Universidade do Minho
Escola de Engenharia

Universidade do Minho

Mestrado em Engenharia Eletrónica Industrial e de Computadores

Projeto Integrador em Eletrónica Industrial e Computadores

Sistema de Spoofing para GPS Baseado em SDR

Tiago da Silva Matos – PG56204

Professores: Paulo Mateus Mendes

Hugo Daniel Costa Dinis

Resumo

Este documento descreve o desenvolvimento de um sistema de *spoofing* para GPS utilizando um rádio definido por software (SDR), cujo principal objetivo é demonstrar a vulnerabilidade dos sistemas de posicionamento global através da transmissão de sinais GPS simulados. O projeto foi implementado em GNU Radio, onde se desenvolveu o algoritmo responsável pela geração e manipulação dos sinais GPS, incluindo a configuração dos parâmetros de transmissão e a simulação de trajetórias fictícias. Após esta fase, foram realizadas simulações para validar a coerência dos sinais gerados e a sua capacidade de influenciar dispositivos recetores. Por fim, o sistema foi testado num ambiente controlado para avaliar o impacto do *spoofing* em dispositivos GPS reais.

Para a transmissão dos sinais simulados, utilizou-se um módulo SDR HackRF One, capaz de transmitir na banda de frequências utilizada pelos satélites GPS. Os sinais foram gerados a partir do software GPS-SDR-SIM, que permitiu a definição de coordenadas arbitrárias e a criação de cenários de *spoofing* controlados. Os sinais transmitidos foram então captados por um dispositivo GPS alvo, que interpretou as informações sintetizadas como legítimas, alterando assim a sua posição percebida.

O processo de desenvolvimento foi dividido em etapas, começando pela configuração e testes no GNU Radio, onde os parâmetros do sinal foram ajustados para garantir a fidelidade da transmissão. Em seguida, foram realizadas simulações para avaliar a robustez dos sinais gerados e a sua capacidade de interferir com sistemas GPS. A fase final consistiu na transmissão dos sinais num ambiente experimental controlado, garantindo a segurança dos testes e evitando interferências indesejadas em sistemas externos.

Ao longo deste documento, são detalhadas as diferentes fases do desenvolvimento, desde as validações iniciais em software até à implementação final com hardware SDR. Também são discutidos os desafios enfrentados, como a precisão na geração dos sinais GPS e a mitigação de interferências, bem como as soluções adotadas para garantir um sistema funcional e seguro.

Palavras-chave: Rádios definidos por software, HackRF One, GPS, spoofing, jamming.

Conteúdo

Lista de Figuras

Lista de Tabelas

1 Introdução

Neste primeiro capítulo, será apresentado o âmbito e a motivação que levaram ao desenvolvimento do presente projeto, assim como os objetivos que se pretendem atingir.

1.1 Motivação

No âmbito da Unidade Curricular de Projeto Integrador em Eletrónica Industrial e Computadores, foi proposto que os alunos se organizassem em grupos de 1 ou 2 elemento(s) para desenvolverem um projeto à sua escolha, previamente proposto por vários docentes.

Os sistemas de GPS são amplamente utilizados há vários anos em diversas aplicações, e desempenham um papel fundamental na navegação e localização precisa de veículos, como automóveis e drones. Com o aumento da dependência destes sistemas, a sua segurança torna-se cada vez mais um fator crítico, especialmente face à disponibilidade de tecnologias de baixo custo para radiofrequência. Entre essas tecnologias, destacam-se os rádios definidos por software (SDR), que permitem a manipulação de sinais de radiofrequência de forma flexível e acessível.

Esta evolução tecnológica abre caminho para possíveis ameaças, como o *spoofing*, que consiste no envio de informações sintetizadas para enganar os sistemas de posicionamento, e o *jamming*, que interfere na receção dos sinais, comprometendo a fiabilidade da localização. Assim, torna-se essencial compreender e explorar estas vulnerabilidades, não apenas para demonstrar os riscos inerentes, mas também para desenvolver soluções que reforcem a resiliência dos sistemas GPS contra ataques desta natureza.

1.2 Objetivos

O principal objetivo deste trabalho foi desenvolver um sistema de *spoofing* para GPS baseado em SDR. Com este projeto, pretende-se testar a segurança e explorar as vulnerabilidades associadas aos sistemas de posicionamento global, permitindo compreender em profundidade o funcionamento do GPS, bem como as ameaças que este enfrenta. Além disso, pretende-se desenvolver competências práticas na utilização de SDR para gerar e manipular sinais de navegação, demonstrando o impacto de ataques de *spoofing* e *jamming* em ambientes controlados.

2 Enquadramento Teórico

Neste capítulo, apresentam-se os conceitos teóricos que fundamentam o projeto. É descrito o funcionamento dos sistemas GPS e as suas principais vulnerabilidades, como os ataques de *spoofing* e jamming. Aborda-se também a tecnologia SDR, essencial pela sua flexibilidade na manipulação de sinais. Por fim, reforça-se a importância de realizar os testes em ambiente controlado e de acordo com a legislação aplicável.

2.1 Sistemas de Posicionamento Global (GPS)

O Sistema de Posicionamento Global, o famoso GPS, é um sistema de navegação via satélite que nasceu no Departamento de Defesa dos EUA, mas que hoje está acessível para todos. Ele faz parte dos chamados GNSS (*Global Navigation Satellite Systems*), que englobam outras redes mundiais, como o GLONASS da Rússia, o Galileo da União Europeia e o BeiDou da China.

O funcionamento do GPS baseia-se numa constelação de, pelo menos, 24 satélites ativos em órbita terrestre. Estes satélites transmitem continuamente sinais de rádio, que são captados por recetores GPS. Através da trilateração de sinais provenientes de, no mínimo, três satélites, o recetor consegue determinar a sua posição tridimensional – latitude, longitude e altitude – com elevada precisão.

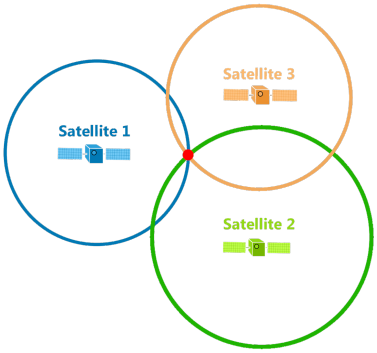


Figura 1: Princípio de trilateração na determinação da posição por satélites GPS.

Os sinais do GPS contêm códigos especiais, os chamados códigos de pseudo-ruído (*Pseudo Random Noise*, PRN), que ajudam a identificar e sincronizar os satélites. Os dois códigos principais originais são:

- **C/A (Coarse/Acquisition)**: usado no dia a dia, permitindo que os aparelhos GPS comuns captem e acompanhem os sinais GPS. É um código PRN de 1.023 bits que se repete a cada milésimo de segundo e é transmitido a 1,023 Mbit/s na banda L1.
- **P(Y) (Precision)**: exclusivo para fins militares e oferece uma precisão maior em comparação com o C/A. O código P pode ser encriptado, transformando-se no código Y, e então transmitido a 10,23 Mbit/s, nas bandas L1 e L2.

