso é chamado de correlação cruzada. Se o código estiver correlacionado com o sinal a qualquer tempo diferente de zero, a correlação deve ser o mais próxima possível de zero. Isso é conhecido como autocorrelação e é usado para rejeitar a interferência de vários caminhos.

2.6 Ortogonal Frequency-Division Multiplexing

A Multiplexagem por Divisão de Frequência Ortogonal (OFDM) é um esquema de modulação de portadora múltipla digital que estende o conceito de modulação de subportadora única usando múltiplas subportadoras dentro do mesmo canal. Em vez de transmitir um fluxo de dados de taxa alta numa única subportadora, o OFDM faz uso de um grande número de subportadoras ortogonais espaçadas próximas, entre si, que são transmitidas em paralelo. Cada subportadora é modulada com um esquema de modulação digital convencional (como QPSK, 16QAM, etc.) com baixa taxa de símbolos. No entanto, a combinação de muitas subportadoras permite taxas de dados semelhantes aos esquemas convencionais de modulação de portadora dentro de larguras de banda equivalentes. [33]
Esta técnica baseia-se na técnica conhecida como Multiplexagem por Divisão de Frequência (FDM). No FDM, diferentes fluxos de informação são mapeados em canais de frequência paralelamente separados. Cada canal FDM é separado dos outros por uma banda de proteção de frequência para reduzir a interferência entre os canais adjacentes [33].
O esquema OFDM difere do FDM tradicional nos seguintes pontos [33]:

1. Múltiplas portadoras (chamadas subportadoras) carregam o fluxo de informações;
2. As subportadoras são ortogonais entre si;
3. Um intervalo de guarda é adicionado a cada símbolo para minimizar a dispersão do atraso do canal e a interferência intersimbólica.

A Figura 11, ilustra os principais conceitos de um sinal OFDM e a relação entre os domínios de frequência e tempo. No domínio da frequência, as subportadoras são modeladas independentemente com dados complexos. Uma transformada Inversa de FFT é executada nas subportadoras de domínio de frequência para produzir o símbolo OFDM no domínio do tempo. Então, no domínio do tempo, intervalos de guarda são inseridos entre cada um dos símbolos para evitar interferência inter-símbolo no receptor causada por propagação de atraso de múltiplos caminhos no canal de rádio. Vários símbolos podem ser concatenados para criar o sinal de rajada OFDM final. No receptor, uma FFT é executada nos símbolos OFDM para recuperar os bits de dados originais. [33]

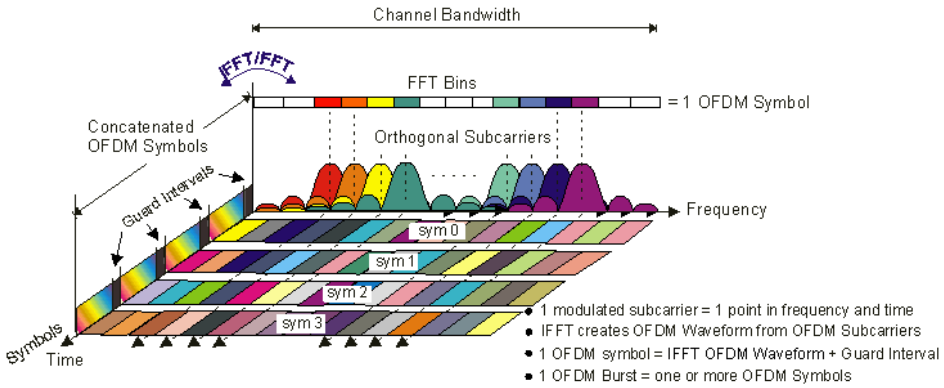

Figura 11-Relação frequência-tempo no OFDM [33]

2.7 Phase-Shift Keying

O Phase-Shift Keying (PSK) é um tipo de modulação digital que transmite dados modulando a fase de um sinal de referência de frequência constante. A modulação é realizada variando as entradas de seno e cosseno num determinado momento. Qualquer esquema de modulação digital utiliza um número finito de sinais distintos para representar dados digitais. O PSK usa um número finito de fases, cada uma atribuída a um padrão único de dígitos binários. Normalmente, cada fase codifica um número igual de bits. Cada padrão de bits forma o símbolo que é representado pela fase particular [34].

2.7.1 Binary Phase-Shift Keying

O BPSK é a forma mais simples de PSK. Ele utiliza duas fases que são separadas por 180° e, portanto, também pode ser denominado 2PSK. Não importa exatamente onde os pontos da constelação estão posicionados, e na Figura 12 eles são mostrados no eixo real, em 0 ° e 180°. No entanto, apenas é capaz de modular a 1 bit / símbolo (Figura 12) e, portanto, é inadequado para aplicações de taxa de dados alta [34].

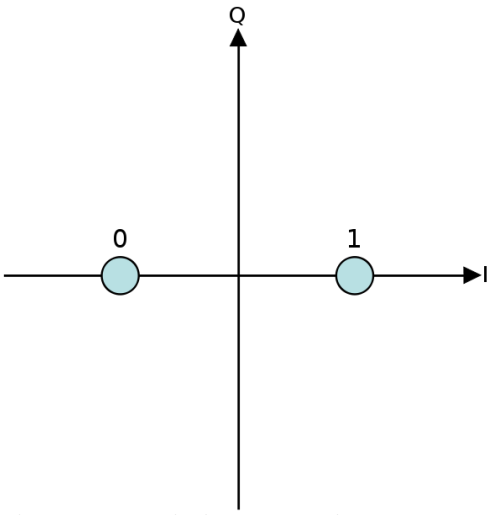

Figura 12-Exemplo de uma constelação BPSK[34]

2.7.2 Quadrature Phase-Shift Keying

O QPSK utiliza quatro pontos no diagrama de constelação, dispostos em torno de um círculo. Com quatro fases (Figura 13), o QPSK pode codificar dois bits por símbolo, mostrados no diagrama com a codificação Gray para minimizar a taxa de erro de bit (BER) - às vezes mal interpretado como o dobro do BER do BPSK. A análise matemática mostra que o QPSK pode ser usado para dobrar a taxa de dados em comparação com um sistema BPSK, mantendo a mesma largura de banda do sinal, ou para manter a taxa de dados do BPSK, mas reduzindo pela metade a largura de banda necessária [34].

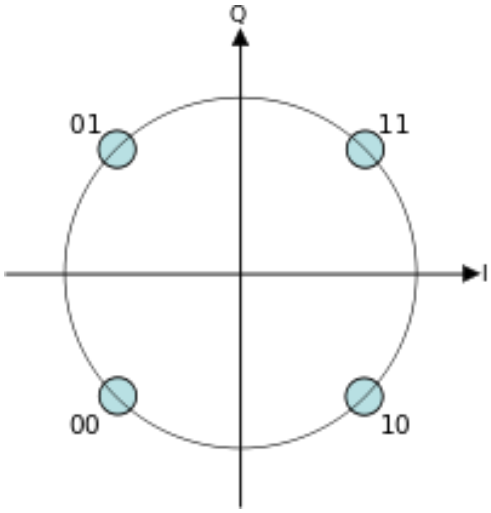

Figura 13-Exemplo de uma constelação QPSK[34]

2.8 Técnicas de Jamming

Nesta parte irão ser apresentados diversos tipos de técnicas de jamming que serão aplicadas nesta dissertação para tentar interferir com o link de comunicações dos drones. Estas técnicas foram retiradas de [29] e têm por base os trabalhos de Poisel [26], Lichtman [35] e Grover [36]. Cada uma destas técnicas apresenta as respetivas vantagens e desvantagens.
Na Figura 14 é possível observar o espectro de vários canais, utilizando o espalhamento por saltos de frequência.

Figura 14-Espectro em cada canal [28]

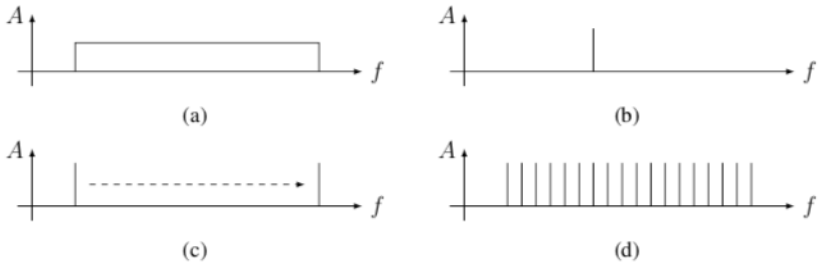

Figura 15-Espectro nos canais de 4 técnicas de jamming [28]

(a)-Barrage Jamming (b)-Tone Jamming (c)-Sweep Jamming
(d)Protocol-aware Jamming

2.8.1 Barrage Jamming

É a forma mais simples de interferência e é geralmente definido como um jammer (Figura 15 (a)) que transmite ruído em todo o espectro. Este jammer aumenta o nível de ruído no recetor, o que dificulta a comunicação. É bastante utilizado quando não se tem qualquer conhecimento do alvo. Umas das desvantagens é que consome bastante energia e não existe nenhuma maneira de selecionar qual o sinal que se deve bloquear.
Este é o melhor jammer para ser utilizado num caso em que não se conheça o sinal alvo [37].

2.8.2 Tone Jamming

Este jammer (Figura 15 (b)) é utilizado apenas para interferir com uma frequência. Também existe o multitone jamming em que neste caso se consegue interferir com mais frequências. No tone jamming a potência é utilizada apenas numa frequência, enquanto que no multitone jamming a potência é distribuída por todas as frequências.
O bloqueio de tons apresenta desvantagens similares em comparação com o bloqueio de barragem ao atacar sistemas de espectro expandido. Para que o jamming funcione contra sistemas de espalhamento espectral, ele precisa superar a margem de interferência e, portanto, possuir altos requisitos de energia, o que resulta numa alta probabilidade de deteção.

2.8.3 Sweep Jamming

Este jammer (Figura 15 (c)) é uma combinação do barrage jamming com tone jamming. É parecido com o barrage jamming pois transmite um sinal em todo o espectro e com o tone jamming pois apenas uma parte desse mesmo espectro é bloqueada por um determinado período de tempo.
Também é possível setorizar a estratégia de interferência e evitar interferir em determinadas bandas que possam ser necessárias do ponto de vista do utilizador. Isto é verdade apenas quando a temporização é feita sob medida para os recetores alvo, de modo que o sinal de interferência esteja presente no recetor por um tempo adequado.

2.8.4 Protocol Jamming

É uma técnica de jamming (Figura 15 (d)) em que se procura interferir com um sinal, utilizando os mesmos parâmetros do protocolo desse mesmo sinal. Alguns desses parâmetros podem ser o tipo de modulação utilizada ou a largura de banda. Uma das vantagens deste jammer é ele não congestionar outros sistemas que operarem na mesma frequência.
A capacidade de sincronizar a forma de onda de interferência com o sinal de destino também é necessária em interferência com reconhecimento de protocolo. Este problema é exacerbado pelo tempo de voo do alvo e pelos sinais de interferência, o que é difícil de prever.
A viabilidade do uso deste jamming tem sido estudada principalmente em sistemas de comunicação de rede local sem fio baseados em IEEE 802.11 e concluiu-se que podem atingir interferência efetiva com requisitos de energia muito baixos e baixa probabilidade de deteção do sinal de interferência [38] [39]. O jamming com reconhecimento de protocolo também evita o congestionamento de outros sistemas de comunicação que operam na mesma banda de RF, porque o sinal de atolamento com reconhecimento de protocolo é apenas nas partes da banda que são usadas pelo sinal alvo.

2.9 Fórmula de Friis

A fórmula de Friis é utilizada na área das telecomunicações e relaciona a potência transmitida de uma antena para outra em determinadas condições ideais. A fórmula é descrita da seguinte maneira. Dadas duas antenas, a razão da potência recebida pela antena de receção, Pr, sobre a potência transmitida à antena de receção, Pt, é dado por:

$$\frac{Pr}{Pt} = Gt \times Gr \times (\frac{\lambda}{4\pi R})^2 \quad (5)$$

Onde Gt e Gr, são os ganhos das antenas de transmissão e receção, respetivamente, λ é o comprimento de onda e R a distância entre antenas. Os ganhos das antenas são obtidos com antenas isotrópicas (em unidades lineares), com o comprimento de onda e a distância nas mesmas unidades.
A fórmula afirma que a quantidade de potência transferida entre duas antenas é proporcional ao produto dos ganhos das antenas. De acordo com isto, problemas de baixo ganho em antenas de transmissão podem ser compensadas com um ganho alto em antenas de receção e vice-versa. Isto é muito importante em várias aplicações práticas, dado que é por vezes é necessária uma antena ter baixo ganho devido a restrições de tamanho, peso ou potência disponível, como acontece com as antenas situadas em satélites ou naves espaciais [40].
Esta equação é aplicável nas seguintes condições ideais [40]:

- As antenas estão em espaço aberto e não obstruído;
- Pr representa a potência disponível nos terminais da antena de receção. Não é totalmente entregue ao recetor a não ser que exista adaptação de impedância com a antena;
- Pt representa a potência disponível nos terminais da antena de transmissão. Não é totalmente entregue à potência de transmissão a não ser que exista adaptação de impedância com a antena;
- As antenas têm que estar alinhadas sobre a mesma polarização e orientadas de maneira a que cada antena radie na direção máxima da outra.

As condições ideias quase nunca são alcançadas em condições terrestres normais, devido a obstruções, reflecções em edifícios e, ainda mais importante, devido a reflecções na terra. Uma situação onde a equação é razoavelmente eficiente é em comunicações por satélite, onde a absorção atmosférica é desprezável [40].

2.10 Técnica Rohde & Schwarz

A técnica Rohde & Schwarz permite detetar, identificar, localizar e atacar o alvo no menor tempo possível. Esta técnica foca-se nos seguintes pontos:

- Rápida resposta: deteção, identificação, encontrar e efetuar o jamming de ameaças em menos de 20s;
- Alcance de frequências: cobre grande parte das frequências usadas pelos drones modernos (433 MHz, 2.4 GHz, 5.8 GHz);
- Jamming efetivo: dispositivo avançado com o propósito de atacar, onde apenas o sinal de rádio controlo do drone deve ser atacado e os outros sinais legais na mesma banda de frequência não devem ser afetados.

Jamming efetivo do link de rádio controlo do drone pode ter várias consequências, tais como forçar a sua aterragem no chão, reprogramar a posição do drone, causando a sua aterragem ou eventualmente a ativação do modo return-to-home. O objetivo do jamming é criar uma forte interferência no link de rádio controlo, de modo a assim ser possível desativar as comunicações com o operador e eliminar uma possível ameaça hostil. É possível efetuar jamming com o R&S jammer a partir de 2/3 de distância, como se pode observar na Figura 16.

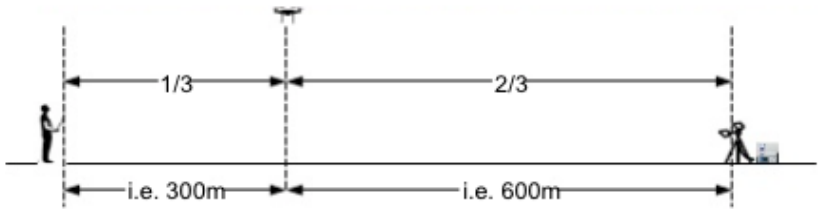

Figura 16-Jamming com sucesso do link de comunicações [41]

O sucesso do bloqueio RC está no reconhecimento abrangente prévio. Uma lista de links RC (FHSS) com ameaças potenciais é conhecida pelo usuário do sistema de interferência, incluindo os seus parâmetros de modulação principais (por exemplo, frequências de salto, tempo, taxa de salto, largura de banda do canal, tipo de modulação, taxa de símbolos). O jammer é especialmente adaptado e útil para o servir de contramedida aos drones, onde cada um dos saltos contém as informações RC do drone e todos devem estar atolados [41].
Em vez do bloqueio de barragem, que precisa de um poder de transmissão muito maior, a solução única fornecida pela R&S baseia-se num modo de interferência "seguidor", em que cada rajada única do sinal RC é atacada, mas não os outros sinais legais. Isso permite o bloqueio do RC selecionado com quase nenhuma perturbação de outros sinais de comunicação dentro da mesma faixa de frequência (por exemplo, comunicações WLAN/Wi-Fi). O tempo é um critério muito crítico no bloqueio do drone. Uma vez que o link RC direcionado é detetado dentro da largura de banda em tempo real, a resposta do jammer deve ser rápida o suficiente para atingir o salto enquanto ele ainda está no ar. A solução de bloqueio R&S é capaz de detetar e responder a uma única rajada ativa. Uma vez que o próximo salto está ativo, o sistema deteta-o imediatamente dentro da largura de banda em tempo real de 80 MHz e responde de acordo. Todas as emissões detetadas e cada transmissão de interferência são exibidas em diagramas estatísticos e podem ser adicionalmente observadas em um espectro de RF [41].

Capítulo 3. Hardware e Software

Neste capítulo é apresentado em detalhe o Hardware e o Software utilizado nesta dissertação, as suas especificações e o seu funcionamento.

