UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE ENGENHARIA ELÉTRICA
ENGENHARIA ELETRÔNICA E DE TELECOMUNICAÇÕES
CAMPUS PATOS DE MINAS

ARTHUR HENRIQUE SILVA

UM ESTUDO DAS INTERFERÊNCIAS INTENCIONAIS NO SINAL L1 DO GPS UTILIZANDO RÁDIO DEFINIDO POR SOFTWARE

Patos de Minas - MG
2023

ARTHUR HENRIQUE SILVA

UM ESTUDO DAS INTERFERÊNCIAS INTENCIONAIS NO SINAL L1 DO GPS UTILIZANDO RÁDIO DEFINIDO POR SOFTWARE

Projeto de pesquisa apresentado à banca examinadora como requisito parcial de avaliação da disciplina de PFC II da graduação em Engenharia Eletrônica e de Telecomunicações, da Faculdade de Engenharia Elétrica, da Universidade Federal de Uberlândia, Campus Patos de Minas.

Orientador: Prof. Dr. Davi Sabbag Roveri

Patos de Minas - MG
2023

ARTHUR HENRIQUE SILVA

UM ESTUDO DAS INTERFERÊNCIAS INTENCIONAIS NO SINAL L1 DO GPS UTILIZANDO RÁDIO DEFINIDO POR SOFTWARE

Projeto Final de Curso da Universidade Federal de Uberlândia como requisito parcial para aprovação na disciplina de PFCII.

Patos de Minas, junho de 2023

Banca Examinadora:

_____

Dr. André Antônio dos Anjos – UFU

_____

Dr. Davi Sabbag Roveri – UFU (Orientador)

_____

Dra. Karine Barbosa Carbonaro - UFU

Dedico este trabalho aos meus amados pais, cujo apoio e amor inspiraram-me a persistir, superar desafios e ser uma pessoa melhor.

AGRADECIMENTOS

Gostaria de expressar minha profunda gratidão ao meu estimado orientador, Dr. Davi, por acreditar em mim e no potencial do meu trabalho. Sua orientação, incentivo e motivação foram essenciais para que eu persistisse, mesmo diante dos grandes desafios que se apresentavam. Sou imensamente grato por sua confiança e por me guiar nessa jornada acadêmica.

Agradeço também à professora Dra. Karine, que se tornou para mim verdadeiro exemplo de dedicação, empatia e excelência no ensino. Sua paixão pela educação e seu apoio constante foram fundamentais para o meu crescimento pessoal e acadêmico.

Não posso deixar de mencionar o professor Dr. André, cujo apoio durante todo o meu Trabalho de Conclusão de Curso foi inestimável. Sua experiência, conhecimento e disposição para compartilhar sua sabedoria foram essenciais para o sucesso deste trabalho.

Minha gratidão se estende à Universidade Federal de Uberlândia, que proporcionou as bases e o conhecimento necessários para minha formação como engenheiro. Sou grato por fazer parte desta instituição que valoriza o aprendizado, a pesquisa e o desenvolvimento acadêmico.

À minha amada família, que esteve ao meu lado em todos os momentos, especialmente nos mais desafiadores, meu profundo agradecimento. Seu amor, apoio e encorajamento deram a força que me impulsionou a seguir em frente.

Por fim, mas não menos importante, expresso minha gratidão a Deus, fonte de toda sabedoria e inspiração. Sua presença e guia foram fundamentais em cada etapa dessa jornada acadêmica. Sem Sua graça e orientação, nada disso seria possível.

A todos que contribuíram direta ou indiretamente para a realização deste trabalho, meu sincero agradecimento. Vocês são parte fundamental dessa conquista e sempre terão meu reconhecimento.

RESUMO

O presente trabalho trata da utilização de um rádio definido por software (SRD) para causar propositalmente interferência nos sinais de satélites utilizados para navegação, fazendo com que os dispositivos receptores próximos não funcionem corretamente. O sistema opera como um transmissor de sinal na frequência da portadora de forma a impedir que os dados reais sejam lidos pelos dispositivos. Muitos dos sistemas que são utilizados cotidianamente dependem do correto funcionamento dos sinais recebidos de constelações de satélites e entender como eles funcionam pode colaborar para que os sistemas se tornem mais seguros. Para gerar esses sinais de interferência é utilizado um rádio definido por software, ou seja, um dispositivo que pode receber e transmitir em uma ampla gama de frequências do espectro eletromagnético. O rádio é configurado via software para transmitir sinais com diferentes formas de onda na frequência L1 do sistema GPS (1575,42 MHz). Para verificação da efetividade do dispositivo de interferência é utilizado um smartphone com um aplicativo que fornece informações sobre os sinais de geoposicionamento. Pretende-se estudar os efeitos causados e avaliar a distância máxima (raio) em que os diferentes formatos de onda do sinal interferente conseguem impedir a leitura do sinal correto de GPS. Por meio dos resultados discutir o nível de vulnerabilidade a que os dispositivos de uso civil estão expostos, servindo assim como referência futura para melhorias na segurança desses dispositivos.

Palavras-chave: GNSS; GPS; Interferência intencional; Rádio Definido por Software; SDR; Geolocalização.

ABSTRACT

The present work deals with the use of a software-defined radio (SRD) to intentionally cause interference in the satellite signals used for navigation, making nearby receiver devices not work correctly. The system operates as a signal transmitter on the carrier frequency in order to prevent the real data from being read by the devices. Many of the systems that are used daily depend on the correct functioning of the signals received from satellite constellations and understanding how they work can help to make the systems more secure. To generate these interference signals, a software-defined radio is used, that is, a device that can receive and transmit in a wide range of frequencies of the electromagnetic spectrum. The radio is configured via software to transmit signals with different waveforms on the L1 frequency of the GPS system (1575.42 MHz). To check the effectiveness of the interference device, a smartphone with an application that provides information about the geopositioning signals is used. It is intended to study the effects caused and evaluate the maximum distance (radius) at which the different waveforms of the interfering signal manage to prevent the reading of the correct GPS signal. Through the results, discuss the level of vulnerability to which civil use devices are exposed, thus serving as a future reference for improvements in the security of these devices.

Keywords: GNSS; GPS; Intentional interference; Software Defined Radio; SDR; Geolocation.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ADC	Conversor analógico digital
ANATEL	Agência Nacional de Telecomunicações
BER	*Bit Error Rate*
BSR	Bloqueador de sinal de radiocomunicações
FDMA	*Frequency Division Multiple Access*
GNSS	*Global Navigation Satellite System* (Sistema Global de Navegação por Satélite)
GPS	*Global Positioning System*
IRNSS	*Indian Regional Navigation Satellite System*
RF	Rádio Frequência
SNR	Relação Sinal Ruído
UFU	Universidade Federal de Uberlândia

SUMÁRIO

CAPÍTULO 1

1.1 INTRODUÇÃO

As constelações de satélites que fornecem um serviço de geolocalização com cobertura global possibilitam que pequenos receptores eletrônicos, cada vez mais baratos, determinem suas coordenadas geográficas (longitude, latitude e altitude) com um erro pequeno (poucos metros) em qualquer ponto da superfície terrestre ou da atmosfera, por meio do processamento dos sinais de radiofrequência transmitidos. (MONICO, 2008)

Dentre as redes há o US NAVSTAR *Global Positioning System* (GPS), que está totalmente operacional desde 1995, contudo foi apenas no ano 2000 que o governo dos Estados Unidos o abriu gratuitamente para uso civil. O sistema russo GLONASS, totalmente operacional desde dezembro de 2011. O sistema europeu Galileo, que entrou em serviço em 15 de dezembro de 2016, esteve em fase de implementação até o ano de 2023 quando entrou em nível operacional. A China criou o seu sistema de posicionamento Beidou, que operou a nível regional até o ano de 2020, quando passou a operar globalmente. Finalmente, tem-se a Índia desenvolvendo o IRNSS (*Indian Regional Navigation Satellite System*), um sistema GNSS (*Global Navigation Satellite System)* de nova geração. (EL-RABBANY, 2002)

A quantidade de dispositivos que funcionam baseados em coordenadas geográficas aumentou muito desde que essa tecnologia foi liberada para uso civil. Essa liberação alavancou uma diversidade de aplicações e recursos que facilitam o comércio e beneficiam diretamente toda a cadeia produtiva e de distribuição de produtos.