A utilização de códigos diferentes para cada satélite, através da técnica de *Code Division Multiple Access* (CDMA), permite que vários sinais sejam enviados na mesma frequência sem que um atrapalhe o outro. Cada código PRN é único, o que permite que o aparelho identifique os satélites, num processo chamado *Direct Sequence Spread Spectrum* (DSSS). Isso também aumenta a proteção contra interferências de rádio frequência.

Banda	Frequência (MHz)	Código	Modulação	Utilização
L1	1575,42	C/A, P(Y)	BPSK	Navegação civil e militar
L2	1227,60	P(Y)	BPSK	Navegação militar precisa
L5	1176,45	L5I	BPSK	Serviços de segurança de aviação

Tabela 1: Diferentes frequências dos sinais GPS.

O sinal C/A na banda L1 usa modulação BPSK (*Binary Phase Shift Keying*), enquanto o P(Y) também usa BPSK, mas é transmitido em quadratura com o sinal C/A, ou seja, com um desfasamento de 90°, permitindo que os sinais se misturem sem interferência direta.

Além do código PRN, cada sinal carrega uma mensagem de navegação que contém informações importantes para calcular a posição e sincronização. Essa mensagem é transmitida a 50 bit/s e inclui:

- **Subtrama 1:** dados sobre o estado do satélite, data e hora GPS;
- **Subtramas 2 e 3:** dados de efemérides;
- **Subtrama 4:** informações sobre a ionosfera, almanaque e estado de saúde dos satélites com PRN de 25 a 32, tempo UTC;
- **Subtrama 5:** informações sobre o almanaque e o estado de saúde dos satélites com PRN de 1 a 24

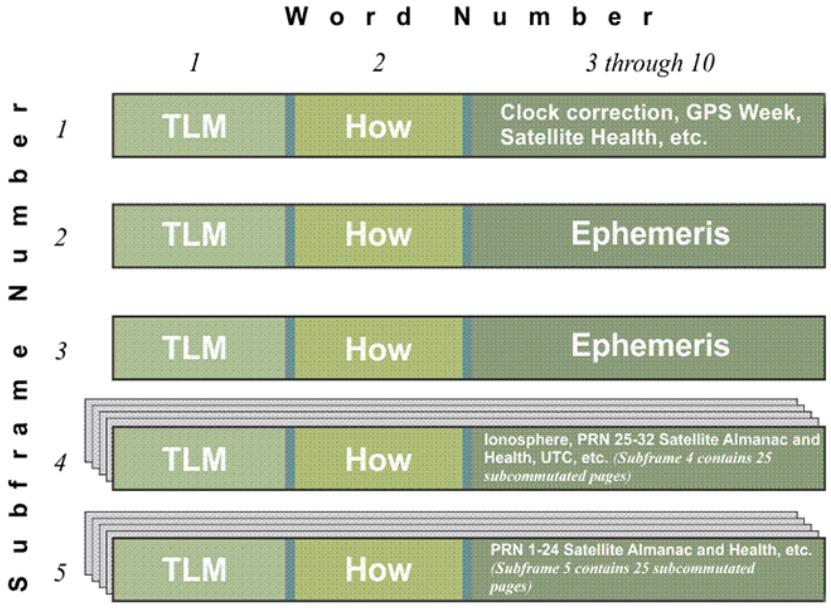


Figura 2: Diagrama da estrutura da mensagem de navegação.

O GPS tornou-se uma ferramenta omnipresente, marcando presença em áreas diversas como a orientação de carros e aviões, a gestão precisa de equipamentos agrícolas, a organização temporal de redes de comunicação e até em atividades das forças armadas.

Apesar de sua importância vital para muitas áreas, o GPS, assim como outros sistemas GNSS, sofre de fragilidades consideráveis. A facilidade com que pode ser enganado por ataques de *spoofing* ou bloqueado por *jamming* mostra a urgência de se pesquisar e criar formas de defender e fortalecer esses sistemas.

2.2 Vulnerabilidades dos Sistemas GPS: Spoofing e Jamming

O *spoofing* e o *jamming* são duas abordagens distintas de interferência nos sinais GPS, que diferem na forma como interferem com os sinais de navegação.

No *jamming*, é emitida uma interferência, que é um sinal de elevada potência sem informação nenhuma, na mesma banda de frequência dos sinais GPS, de forma a saturar o ambiente de comunicação. Esta interferência impede que o recetor consiga captar os sinais legítimos dos satélites, o que leva à perda da capacidade de calcular uma posição ou a atualizar a informação de tempo. Em termos teóricos, o *jamming* bloqueia a receção sem fornecer dados alternativos.

Por outro lado, o *spoofing* consiste na transmissão de sinais simulados que imitam os sinais GPS reais. Nesta abordagem, geram-se sinais com os mesmos formatos e características dos sinais autênticos, mas com informações deliberadamente alteradas, em vez de apenas interromper a receção dos sinais, como no *jamming*. Assim, o recetor é enganado e passa a calcular uma posição ou tempo incorreto. Do ponto de vista teórico, o *spoofing* é um ataque mais sofisticado que requer uma emulação precisa dos sinais de navegação, de modo a fazer com que os sinais simulados sejam interpretados como legítimos pelo recetor.

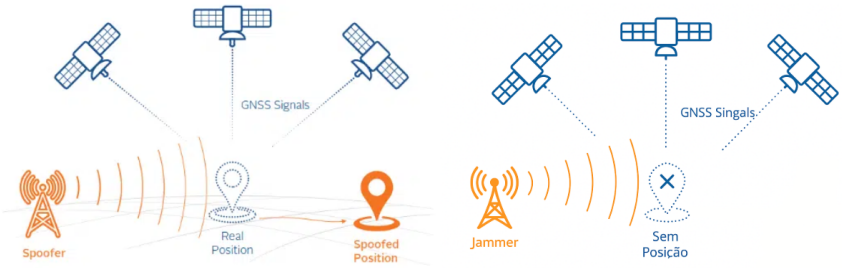


Figura 3: Ilustração dos métodos de spoofing e jamming.

Em conclusão, apesar de ambos os métodos afetarem os sistemas GPS, os seus impactos e técnicas de mitigação são diferentes. Enquanto o *jamming* leva à indisponibilidade do sinal, o *spoofing* pode permitir o controlo ou manipulação das informações de localização e tempo, o que tem implicações sérias em aplicações como a navegação autónoma e sistemas de segurança.

2.3 Rádios Definidos por Software (SDR)

Os rádios definidos por software (SDR – *Software Defined Radio*) constituem hoje um dos paradigmas mais inovadores nas telecomunicações, ao transferir para o domínio do software funções tradicionalmente implementadas em hardware, tais como *mixers*, filtros, moduladores e desmoduladores. Este paradigma permite que um único dispositivo seja capaz de operar em vários protocolos de comunicação através da simples atualização de software, eliminando a necessidade de modificações físicas nos componentes.