3.1 Hardware

3.1.1 BladeRF

Como foi falado no capítulo 2, nesta dissertação a plataforma de SDR que irá ser utilizada é a BladeRF. Esta plataforma foi desenvolvida para permitir que universitários e entusiastas conseguiam estudar as comunicações de RF. Este hardware consegue funcionar em Linux, OSX e Windows. As suas especificações encontram-se em [42]. Na Figura 17 é possível visualizar a arquitetura da BladeRF ao detalhe.

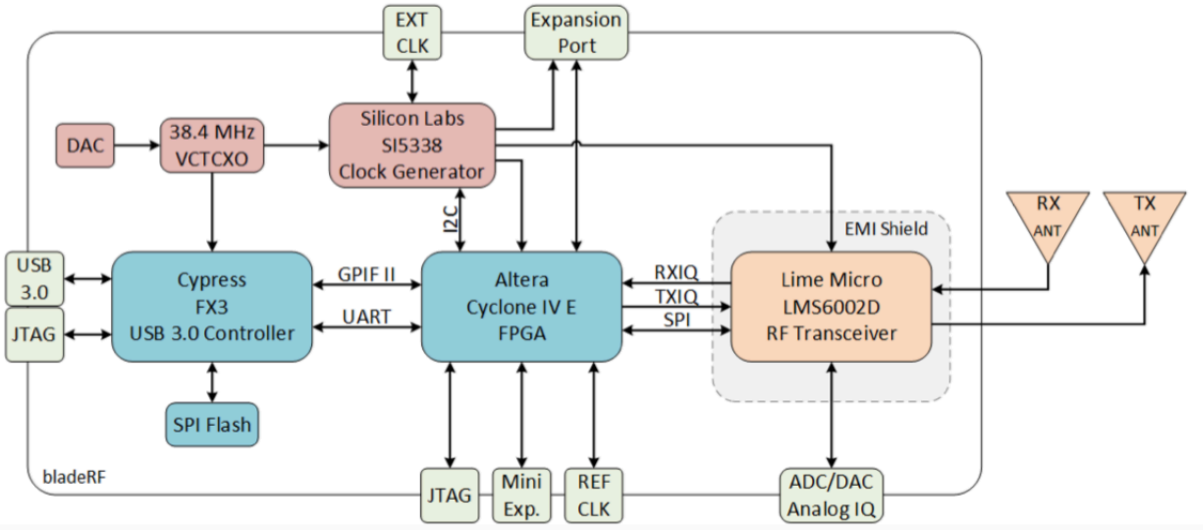

Figura 17-Arquitetura da BladeRF [42]

A arquitetura da BladeRF encontra-se dividida em três grandes partes:

- O FPGA é um chip que suporta a implementação de circuitos lógicos relativamente grandes. Consiste num grande conjunto de blocos lógicos configuráveis contidos num único circuito integrado. Cada bloco contém capacidade computacional para implementar funções lógicas e realizar roteamento para a comunicação entre elas.
  No interior de cada bloco lógico do FPGA existem vários modos possíveis para implementação de funções lógicas. O mais utilizado pelos fabricantes de FPGA como, por exemplo, a empresa Altera Corp, é o bloco de memória LUT (Look-Up Table). Esse tipo de bloco lógico contém células de armazenamento que são utilizadas para implementar pequenas funções lógicas. Cada célula é capaz de armazenar um único valor lógico: zero ou um. Nos FPGAs disponíveis comercialmente como, por exemplo, da empresa Altera Corp, os blocos lógicos LUTs possuem geralmente quatro ou cinco entradas, o que permite endereçar 16 ou 32 células de armazenamento. Quando um circuito lógico é implementado num FPGA, os blocos lógicos são programados para realizar as funções necessárias, e os canais de roteamento são estruturados de forma a realizar a interconexão necessária entre os blocos lógicos [43];

- O LMS6002D pode ser configurado digitalmente para operar em qualquer faixa de frequência de comunicações móveis (300MHz a 3.8GHz) e ser usado em qualquer padrão de comunicações móveis 2G, 3G ou 4G. Além disso, os utilizadores podem configurar facilmente o dispositivo com 16 larguras de banda de até 28MHz. O chip incorpora múltiplas entradas e saídas de RF para permitir que uma ampla gama de recursos seja implementada. Os seus blocos ADC e DAC de 12 bits permitem a interface direta com praticamente qualquer IC de banda base, DSP e FPGA. O LMS6002D possui uma Interface de Porta Serial (SPI) padrão para programação e inclui provisão para uma calibração completa de RF. O dispositivo combina LNA, driver PA, mixers RX / TX, filtros RX / TX, sintetizadores, controlo de ganho RX e controlo de potência TX. Também substitui vários chips individuais e permite que o equipamento seja reconfigurado de forma rápida e simples [44];

- Cypress EZ-USB FX3 é o único controlador de periféricos SuperSpeed USB 3.0 da indústria que permite aos programadores adicionar a funcionalidade do dispositivo USB 3.0 a qualquer sistema. O EZ-USB FX3 possui uma Interface Geral Programável (GPIFII) totalmente configurável que pode interagir com qualquer processador, ASIC, sensor de imagem ou FPGA [45].

3.1.2 XB300

O XB-300 (Figura 18) é um cartão de expansão amplificador que aumenta o desempenho de RF da BladeRF. A placa amplificadora possui um LNA, um combinador de diversidade para RX, e um amplificador de potência, comutador TRX e ADC de alta precisão para medir a potência de saída para TX. Na Figura 19 encontra-se representada uma tabela que contêm os consumos e as diversas configurações possíveis quando a BladeRF se encontra ligada ao amplificador [46]. Em [47] é possível visualizar a arquitetura do amplificador e em [46] encontram-se as especificações.

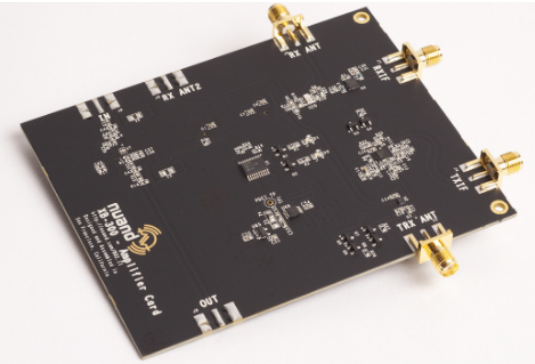

Figura 18-XB300 [46]

RX	TX	RX / TX Freq (MHz)	IBW (MHz) / SR (MSPS)	RX Gains (dB) LNA / VGA1 / VGA2	TX Gains (dB) VGA1 / VGA2	Power (W)
OFF	OFF	2402 / 2400	28 / 40	6 / 30 / 30 (max)	-4 / 25 (max)	2.314
ON	OFF	2402 / 2400	28 / 40	6 / 30 / 30 (max)	-4 / 25 (max)	3.133
OFF	ON	2402 / 2400	28 / 40	6 / 30 / 30 (max)	-4 / 25 (max)	8.584
ON	ON	2402 / 2400	28 / 40	6 / 30 / 30 (max)	-4 / 25 (max)	**9.013**

Figura 19-Tabela de potências [48]

3.1.3 Apex TG.30 Ultra-Wideband Dipole LTE Antenna

A antena Dipole LTE (Figura 20) de banda extralarga Apex TG.30 - é projetada para o uso com módulos 4G LTE e dispositivos que exigem a mais alta eficiência e ganho de pico para oferecer a melhor produtividade em todas as principais gerações em todo o mundo para pontos de acesso, terminais e routers. A antena é uma antena independente do plano terra com um conector SMA (M) e um mecanismo giratório que permite que a parte da antena seja girada. O Apex exibe alta eficiência em toda a banda ultra larga e é compatível com 2G e 3G, como GSM, LTE, UMTS, WI-FI e até mesmo GPS incluído para aplicações de GPS Assistido e/ou E911. Com uma eficiência muito alta em todas as bandas móveis, é uma solução ideal para qualquer dispositivo que exija um desempenho alto e confiável. Também é garantido que atenda a qualquer tipo de aprovação ou requisitos de certificação de transportadora do ponto de vista de RF. É uma antena omnidirecional e os padrões de radiação mostram isso e são estáveis em todas as bandas [49].

Figura 20-Antena Dipole LTE de banda extralarga Apex TG.30 [49]

A antena apresenta algumas características, das quais vale a pena destacar [49]:

- O diagrama de radiação (Figura 21) para as frequências apresentadas;
- A impedância de 50 Ohm;
- Intervalo de frequências da antena de 1710-2700 MHz.

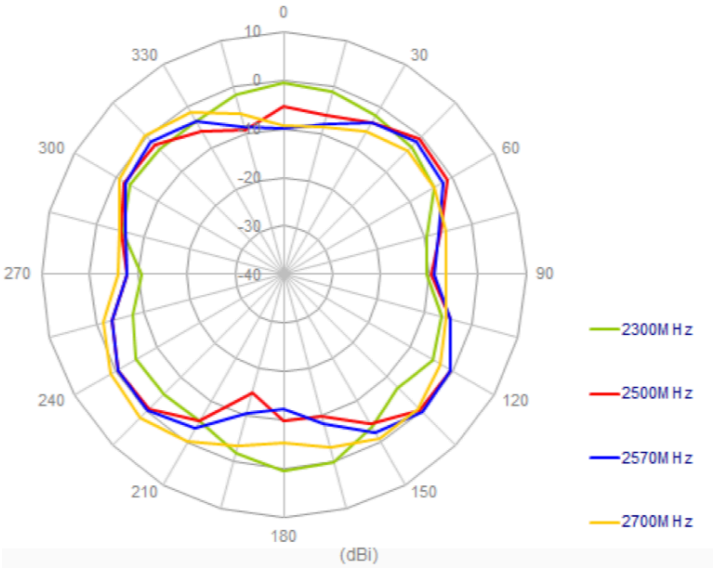

Figura 21-Diagrama de radiação [49]

3.1.4 4G/3G/GSM Aerial Antenna

A antena 4G/3G/GSM (Figura 22) permite melhorar a comunicação de dados e aumentar a velocidade de transferência de dados do sinal 4G/3G e GSM, usando uma banda de frequência dupla. A antena tem um cabo de 7 metros para montá-la num local que garanta uma ótima receção ou transmissão [50].

Figura 22-Antena 4G/3G/GSM Aerial [50]

As principais características desta antena são [50]:

- Impedância de 50 Ohm;
- Intervalo de frequências da antena de 698-2700 MHz;
- Polarização vertical de 55º;
- Polarização horizontal de 60º.

3.2 Software

3.2.1 BladeRF cli

O programa BladeRF-cli permite executar diversos comandos, que permitem realizar várias operações. Algumas destas operações encontram-se disponíveis nas figuras que se seguem.
Na Figura 23 encontram-se dois comandos que permitem saber o número de série do dispositivo, o valor de calibração VCTCXO DAC, informações sobre o FPGA, entre outros aspetos.

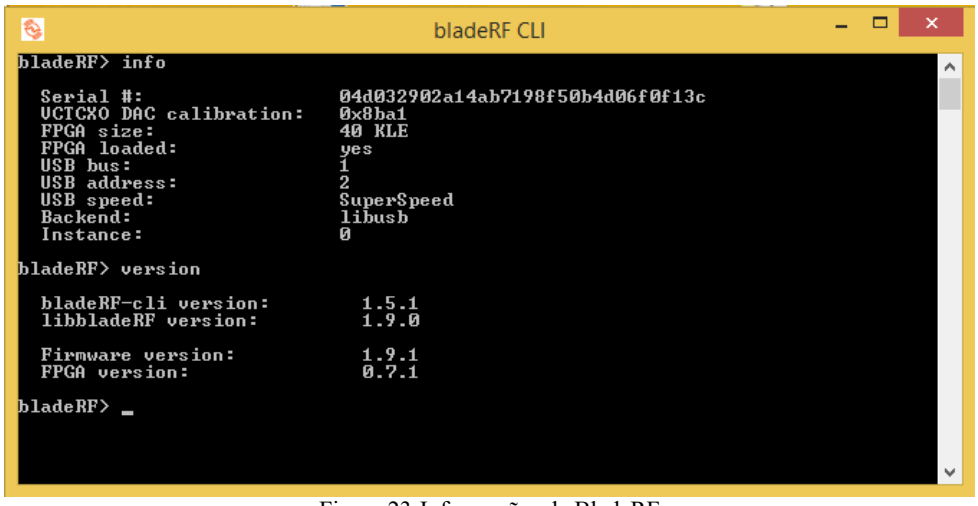

Figura 23-Informações da BladeRF

Na Figura 24 são apresentados vários comandos que permite ao utilizador saber o ganho de diversas variáveis relacionadas com o RX da BladeRF e ainda alterar as mesmas para outro valor.

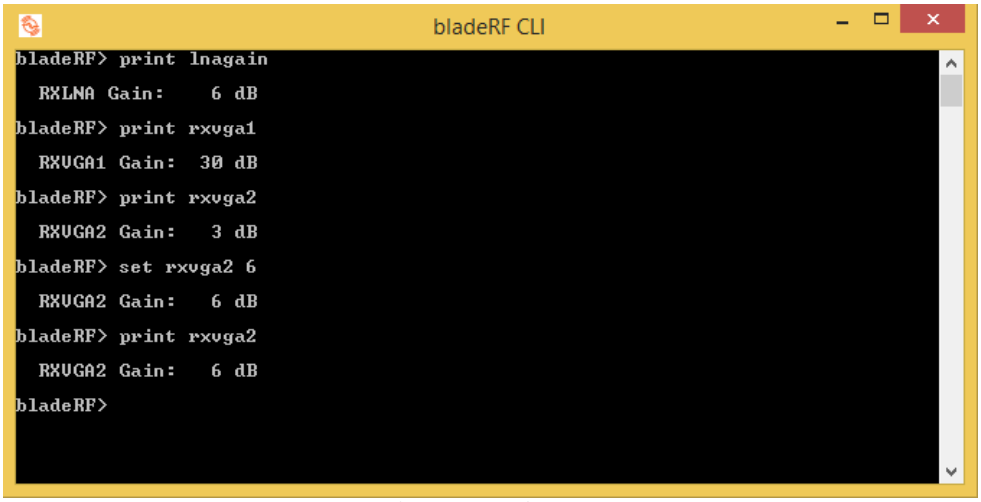

Figura 24-Ganhos RX

Na Figura 25 são apresentados vários comandos que permite ao utilizador saber o ganho de diversas variáveis relacionadas com o TX da BladeRF e ainda alterar as mesmas para outro valor.

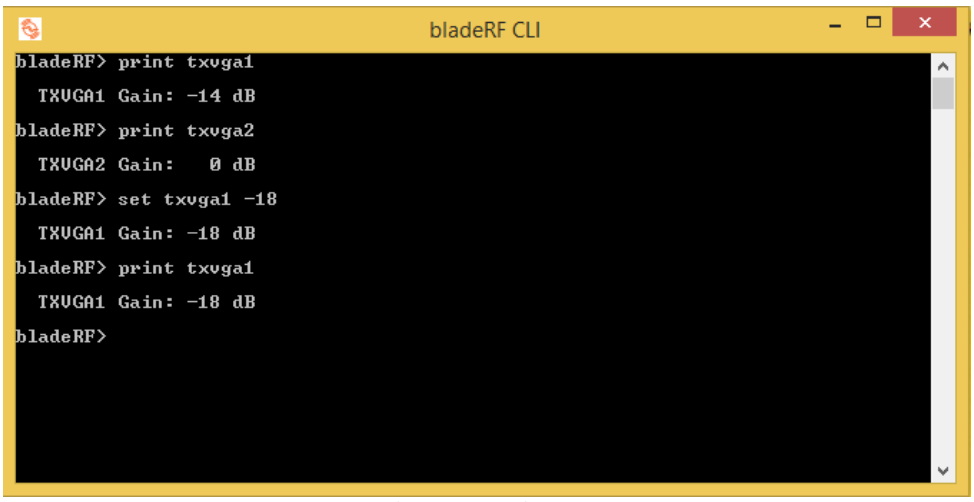

Figura 25-Ganhos TX

Os comandos apresentados na Figura 26 permitem visualizar e alterar a largura de banda. Este comando tanto altera as larguras de banda para os módulos TX e RX.

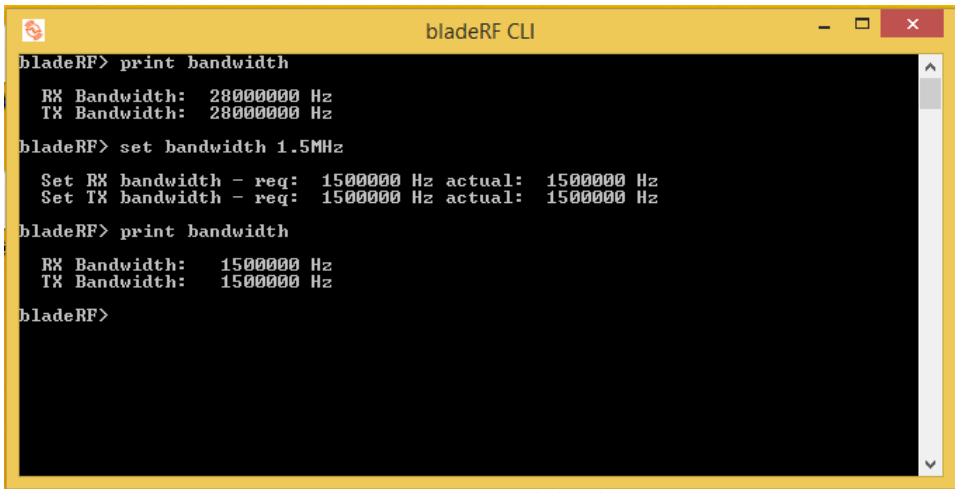

Figura 26-Largura de banda

Na Figura 27 encontram-se comandos que permitem saber a frequência nos módulos RX e TX. Este comando permite alterar a frequência de ambos os módulos.