As empresas da área de tecnologia e desenvolvimento de aplicativos têm estudado como aproveitar esse recurso de posicionamento e acompanhamento de rota dos dispositivos para aprimorar a recomendação de serviços (restaurantes, hotéis, pontos turísticos, postos de combustíveis etc.) e ofertas de produtos cada vez mais específicos para cada potencial cliente. Como exemplo, existe o Google Maps, distribuído pela Google, uma aplicação gratuita para o usuário e pioneira em navegação, contando com imagens de satélite além de imagens obtidas localmente, visando a melhor orientação durante o seu uso.

Por se tratar de um serviço que facilita a navegação, como ilustrado na Figura 1.1, unindo fotos e coordenadas, o Google Street View processa a imagem registrada com a respectiva coordenada obtida com um sistema GNSS. Caso houvesse uma interrupção no sinal dos satélites durante o registro fotográfico, as imagens capturadas pelas câmeras do Google no local não possuiriam relação com a real posição e perderiam o seu propósito.

Figura 1.1 – Prédio da UFU em Patos de Minas capturada no serviço *Street View*

Fonte: Google *Street View*

1.2 TEMA DO PROJETO

Atualmente, o sinal de algum GNSS pode ser obtido em qualquer lugar do mundo, sendo um sistema amplamente utilizado de forma aberta e funcionando como referência para diversos setores. Dentre os sistemas, o mais utilizado, apesar de estar liberado para uso civil, é o GPS que é controlado e mantido pelo governo dos Estados Unidos. (KAPLAN; HEGARTY, 2017)

Entretanto, esse tipo de sistema não está imune a interferências e por si só é incapaz de reconhecer a presença de equipamentos interferidores, fornecendo aos dispositivos receptores informações ou parâmetros verificadores que atestem a sua real localização. Faz se necessário, assim, conhecer os possíveis efeitos de bloqueadores sobre os sinais reais (aqueles enviados pelas constelações de satélites). (MONICO, 2008)

O projeto visa utilizar um rádio transmissor para impedir que dispositivos próximos a ele detectem com confiabilidade a sua localização.

1.3 PROBLEMATIZAÇÃO

Em junho de 2013, um grupo de estudantes de pós-graduação da *Cockrell Scholl of Engineering* (Texas, EUA) sob a orientação de Todd Humphreys, realizaram com sucesso o desvio do curso de um iate de luxo no mar mediterrâneo. O dispositivo criado por eles enviava sinais falsos de GPS *(Spoofing)* para as antenas do iate informando que ele estaria supostamente se desviando do percurso. A informação adulterada foi apresentada nos equipamentos de navegação sem nenhum tipo de alerta, fazendo com que a tripulação, que foi informada do teste

em andamento, corrigisse o leme para a rota em que o iate supostamente deveria estar. Desse modo, os estudantes puderam definir o curso da embarcação. (DAILY MAIL REPORTER, 2013)

O embaralhamento ou bloqueio de sinais GNSS que impeçam a obtenção precisa da posição do receptor pode causar graves perdas financeiras, acidentes, atrasos ou desorientação. Sendo assim, entender como esses dispositivos bloqueadores de sinal funcionam é de extrema importância para projetar futuramente soluções que visem reconhecer possíveis ataques, bem como medidas corretivas.

1.4 HIPÓTESES

Decorre da problematização as seguintes hipóteses, que guiam a pesquisa aqui proposta:

- Se é possível utilizar um Rádio Definido por Software (SDR) que opere na frequência do L1 GPS (1575,42 MHz) transmitindo um sinal em diferentes formatos de onda, degradando a qualidade do sinal recebido da constelação de satélites, bem como o raio de efetividade desse transmissor interferidor;
- Se é possível verificar no dispositivo receptor a ausência do sinal verdadeiro do sistema L1 GPS.

1.5 OBJETIVOS

1.5.1 Objetivos Gerais

Investigação sobre a possibilidade do desenvolvimento de um sistema interferidor utilizando um rádio definido por software, com o objetivo de inviabilizar a operação de receptores na frequência L1 do GPS.

1.5.2 Objetivos Específicos

- Estudo sobre quais formas de onda contribuem para um melhor desempenho do interferidor.
- Compreensão do software GNU Radio combinada ao uso de um rádio definido por software (SDR).

- Impedir a correta detecção de sinais de GPS válidos em dispositivos receptores próximos a um transmissor de radiofrequência que envie um sinal com diferentes formas de onda na frequência do sistema L1 GPS.

1.6 JUSTIFICATIVAS

Esse estudo tem em vista adicionar uma nova visão ao escasso material em língua portuguesa destinado a descrever os dispositivos interferidores (*jammers*) que operam em frequências de sistemas GNSS.

1.7 CONSIDERAÇÕES FINAIS

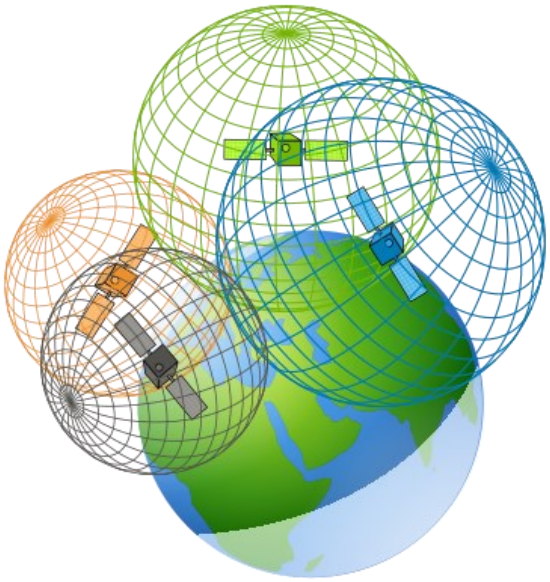
Tendo em vista um amplo e crescente mercado em serviços de geolocalização, se torna útil entender sobre os dispositivos interferidores de sinais nas frequências destinadas para uso nesses serviços.

CAPÍTULO 2

2.1 SISTEMAS DE POSICIONAMENTO GLOBAL POR SATÉLITES

O satélite transmite um sinal que contém a sua posição e a hora de transmissão do próprio sinal, obtida de um relógio atômico altamente preciso e que mantem a sincronização com os demais satélites da constelação. O receptor compara a hora da transmissão com a de seu próprio relógio interno, o tempo que leva para o sinal chegar do satélite até o receptor é utilizado para cálculo da posição relativa. Diversas medições podem ser feitas simultaneamente com diferentes satélites, dessa forma obtém-se o posicionamento em tempo real. (KAPLAN; HEGARTY, 2017)

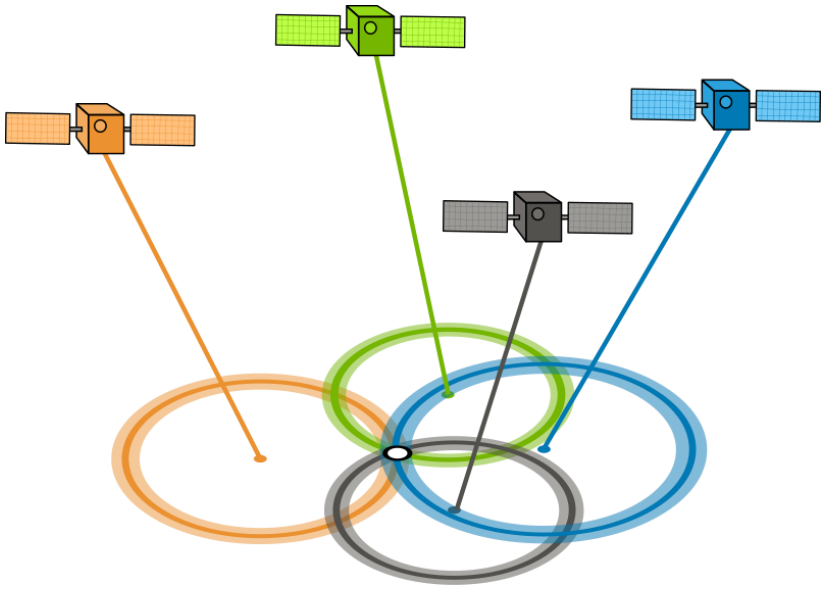
Figura 2.1 – Representação da propagação dos sinais dos satélites.