A arquitetura típica de um sistema SDR, apresentada na figura 4 inclui um *front-end* de radiofrequência, composto por uma antena, filtros passa-banda e amplificador de baixo ruído (LNA), que prepara o sinal recebido antes da conversão de analógico para digital. Esta conversão consiste numa amostragem do sinal em banda-base ou numa frequência intermédia e o transforma em fluxo de dados digitais. Posteriormente, é efetuado um processamento digital do sinal, numa unidade central de processamento, que implementa algoritmos de filtragem, desmodulação e descodificação. Para a transmissão, o processo é invertido, utilizando conversores digital-analógico e amplificadores de potência.

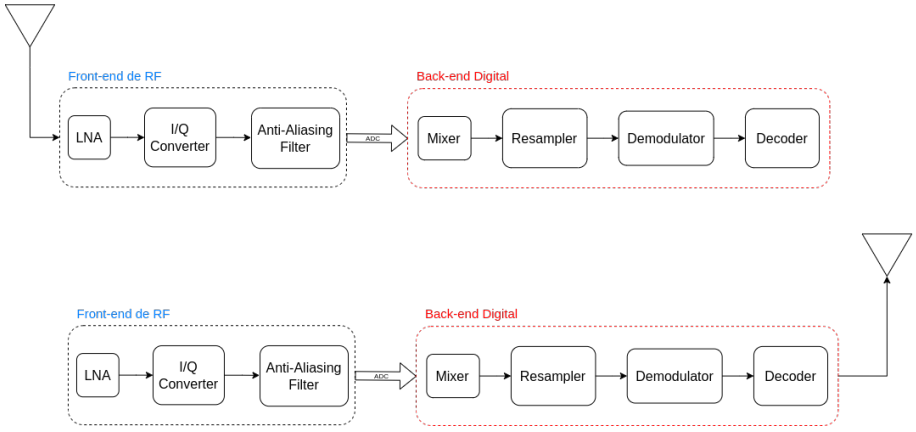


Figura 4: Arquitetura típica de um Rádio Definido por Software.

Das principais vantagens dos SDRs destacam-se a flexibilidade, uma vez que estes permitem a adaptação rápida a novos padrões de comunicação, devido à eliminação da necessidade de hardware específico para cada aplicação e a capacidade de se reconfigurar em tempo real, possibilitando alterações nos parâmetros de transmissão, como frequência e largura de banda.

As suas aplicações são vastas, abrangendo desde o sector militar e defesa até às comunicações civis. Além disso, os SDRs são amplamente utilizados em ambientes de investigação, facilitando o desenvolvimento e teste de novos algoritmos de comunicação.

Em suma, os SDRs representam uma mudança de paradigma ao deslocar a maior parte da complexidade do hardware para o software, promovendo evolução contínua, adaptabilidade e maior eficiência na utilização do espectro, que são fatores cruciais para enfrentar os desafios das redes de comunicação do futuro.

2.4 Ambiente Controlado e Respeitar Regulamentação Legal

A realização de testes com sinais GPS simulados exigiu um cuidado rigoroso na definição do ambiente de ensaio, de forma a garantir o cumprimento das regulamentações legais vigentes. A utilização de sinais GPS sintetizados, mesmo em ambientes de teste, pode interferir com sistemas de navegação reais, colocando em risco a segurança de equipamentos e utilizadores. Assim, foi imprescindível que os testes fossem conduzidos em ambientes totalmente controlados e isolados do exterior, como, neste caso, uma câmara anecoica.

Figura 5: Câmara Anecoica.

Para além do controlo físico do ambiente, foi essencial respeitar a legislação nacional e internacional que regula a emissão de sinais de navegação por satélite. Em muitos países, a transmissão de sinais GPS simulados é estritamente proibida sem autorização prévia das autoridades competentes. Desta forma, qualquer atividade de emulação de sinais deve ser precedida de uma análise rigorosa das obrigações legais e, se necessário, da obtenção de licenças específicas para a realização dos ensaios.

O respeito pelo ambiente controlado e pela regulamentação legal não só assegurou a conformidade com as normas em vigor, como também protegeu a integridade dos resultados obtidos nos testes. A criação de condições seguras e regulamentadas foi um requisito fundamental para a validação científica e tecnológica de soluções de navegação baseadas em sinais GPS simulados.

3 Metodologia

Neste capítulo, apresenta-se a metodologia seguida para o desenvolvimento do sistema de *spoofing* GPS. São descritas as principais ferramentas utilizadas, como o HackRF One, GNU Radio e GPS-SDR-SIM. Também se explica o processo de geração de sinais GPS realistas, incluindo a criação de localizações arbitrárias e a manipulação de ficheiros binários. Segue-se a implementação do sistema em GNU Radio e, por fim, o desenvolvimento da interface gráfica, destacando as tecnologias empregues e as funcionalidades implementadas para facilitar a utilização do sistema.

3.1 Análise do Problema e Arquitetura do Sistema

O desafio central deste projeto consistiu em desenvolver um sistema capaz de simular sinais GPS de forma controlada e realista, com o objetivo de induzir localizações sintetizadas em dispositivos recetores. Esta problemática insere-se no contexto das vulnerabilidades de sistemas de navegação por satélite, nomeadamente ataques de *spoofing*, cuja eficácia depende da fidelidade dos sinais gerados e da capacidade de controlo sobre a emissão.

A arquitetura do sistema foi desenhada com os seguintes objetivos fundamentais:

- Permitir a geração de sinais GPS artificiais com coordenadas arbitrárias;
- Controlar a emissão dos sinais em ambiente local, sem interferência com sistemas reais;
- Assegurar compatibilidade com recetores comerciais (e.g., telemóveis);
- Implementar uma solução modular e reconfigurável;
- Facilitar a integração com uma interface gráfica de controlo.

O processo de geração e emissão dos sinais GPS inicia-se no computador, onde o GPS-SDR-SIM cria um ficheiro binário correspondente a uma localização arbitrária. Esse ficheiro é transmitido via GNU Radio, que modula e prepara o sinal digital. O HackRF One converte esse sinal em um de radiofrequência e emite-o por uma antena. Um recetor GPS, como um telemóvel com a aplicação GPS Test App, interpreta os sinais como válidos e assume a localização simulada como verdadeira.

A figura 6 ilustra a arquitetura modular do sistema desenvolvido:

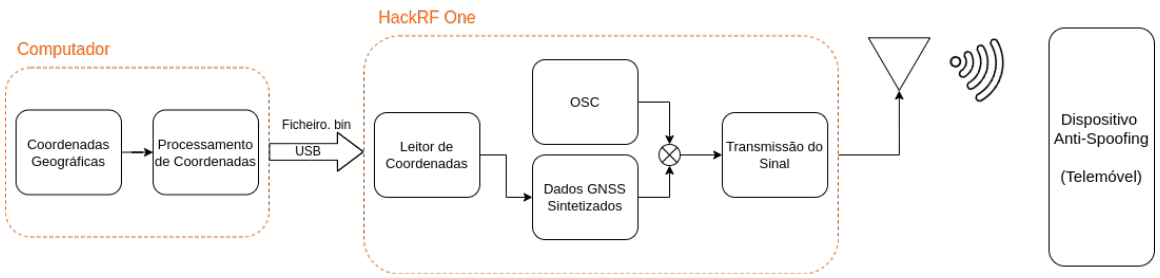


Figura 6: Diagrama de blocos do sistema.