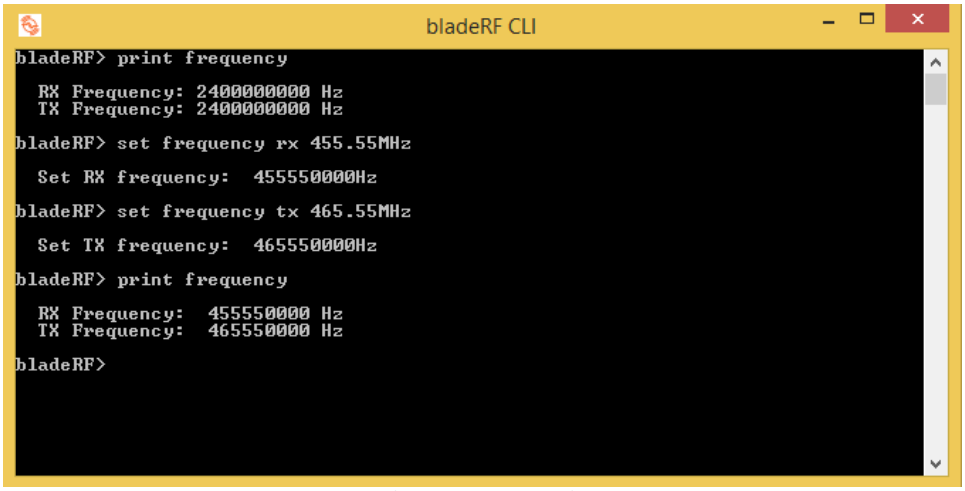

Figura 27-Frequência

Na Figura 28 são apresentados vários comandos que permitem saber o ritmo de amostras de ambos os módulos e ainda alterar para outros valores.

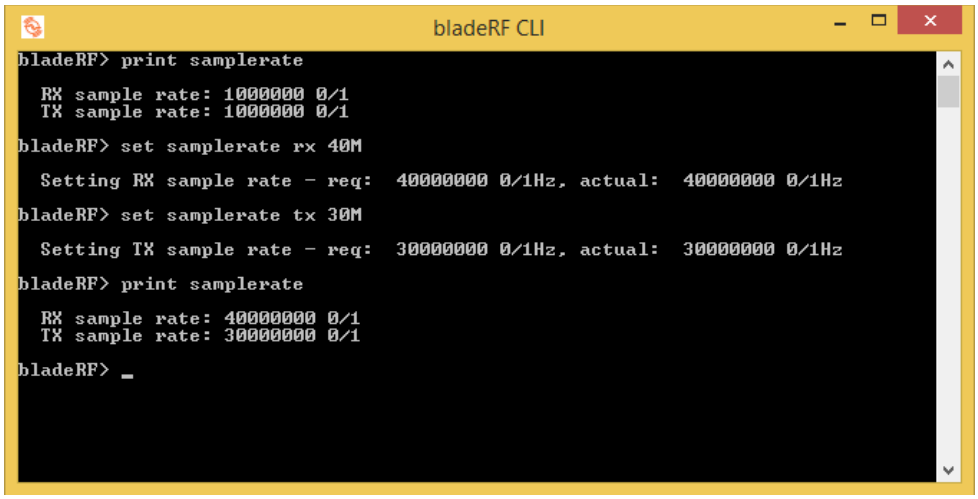

Figura 28-Ritmo de amostras

3.2.2 GNURadio

O GNU Radio é software gratuito de desenvolvimento e de código aberto que fornece blocos de processamento de sinais para implementar rádios de software. Ele pode ser usado com hardware de RF externo de baixo custo prontamente disponível para criar rádios definidos por software ou sem hardware num ambiente de simulação.
O software GNU Radio [51] fornece a estrutura e as ferramentas para construir e executar software de rádio ou apenas aplicações gerais de processamento de sinais. Como em todos os sistemas SDR, a configurabilidade é um recurso importante. Em vez de usar rádios diferentes projetados para propósitos específicos, um único rádio de uso geral pode ser usado como front-end de rádio, e o software de processamento de sinal processa o processamento específico para a aplicação de rádio.
O GNU Radio Companion é uma interface gráfica de front-end para o GNU Radio. É uma ferramenta que cria automaticamente programas python que são programas de rádio de software. As próprias aplicações de Rádio GNU são conhecidos como gráficos de fluxo, que são uma série de blocos de processamento de sinal conectados juntos.

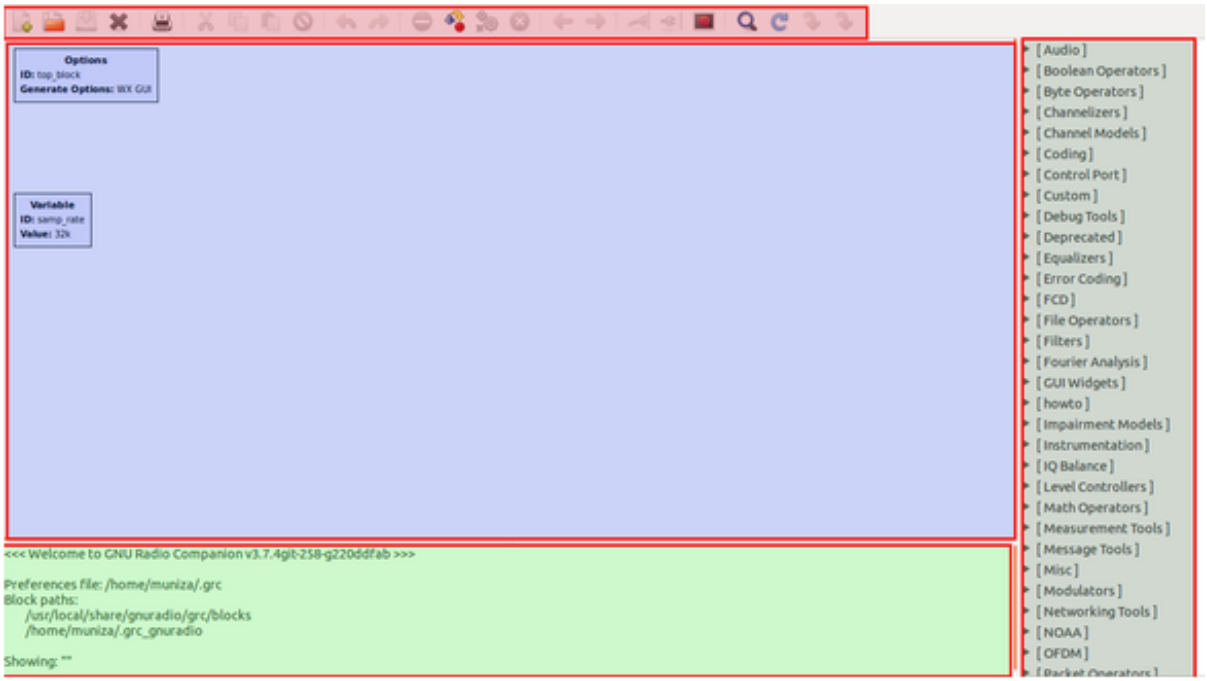

Figura 29-Interface do GNURadio [52]

Na Figura 29 é possível observar que este software é composto por 4 partes [52]:

1. A biblioteca corresponde ao local onde se encontram todos os blocos que podem ser utilizados.
2. A barra de ferramentas que contem algumas funções que grande parte dos softwares possuem, tais como: novo, guardar, abrir, entre outras. Existem algumas funções que caracterizam este software, como: gerar fluxograma, executar fluxograma e parar fluxograma.
3. O terminal permite visualizar o que o programa está a fazer.
4. O workspace é o local onde são criados os fluxogramas.

Estes gráficos de fluxo podem ser escritos em C ++ ou na linguagem de programação Python. A Figura 30 mostra um mero exemplo visual de tais gráficos de fluxo. A infra-estrutura do GNU Radio é escrita inteiramente em C ++, e muitas das ferramentas do utilizador são escritas em Python.

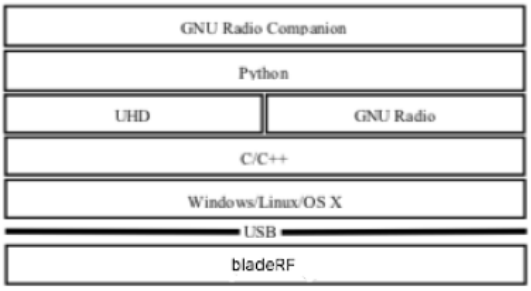

Figura 30-Antena 4G/3G/GSM Aerial [53]

3.2.3 Gqrx

O Gqrx é um software de código aberto, que funciona como um recetor de SDR. Este programa foi desenvolvido pelo GNURadio e pelo kit de ferramentas Qt.
O Gqrx suporta muitos dos hardwares SDR disponíveis, incluindo as plataformas Airspy, Funcube Dongles, rtl-sdr, HackRF, USRP e BladeRF. As especificações de software encontram-se disponíveis em [54]. Na Figura 31 é possível visualizar a interface do utilizador.

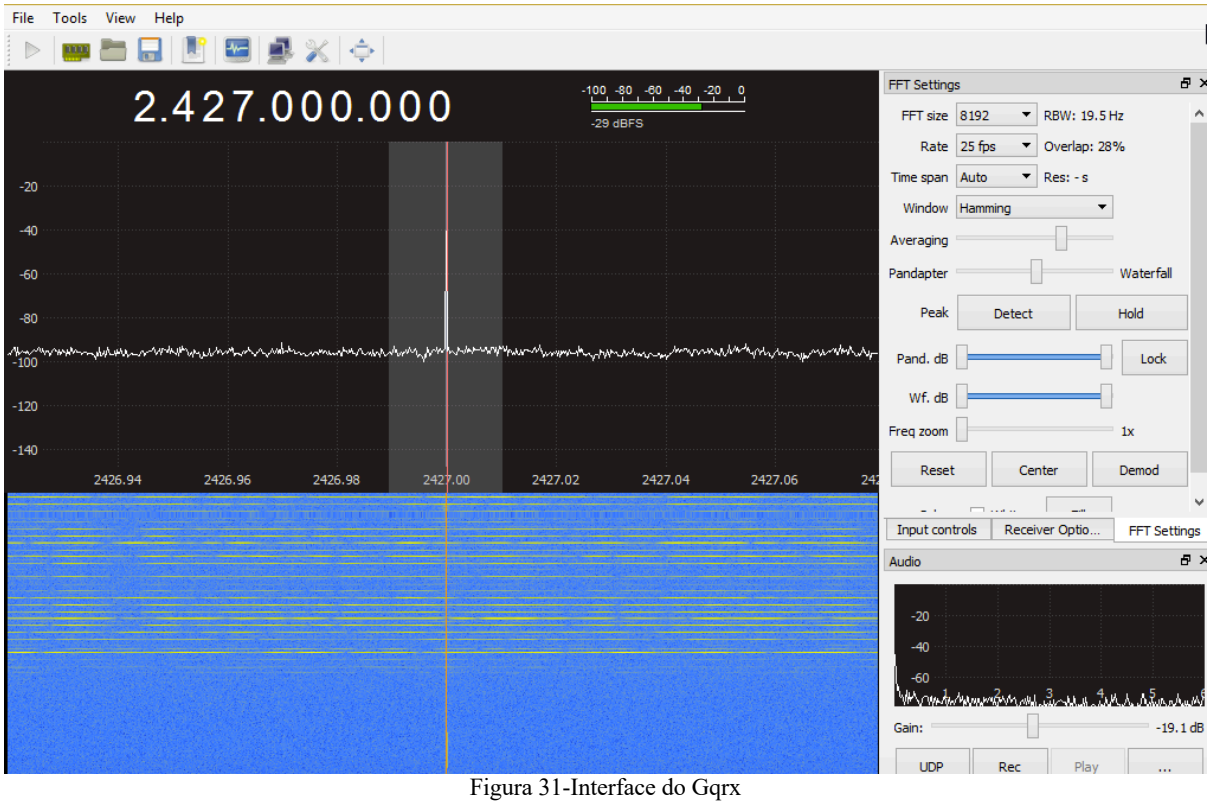

Figura 31-Interface do Gqrx

Capítulo 4. Implementação dos jammers

Neste capítulo são apresentados os jammers desenvolvidos no software GNURadio e explicado o seu funcionamento.

4.1 Barrage Jamming

Na Figura 32 é possível visualizar o diagrama de blocos do Barrage Jamming. Este jammer é constituído inicialmente por um bloco de "Fast Noise Source", que é uma fonte de ruído rápido. Os parâmetros deste bloco são os inicialmente colocados pelo software. Este bloco encontra-se ligado ao bloco de "osmocom Sink", que é um bloco que permite que a BladeRF transmita o ruído criado. Este bloco apresenta vários parâmetros configuráveis, dos quais se destacam:

- Device Arguments: que é o local onde é necessário inserir qual a plataforma que irá transmitir o ruído.
- Sample Rate: é o ritmo das amostras e neste caso foi escolhido o valor de 300k, pois era o valor que permitia melhor interferência. Este valor foi usado para os outros jammers para conseguir perceber qual o melhor deles.
- Frequency: representa qual a frequência em que a plataforma irá transmitir o ruído.
- RF Gain: representa a potência máxima da BladeRF.
- BB Gain: representa o ganho da banda base. Quanto maior o valor melhor, pois assim o ruido não é amplificado demasiado.
- Bandwidth: é a largura de banda que vai ocupar o ruído transmitido. Neste caso foi escolhido 20MHz pois é a maior largura de banda a que a BladeRF consegue funcionar.

Os blocos "QT GUI Range" permitem que o utilizador escolha quais os valores do RF e BB Gain a que a BladeRF vai funcionar. O BB Gain pode funcionar entre os valores de -35[dB] e -4[dB], enquanto o RF Gain pode funcionar entre valores de 0 [dB] e 25[dB] [55].
O bloco "QT GUI Sink" que também se encontra ligado ao "Fast Noise Source", é um bloco de interface ao utilizador que permite ao utilizador perceber como se comporta a informação que pretende enviar. Este bloco permite visualizar "Frequency Display", "Waterfall Display", "Time Domain Display" e "Constellation Display".

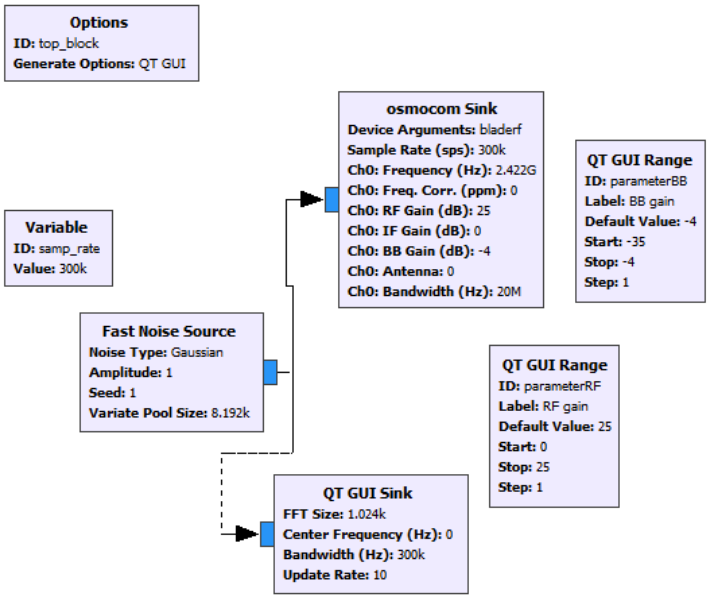

Figura 32-Barrage Jamming

4.2 Tone Jamming

O diagrama de blocos da Figura 33 é bastante parecido com o anterior. Algumas diferenças visíveis é que em vez de a BladeRF transmitir ruído, neste caso é utilizado o bloco "Signal Source" que irá transmitir um sinal cosseno com os parâmetros colocados inicialmente no software. Outra das diferenças é o facto de existir um bloco designado por "QT GUI Range" que permite ao utilizador variar a frequência a que a BladeRF se encontra a transmitir. E por último, no bloco "osmocom Sink" a largura de banda é de 0 [MHz] pois este jammer apenas tenciona interferir com uma frequência.