Fonte: https://www.pngegg.com/pt/png-iyjwe

Cada medida de distância, independentemente do sistema utilizado, identifica uma esfera que tem um satélite como centro, o posicionamento é obtido a partir da interseção dessas esferas. No entanto, no caso de receptores de movimento rápido, a posição do receptor se move conforme os sinais são recebidos. Além disso, os sinais de rádio atrasam ligeiramente à medida que passam pela ionosfera e esse atraso varia com o ângulo entre o receptor e o satélite, pois isso altera a distância percorrida pela ionosfera.

Figura 2.2 – Representação do ponto de intersecção dos sinais.



Fonte: https://www.pngegg.com/pt/png-epkab

O cálculo básico tenta então encontrar a linha direta mais curta tangente a quatro esferas centradas em quatro satélites. Os receptores reduzem os erros usando combinações de sinais de vários satélites e vários correlacionadores e, novamente, usando técnicas como o filtro de Kalman para mesclar dados ruidosos, parciais e que variam constantemente em uma única estimativa de posição, tempo e velocidade. O filtro de Kalman utiliza a dinâmica do alvo que define sua evolução ao longo do tempo para obter melhores dados, eliminando assim o efeito do ruído. Esses dados podem ser calculados para o momento presente (filtragem), no passado (suavização) ou em um horizonte futuro (previsão). Por exemplo, quando se deseja rastrear um alvo, os dados sobre sua posição, sua velocidade e sua aceleração são medidos a todo momento, mas com enormes perturbações devido a ruídos ou erros de medição. (EL-RABBANY, 2002)

2.2 TIPOS DE INTERFERÊNCIA

2.2.1 Intencional

Dispositivos capazes de bloquear ou interferir diretamente no funcionamento de receptores GNSS são preocupantes desde que foram utilizados em guerras pela primeira vez, pois a quantidade de ataques a dispositivos civis tem crescido constantemente. Não é difícil encontrar aparelhos à venda na internet para esse propósito e por um preço acessível. Na Figura

2.3 ilustra-se um exemplo de dispositivo jammer criado para interferir tanto nos sinais de posicionamento global quanto nos de telefonia sendo vendido sem dificuldades na internet.

Figura 2.3 – Dispositivo de interferência à venda

Fonte: https://produto.mercadolivre.com.br

Existem diversos tipos de dispositivos com diferentes aplicações e potências de transmissão, contudo podem ser classificados em dois tipos: Os jammers, que serão abordados adiante no trabalho, e os spoofers que fazem um embaralhamento do sinal enviando informações adulteradas na tentativa de confundir os dispositivos receptores. (HUGHES, 2005)

2.2.2 Não intencional

Todos os dispositivos que operam em Rádio Frequência (RF) estão sujeitos a interferência, mesmo que pequena, de outros dispositivos. Quando há um cuidado no projeto e alocação de bandas específicas de segurança (banda de guarda) essa interferência diminui, porém não é totalmente anulada. Existem mais sistemas que também operam na banda L e que podem ser fontes não intencionais de interferência.

A banda de 1.559 - 1.610 MHz é exclusiva para uso de sinais de navegação por satélite na maioria dos países. Os sinais L1 de GPS, GLONASS, Galileo, BeiDou, QZSS e SBAS estão dentro desta banda protegida. Na banda de 1.240 - 1.300 MHz encontram-se os sinais GLONASS L2, Galileo E6, BeiDou B3 e QZSS L6. Os sinais L2 de GPS e QZSS estão na banda de 1.215 - 1.240 MHz onde também há sistemas de radares que podem causar interferência não intencional no sinal. Os sinais GPS L5, Galileo E5A e E5B, BeiDou B2, NAVIC L5, QZSS L5 e SBAS L5 estão na faixa de 1.164 - 1.215 MHz. A banda de 960 - 1.215

MHz também é usada mundialmente para auxílios eletrônicos à navegação aérea. (KAPLAN; HEGARTY, 2017)

As interferências não intencionais são causadas principalmente por harmônicos vindos de outras fontes, interferências de bandas adjacentes que foram mal dimensionados ou operam acima da potência permitida ou resultado de intermodulação ocorrem quando dois ou mais sinais em frequências diferentes são passados por uma não linearidade. Além disso, mesmo que um sinal RF esteja fora da banda de interesse dos receptores GNSS, se esses sinais forem fortes ainda podem deteriorar o desempenho do receptor GNSS, saturando os amplificadores de baixo ruído usados no *front-end* do receptor. (KAPLAN; HEGARTY, 2017)

Existem outras fontes de causas de interferências não intencionais que fogem ao escopo desse trabalho, mas que valem a pena ser mencionadas:

- Satélite: erro da órbita, erro do relógio, relatividade etc.;
- Propagação do sinal: refração troposférica, refração ionosférica, Perdas de ciclo, sinais refletidos, rotação da terra etc.;
- Receptor/Antena: erro do relógio, Erro entre os canais, Centro de fase da antena, atraso do hardware etc.;
- Estação: erro nas coordenadas, sinais refletidos, marés terrestres, movimento do polo, Carga dos oceanos e Carga da atmosfera.

2.3 JAMMER

O objetivo do *jammer* é inserir um sinal interferente dentro da banda de operação do sistema alvo. Por estar próximo dos dispositivos receptores e ser projetado para transmitir com uma potência maior do que o sinal verdadeiro, a relação entre sinal ruído e interferência (SNRI) fica baixa. É classificado no Brasil como um bloqueador de sinal de radiocomunicações (BSR), sendo o conceito mais simples de bloqueador de sinal. A legislação que aborda esse assunto é composta pela resolução da Agência Nacional de Telecomunicações (ANATEL) nº 308, de 11 de setembro de 2002 e o disposto nos arts. 75, 160 e 163, § 2º, inciso I, da Lei nº 9.472, de 16 de julho de 1997. (HUGHES, 2005)

Como medida defensiva contra jammers alguns automóveis possuem receptores que identificam esse tipo de ataque e desligam o veículo caso um sinal com essas características seja percebido.(HUGHES, 2005)

Um parâmetro que pode ser usado para verificar o desempenho de sistemas de comunicação quando estão na presença de interferência é a Taxa de Erro de Bit (BER - *Bit Error Rate*). A BER mede a taxa de bits incorretos recebidos em relação ao número total de bits transmitidos. O resultado da BER não possui uma unidade pois se caracteriza por uma proporção, desse modo deseja-se que a BER seja a menor possível, fazendo com que ocorra o melhor desempenho de comunicação do sistema. À medida que a potência do *jammer* aumenta, maior a interferência e consequentemente maior a quantidade de bits errados ou ausentes, prejudicando a qualidade da comunicação. Uma forma de descrever a BER é a equação 2.1. (IAN POOLE, 2021)

$$BER = \frac{número\ de\ bits\ errados}{numero\ total\ de\ bits\ transmitidos} \tag{2.1}$$