- **Coordenadas Geográficas:** Definição das coordenadas geográficas em latitude, longitude e altitude;
- **Processamento de Coordenadas:** Conversão de coordenadas para parâmetros orbitais e temporais;
- **Leitor de Coordenadas:** Interface de leitura dos dados de entrada (ficheiro binário);
- **Dados GNSS Sintetizados:** Geração de mensagens de navegação GPS sintetizadas;
- **Oscilador:** Contêm uma portadora, que oscila à frequência dos sinais GPS, que posteriormente é combinada com os dados GPS simulados;
- **Transmissão do Sinal:** Modulação e emissão dos sinais GNSS através de um SDR;
- **Antena:** Responsável por emitir o sinal GPS sintetizado. Deve estar corretamente posicionada e isolada de equipamentos externos, por motivos legais e técnicos.
- **Dispositivo Recetor (Telemóvel):** Recetor de sinais GNSS que, ao captar o sinal simulado, determina uma localização baseada na informação sintetizada recebida.

Esta arquitetura permitiu alcançar um elevado grau de controlo sobre o processo de *spoofing*, constituindo uma base sólida para os testes experimentais descritos nas secções seguintes.

3.2 Ferramentas Utilizadas

Para implementar o sistema de emulação e análise de sinais GPS, foi utilizado um conjunto de ferramentas, tanto de *hardware*, como de *software*, que garantem a geração, manipulação, transmissão e receção dos sinais de forma controlada. Esta secção descreve os principais componentes, dos quais são: o HackRF One, utilizado para emitir os sinais; o GNU Radio Companion, para construção dos fluxos de sinal; o GPS-SDR-SIM, responsável pela geração dos ficheiros de simulação; e a aplicação GPS Test App, usada para monitorizar e validar a receção dos sinais. Cada ferramenta desempenha um papel crucial na eficácia do sistema de *spoofing*.

3.2.1 HackRF One

O HackRF One é um transcetor de rádio definido por software de banda larga, concebido para aplicações de investigação, desenvolvimento e testes em sistemas de comunicações sem fios. Desenvolvido pela Great Scott Gadgets, o HackRF One destaca-se pela sua versatilidade e custo reduzido, o que o torna numa ferramenta amplamente utilizada tanto em ambientes académicos como profissionais.

Figura 7: Radio Definido por Software HackRF One.

Este dispositivo opera na gama de frequências que vai aproximadamente de 1 MHz a 6 GHz, cobrindo assim uma vasta variedade de bandas utilizadas em comunicações comerciais, científicas, militares e amadoras. Esta ampla cobertura de espectro junto à capacidade de transmissão e receção, permite a realização de experiências em diversas áreas das telecomunicações sem a necessidade de múltiplos equipamentos especializados.

A arquitetura do HackRF One segue os princípios de um SDR típico, sendo composto por um front-end de radiofrequência, conversores de analógico para digital e também de digital para analógico, bem como um microcontrolador integrado responsável pela interface com o computador anfitrião. O processamento de sinal é feito pelo computador, onde ferramentas como GNU Radio Companion podem ser utilizadas para desenhar e executar sistemas de comunicação personalizados.

Caraterística	**Valor/Descrição**
Gama de Frequências	1 MHz a 6 GHz
Capacidade de Operação	Transcetor half-duplex
Taxa de Amostragem	Até 20 milhões de amostras por segundo (20 Msps)
Formato das Amostras	Amostras em quadratura de 8 bits (8-bit I e 8-bit Q)
Compatibilidade de software	Compatível com GNU Radio, SDR# e outras ferramentas SDR
Ganhos e filtros configuráveis por software	Controlo via software do ganho de receção/transmissão e do filtro banda-base
Alimentação da porta de antena	Alimentação controlada por software (50 mA a 3.3 V)
Conetores SMA	Conetores SMA fêmea para antena e para entrada/saída de clock
Sincronização externa	Entrada e saída de clock para sincronização entre dispositivos
Interface de comunicação	USB 2.0 (alta velocidade)
Alimentação	Alimentado via USB
Expansibilidade	Conectores de pinos internos para expansão
Tipo de hardware	Hardware open source

Tabela 2: Tabela com as especificações técnicas principais do HackRF One.

Entre as principais capacidades do HackRF One, apresentadas na tabela 2, destaca-se ainda a possibilidade de modulação e desmodulação de múltiplos tipos de sinais, bem como o suporte a clock externo, uma funcionalidade essencial em aplicações que exijam maior rigor temporal ou sincronização entre dispositivos.

A simplicidade da arquitetura e a disponibilidade de *firmware open-source* incentivam a personalização e extensão das capacidades do HackRF One, o que o torna especialmente atrativo para projetos de investigação em segurança de radiofrequência, prototipagem de novos protocolos de comunicação e demonstrações educativas.

Contudo, apesar das suas potencialidades, o HackRF One também apresenta limitações, nomeadamente na potência de transmissão, que é relativamente baixa, e na necessidade de filtros externos para mitigar sinais indesejados em algumas aplicações críticas.

Em conclusão, o HackRF One constitui uma plataforma acessível e poderosa para a experimentação em rádio definido por software, proporcionando uma ponte entre o mundo académico e industrial, e promovendo a inovação em comunicações sem fios.

3.2.2 GNU Radio Companion

O GNU Radio Companion é um ambiente de desenvolvimento gráfico destinado à criação de fluxogramas para processamento digital de sinal. Este ambiente fornece uma interface visual intuitiva que permite testar e implementar sistemas de rádio definidos por software de forma eficiente e sem a necessidade de programação extensiva em linguagens de baixo nível.

Este funciona como uma ferramenta de alto nível que gera automaticamente o código Python correspondente ao fluxograma desenhado, permitindo assim a rápida implementação de sistemas de comunicações e outros tipos de aplicações de processamento de sinal. A biblioteca do GNU Radio disponibiliza uma vasta gama de blocos funcionais prontos a utilizar, incluindo filtros, moduladores, desmoduladores, codificadores e descodificadores para rádios definidos por software como o HackRF One.

Entre as principais características do GNU Radio Companion destaca-se a sua extensibilidade, permitindo aos utilizadores criar blocos personalizados em Python, ampliando assim as capacidades do sistema para necessidades específicas. O GNU Radio Companion também é compatível com múltiplas plataformas, incluindo Linux, Windows e macOS, e é distribuído sob licença open-source, fomentando a colaboração e a inovação na comunidade académica e industrial.

A sua flexibilidade e modularidade tornam-no ideal para aplicações de ensino de processamento de sinais digitais, desenvolvimento de novos protocolos de comunicação e análise de segurança em redes sem fios. Adicionalmente, este disponibiliza ferramentas de visualização, como analisadores de espectro e medições em tempo real, o que facilita o diagnóstico dos sistemas desenvolvidos.

Apesar das suas inúmeras vantagens, o GNU Radio Companion apresenta também desafios, nomeadamente a curva de aprendizagem inicial para utilizadores sem experiência em processamento de sinal e a necessidade de recursos computacionais relativamente elevados para executar aplicações complexas em tempo real.