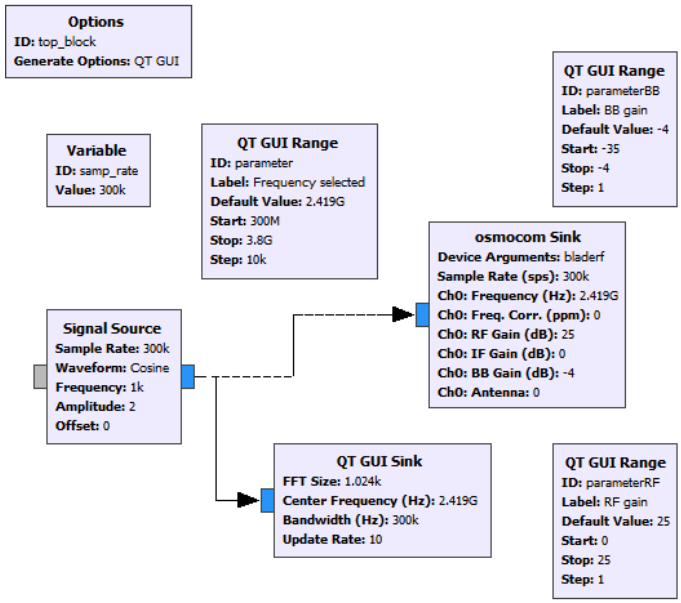

Figura 33-Tone Jamming

4.3 Sweep Jamming

Este jammer baseia-se no Tone Jamming, a única diferença é que em vez de ser o utilizador a mudar a frequência a que a BladeRF se encontra a transmitir, a frequência vai mudando automaticamente. Para isto, foi necessário alterar o código python (Figura 34) do Tone Jamming para cumprir este propósito.

```
def main(top_block_cls=top_block, options=None):

    from distutils.version import StrictVersion
    if StrictVersion(Qt.qVersion()) >= StrictVersion("4.5.0"):
        style = gr.prefs().get_string('qtgui', 'style', 'raster')
        Qt.QApplication.setGraphicsSystem(style)
    qapp = Qt.QApplication(sys.argv)
    tb = top_block_cls()
    tb.start()

    while tb.get_frequencia()<2.425e9:
            frequencia= tb.get_frequencia() + 0.001e9
            tb.set_frequencia(frequencia)
            tb.osmosdr_sink_0.set_center_freq(frequencia, 0)
            print tb.get_frequencia()

            if tb.get_frequencia()>=2.425e9:
                tb.set_frequencia(2.415e9)



    tb.show()
```

Figura 34-Código alterado

A parte alterada em python foi o ciclo while que se encontra dentro da definição do método main. O ciclo while faz o seguinte:

1. Verifica se a frequência da BladeRF é inferior a 2.425 [GHz], e caso isso seja verdade entra dentro do ciclo while.
2. A variável "frequência" irá ser igual à soma da frequência da BladeRF com 1 [MHz].
3. De seguida altera-se a frequência da BladeRF para o valor da variável "frequência" e assim sucessivamente.
4. E passa para o ponto 1 e assim sucessivamente.
5. Caso a frequência para a qual se quer alterar a frequência da BladeRF seja maior ou igual que 2.425 [GHz] coloca-se a frequência da BladeRF a 2.415 [GHz].

4.4 Protocol Jamming

4.4.1 Wi-Fi Jamming

Na Figura 35 é possível visualizar o diagrama de blocos do Wi-Fi Jamming. Inicialmente foi utilizado o bloco "Signal Source" com o formato de cosseno. Este cosseno tem um ritmo de amostra por segundo de 20MHz pois corresponde ao ritmo de amostra do Wi-Fi [56]. Este bloco encontra-se ligado ao bloco "OFDM Mod". O sinal Wi-Fi utiliza o método de OFDM para codificar digitalmente várias subportadoras do sinal. A técnica de modulação utiliza neste bloco é o BPSK pois as subportadoras do sinal Wi-Fi são modeladas em BPSK. No bloco "osmocom Sink" a largura de banda é de 20MHz, que corresponde à largura de banda do sinal Wi-Fi [56].

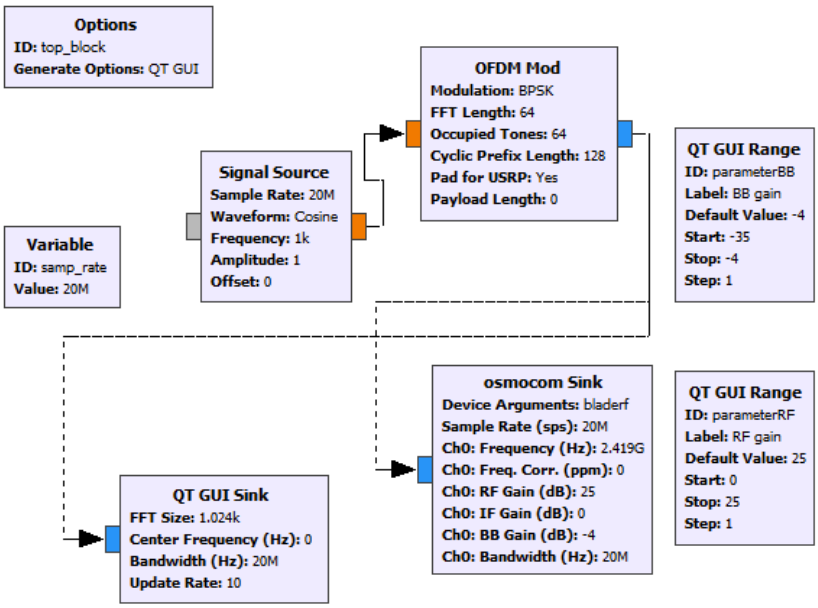

Figura 35-Wi-Fi Jamming

4.4.2 CDMA-QPSK Jammer

Na Figura 36 é possível visualizar o diagrama de blocos do CDMA-QPSK Jamming. Este diagrama de blocos é bastante mais complexo, quando em comparação com os outros anteriores. Este diagrama pode-se dividir em duas partes. Numa primeira parte encontra-se descrita a multiplexagem do tipo CDMA. O CDMA consiste em ligar os blocos "Signal Source" e "Random Source" ao bloco "XOR". São utilizados dois blocos "Random Source" e um "Signal Source", para assim ser possível obter dois sinais diferentes resultantes do bloco "XOR". De seguida são utilizados os blocos "UChar To Float" que é um conversor de dados. Com o tipo de dados "Float" já é possível passar para a segunda parte deste jammer. A segunda parte consiste na modulação QPSK. As saídas dos conversores são ligadas ao bloco "Multiply Const", em que a constante é 2, de seguida são ligados ao bloco "Add Const" é que a constante é -1. Assim os sinais foram modulados em BPSK. Depois os sinais modulados em BPSK são ligados ao bloco "Float to Complex", na parte real e imaginária. Deste bloco resulta um sinal QPSK que é ligado ao bloco "osmocom Sink" e é transmitido.

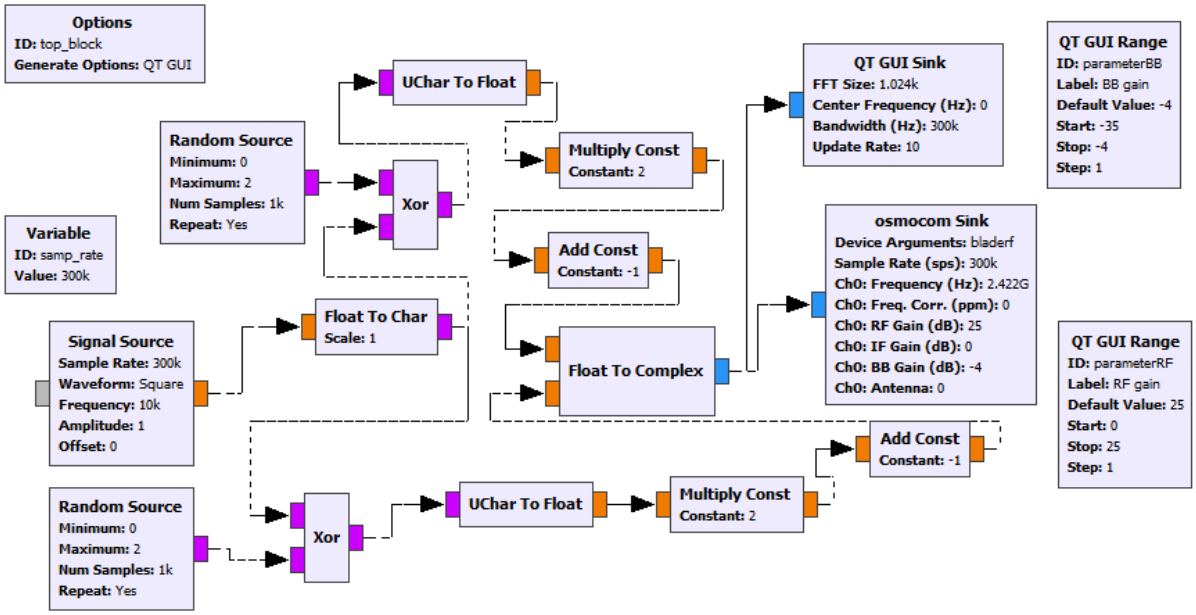

Figura 36-CDMA-QPSK Jamming

Capítulo 5. Montagem e testes

Neste capítulo é apresentada a montagem para interferir com o link de comunicações, o alvo do jammers e ainda os testes feitos, recorrendo aos softwares GNURadio e Gqrx.

5.1 Esquema de montagem

Na Figura 37 encontra-se o esquema de montagem utilizado nos testes para interferir com o link de comunicações. São necessárias duas BladeRF ligadas ao computador, é necessária uma para descobrir a frequência do link de comunicações visto que é dinâmico, utilizado o software Gqrx e outra para interferir com essa frequência. A BladeRF que irá interferir encontra-se ligada a um amplificador, que serve para aumentar o ganho da antena 4G/3G/GSM Aerial Antenna e assim conseguir interferir melhor com o link de comunicações em maiores distâncias. O amplificador encontra-se ligado a uma tomada elétrica pois oferece uma maior potência, em comparação com a entrada USB3.0, o que resulta num aumento dos ganhos. A BladeRF de transmissão encontra-se ligada a uma antena na porta TX, enquanto a BladeRF de recepção encontra-se ligada a uma antena na porta RX.

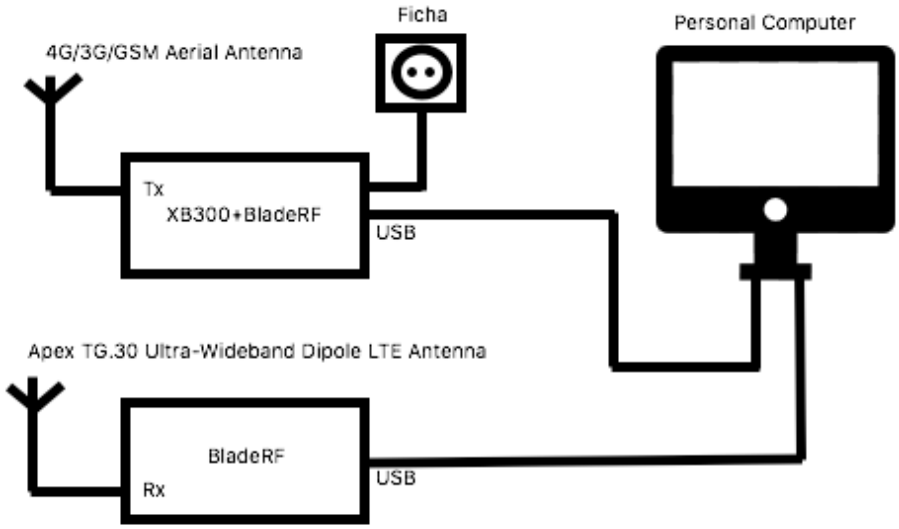

Figura 37-Esquema de Montagem

5.2 Spektrum RC

Antes de serem apresentados os testes dos jammers, é necessário perceber qual irá ser o alvo dos jammers. Nesta tese de dissertação o alvo dos jammers irá ser o link de comunicações do Spektrum RC (Figura 38). O link de comunicações representa, de modo simples, um canal de dados pelo qual são enviados os comandos que o drone (Figura 39) tem que executar. Este link de comunicações funciona no intervalo de 2.400-2.4835 [GHz] [57]. A frequência do link de comunicações não é estática, pois por cada vez que se liga o comando a sua frequência de funcionamento varia ligeiramente, por isso pode-se dizer que a frequência do link de comunicações é dinâmica.

Figura 38-Spektrum RC

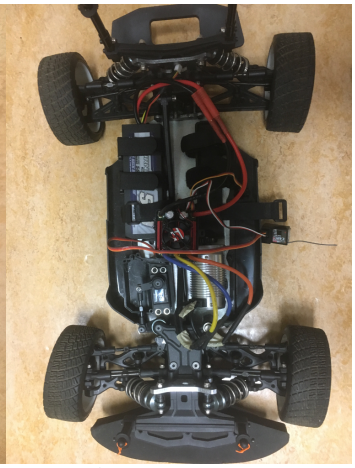

Figura 39-Drone terrestre

O drone terrestre que é controlado pelo Spektrum RC através do link de comunicações, é composto pelo [58]:

- Transmissor- o papel é converter o movimento dos sticks de controlo em sinais digitais, que são enviados via ondas de rádio para o recetor. Os transmissores oferecem vários canais para controlar várias componentes. Por exemplo, se um transmissor tiver 5 canais, é possível controlar até 5 servos ou motores;
- Recetor- recolhe os dados do stick de controlo do transmissor e distribui os sinais aos servos e motores do veículo R/C;
- Servo- são moto redutores projetados para controlo de precisão sobre movimento. Dentro de um servo existe uma placa de circuito, um pequeno motor de corrente contínua e uma série de engrenagens. O recetor emite um sinal de modulação por largura de pulso (PWM) para o servo, que a placa de circuito traduz em sinais de controlo precisos para o motor CC. A placa de circuito também recebe a entrada de um potenciômetro de realimentação ligado ao eixo de saída do servo para detetar a sua rotação. De seguida, é comparada a posição do eixo desejada, com base no sinal PWM, com a posição real para saber qual a caminho seguir e quando parar;
- Motor e Controlador de Velocidade Eletrónico- Para controlar um motor, é necessário um controlador eletrónico de velocidade (ESC). O seu objetivo é pegar no sinal de baixa potência do recetor e transformá-lo em sinais de controlo de alta corrente para acionar o motor.

5.3 Testes

Nesta subsecção são apresentados os testes que foram realizados para interferir com o link de comunicações.

5.3.1 Espectro sem nenhum jammer

Na figura 40 é possível observar o espectro de frequência na ordem dos 2.42 [GHz]. Esta imagem representa o espectro de uma frequência, em que não se encontra a ser transmitido nenhum jammer e o link de comunicações ainda não se encontra ativo.

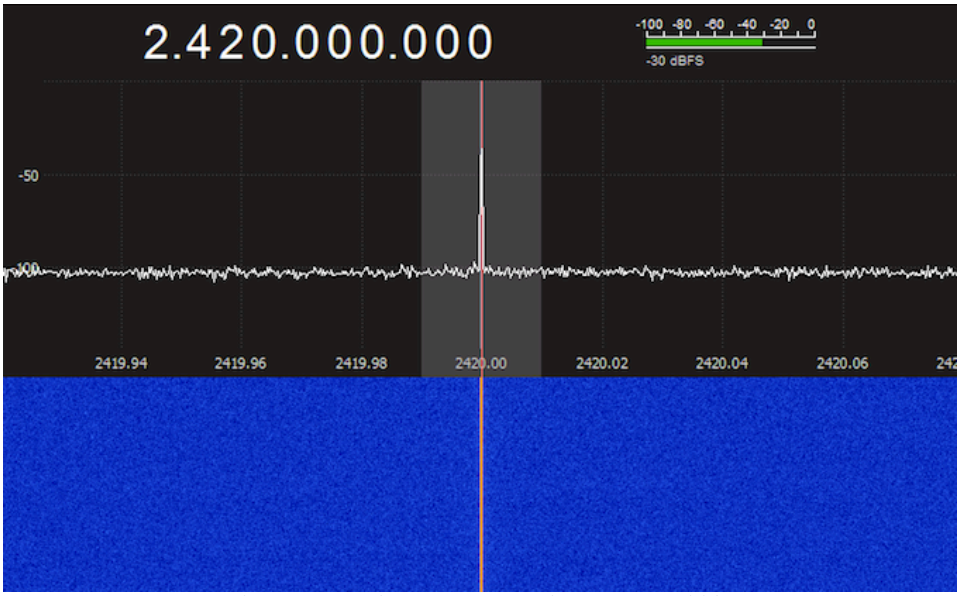

Figura 40-Interface Gqrx sem nada a ser transmitido

5.3.2 Espectro do link de comunicações

A largura de banda do Spektrum RC é de 1 MHz como é possível observar em [59]. Nas figuras abaixo encontra-se o espectro de frequências em diversas frequências. As frequências em que neste caso o link de comunicações se encontra a funcionar são 2.414GHz (Figura 42) e 2.415GHz (Figura 43), pois são aquelas em que o espectro apresenta maior ganho. Enquanto nas outras frequências (Figura 41 e Figura 44) é possível observar que os ganhos são bastante mais baixos em comparação com as outras frequências. A frequência que neste caso iria ser colocado no jammer para interferir com o link de comunicações era a de 2.414GHz pois apresenta maior ganho em comparação com 2.415GHz.