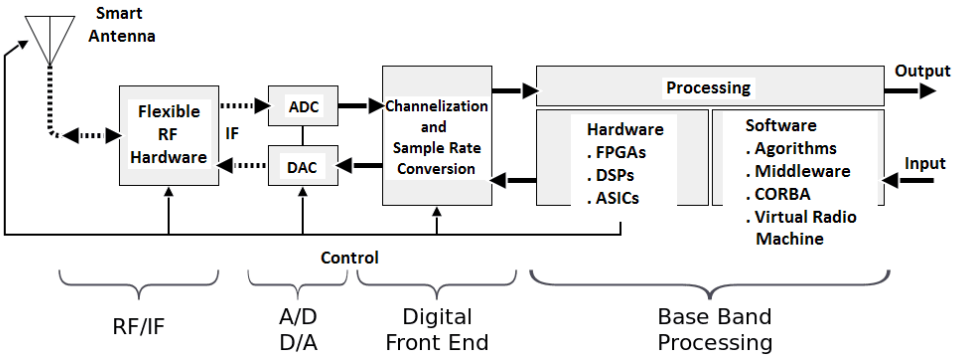
2.4 RÁDIO DEFINIDO POR SOFTWARE

Um Rádio Definido por Software (SDR) usa técnicas digitais para substituir os componentes do hardware do rádio tradicional, como mixers, moduladores, demoduladores e circuitos analógicos relacionados. Ao digitalizar diretamente os sinais de rádio usando um conversor analógico-digital (ADC) adequado, um SDR pode implementar todas essas funções em software, permitindo que o mesmo hardware seja usado para vários modos de recepção ou transmissão. O resultado é um rádio extremamente flexível que pode ser rapidamente reconfigurado para diferentes tecnologias de comunicação.

O hardware apenas fornece a base necessária, da antena à digitalização, para que o software possa assumir. Com SDRs, os modos de modulação e operação são definidos usando softwares (de)moduladores e (de)codificadores. Ao invés de ter componentes projetados para funcionarem em uma banda específica, é possível trabalhar os diferentes modos substituindo o software/código. (ROUPHAEL, 2009)

Na Figura 2.5 tem-se a ilustração dos blocos que compõem um SDR. Todas as funções no receptor SDR após o Conversor Analógico/Digital (ADC) são implementadas usando circuitos digitais programáveis, o que permite alterações e análises posteriores dentro do código. O SDR possui a mesma estrutura de componentes que os rádios transmissores convencionais, contudo, o diferencial é que esses componentes são reconfiguráveis para permitir a operação em uma faixa maior de frequências.

Figura 2.4 – Diagrama de blocos de um SDR



Fonte: https://www.nucleodoconhecimento.com.br/tecnologia/radio-definido

Entretanto é possível destacar algumas desvantagens que ainda justificam o grande uso de dispositivos “tradicionais” de comunicação, sendo alguns:

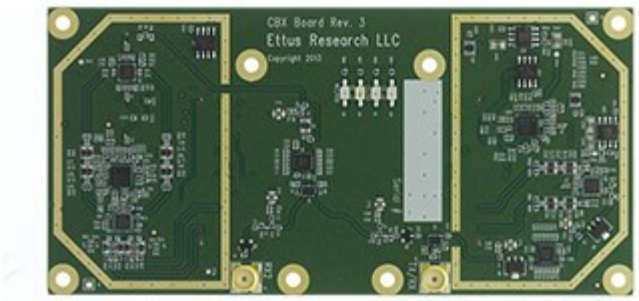
- Os ADCs limitam as frequências mais altas que poderiam ser usadas;
- Um circuito simples de SDR ainda é muito mais caro do que um circuito tradicional de AM ou FM, por exemplo;
- São necessárias habilidades e conhecimento de softwares para o melhor uso do potencial de um SDR;
- Ainda é necessária a participação de componentes analógicos, como por exemplo a antena, que podem necessitar de diferentes modelos para diferentes aplicações.

Para esse projeto utiliza-se o SDR da marca Ettus modelo USRP N210 com a placa de expansão CBX (40 MHz) com faixa de operação entre 1,2 a 6 GHz. As figuras 2.6 e 2.7 ilustram o SDR e a placa de expansão respectivamente.

Figura 2.5 – Rádio Ettus USRP N210

Fonte: https://www.ettus.com/all-products/un210-kit/

Figura 2.6 – Placa de expansão CBX (40 MHz)



Fonte: https://www.ettus.com/all-products/cbx/

2.5 SINAL L1 DO GPS

O sinal L1 do GPS foi projetado para transmitir informações de posicionamento e temporização para dispositivos receptores GPS. Esse sinal possui diversas características sendo as principais:

- Frequência central em 1575,42 MHz e isso significa que a operação ocorre na faixa de micro-ondas permitindo uma boa propagação por longas distâncias com baixa atenuação.
- A transmissão é feita a uma taxa de 50 bits por segundo. Esses pacotes contêm informações como os dados orbitais do satélite (posição e horário) e além de informações sobre os satélites GPS em órbita.
- A potência varia entre 25 e 30 watts e isso foi definido para economizar a energia nos satélites e prolongar a vida útil das baterias.
- A precisão do posicionamento usando apenas o sinal L1 varia entre 5 e 10 metros, desse modo, para melhorar essa precisão os sistemas L2 e L5 são utilizados em conjunto.
- A portadora é modulada usando a técnica de modulação em fase (BPSK - *Binary Phase-Shift Keying*). Essa técnica utiliza a inversão da fase da portadora de acordo com os bits que serão transmitidos.

2.6 FORMATOS DE ONDA DO SINAL INTERFERIDOR

Dentre os possíveis formatos de onda disponíveis para serem utilizados, optou-se por avaliar o estudo com quatro tipos, sendo: senoidal, triangular, quadrada, além do ruído gaussiano.

2.6.1 Onda Senoidal:

A amplitude da tensão do sinal de interferência (V_{si}) da onda senoidal é dada pela equação 2.1:

$$V_{si} = A * sin(2\pi ft + \varphi)[\text{V}] \quad (2.2)$$

onde A é a amplitude, f é a frequência em Hertz, t é o tempo e φ é a fase em radianos.

A transformada de Fourier de uma onda senoidal resulta em dois picos no domínio da frequência, localizados em f e -f, com amplitudes iguais a A/2. (OPPENHEIM; WILLSKY, 2010)

2.6.2 Onda Triangular:

É dada pela equação 2.2:

$$V_{si} = \left(\frac{2A}{T}\right) * \left(\frac{t}{T} - \left\lfloor\frac{t}{T}\right\rfloor - \frac{1}{2}\right)[\text{V}] \quad (2.3)$$

onde A é a amplitude, T é o período e ⌊t/T⌋ é o valor inteiro de t/T.

A transformada de Fourier de uma onda triangular é uma função em forma de *sinc*, que possui um lóbulo principal centrado na frequência fundamental e lóbulos secundários decaindo em amplitude. A largura do lóbulo principal está relacionada com a taxa de variação da forma triangular, enquanto a amplitude dos lóbulos secundários diminui à medida que se afastam da frequência da fundamental. (OPPENHEIM; WILLSKY, 2010)

2.6.3 Onda Quadrada:

É dada pela equação 2.3:

$$V_{si} = A * sign(\sin(2\pi ft))[\text{V}] \quad (2.4)$$

onde A é a amplitude, f é a frequência e sign(x) é a função de sinal, que retorna 1 para x >= 0 e -1 para x < 0.

A transformada de Fourier de uma onda quadrada é uma série de lóbulos no domínio da frequência com a mesma distância entre si, localizados em valores múltiplos da frequência fundamental e com amplitudes proporcionais ao inverso desses múltiplos. (OPPENHEIM; WILLSKY, 2010)

2.6.4 Ruído Gaussiano:

O ruído gaussiano apresenta amplitude constante em todas as frequências, o que significa que sua densidade espectral de potência é uniforme. Essa uniformidade é o que faz o ruído ser chamado de "ruído branco". Essa característica torna o ruído gaussiano uma referência comum em várias aplicações de processamento de sinais, pois sua natureza aleatória e propriedades estatísticas bem definidas permitem análises e modelagem precisas.

CAPÍTULO 3

3.1 METODOLOGIA

O início do projeto se dá com a definição do tema, assim como a pesquisa sobre o funcionamento e as viabilidades técnica e financeira. Também é necessário verificar possíveis fontes de pesquisa bibliográfica dentre livros e artigos que podem ser usados como referência.