Em conclusão, o GNU Radio Companion estabelece-se como uma ferramenta essencial no ecossistema de rádios definidos por software, combinando fatores como a facilidade de utilização com uma elevada capacidade de personalização. Assim, contribui de forma significativa para a evolução da investigação e inovação tecnológica em comunicações digitais.

3.2.3 GPS-SDR-SIM

O GPS-SDR-SIM é uma ferramenta de código aberto desenvolvida para gerar sinais GPS simulados, destinada a ambientes de teste e investigação em sistemas de navegação por satélite. Esta ferramenta permite a criação de ficheiros de amostras de sinais GPS, que podem posteriormente ser transmitidos utilizando rádios definidos por software. Desta forma, possibilita-se a avaliação de recetores GPS em cenários controlados, sem a necessidade de acesso a satélites reais.

Esta ferramenta funciona como um simulador de sinais GPS, responsável por gerar arquivos binários que contêm sequências de navegação, que incorporam parâmetros como coordenadas geográficas e efemérides de satélites. Esses arquivos são posteriormente transmitidos por dispositivos SDR, emulando a presença de satélites GPS reais.

Entre as suas principais características destaca-se a utilização simples e a capacidade de criar simulações realistas de receção de sinais GPS. Esta funcionalidade é especialmente útil para a investigação de técnicas de *spoofing* e para tecnologias de navegação.

Apesar de seu potencial, o GPS-SDR-SIM apresenta desafios significativos. A configuração requer conhecimento técnico em sistemas de navegação por satélite e familiaridade com SDR, além de demandar atenção a questões legais e éticas, já que a transmissão não autorizada de sinais GPS pode violar as regulamentações locais.

Concluindo, o GPS-SDR-SIM constitui uma ferramenta essencial para a investigação e desenvolvimento em sistemas de navegação por satélite, proporcionando uma plataforma acessível e poderosa para simulação e teste em ambientes controlados.

3.2.4 GPS Test App

O GPS Test App é uma aplicação móvel voltada para análise em tempo real do desempenho de receptores GPS integrados a smartphones. Desenvolvida para utilizadores técnicos e entusiastas, esta aplicação fornece uma interface gráfica intuitiva que apresenta em tempo real dados de posição e altitude, bem como informações detalhadas sobre os satélites visíveis e os sinais recebidos.

A aplicação é compatível com múltiplos sistemas GNSS, incluindo o GPS, GLONASS, Galileo e BeiDou. Esta permite visualizar parâmetros como intensidade de sinal, número de satélites e precisão estimada da localização. Além disso, disponibiliza ferramentas de análise como mapas de constelações de satélites e um mapa com as coordenadas geográficas recebidas.

Entre as principais características desta aplicação destacam-se a facilidade de utilização, a ampla compatibilidade com diversos dispositivos Android e a possibilidade de realizar testes de desempenho em ambientes controlados. Estas funcionalidades tornam-na útil tanto para utilizadores profissionais que pretendam validar sistemas de navegação como para utilizadores particulares interessados em melhorar a precisão do seu dispositivo móvel.

Apesar das suas vantagens, a aplicação apresenta limitações relacionadas com a dependência do hardware GNSS integrado no dispositivo, o que pode afetar a qualidade dos dados recolhidos. Adicionalmente, algumas funcionalidades avançadas podem requerer versões pagas ou permissões específicas do sistema operativo.

Em conclusão, esta aplicação é uma ferramenta prática e acessível para a monitorização e análise de desempenho de sistemas de navegação por satélite em dispositivos móveis, contribuindo para a validação, diagnóstico e otimização de soluções GNSS.

3.3 Emular Sinais GPS Realistas

A emulação de sinais GPS realistas surge como uma necessidade crítica no contexto de desenvolvimento de sistemas de navegação por satélite, especialmente em ambientes onde o acesso a sinais reais é limitado, controlado ou inviável. O problema principal consistiu em reproduzir, de forma precisa e controlada, as condições de receção de sinais GPS, de modo a avaliar o comportamento do recetor sem dependência de fatores externos imprevisíveis, como condições atmosféricas ou disponibilidade de satélites.

3.3.1 Criação de Localizações Arbitrárias

A criação de localizações geográficas arbitrárias constitui um passo essencial na simulação de sinais GPS para cenários de *spoofing*. Esta funcionalidade permite definir coordenadas geográficas (latitude, longitude) que servirão de referência para os sinais GPS a serem gerados, independentemente da posição real do sistema de transmissão.

A possibilidade de especificar localizações fictícias é fundamental para a avaliação do comportamento de recetores perante situações de engano deliberado na origem dos sinais. Esta abordagem possibilita simular que um dispositivo se encontra num local distante, permitindo a análise de reações e a identificação de potenciais vulnerabilidades.

As coordenadas definidas são posteriormente utilizadas na geração de ficheiros de simulação, assegurando que o sinal emitido representa com rigor a posição fictícia pretendida. Esta separação entre a definição da localização e a geração dos sinais facilita a organização do processo e permite uma maior flexibilidade na construção dos cenários de teste.

3.3.2 Preparação e Manipulação dos Ficheiros Binários

A preparação de ficheiros binários constitui uma etapa fundamental na implementação do sistema de *spoofing* de sinais GPS. Este procedimento visa gerar um sinal sintético de navegação GPS com parâmetros configuráveis, passível de transmissão via rádio definido por software, como o HackRF One, e reconhecido como legítimo por recetores GPS comerciais. Para o efeito, recorreu-se a dados de efemérides de satélites, obtidos através de ficheiros brdc (*Broadcast Ephemeris Files*), e à ferramenta *open-source* GPS-SDR-SIM para geração de sinais de banda-base GPS.

Os ficheiros brdc contêm efemérides precisas de todos os satélites da constelação GPS para um dia específico. Disponibilizados publicamente por entidades como a NASA, através do serviço CDDIS (*Crustal Dynamics Data Information System*), são atualizados diariamente. A sua nomenclatura segue a convenção brdcDDD.YYn, em que DDD representa o dia do ano e YY o ano de referência (e.g., brdc1430.25n corresponde ao dia 143 de 2025). Estes dados garantem que os sinais simulados incorporem informações coerentes com a estrutura das mensagens de navegação GPS autênticas, incluindo parâmetros orbitais, correções de relógio dos satélites e dados temporais.

Após a aquisição do ficheiro brdc, procedeu-se à compilação e operacionalização do GPS-SDR-SIM. Este simulador gera um ficheiro de dados I/Q (*In-phase/Quadrature*) representativo do sinal de banda-base GPS, apto para transmissão via SDR. A compilação foi realizada em ambiente Linux, conforme detalhado na figura 8.

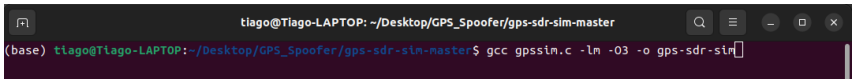


Figura 8: Compilar GPS-SDR-SIM.

A geração do sinal GPS obteve-se mediante execução do comando ilustrado na figura 9, com os seguintes parâmetros:

- -b 8: Define amostragem I/Q de 8 bits (formato compatível com o HackRF One);
- -e [ficheiro_brdc]: Especifica o ficheiro de efemérides;
- -l [coordenadas]: Define as coordenadas geográficas da localização simulada.