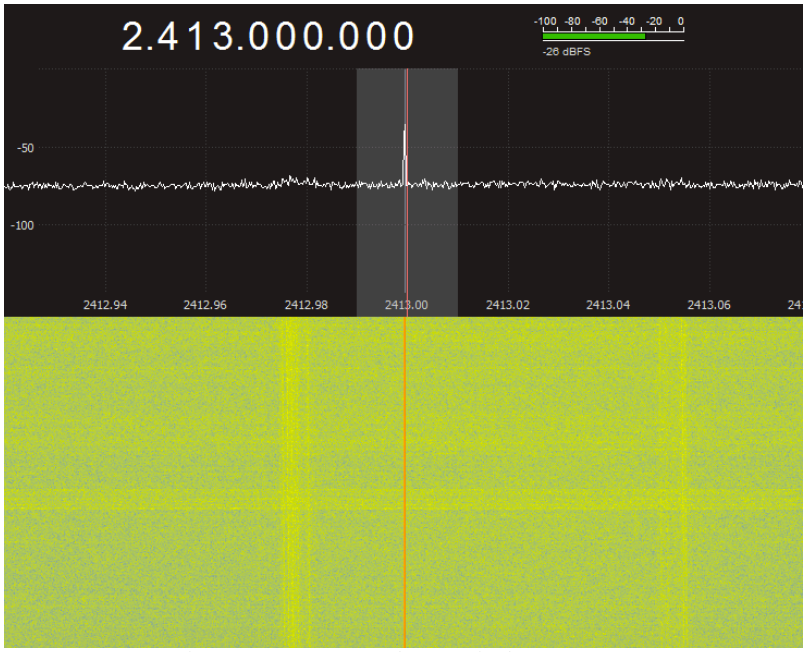

Figura 41-Espectro na frequência de 2.413 GHz

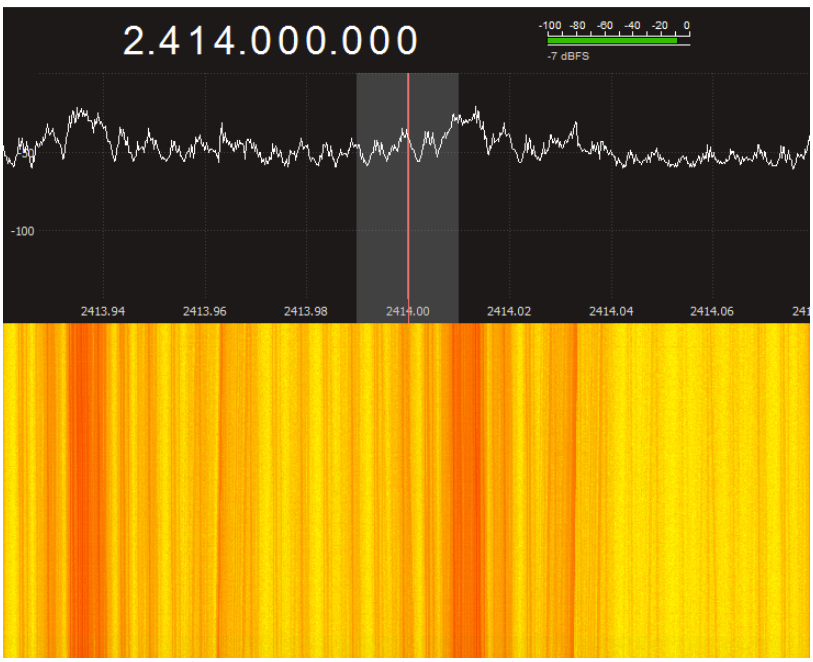

Figura 42-Espectro na frequência de 2.414 GHz

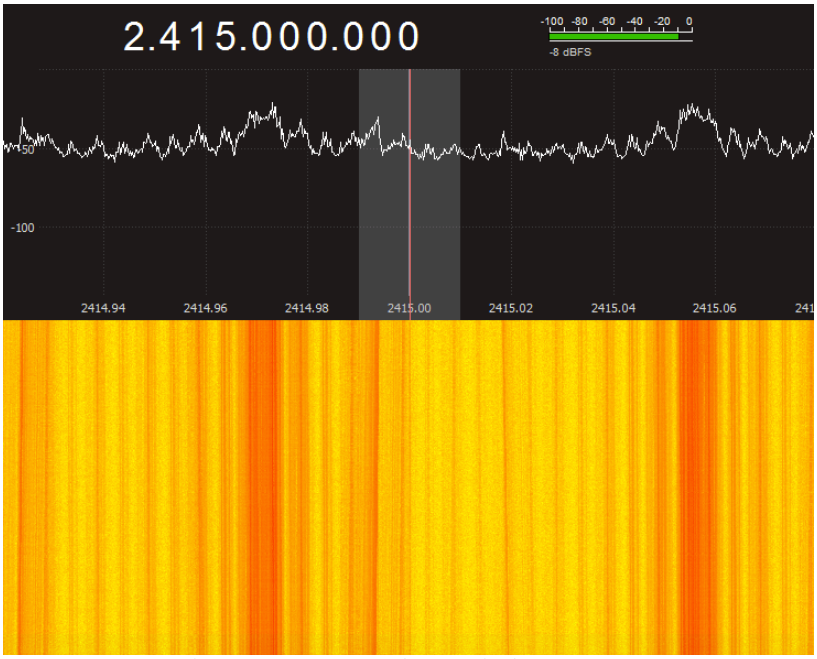

Figura 43-Espectro na frequência de 2.415 GHz

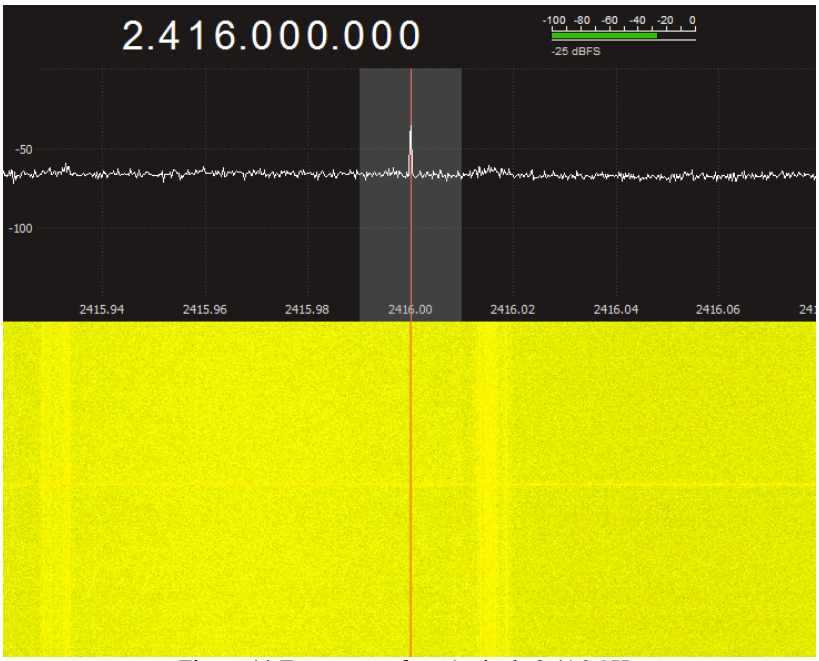

Figura 44-Espectro na frequência de 2.416 GHz

5.3.3 Barrage Jamming

Nas Figuras 45, 46, 47 e 48 é possível visualizar a interface do utilizador referente ao bloco "QT GUI Sink".
A Figura 45 corresponde ao espectro de frequência. No eixo dos x temos a frequência e no eixo dos y o ganho. A frequência central neste caso é 0 kHz, que corresponde à frequência colocada no bloco "QT GUI sink". O espectro é não é uniforme pois o que se está a transmitir é ruído, ou seja, um sinal aleatório.

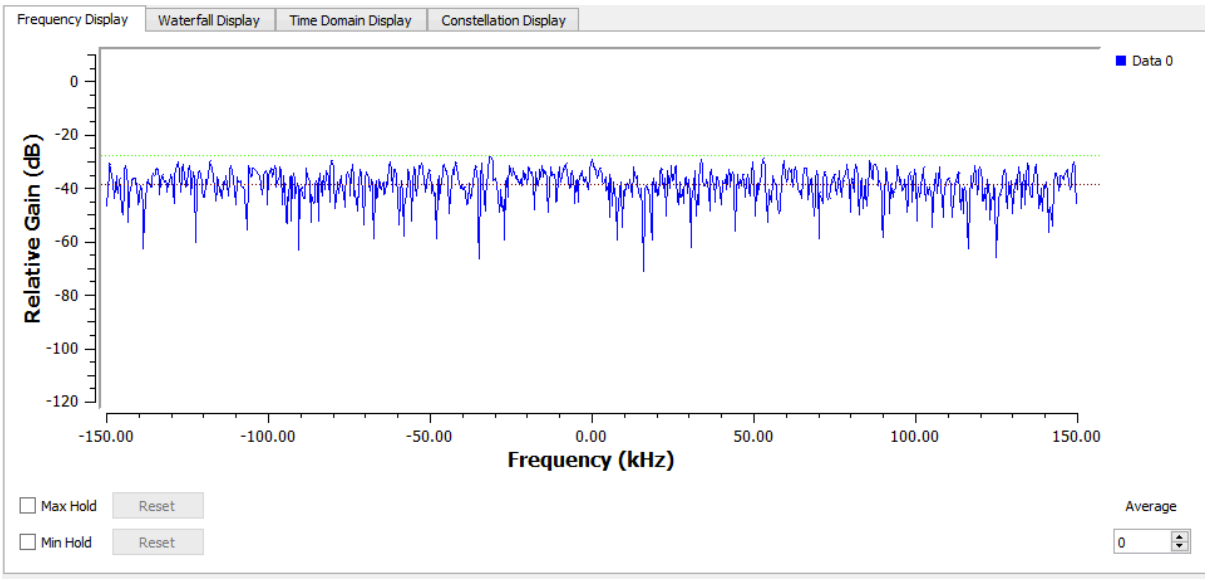

Figura 45-Espectro de frequência

A Figura 46 corresponde à relação entre a frequência e tempo. No eixo dos x temos a frequência e no eixo dos y o tempo. O gráfico encontra-se todo a vermelho pois o jammer tem largura de banda de 20MHz, o que faz com que esteja a ocupar todas essas frequências durante o tempo estipulado.

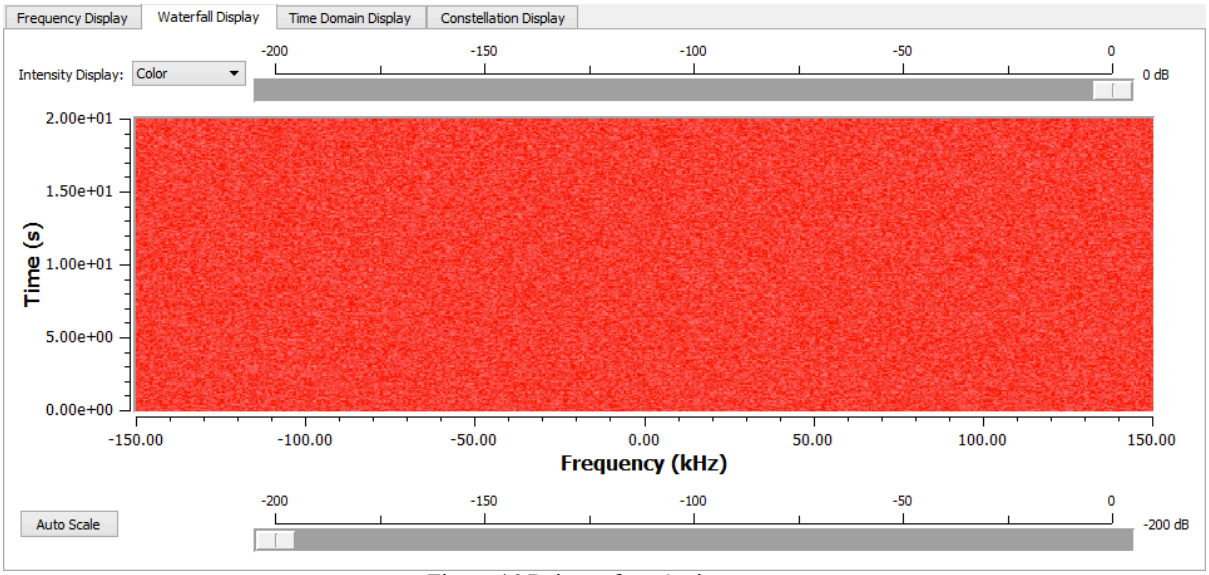

Figura 46-Relação frequência-tempo

A Figura 47 mostra a relação entre a amplitude e tempo. No eixo dos x temos o tempo e no eixo dos y a amplitude. O ruído que o jammer está a transmitir é complexo, ou seja, tem parte real e parte imaginária. O sinal a azul corresponde à parte real, enquanto o sinal a vermelho corresponde à parte imaginária.

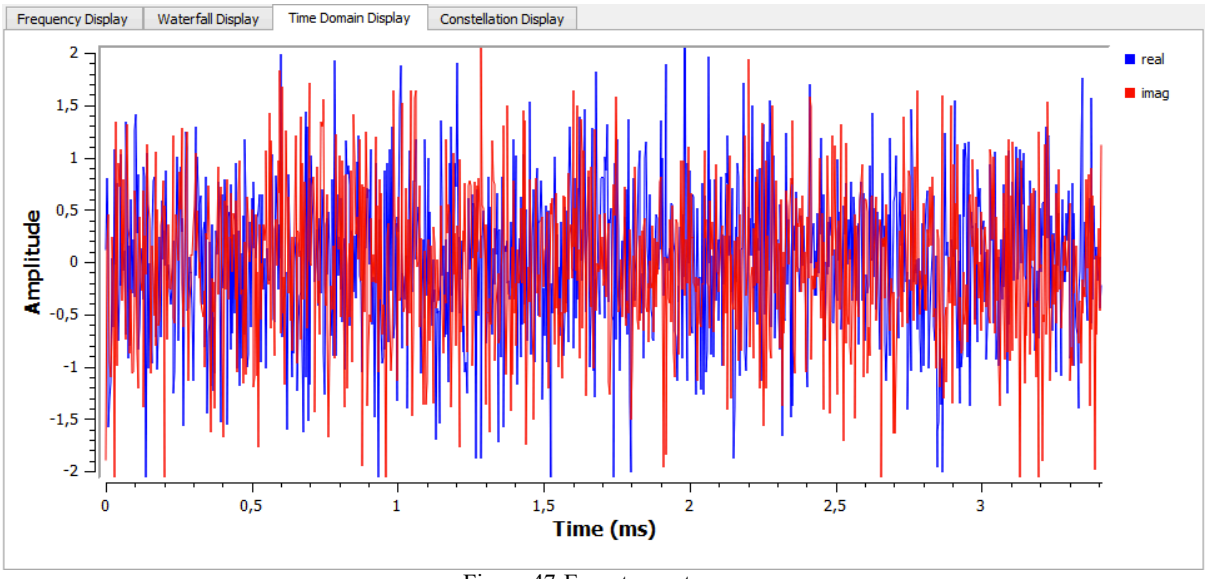

Figura 47-Espectro no tempo

A Figura 48 mostra constelação do sinal enviado. No eixo dos x temos a parte real e no eixo dos y a parte imaginário. Cada ponto no gráfico representa um número complexo que foi transmitido, que representa o ruído transmitido.

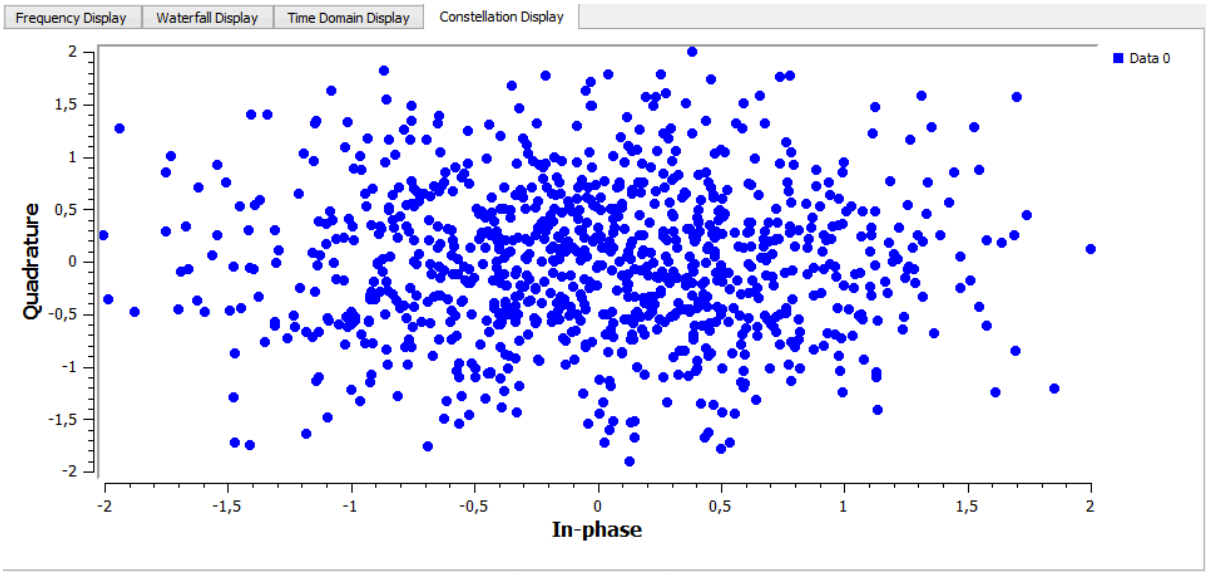

Figura 48-Constelação

Com este jammer foi possível interferir com o link de comunicações do Spektrum RC. Na Figura 49 são apresentadas distâncias a partir do qual é possível bloquear o sinal, variando o ganho RF da BladeRF.
Na Figura 49 (a), o valor de RF é de 25dB que corresponde à potência máxima da BladeRF. Neste caso o jammer começa a bloquear o link de comunicações, quando o carro se encontrar a 24m ou menos da antena.
Na Figura 49 (b), o valor de RF é de 12dB que corresponde à potência média da BladeRF. Neste caso o jammer começa a bloquear o link de comunicações, quando o carro se encontrar a 12m ou menos da antena.
Na Figura 49 (c), o valor de RF é de 0dB que corresponde à potência mínima da BladeRF. Neste caso o jammer começa a bloquear o link de comunicações, quando o carro se encontrar a 2m ou menos da antena.