O passo seguinte é a definição do escopo do trabalho e dos objetivos já mencionados no capítulo 1. Essa definição é necessária para que o trabalho tenha um foco claro e se mantenha dentro da proposta e de estudo que se pretende alcançar.

O SDR se conecta ao notebook diretamente pela porta ethernet, sendo necessário, além de instalar o driver do dispositivo, configurar uma conexão local entre ambos os equipamentos. Para estabelecer os parâmetros de operação do SDR e enviar as instruções de funcionamento para o Rádio, utiliza-se o software GNU Radio.

O GNU Radio é um conjunto de ferramentas gratuito e de código aberto para desenvolvimento de softwares, que oferece blocos de processamento de sinal para a implementação em SDR. O GNU Radio é amplamente utilizado em diversas áreas, como pesquisa, indústria, academia, governo e por entusiastas, tanto para suportar pesquisas em comunicações sem fio quanto para sistemas de rádio reais. (GNU RADIO PROJECT, 2023)

Uma vez que os dispositivos estejam conectados e o código implementado no GNU Radio, os testes são realizados. A frequência de transmissão é definida em 1575,43 MHz por ser a frequência do sinal L1 do GPS e a largura de banda em 1 MHz. Esse valor de largura de banda foi definido em testes que levaram em consideração a potência fornecida para transmissão no SDR. Opou-se por utilizar a frequência de 100 kHz para gerar as formas de onda que serão enviadas interferir no sinal verdadeiro.

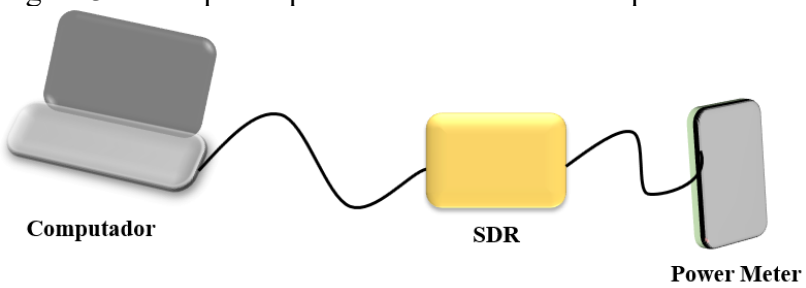
Para caracterizar as potências de transmissão na saída do SDR utiliza-se um instrumento de testes para aferição da potência do sinal transmitido (*power meter*) da marca Agilent modelo V3500A conectado diretamente via cabo. Variam-se os ganhos absolutos em diferentes formatos de onda, a fim de que os valores de potência (em dBm) apresentados no *power meter* sejam adicionados a uma tabela que relaciona esses dois parâmetros. Os formatos de onda escolhidos dentre as opções disponíveis são senóide, triangular, quadrada e ruído gaussiano.

Com os valores de potência transmitida parametrizados, uma antena genérica (com faixa de operação variando de 100 k – 1,8 GHz) do tipo monopolo é conectada à saída do SDR. O aplicativo “GPS Data” instalado em um *smartphone* Samsung Galaxy Note 10+ é utilizado para

verificar a quantidade de sinais de satélites transmitindo na frequência L1 do GPS. Baseado na referência teórica mencionada no capítulo 2 deste trabalho, são necessários pelo menos quatro sinais estáveis de satélite para definir a posição de um dispositivo receptor. A efetividade do bloqueador de sinais com diferentes ganhos e formatos de onda será considerada a partir da antena até a distância onde for possível registrar o sinal estável de quatro satélites. É possível comparar, desse modo, a relação da potência transmitida combinada ao formato de onda do sinal para causar interferência nos dispositivos receptores.

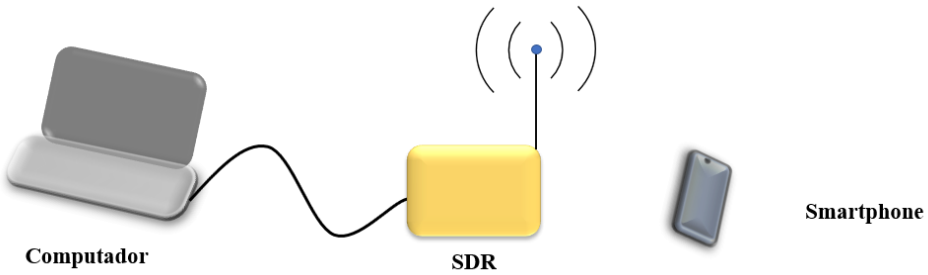
A figura 3.1 ilustra o esquema de montagem para a parametrização dos valores de potência transmitidas pelo SDR e a figura 3.2 ilustra o *setup* de como são feitos os testes.

Figura 3.1 – Esquema para a coleta dos dados de potência do SDR



Fonte: O autor

Figura 3.2 – Esquema de montagem para coleta dos dados em campo



Fonte: O autor

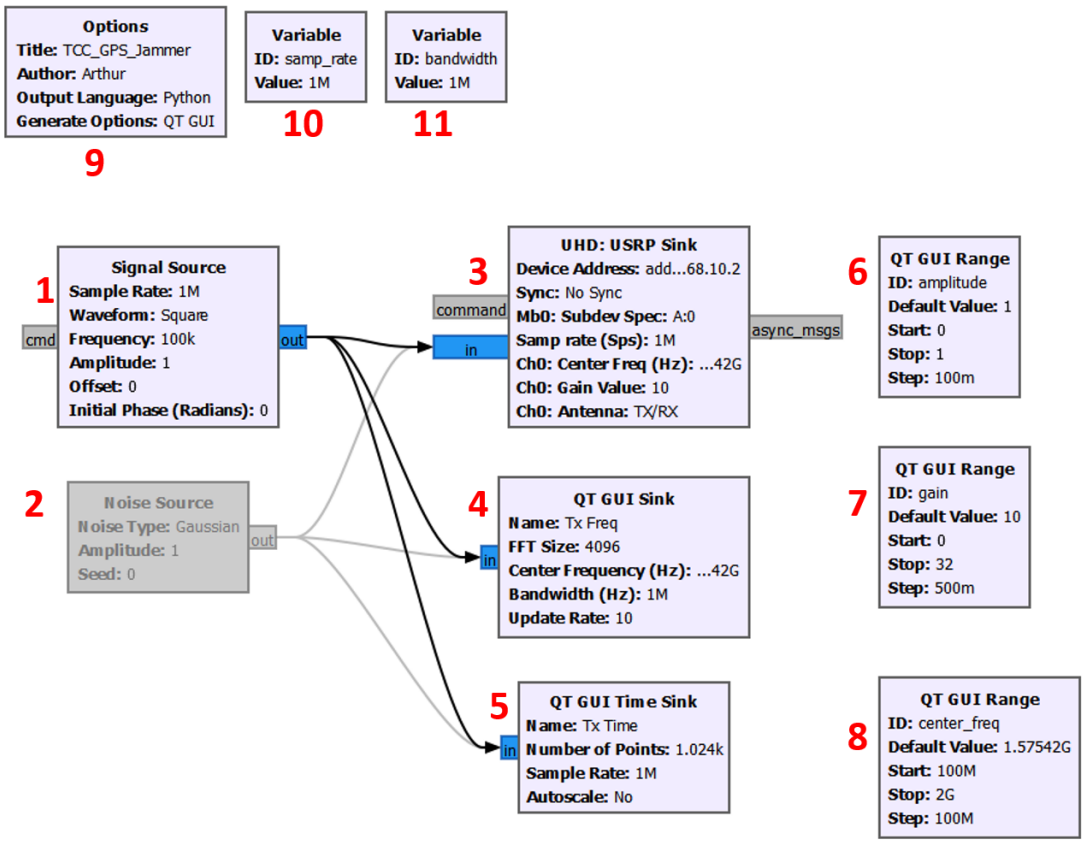
A partir dos resultados coletados, é iniciado o estudo da efetividade desse modelo de esquema para interferir nos sinais reais de GNSS, levantar e coletar dados em diferentes aparelhos e assim elaborar as conclusões.