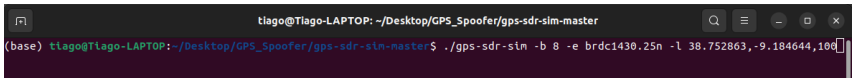


Figura 9: Executar GPS-SDR-SIM.

Estes e demais parâmetros encontram-se sistematizados na Tabela 3, assegurando a configuração adequada do simulador. O GPS-SDR-SIM calcula autonomamente atrasos de propagação decorrentes do movimento dos satélites e estrutura as mensagens de navegação, codificando-as no sinal binário de saída.

Opção	**Argumento**	**Descrição**
-e	<gps_nav>	Ficheiro de navegação para efemérides GPS
-u	<user_motion>	Ficheiro de movimento do utilizador em formato ECEF x, y, z (modo dinâmico)
-l	<location>	Coordenadas Lat, Lon, Altura (modo estático)
-t	<date,time>	Data e hora de início do cenário no formato AAAA/MM/DD,hh:mm:ss
-T	<date,time>	Substitui TOC (Time of Clock) e TOE (Time of Ephemeris) pela hora de início do cenário
-d	<duration>	Duração em segundos (modo dinâmico: máx. 300; modo estático: máx. 86400)
-o	<output>	Ficheiro de saída de dados I/Q (*default*: gpssim.bin)
-s	<frequency>	Frequência de amostragem em Hz (*default*: 2 600 000)
-b	<iq_bits>	Formato dos dados I/Q [1/8/16] (*default*: 16 bits)
-i	-	Desativa o atraso ionosférico (cenário com satélites)
-v	-	Mostra detalhes sobre os canais simulados

Tabela 3: Parâmetros de linha de comando para o GPS-SDR-SIM

O ficheiro resultante, denominado gpssim.bin, e com duração padrão de 300 segundos, é gerado em tempo reduzido tal como mostra a figura 10.

```
(base) tiago@Tiago-LAPTOP:~/Desktop/GPS_Spoofer/gps-sdr-sim-master$ ./gps-sdr-sim -b 8 -e brdc1430.25n -l 38.752863,-9.184644,100
Using static location mode.
xyz =    4916768.8,   -794990.5,   3971021.1
llh =    38.752863,   -9.184644,      100.0
Start time = 2025/05/23,00:14:40 (2367:432880)
Duration = 300.0 [sec]
05  182.7  23.9  23391859.3   3.0
10  326.3   7.3  25227020.6   4.3
12  198.2  24.1  23349821.5   3.0
14   45.1  22.2  23556017.6   3.1
15   17.1  86.5  19885906.4   1.5
17   75.3  14.6  24319043.9   3.7
18  258.6   2.8  25333957.2   5.8
23  297.8  39.7  22007835.1   2.2
24  288.3  56.4  20575941.1   1.7
Time into run = 300.0
Done!
Process time = 14.4 [sec]
```

Figura 10: Gerar ficheiro com o sinal GPS.

Salienta-se que a validade dos ficheiros brdc e a precisão dos parâmetros de entrada impactam diretamente a fidelidade do sinal gerado. A utilização de efemérides desatualizadas, coordenadas inconsistentes ou dados temporais incorretos compromete a receção do sinal por recetores GPS. Assim, todos os recursos foram criteriosamente validados para garantir cenários viáveis e compatíveis com a operacionalidade real do sistema GPS.

Em síntese, a preparação e manipulação de ficheiros binários revelaram-se etapas críticas para a materialização prática deste projeto. A correta utilização de efemérides e a parametrização rigorosa do GPS-SDR-SIM foram determinantes para a geração de sinais GPS sintéticos fidedignos.

3.4 Implementação do Sistema de Spoofing em GNU Radio

A implementação do sistema de *spoofing* em GNU Radio é um elemento central na materialização prática da emissão de sinais GPS simulados através do dispositivo HackRF One. A figura 11 representa o fluxo de processamento de sinal construído com o GNU Radio Companion, uma ferramenta gráfica que permite a criação de sistemas de rádio definidos por software de forma modular e intuitiva.

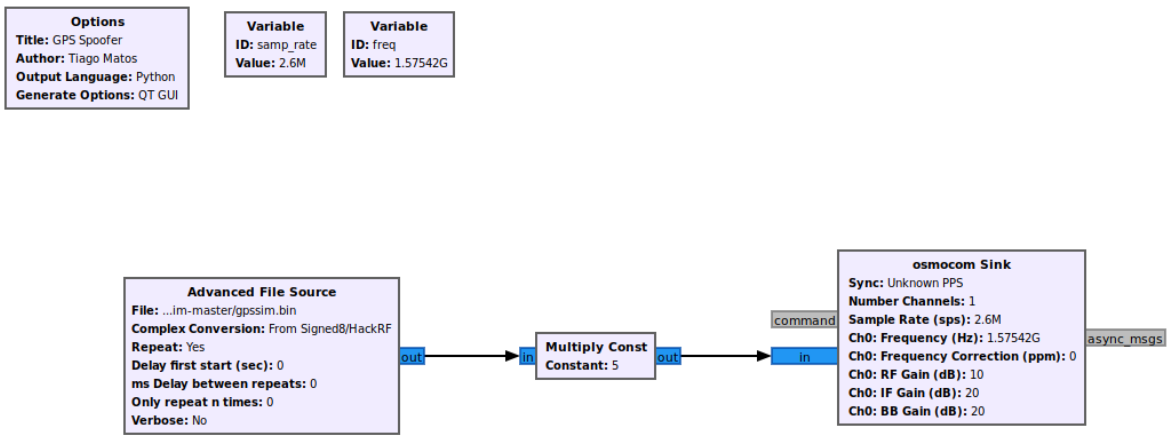


Figura 11: Fluxograma de transmissão de sinal.

O fluxo inicia-se com o bloco *Advanced File Source*, cuja função é ler, de forma contínua e sem atrasos, o ficheiro binário gpssim.bin previamente gerado pelo GPS-SDR-SIM. Este ficheiro contém amostras I/Q codificadas no formato Signed 8-bit, compatíveis com o dispositivo HackRF. O bloco está configurado para repetir indefinidamente o conteúdo do ficheiro sem qualquer atraso entre repetições, assegurando uma emissão contínua do sinal GPS simulado.

As amostras provenientes do ficheiro são de seguida encaminhadas para o bloco *Multiply Const*, cuja função é multiplicar cada amostra por uma constante, neste caso, 5. Esta operação visa amplificar o sinal digital antes de ser transmitido, aumentando a sua potência relativa e, consequentemente, melhorando a robustez da receção por dispositivos próximos. A escolha do fator de multiplicação é empírica e pode ser ajustada consoante o desempenho desejado ou as limitações impostas pelo ambiente de testes.

O sinal amplificado é então direcionado para o bloco *Osmocom Sink*, responsável por transmitir as amostras via HackRF. Este bloco permite configurar múltiplos parâmetros essenciais para a transmissão, dos quais, a taxa de amostragem (*Sample Rate*), que foi fixada em 2,6 Msps (*Megasamples per second*), valor compatível com as exigências do protocolo GPS L1. A frequência central da portadora foi definida como 1.57542 GHz, correspondente à banda L1 dos sinais GPS civis. Adicionalmente, foram definidos os ganhos de transmissão em três níveis distintos: RF Gain (10 dB), IF Gain (20 dB) e BB Gain (20 dB), de modo a garantir uma emissão eficaz sem distorções significativas.