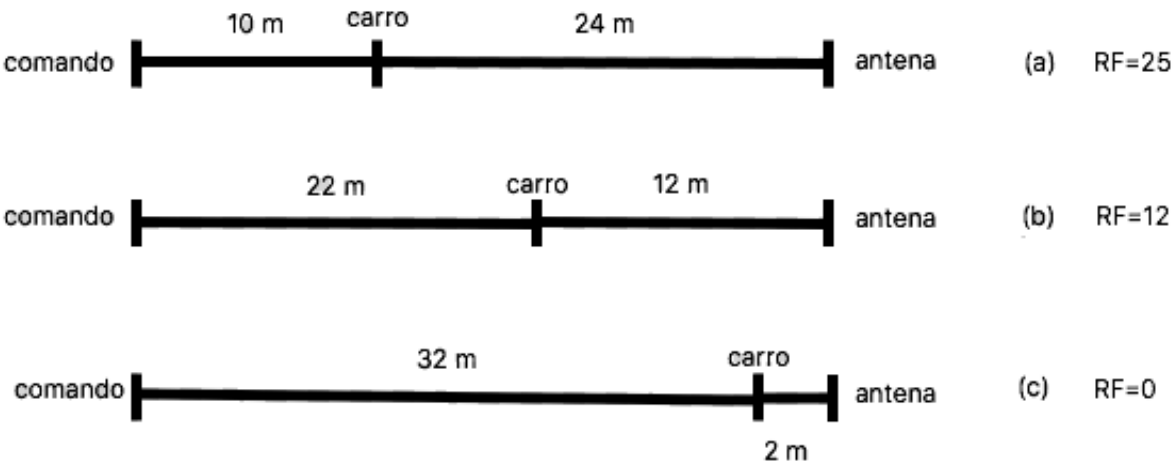

Figura 49-Resultados

5.3.4 Tone Jamming

A Figura 50 corresponde ao espectro de frequência. A frequência central neste caso é 2.419GHz, que corresponde à frequência colocada no bloco "QT GUI Sink". O espectro é não uniforme pois o que se está a transmitir é um cosseno.

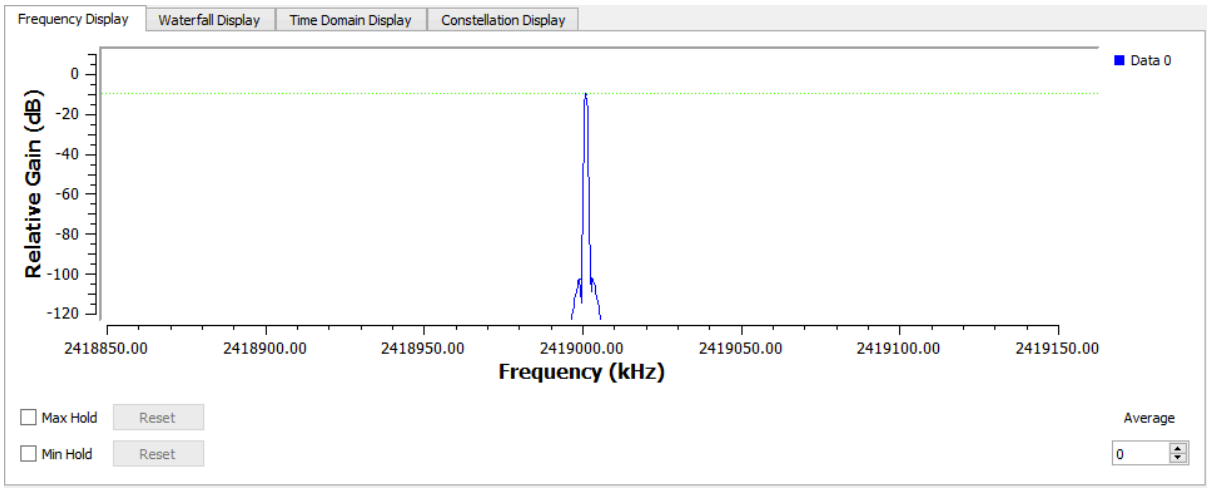

Figura 50-Espectro de frequência

A Figura 51 corresponde à relação entre a frequência e tempo. Como o jammer se encontra a transmitir na frequência de 2.419GHz, essa frequência encontra-se ocupada a vermelho. Como não foi colocada largura de banda no bloco de transmissão, teoricamente o jammer apenas devia ocupar essa frequência, mas como é possível observar as frequências perto da escolhida também se encontram a ser ocupadas, pois existe uma largura de banda mínima, ainda que o ganho seja muito reduzido, em comparação com o da frequência transmitida.

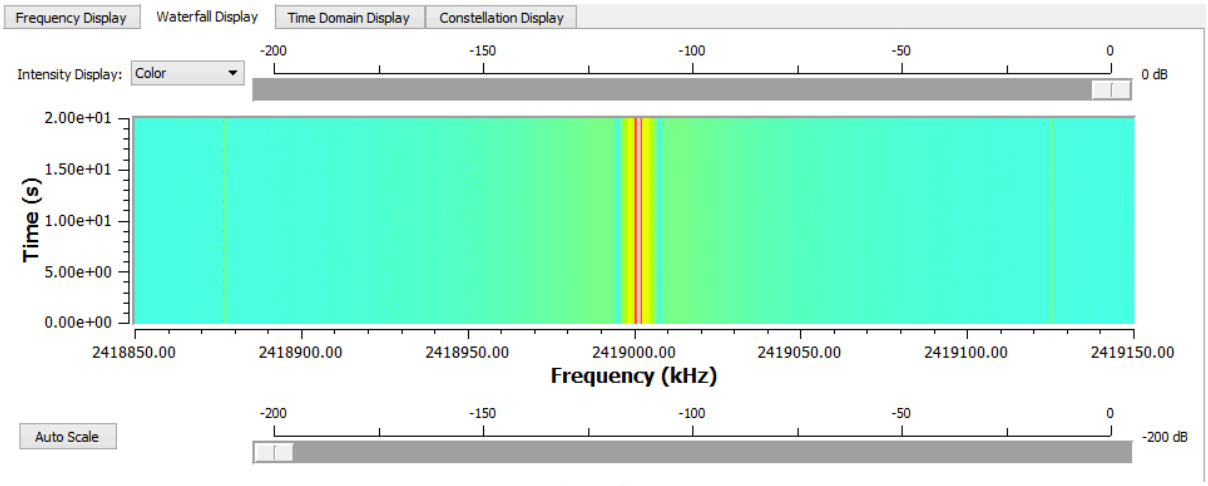

Figura 51-Relação frequência-tempo

A Figura 52 mostra o espectro no tempo. O cosseno que o jammer está a transmitir é complexo, ou seja, tem parte real e parte imaginária. O sinal a azul corresponde à parte real, enquanto o sinal a vermelho corresponde à parte imaginária. Tanto a parte real como a parte imaginária têm como amplitude máxima e mínima de 1 e -1 respetivamente, pois foi a amplitude colocada no bloco "Signal Source". As duas partes têm uma desfasagem de 90 graus.

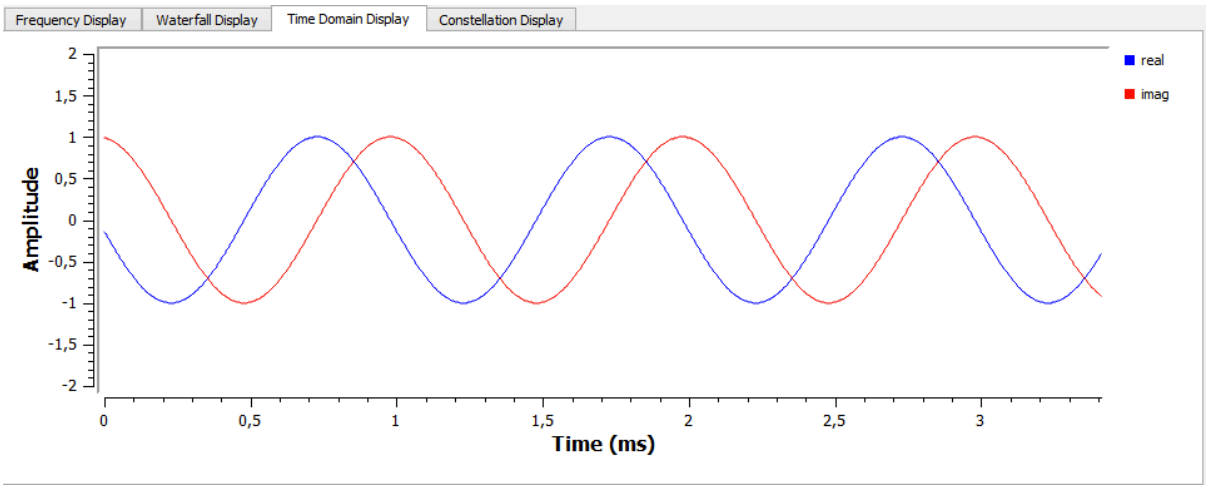

Figura 52-Espectro no tempo

A Figura 53 mostra a constelação do sinal transmitido. Cada ponto no gráfico representa um número complexo que foi transmitido. Neste caso a norma de cada número complexo é de 1, pois a amplitude escolhida representa o raio da circunferência, caso os eixos estivessem iguais.

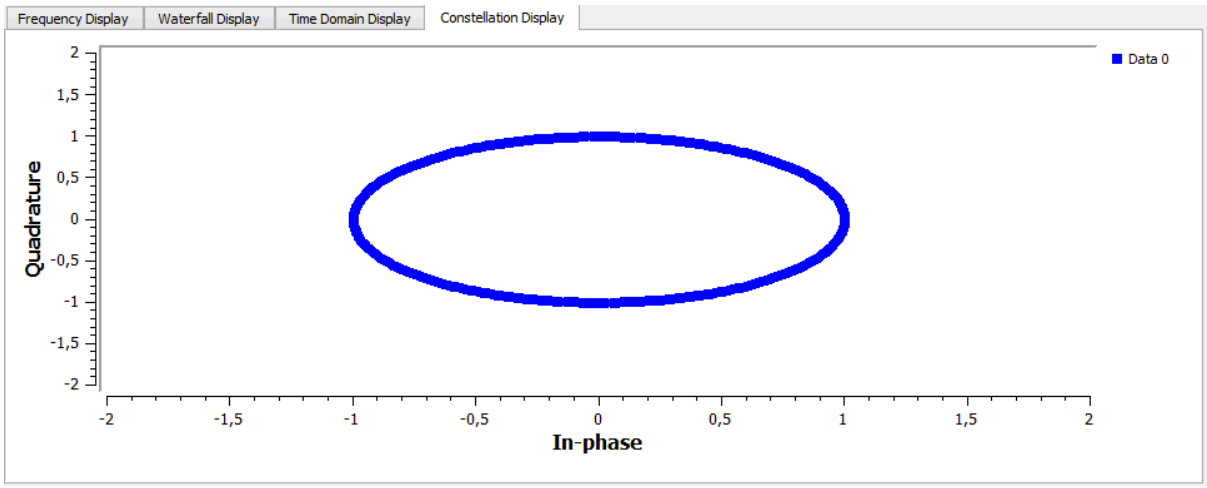

Figura 53-Constelação

5.3.5 Sweep Jamming

Na Figura 54 é possível observar a consola do Python, em que vão aparecendo em quais as frequências a que BladeRF se encontra a transmitir. Este jammer não apresenta interface do utilizador, em comparação com os outros jammers, pois a interface é igual à do tone jamming, a única diferença é que a frequência de transmissão vai variando automaticamente.

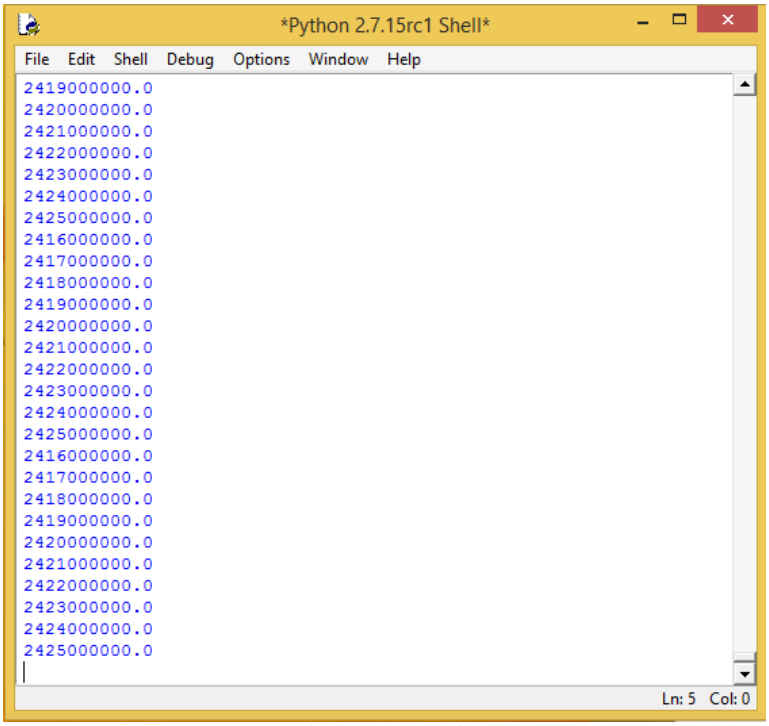

Figura 54-Consola

5.3.6 Protocol Jamming

5.3.6.1 Wi-Fi Jamming

A Figura 55 corresponde ao espectro de frequência. A frequência central neste caso é 0 MHz, que corresponde à frequência colocada no bloco "QT GUI sink". O espectro apresenta este comportamento pois foi multiplexado utilizando a técnica, OFDM e foi modulado em BPSK.

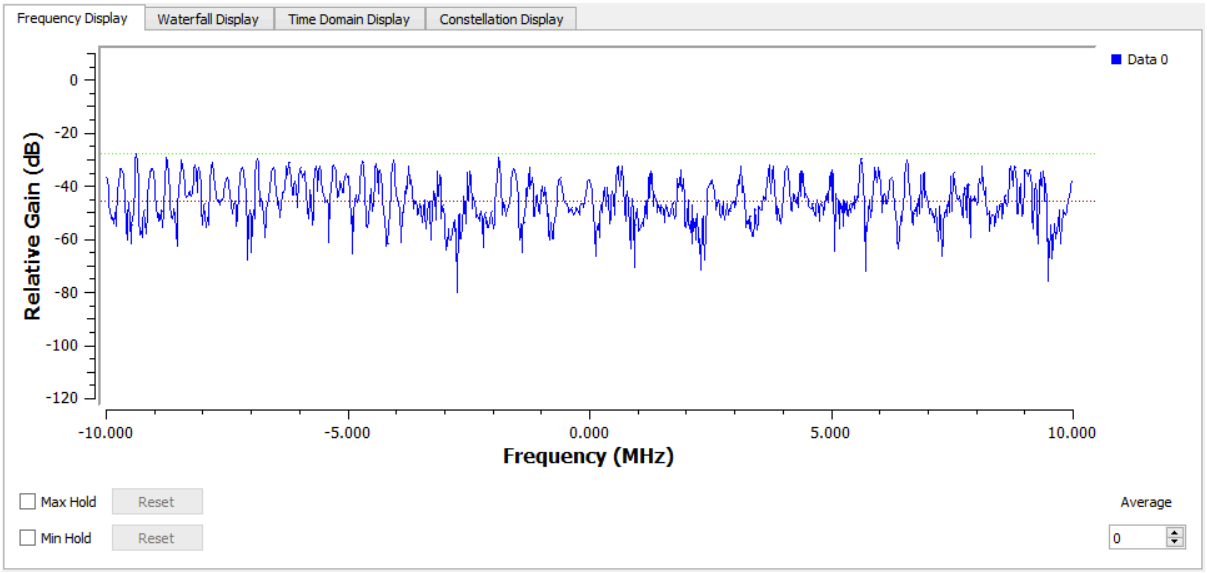

Figura 55-Espectro de frequência

A Figura 56 corresponde à relação entre a frequência e tempo. O gráfico encontra-se todo a vermelho pois o jammer tem largura de banda de 20MHz, o que faz com que esteja a ocupar todas essas frequências durante o tempo estipulado.