CAPÍTULO 4

4.1 RESULTADOS

A primeira etapa consiste no projeto do sistema dentro do GNU Radio. A figura 4.1 apresenta o diagrama de blocos, sendo os principais o bloco 1 "*Signal Source*" e o 2 "*Noise Source*" responsáveis por gerar sinais com diferentes formatos de onda e o bloco 3, "*UHD:USRP Sink*", que fará a conexão com o SDR. As definições de conexão e parâmetros de funcionamento do SDR estão contidas no bloco 3. Os blocos 4 e 5 apresentam os resultados da transmissão de forma gráfica, sendo o 4 no domínio do tempo e o 5 no domínio da frequência. Os blocos 6,7 e 8 adicionam uma barra de seleção variável ao projeto, permitindo a alteração durante a execução da amplitude, do ganho e da frequência central, respectivamente.

Figura 4.1 – Montagem dos blocos dentro do GNU Radio



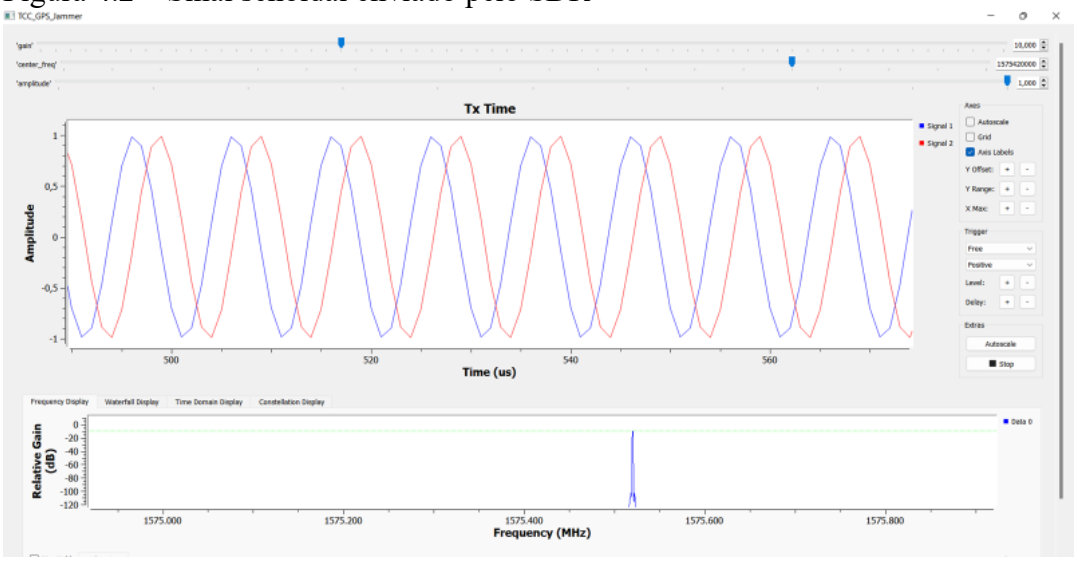
Fonte: O autor

Os testes foram feitos um de cada vez com quatro formas de sinais diferentes, sendo elas: senoidal, triangular, quadrada e ruído gaussiano. O bloco que gera o sinal com ruído ("*Noise Source*") é diferente do bloco que gera sinal com os demais formatos de onda ("*Signal*

Source"), por esse motivo apenas um deles fica ativo de cada vez. Não é possível transmitir diferentes formatos de onda simultaneamente.

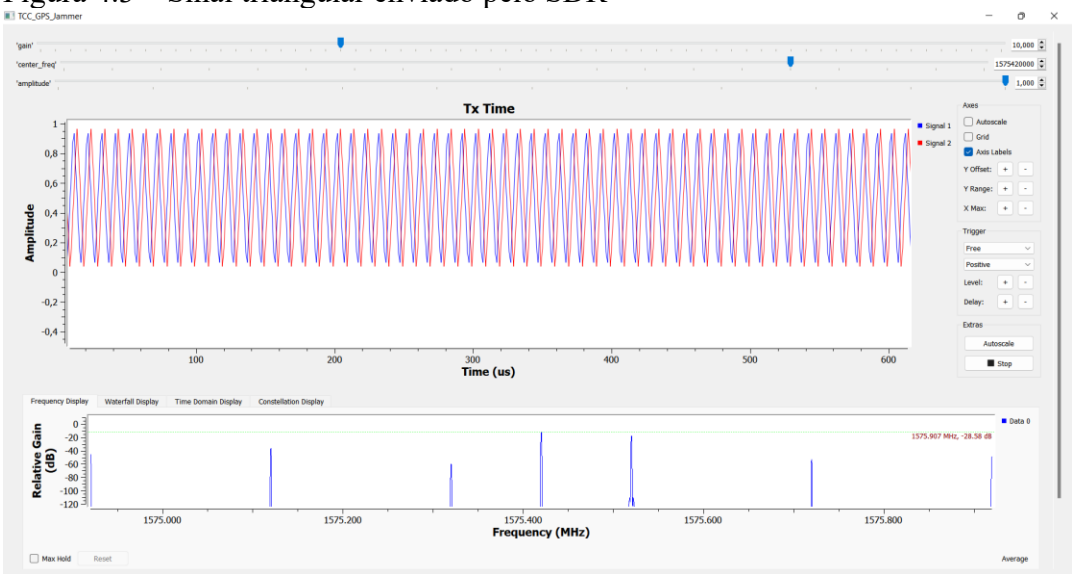
Nas figuras 4.2, 4.3, 4.4 e 4.5 são apresentados os sinais que foram enviados para o SDR sendo respectivamente o sinal senoidal, o triangular, o quadrado e o ruído gaussiano. Cada um dos sinais é apresentado tanto no domínio do tempo na parte superior, quanto no domínio da frequência na parte inferior.