Este sistema modular de três blocos assegura uma cadeia de transmissão eficiente, permitindo a emissão de sinais GPS simulados com parâmetros controlados, diretamente a partir do GNU Radio. A arquitetura evidenciada é suficientemente flexível para permitir futuras extensões, como o controlo em tempo real dos parâmetros de emissão. Esta implementação demonstra a eficácia e a versatilidade do GNU Radio na conceção de sistemas de *spoofing* GNSS, constituindo uma ferramenta poderosa para investigação académica e validação experimental em ambientes controlados.

3.5 Desenvolvimento da Interface Gráfica (GUI)

O desenvolvimento de uma interface gráfica surgiu como uma necessidade prática no contexto deste projeto, com o objetivo de facilitar a interação com o sistema de emulação de sinais GPS. Ao permitir ao utilizador definir localizações arbitrárias e iniciar os processos de geração e transmissão de sinais de forma intuitiva, a GUI contribui significativamente para a usabilidade e acessibilidade da solução desenvolvida.

Neste subcapítulo, apresentam-se as motivações que justificaram a criação da interface, os objetivos funcionais que orientaram o seu desenho, as tecnologias selecionadas para a sua implementação e as funcionalidades concretas que foram desenvolvidas. A GUI assume, assim, um papel central na integração entre as diferentes ferramentas utilizadas, promovendo uma experiência de utilização eficiente e segura.

3.5.1 Motivação e Objetivos da GUI

A motivação subjacente ao desenvolvimento de uma interface gráfica de utilizador (GUI) no contexto deste projeto prendeu-se com a necessidade de simplificar e tornar mais acessível o processo de configuração, geração e transmissão de sinais GNSS simulados. Dado o nível de complexidade técnica associado à utilização direta de ferramentas como o GPS-SDR-SIM ou GNU Radio, tornou-se evidente a vantagem de disponibilizar uma camada de abstração que permita ao utilizador interagir com o sistema de forma mais intuitiva e eficiente.

A GUI foi desenvolvida com dois objetivos principais: permitir a seleção intuitiva de coordenadas geográficas por parte do utilizador, possibilitando a definição da localização a simular com simplicidade e precisão; e fornecer um mecanismo prático de gestão da transmissão dos sinais GNSS, incluindo o seu arranque e término, sem necessidade de interação direta com o terminal. Deste modo, a GUI contribui para a operacionalização eficiente do sistema de *spoofing*, ao mesmo tempo que melhora a usabilidade e reduz a probabilidade de erro humano no processo de simulação.

3.5.2 Tecnologias e Funcionalidades Implementadas

A interface gráfica foi desenvolvida com o principal objetivo de disponibilizar ao utilizador uma forma simples, intuitiva e eficiente de interagir com o sistema de *spoofing* GPS. Para tal, recorreu-se à biblioteca PyQt5, uma das ferramentas mais completas e amplamente utilizadas para o desenvolvimento de interfaces gráficas em Python.

Embora desenvolvida em Python, a PyQt5 é um conjunto de *bindings* para a biblioteca Qt, originalmente escrita em C++, reconhecida pela sua robustez e desempenho no desenvolvimento de aplicações com interfaces gráficas modernas e responsivas. A sua adoção justifica-se pela maturidade da *framework*, compatibilidade multiplataforma e vasto conjunto de componentes visuais e funcionais, que facilitam tanto a criação de interfaces complexas como a separação clara entre a lógica de programação e a camada de apresentação. Esta separação foi determinante para facilitar a manutenção e evolução do projeto.

Com base nesta biblioteca, foram integrados diversos elementos interativos essenciais para a operacionalidade da aplicação. Destacam-se os botões de controlo das principais funcionalidades e a incorporação de um mapa interativo através do componente *QWebEngineView*, que permitiu carregar conteúdos baseados em HTML e JavaScript. O mapa, desenvolvido com recurso à biblioteca *Leaflet*, possibilitou a seleção visual e intuitiva de coordenadas geográficas, que foram posteriormente utilizadas para simular localizações GPS arbitrárias.

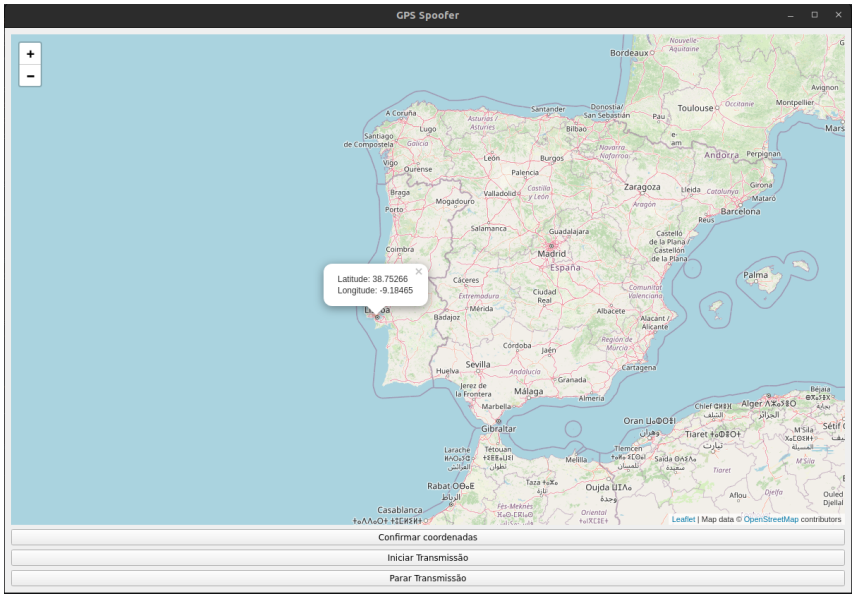


Figura 12: Interface gráfica com o mapa interativo e os controlos principais.

Adicionalmente, outras classes da Qt5 foram utilizadas, como o *QWebChannel*, que permitiu estabelecer comunicação bidirecional entre o conteúdo HTML e o ambiente em Python. Esta funcionalidade revelou-se crucial para garantir a transferência automática das coordenadas selecionadas no mapa para os módulos responsáveis pela geração dos sinais GPS em formato binário.

Classe	Descrição	Utilização no Projeto
QMainWindow	Classe base para a criação de janelas principais	Estrutura da janela principal da aplicação
QPushButton	Botão interativo	Confirmar seleção de coordenadas e começar/parar transmissão
QWebChannel	Canal de comunicação entre diferentes linguagens	Permite a comunicação entre o mapa (HTML) e o ambiente Python
QObject	Base fundamental para todos os objetos	Receber e armazenar coordenadas geográficas enviadas a partir do mapa
QWebEngineView	Componente que permite a visualização de conteúdo HTML	Integração com o mapa interativo (Leaflet)
QVBoxLayout	Gestor de layout vertical	Organização vertical dos widgets na janela
QMessageBox	Caixa de mensagem para alertas e notificações	Exibir mensagens de erro ou confirmação

Tabela 4: Principais classes da PyQt5 utilizadas no desenvolvimento da GUI

A seleção criteriosa das tecnologias utilizadas foi complementada pela definição e implementação de funcionalidades que garantissem uma experiência de utilização fluida e completa, desde a escolha da localização até à execução dos processos técnicos. A interface gráfica foi concebida não apenas como uma camada visual, mas como um ponto central de controlo de todo o sistema, dispensando a necessidade de interação direta com a linha de comandos.