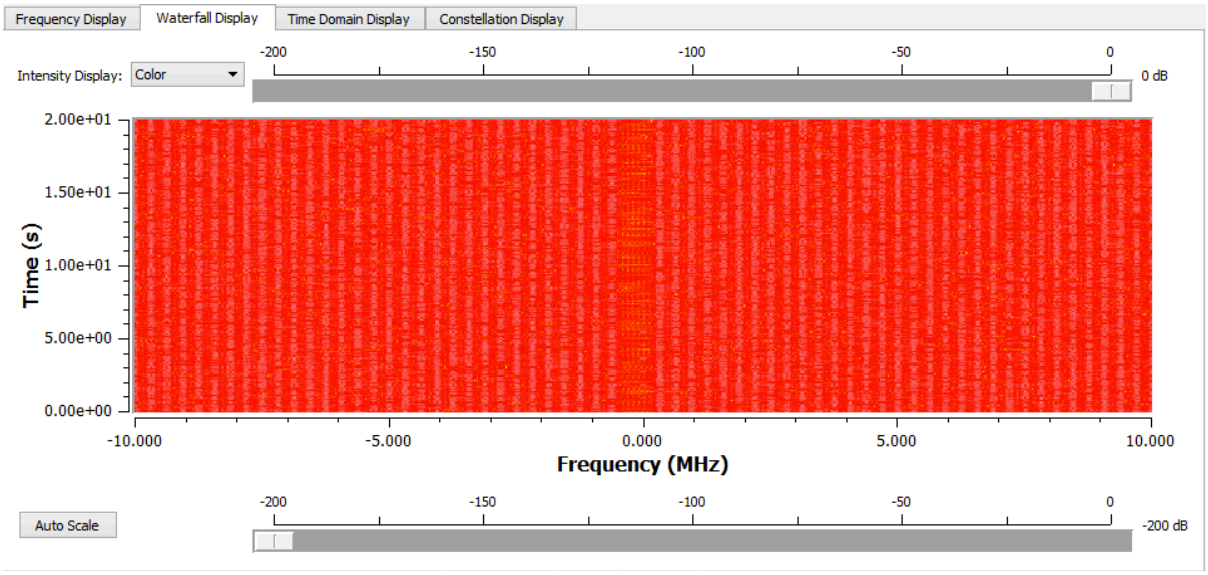

Figura 56-Relação frequência-tempo

A Figura 57 mostra a relação entre a amplitude e tempo. O ruído que o jammer está a transmitir é complexo, ou seja, tem parte real e parte imaginária. O sinal a azul corresponde à parte real, enquanto o sinal a vermelho corresponde à parte imaginária.

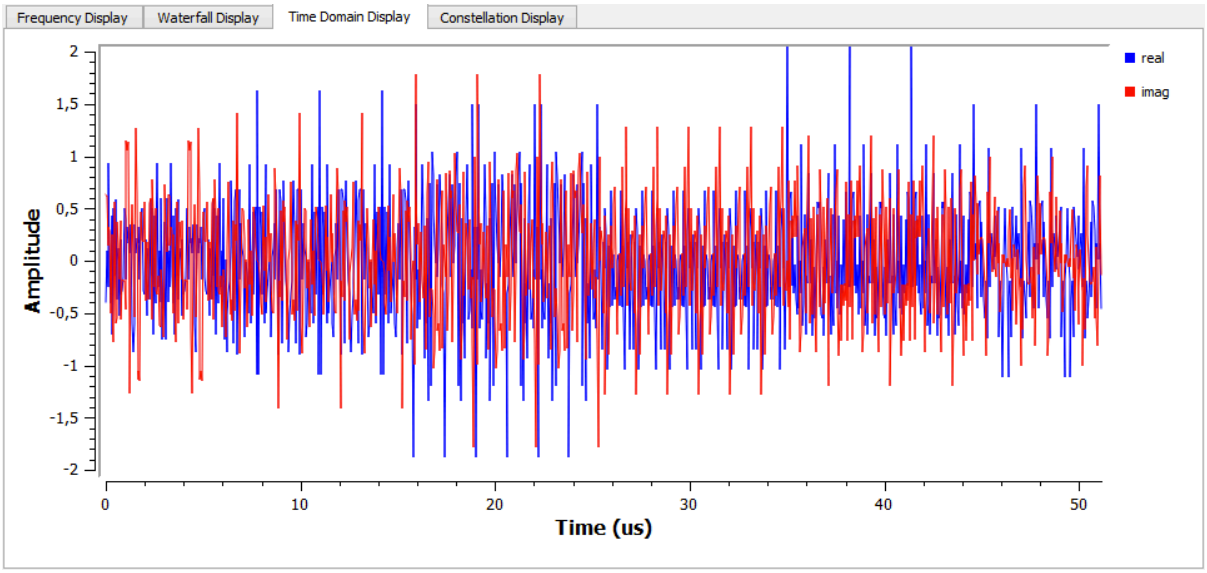

Figura 57-Espectro no tempo

A Figura 58 mostra constelação do sinal enviado. Cada ponto no gráfico representa um número complexo que foi transmitido.

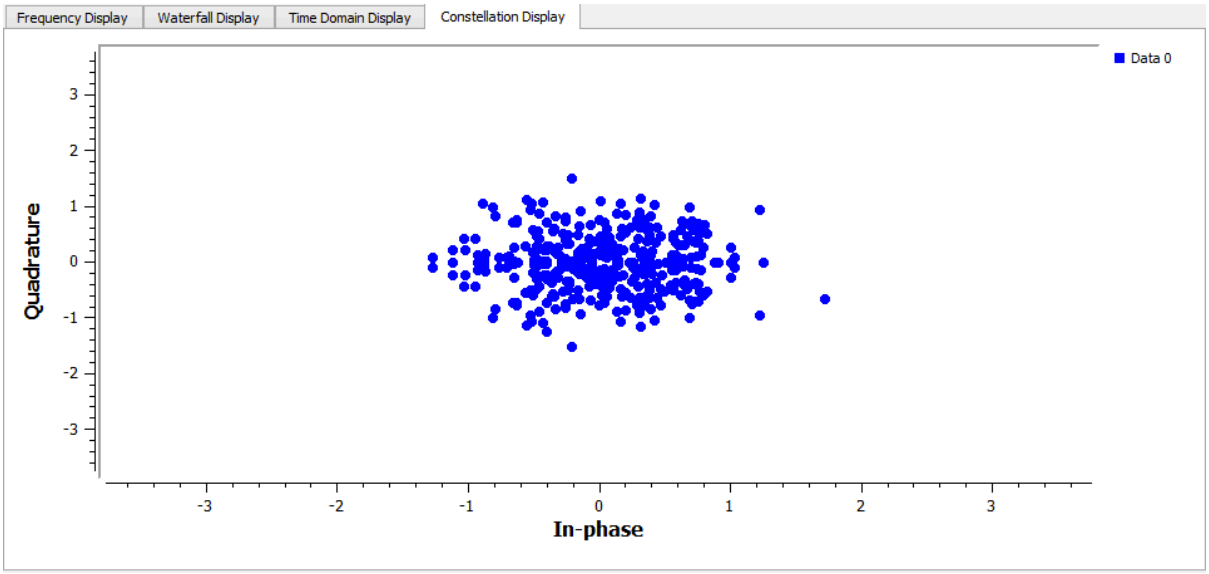

Figura 58-Constelação

5.3.6.2 CDMA-QPSK Jamming

A Figura 59 corresponde ao espectro de frequência. A frequência central neste caso é 0 KHz, que corresponde à frequência colocada no bloco "QT GUI sink". O espectro apresenta este comportamento pois foi multiplexado utilizando a técnica, CDMA e foi modulado em QPSK.

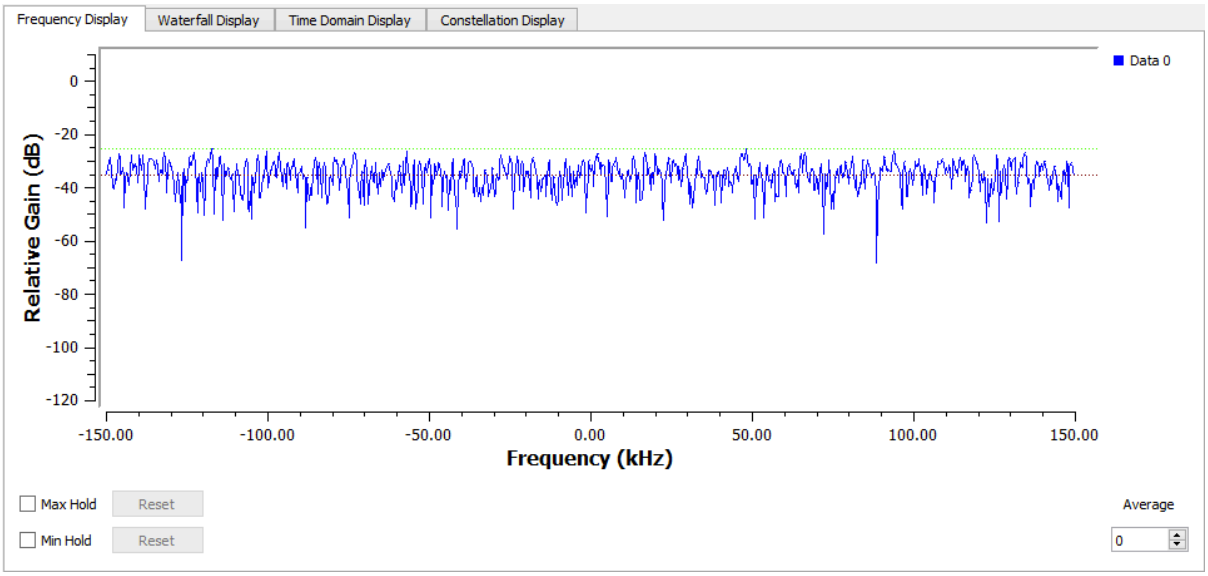

Figura 59-Espectro de frequência

A Figura 60 corresponde à relação entre a frequência e tempo. No eixo dos x temos a frequência e no eixo dos y o tempo. O gráfico encontra-se todo a vermelho pois o jammer tem largura de banda de 20MHz, o que faz com que esteja a ocupar todas essas frequências durante o tempo estipulado.

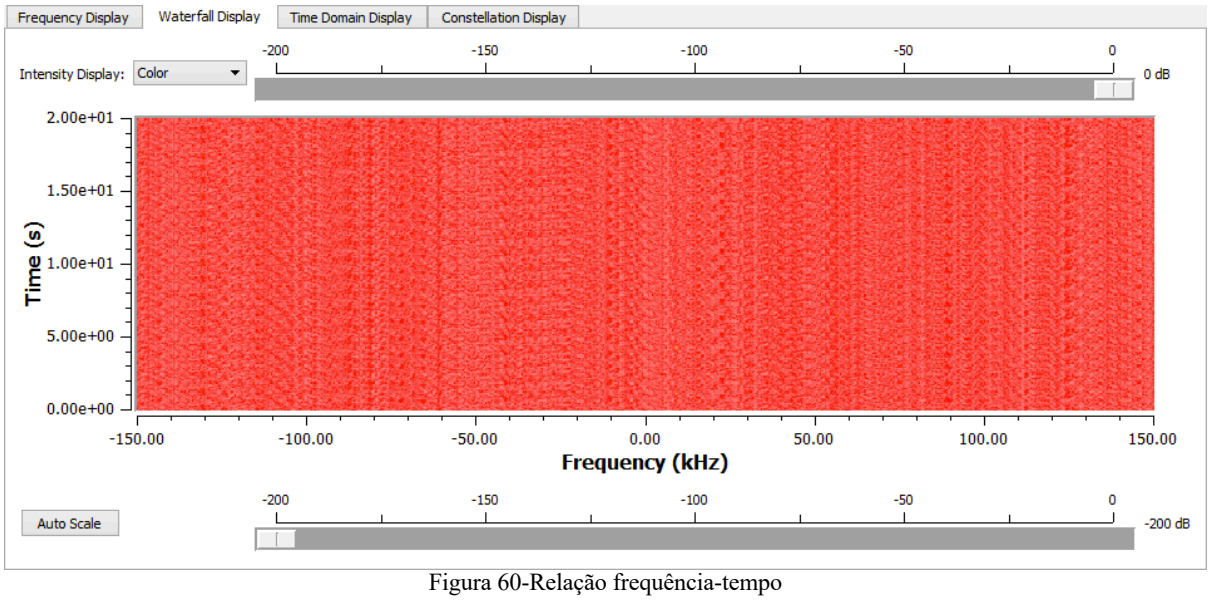

Figura 60-Relação frequência-tempo

A Figura 61 mostra a relação entre a amplitude e tempo. No eixo dos x temos o tempo e no eixo dos y a amplitude. O sinal a azul corresponde à parte real, enquanto o sinal a vermelho corresponde à parte imaginária. Ambas as partes são bits e têm como amplitude máxima e mínima, respetivamente, 1 e -1.

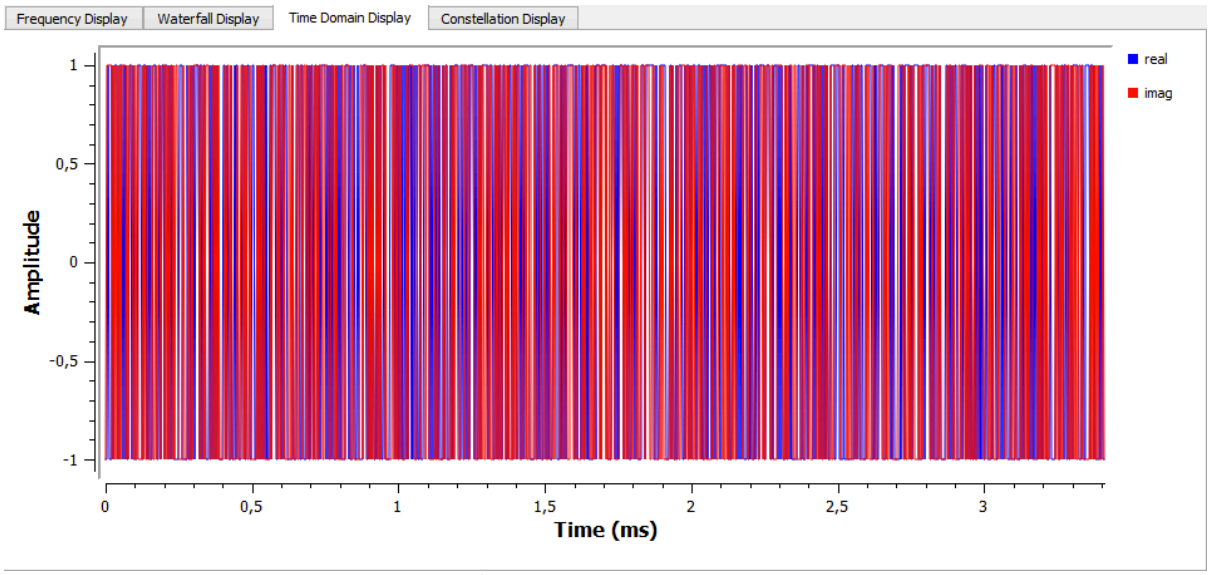

Figura 61-Espectro no tempo

A Figura 62 mostra a constelação do sinal transmitido. No eixo dos x temos a parte real e no eixo dos y a parte imaginário. Cada ponto no gráfico representa um número complexo que foi transmitido. Na figura temos a constelação QPSK em que o sinal foi modulado.