Figura 4.2 – Sinal senoidal enviado pelo SDR



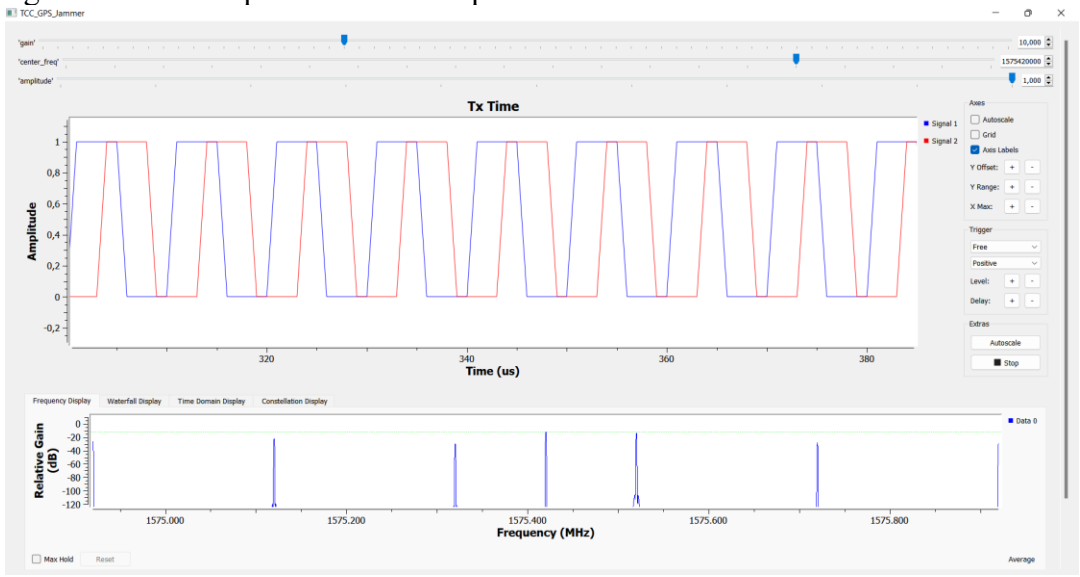
Fonte: O autor

Figura 4.3 – Sinal triangular enviado pelo SDR



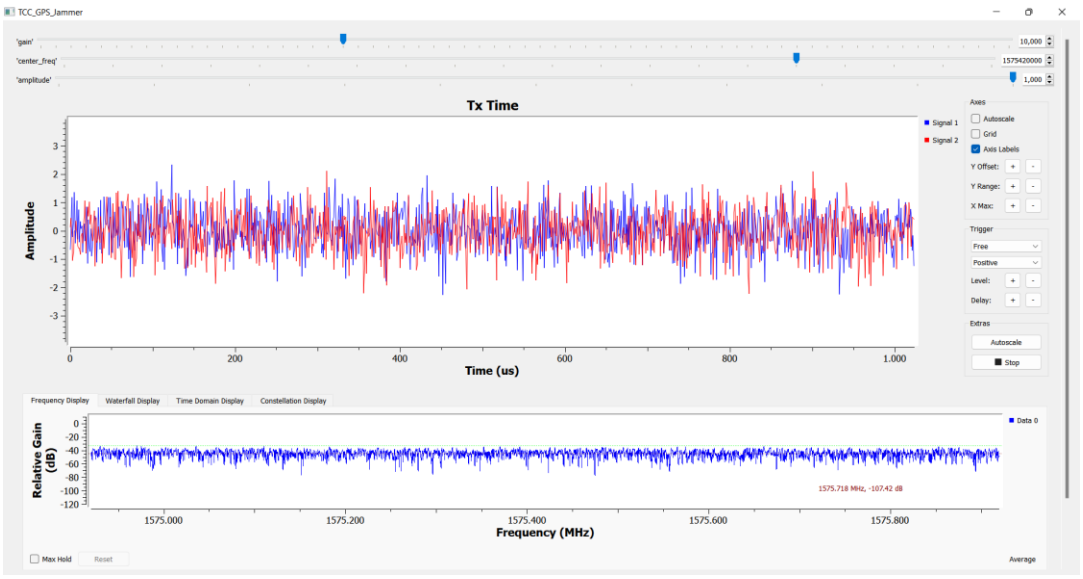
Fonte: O autor

Figura 4.4 – Sinal quadrado enviado pelo SDR



Fonte: O autor

Figura 4.5 – Ruído gaussiano enviado pelo SDR



Fonte: O autor

Após entender o funcionamento e especificidades de cada um dos equipamentos, montou-se o setup para a construção da tabela de relação do ganho com o formato de onda, de acordo com o proposto na metodologia. A figura 4.6 apresenta uma foto da montagem do setup com o power meter conectado diretamente à saída do SDR. O cabo usb que conecta o power meter ao computador não transmite dados, sendo usado apenas para manter a carga da bateria.

Figura 4.6 – Montagem do setup para definição do ganho.

Fonte: O autor

Como resultado obteve-se a tabela 4.1 com os valores medidos em dBm. Essa etapa caracteriza diretamente o sinal que é transmitido diretamente do SDR sem nenhum tipo de perda. O ganho absoluto de 32 dB é o máximo possível no SDR. De acordo com as especificações do fabricante, o power meter opera em uma faixa de potência entre -63 dBm e +20 dBm, estando todos os valores medidos nesse escopo. (NEWARK, 2023)

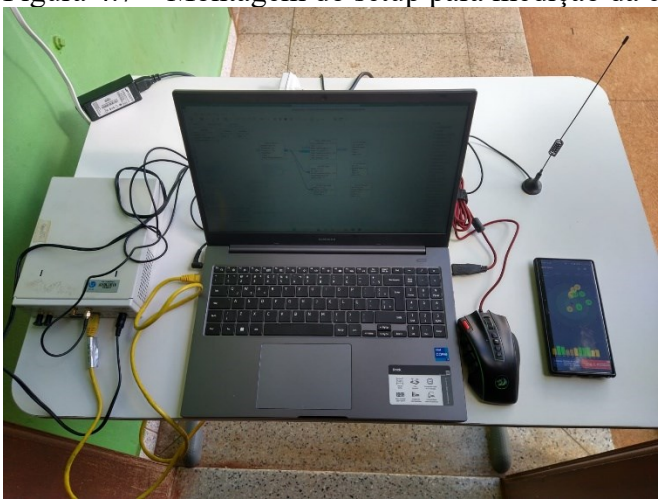
Tabela 4.1 – Potência (dBm) medida com o power meter conectado ao SDR

Ganho absoluto [dB]	Senóide [dBm]	Triangular[dBm]	Quadrada[dBm]	Ruído[dBm]
32	-34,52	-35,26	-36,47	-35,84
25	-36,34	-38,56	-38,8	-39,35
20	-43,75	-45,7	-45,55	-46,6
15	-49,8	-51,3	-51	-51,5
10	-53,5	-54	-53,7	-54

Fonte: o autor

A segunda etapa do consiste em substituir o power meter por uma antena e ir a um lugar aberto medir a efetividade do sinal de interferência, sendo um campo de futebol escolhido para esse fim. Na figura 4.7 é apresentada uma foto com a montagem do setup em campo com a antena conectada ao SDR e com o smartphone executando o aplicativo de leitura de sinais GNSS.

Figura 4.7 – Montagem do setup para medição da capacidade de interferência.



Fonte: O autor

As medidas foram realizadas na pista de atletismo da Universidade de Patos de Minas, contudo em dias e horários diferentes ocasionando situações climáticas distintas. Dia 25 de maio de 2023 às 10h foi realizada a primeira coleta de dados com o tempo ensolarado e sem nuvens. A figura 4.8 apresenta uma foto do local de medição no dia 01 de junho de 2023 às 7 h 30 min com intensa neblina.

Nessa situação de neblina intensa, com grande quantidade de gotículas de água no ambiente, os sinais vindos dos satélites L1 do GPS encontram muito mais dificuldade para chegar ao receptor. Gotículas de água possuem a capacidade de absorver, dispersar, distorcer e refletir sinais de rádio. Quanto mais densa a neblina, maior a atenuação do sinal. O sinal transmitido pelo SDR também será atenuado nessas condições, contudo a sua potência e proximidade são maiores se comparado aos sinais transmitidos pelos satélites. A relação de potência entre o sinal dos satélites e a do SDR nessa condição faz com que a interferência seja mais efetiva.

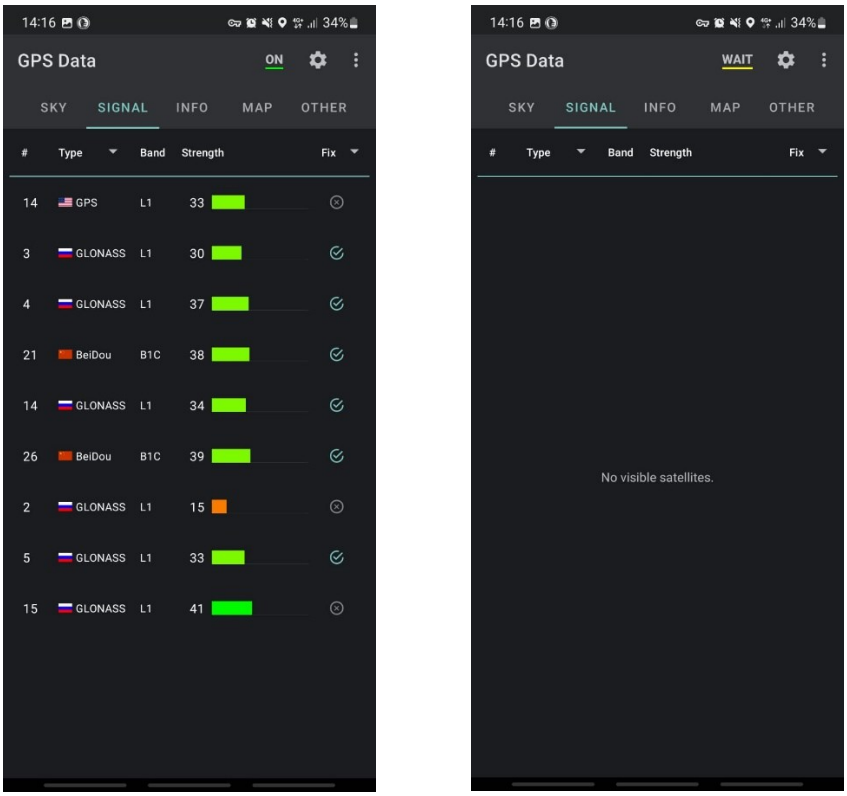
Figura 4.8 – Patos de Minas -MG sob intensa neblina dia 01/06/2023 às 7:30 AM.