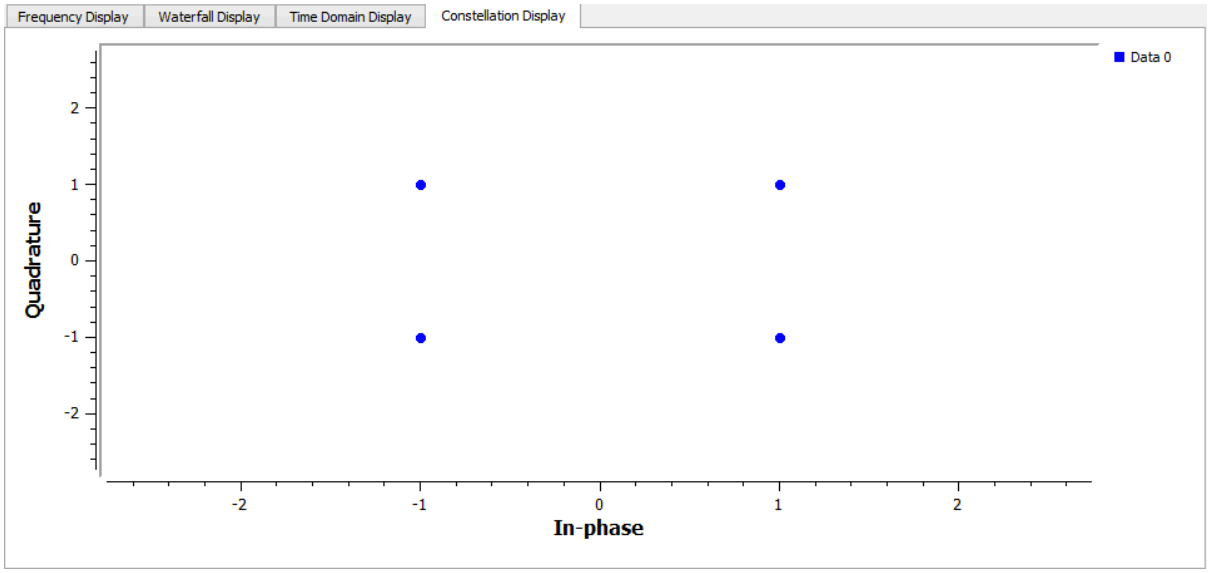

Figura 62-Constelação

Com este jammer foi possível interferir com o link de comunicações do Spektrum RC. Na Figura 63 são apresentadas distâncias a partir do qual é possível bloquear o sinal, variando o ganho RF da BladeRF.
Na Figura 63 (a), o valor de RF é de 25dB que corresponde à potência máxima da BladeRF. Neste caso o jammer começa a bloquear o link de comunicações, quando o carro se encontrar a 25m ou menos da antena.
Na Figura 63 (b), o valor de RF é de 12dB que corresponde à potência média da BladeRF. Neste caso o jammer começa a bloquear o link de comunicações, quando o carro se encontrar a 17m ou menos da antena.

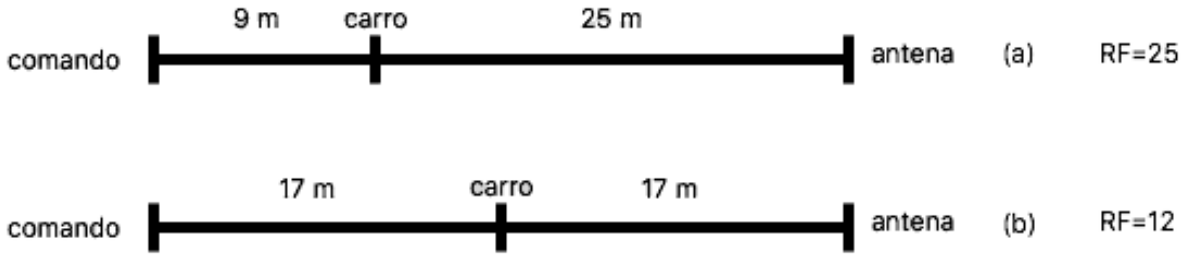

Figura 63-Resultados

Capítulo 6. Conclusões e Futuro Trabalho

6.1 Conclusões

Entre os jammers que foram testados, é possível analisar através da seção anterior, que os únicos que conseguiram bloquear o link de comunicações foram: o Barrage Jamming e CDMA-QPSK Jamming.
O Barrage Jamming conseguiu bloquear o link de comunicações pois apenas transmite ruido com a largura de banda máxima possível e consegue bloquear qualquer frequência nesse intervalo.
O Tone e o Sweep Jamming não conseguiram interferir, uma vez que o link de comunicações apresenta uma largura de banda de 1MHz, e a largura de banda utilizada para interferir não chega a esse valor.
O Wi-Fi Jamming não serve para interferir, pois neste caso o link de comunicações não funciona por Wi-Fi, ou seja, o protocolo está incorreto.
O CDMA-QPSK Jamming serviu para bloquear o link de comunicações pois é o protocolo que está a ser utilizado pelo link de comunicações.
O melhor jammer para bloquear o link de comunicações depende de vários fatores. No Barrage Jamming apenas é necessário alterar a frequência do link de comunicações, apesar de todos os sistemas que funcionem com essa frequência possam ser afetados. É utilizada menos memória do lado do computador, uma vez que que são usados menos blocos em comparação com o outro jammer.
O CDMA-QPSK permite apenas atacar uma determinada frequência que utilize o protocolo indicado. Caso seja preciso alterar para outro protocolo, é necessário mudar este jammer todo, o que torna este jammer pouco adaptável a várias situações. Também utiliza mais memória do lado do computador pois são utilizados mais blocos em comparação com o Barrage Jamming.
Neste sentido, o CDMA-QPSK é o melhor para usar neste caso, pois é o protocolo utilizado pelo link de comunicações.

6.2 Futuro Trabalho

O trabalho descrito foi focado na interferência do link de comunicações, considerando que não existia nenhum obstáculo no caminho do jammer. Um aspeto a explorar poderá considerar a existência de obstáculos entre o jammer e o veículo (drone) para analisar o efeito no bloqueio do link de comunicações. Também no futuro poderia ser efetuado um estudo mais profundo do link de comunicações utilizando um leitor de espectro e assim tentar desenvolver um jammer que tenha a capacidade de transmitir a onda inversa do sinal que estabelece o link de comunicação.

Referências

[1] I. Colomina and P. Molina, "Unmanned aerial systems for photogrammetry and remote sensing: A review," ISPRS Journal of Photogrammetry and Remote Sensing, vol. 92, pp. 79-97, 2014.

[2] "Portugal: 31 acidentes com drones nos aeroportos," Julho 2018. [Online]. Disponível em: https://pplware.sapo.pt/informacao/portugal-31-incidentes-drones-nos-aeroportos/. [acedido em 9 de Julho de 2018].

[3] "Drone bateu em avião na Argentina; EUA registam 100 casos de risco por mês," Julho 2018. [Online]. Disponível em : https://todosabordo.blogosfera.uol.com.br/2017/11/13/drone-bateu-em-aviao-na-argentina-eua-registram-100-casos-de-risco-por-mes/. [acedido em 9 de Julho de 2018].

[4] "5 Foolproof Ways of Taking Down Rogue Drones," Julho 2018. [Online]. Disponível em: https://www.gadgetdaily.xyz/5-foolproof-ways-of-taking-down-rogue-drones/. [acedido em 9 de Julho de 2018].

[5] "The Vulnerability of UAVs to Cyber Attacks- An Approach to the Risk Assessment," Julho 2018. [Online]. Disponível em: www.ccdcoe.org/cycon/2013/proceedings/d3r2s2_hartmann.pdf. [acedido em 27 de Julho de 2018].

[6] "Review of Unmanned Aircraft System (UAS)," Julho 2018 [Online]. Disponível em: http://www.uxvuniversity.com/wp-content/uploads/2014/04/Review-of-Unmanned-Aircraft-System-UAS.pdf. [acedido em 28 de Julho de 2018].

[7] J. Mitola III. Software radios: Survey, critical evaluation and future directions. IEEE Aerospace and Electronic Systems Magazine, 8(4):25–36, 1993.

[8] "What is Software Defined Radio," Julho 2018 [Online]. Disponível em: https://www.wirelessinnovation.org/assets/documents/SoftwareDefinedRadio.pdf. [acedido em 28 de Julho de 2018].

[9] "Development of a Software Defined Radio (SDR) for Cognitive Radio (CR) Communication Systems," Julho 2018 [Online]. Disponível em: https://fenix.tecnico.ulisboa.pt/downloadFile/844820067123822/MScThesis_Germano%20Capela.pdf. [acedido em 28 de Julho de 2018].

[10] "Software-defined Radios: Architecture, State-of-the-art, and Challenges," Julho 2018 [Online]. Disponível em: https://arxiv.org/pdf/1804.06564.pdf. [acedido em 28 de Julho de 2018].

[11] U. L. Rohde and T. T. N. Bucher, "*Communications Receivers: Principles and Design*," 4th ed. McGraw-Hill Education, 1988.

[12] A. Haghighat, "A review on essentials and technical challenges of software defined radio," in *MILCOM 2002. Proceedings*, 2002, pp. 377–382.

[13] T. J. Rouphael, "*RF and digital signal processing for software-defined radio: a multi-standard multi-mode approach,"* Newnes, 2009.

[14] J. J. Carr, "*The technician's radio receiver handbook: wireless and telecommunication technology*," Newnes, 2001.

[15] T. Hentschel, M. Henker, and G. Fettweis, "The digital front-end of software radio terminals," *IEEE Personal Communications*, vol. 6, no. 4, pp. 40–46, 1999.

[16] M. N. O. Sadiku and C. M. Akujuobi, "Software-defined radio: a brief overview," *IEEE Potentials*, vol. 23, no. 4, pp. 14–15, oct 2004.

[17] L. C. Choo and Z. Lei, "CRC Codes for Short Control Frames in IEEE 802.11ah," in *2014 IEEE 80th Vehicular Technology Conference (VTC2014-Fall)*, sep 2014, pp. 1–5.

[18] F. Berns, G. Kreiselmaier, andN.Wehn,"Channel decoder architecture for 3G mobile wireless terminals," in *Proceedings Design, Automation and Test in Europe Conference and Exhibition*, pp. 192–197.

[19] P.-Y. Chiueh, Tzi-Dar and Tsai, *OFDM baseband receiver design for wireless communications*. John Wiley & Sons, 2008.

[20] "67ladeRF Software Defined Radio. Nuand," Julho 2018 [Online]. Disponível em: http://www.nuand.com/. [acedido em 30 de Julho de 2018].

[21] "HackRF Software Defined Radio. One Great Scott Gadgets," Julho de 2018 [Online]. Disponível em: http://greatscottgadgets.com/hackrf/. [acedido em 30 de Julho de 2018].

[22] "USRP Software Defined Radio. National Instruments," Julho de 2018 [Online]. Disponível em: http: //www.ni.com/sdr/usrp/pt/. [acedido em 30 de Julho de 2018].

[23] S. Robert, "The origins of spread-spectrum communications. *IEEE Transac- tions on Communications"*, 30(5):822–854, 1982.

[24] P. Raymond, S. Donald, and M. Laurence. "Theory of spread- spectrum communications–a tutorial. *IEEE transactions on Communications"*, 30(5):855–884, 1982.

[25] "Theory of Spread-Spectrum Communications- A Tutorial," Agosto de 2018 [Online]. Disponível em: https://pdos.csail.mit.edu/archive/decouto/papers/pickholtz82.pdf. [acedido em 3 de Agosto de 2018].

[26] Richard A. Poisel. "*Modern Communications Jamming Principles and Techniques"*. Artech House, 2011.

[27] Earl McCune. *Practical digital wireless signals*. Cambridge University Press, 2010.

[28] P. Karel, "Jamming of Spread Spectrum Communications Used in UAV Remote Control Systems", 2017.

[29] F. John, "Processing gain in spread spectrum signals". *Harris Semiconductor application note*, 1998.

[30] F. Bruce, A. Roberto, C. Praphul, D. Daniel, B. Dan, M. Douglas, L. David, D. Farid and O. Ron. "*RF and Wireless Technologies: Know It All"*. Elsevier, 2007.

[31] M. Guowang, Z. Jens, S. Ki, S. Ben (2016). “Fundamentals of Mobile Data Networks”, Cambridge University Press.

[32] “Code-division multiple access,” Agosto de 2018 [Online]. Disponível em: https://en.wikipedia.org/wiki/Code-division_multiple_access#cite_note-9. [acedido em 3 de Agosto de 2018].

[33] “Concepts of Orthogonal Frequency Division Multiplexing (OFDM) and 802.11 WLAN” [Online]. Disponível em: http://rfmw.em.keysight.com/wireless/helpfiles/89600b/webhelp/subsystems/wlan-ofdm/content/ofdm_basicprinciplesoverview.htm. [acedido em 19 de Setembro de 2018].

[34] “Phase-shift keying”, Setembro de 2018 [Online]. Disponível: https://en.wikipedia.org/wiki/Phase-shift_keying. [acedido em 25 de Setembro de 2018].

[35]Marc Lichtman, Jeffrey D. Poston, SaiDhiraj Amuru, Chowdhury Shahriar, T. Charles Clancy, R. Michael Buehrer, and Jeffrey H. Reed. A communications jamming taxonomy. *IEEE Security & Privacy*, 14(1):47–54, February 2016.

[36] Kanika Grover, Alvin Lim, and Qing Yang. Jamming and anti–jamming techniques in wireless networks: a survey. *International Journal of Ad Hoc and Ubiquitous Computing*, 17(4):197–215, 20.

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

[38] Abid Hussain, Nazar A Saqib, Usman Qamar, Muhammad Zia, and Hassan Mah- mood. Protocol-aware radio frequency jamming in wi-fi and commercial wireless networks. *Journal of communications and networks*, 16(4):397–406, 2014.

[39] 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.

[40] “Fórmula de Friis”, Setembro de 2018 [Online]. Disponível em: https://pt.wikipedia.org/wiki/Fórmula_de_Friis. [acedido em 30 de Setembro de 2018].

[41] “Protecting the Sky,” Julho de 2018 [Online]. Disponível em: https://www.scribd.com/doc/315420957/Protecting-the-Sky. [acedido em 31 de Julho de 2018].

[42] “BladeRF- USB 3.0 Software Defined Radio,” Agosto de 2018 [Online]. Disponível em: http://www.nuand.com/bladeRF-brief.pdf. [acedido em 10 de Agosto de 2018].

[43] “Field-Programmable Gate Array,” Agosto de 2018 [Online]. Disponível em: https://pt.wikipedia.org/wiki/Field-programmable_gate_array. [acedido em 10 de Agosto de 2018].

[44] “Field Programmable RF ICs: LM6002D- Lime Micro,” Agosto de 2018 [Online]. Disponível em: http://www.limemicro.com/products/field-programmable-rf-ics-lms6002d/. [acedido em 11 de Agosto de 2018].

[45] “EZ-USB FX3™ SuperSpeed USB 3.0 peripheral controller,” Agosto de 2018 [Online]. Disponível em: http://www.cypress.com/products/ez-usb-fx3-superspeed-usb-30-peripheral-controller. [acedido em 11 de Agosto de 2018].

[46] “Amplifier | Nuand,” Agosto de 2018 [Online]. Disponível em: https://www.nuand.com/blog/product/amplifier/. [acedido em 11 de Agosto de 2018].

[47] “XB300- Amplifier- Block Diagram,” Agosto de 2018 [Online]. Disponível em: http://nuand.com/xb300.pdf. [acedido em 11 de Agosto de 2018].

[48] “BladeRF Power Consumption,” Agosto de 2018 [Online]. Disponível em: https://github.com/Nuand/bladeRF/wiki/bladeRF-Power-Consumption. [acedido em 11 de Agosto de 2018].

[49] “Apex TG.30 Ultra-Wideband Dipole LTE Antenna,” Agosto de 2018 [Online]. Disponível em: https://www.arcantenna.com/documents/get/document/id/76/. [acedido em 11 de Agosto de 2018].

[50] “3G/4G Antenna 11dB | Konig,” Agosto de 2018 [Online]. Disponível em: https://www.konigelectronic.com/television/antennas/3g4g-antenna-11-db-550562785. [acedido em 11 de Agosto de 2018].

[51] “GNU Radio, the free and open software radio ecosystem,” Agosto de 2018 [Online]. Disponível em: http://gnuradio.org/. [acedido em 12 de Agosto de 2018].

[52] “Guided Tutorial GRC- GNU Radio,” Outubro de 2018 [Online]. Disponível em: https://wiki.gnuradio.org/index.php/Guided_Tutorial_GRC. [acedido em 1 de Outubro de 2018].

[53] “Software Defined Radio for Wi-Fi Jamming,” Agosto de 2018 [Online]. Disponível em: https://www.researchgate.net/publication/301850218_Software_Defined_Radio_for_Wi-Fi_Jamming. [acedido em 12 de Agosto de 2018].

[54] “Gqrx SDR- Open source software defined radio,” Agosto de 2018 [Online]. Disponível em: http://gqrx.dk. [acedido em 12 de Agosto de 2018].

[55] “libbladeRF: Gain control,” Setembro de 2018 [Online]. Disponível em: https://nuand.com/libbladeRF-doc/v1.7.0/group___f_n___g_a_i_n.html. [acedido em 4 de Setembro de 2018].

[56] “digital communications – Sampling rate in Wifi,” Setembro de 2018 [Online]. Disponível em: https://dsp.stackexchange.com/questions/17968/sampling-rate-in-wifi-802-11-20-mhz-enough-with-a-bw-of-20-mhz. [acedido em 4 de Setembro de 2018].

[57] “Spektrum 2.4GHz DSM System,” Setembro de 2018 [Online]. Disponível em: http://www.spektrumrc.com/Articles/Article.aspx?ArticleID=1504. [acedido em 20 de Setembro de 2018].

[58] “Learn the Basics of Spread Spektrum R/C” Setembro de 2018 [Online]. Disponível em: https://makezine.com/2015/06/24/skill-builder-intro-spread-spectrum-rc/. [acedido em 22 de Setembro de 2018].

[59] “RC Spread Spectrum Demystified”. Outubro de 2018 [Online]. Disponível em: https://www.rchelicopterfun.com/RC-Spread-Spectrum.html. [acedido em 4 de Outubro de 2018].