Fonte: O autor

Entre cada uma das medições (ou seja, mantendo-se a forma de onda e alterando-se a potência de transmissão do sinal interferente) o aplicativo do telefone foi encerrado e a memória limpa. Esse processo foi necessário para garantir que os dados residuais de uma medição não interferissem nas seguintes.

Como apresentado na figura 4.9 (a) o aplicativo "GPS Data" mostra uma lista das constelações satélites captados naquele local, bem como se o sinal está estável e válido (lado direito) para ser utilizado. Na figura 4.9 (b) é mostrado um *print* da tela do smartphone ao iniciar a transmissão do sinal de interferência no SDR com o telefone ao lado da antena. Com o receptor ao lado da antena ocorre interferência em todos os sinais e a mensagem "*No visible satellites*" é apresentada, indicando que o bloqueador de sinais está funcionando.

Figura 4.9 – Lista dos satélites no aplicativo GPS Data, com o celular posicionado ao lado da antena transmissora do SDR. (a) situação com o SDR desligado e (b) com o SDR ligado, transmitindo o sinal interferente.



(a) (b)

Fonte: O autor

De acordo com o mencionado na metodologia, o receptor deve ser afastado do transmissor até que no aplicativo seja possível identificar a leitura adequada de quatro sinais de satélites. Lembrando que são necessários os sinais de no mínimo quatro satélites para se definir a posição de um receptor.

Variando os formatos de onda e os ganhos em cada uma delas, as distâncias encontradas, são as apresentadas na tabela 6.2 e 6.3:

Tabela 4.2 – Distâncias (metros) variando forma de onda e ganho em um dia ensolarado.

Ganho absoluto [dB]	Senóide [m]	Triangular [m]	Quadrada [m]	Ruído [m]
32	11,04	10,3	9,65	6,1
20	9,86	6,3	6	3,2

Fonte: o autor

Tabela 4.3 – Distâncias (metros) variando forma de onda e ganho em um dia nublado.

Ganho absoluto [dB]	Senóide [m]	Triangular [m]	Quadrada [m]	Ruído [m]
32	89,6 *	89,6	30,3	14,5
15	42,2	38	15	14,3
10	12,2	8,7	7	7

Fonte: o autor

* No dia nublado, com o ganho absoluto em 32 dB e com a forma de onda senoidal o sinal transmitido pelo SDR foi efetivo para impedir a correta leitura dos sinais verdadeiros de 4 satélites para além do espaço disponível para medição.

4.2 DISCUSSÃO

O GNU Radio é muito útil e prático pois permite configurar os parâmetros de transmissão no SDR de forma gráfica por meio de blocos, tornando o processo mais simples, facilitando a análise do projeto e possíveis correções de erros. Por ser desenvolvido para o sistema operacional Linux, possui algumas etapas a mais de instalação para computadores Windows, contudo nada que limite o seu funcionamento ou recursos. Também permite a programação utilizando linhas de código e a conversão de blocos em código.

O primeiro setup utilizando o *power meter* no lugar da antena foi necessário para que o sinal fosse caracterizado diretamente na sua fonte, ou seja, para que fosse possível determinar exatamente quanto de potência estava sendo transmitida levando em consideração apenas o ganho e a forma de onda. Desse modo é possível desconsiderar as características da antena utilizada, pois ela não foi projetada para operar exclusivamente na frequência estudada nesse trabalho.

Mesmo considerando a variação causada pelo clima, é possível observar que existe uma tendência e uma correlação entre a potência medida com o *power meter* e a efetividade do bloqueador de sinal. Em todos os casos o sinal de interferência com formato senoidal foi o que apresentou melhor efetividade, ou seja, mantidas as condições e variando apenas o formato de onda, a senóide proporcionou o maior alcance. Existe uma relação direta entre a potência apresentada no *power meter* e a efetividade do formato de onda.

Apesar dos resultados obtidos nesse estudo, a forma de onda senoidal transmitida por um bloqueador de sinais pode apresentar desvantagem quando deseja-se interferir em outro sinal. Isso ocorre em sistemas *antijamming* que fazem a verificação do sinal recebido e filtram os sinais nas frequências que estejam causando interferências. O sinal senoidal, por apresentar uma densidade espectral de potência em torno de apenas uma frequência, seria mais facilmente detectado e filtrado. Contudo, nesse caso os dispositivos receptores de GPS não possuem esse sistema. (B.P. LATHI; GREEN, 2006)

4.3 CONCLUSÃO

Os sinais senoidais são mais adequados para bloquear os sinais de GPS do que o triangular, quadrado ou ruído gaussiano devido à sua quantidade de harmônicos (a qual impacta diretamente na densidade espectral de potência deste sinal). Como a energia de um sinal senoidal está concentrada em uma única frequência, toda a potência de interferência é direcionada para a frequência do sistema GPS, afetando a recepção em dispositivos receptores próximos. Além disso, a regularidade temporal do sinal senoidal facilita a transmissão contínua e evita de forma mais eficaz que o receptor receba o sinal GPS verdadeiro com precisão.

Outra vantagem das ondas senoidais é que elas são fáceis de gerar e manipular. Essa facilidade é importante para ajustar o sinal de interferência às características específicas do sistema GPS, maximizando sua eficácia. Além disso, as ondas senoidais são mais eficientes em termos de propagação. Essa eficiência de propagação aumenta a probabilidade de um sinal de interferência senoidal atingir um receptor GPS com potência considerável e interferir na recepção precisa do sinal GPS.

REFERÊNCIAS

B.P. LATHI; GREEN, R. **Sinais e Sistemas Lineares**. 2. ed. [s.l: s.n.].

DAILY MAIL REPORTER. **U.S. students fake GPS signal and take control of an $80million 213-foot superyacht in the Mediterranean**. Disponível em: <https://www.dailymail.co.uk/news/article-2381160/University-Texas-students-fake-GPS-signal-control-80m-213-foot-superyacht.html>. Acesso em: 4 jan. 2023.

EL-RABBANY, A. **Introduction to GPS - The Global Positioning System**. Boston: ARTECH HOUSE, INC, 2002.

GNU RADIO PROJECT. **About GNU Radio**. Disponível em: <https://www.gnuradio.org/about/>. Acesso em: 4 jun. 2023.

HUGHES, K. K. **Hacking GPS**. Indianapolis: Wiley Publishing, Inc., 2005.

IAN POOLE. **Bit Error Rate Testing**. Disponível em: <https://www.electronics-notes.com/articles/radio/bit-error-rate-ber/testing-bert.php>. Acesso em: 10 jul. 2023.

KAPLAN, E. D.; HEGARTY, C. J. **Understanding GPS/GNSS - Principles and Applications**. Third Edition ed. Boston: [s.n.].

MONICO, J. F. G. **Posicionamento Pelo Gnss - Descrição, fundamentos e aplicações**. [s.l.] Unesp, 2008.

NEWARK. **V3500A RF Power Meter**.

OPPENHEIM, A. V.; WILLSKY, A. S. **Sinais e Sistemas**. 2nd. ed. [s.l: s.n.].

ROUPHAEL, T. J. **RF and Digital Signal Processing for Software-Defined Radio: A Multi-Standard Multi-Mode Approach**. [s.l: s.n.].