Entre as funcionalidades implementadas destacam-se:

- **Seleção de coordenadas geográficas** através de interação direta com o mapa;
- **Carregamento de ficheiros de efemérides**, nomeadamente os ficheiros do tipo brdc, fundamentais para a simulação fidedigna dos sinais GPS;
- **Compilação e execução automatizada do GPS-SDR-SIM**, utilizando os parâmetros definidos pelo utilizador e os ficheiros previamente carregados;
- **Exibição de mensagens de estado e erro**, que orientam o utilizador e facilitam a deteção de problemas durante a execução.

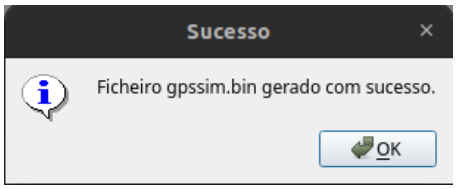


Figura 13: Mensagem de confirmação.

Figura 14: Mensagem de erro.

Em suma, a adoção da biblioteca PyQt5 permitiu alcançar um equilíbrio eficaz entre complexidade técnica e usabilidade, resultando numa plataforma gráfica personalizável e extensível, plenamente alinhada com os requisitos de um sistema de simulação GPS baseado em SDR. A integração harmoniosa entre as tecnologias empregues e as funcionalidades desenvolvidas culminou numa solução robusta e intuitiva, que simplificou a interação do utilizador com o sistema e aumentou significativamente a eficácia dos testes realizados. Esta abordagem, centrada na experiência do utilizador e na automatização dos processos técnicos, revelou-se essencial para garantir a fiabilidade, segurança e reprodutibilidade dos ensaios conduzidos em ambiente experimental.

4 Testes e Resultados

Neste capítulo apresentam-se a metodologia utiliza para a realização dos testes, bem como os resultados obtidos no decurso da implementação do sistema de simulação de sinais GNSS, seguidos da respetiva análise crítica.

4.1 Metodologia de Testes

A estratégia de testes colocada em prática visou confirmar, de forma completa e metódica, a funcionalidade e a robustez da aplicação desenvolvida, bem como aferir a conformidade dos seus resultados com os requisitos previamente definidos. Para isso, delinearam-se vários tipos de situações de teste, que permitiram avaliar tanto os componentes individuais da aplicação como a sua integração global.

A abordagem adotada baseou-se na combinação de diferentes tipos de teste, concebidos para abranger diversas dimensões do comportamento do sistema:

- **Teste de envio:** avaliar o fluxo de transmissão implementado no GNU Radio, para aferir o envio correto do sinal;
- **Teste da interface gráfica:** verificar a possibilidade de escolher as coordenadas no mapa e se o ficheiro binário era criado corretamente;
- **Teste global:** integração dos dois módulos anteriormente testados, com recurso à interface gráfica, para garantir que todo o sistema funcionava de forma coerente e fiável.

Nos testes de envio, utilizou-se um cenário de simulação controlado, em conformidade com as restrições legais relativas à emissão de sinais de radio. A execução do fluxo no GNU Radio foi monitorizada com o auxílio de ferramentas como o analisador de espectro, com o intuito de confirmar a emissão adequada dos sinais. Na parte relativa à interface gráfica recorreu-se ao terminal para conferir se o ficheiro com as localizações arbitrárias foi fidedignamente engendrado.

Com esta metodologia estruturada, procurou-se garantir não só que o aplicativo estivesse de acordo com os objetivos propostos, mas também que ele fosse confiável.

4.2 Resultados Obtidos

Os testes realizados permitiram validar, com evidência empírica, os principais objetivos definidos para a aplicação desenvolvida, nomeadamente a correta geração de ficheiros com coordenadas GPS a partir da interface gráfica e a subsequente transmissão de sinais GPS simulados.

O primeiro teste incidiu sobre a transmissão do sinal gerado por software, recorrendo a um SDR para emissão do sinal de radio no intervalo de frequência do sistema GPS L1 (1575,42 MHz). O gráfico apresentado na figura 15 ilustra o ganho relativo em função da frequência observada durante o teste de envio.

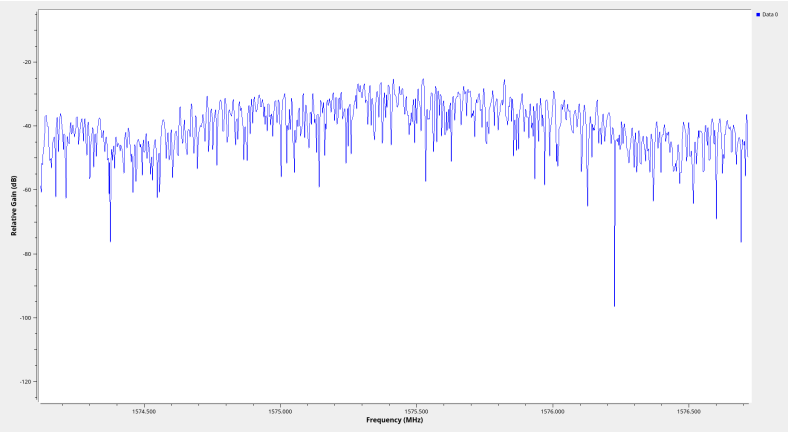


Figura 15: Espectro de frequências do sinal transmitido.

A forma de onda apresenta uma distribuição espectral centrada na banda de interesse, com um nível de potência relativamente baixo (como esperado para simulações em ambientes controlados). Apesar da presença de alguma flutuação de ruído e picos negativos acentuados, que podem ser atribuídos à interferência de fundo, a largura de banda do sinal está alinhada com os requisitos típicos dos sinais GPS.

A interface gráfica constitui o ponto de entrada para o utilizador configurar os parâmetros da simulação. Este teste teve como principais objetivos: verificar a funcionalidade do mapa interativo para seleção de coordenadas e confirmar a correta geração do ficheiro binário com os dados de simulação.

Durante a interação com o mapa incorporado, foi possível selecionar com precisão a localização desejada clicando diretamente sobre o ponto pretendido. As coordenadas em latitude e longitude eram atualizadas automaticamente e exibidas na interface, permitindo ao utilizador confirmar visualmente a posição selecionada. Este mecanismo revelou-se intuitivo e funcional.

Após a seleção das coordenadas, foi gerado um ficheiro binário contendo a informação de navegação codificada segundo o formato apropriado para posterior transmissão via SDR. Para verificar se este foi gerado corretamente, teria-se de obter um resultado semelhante ao da figura 10. Tal como mostra a figura 16, percebe-se que esse objetivo foi atingido com sucesso.

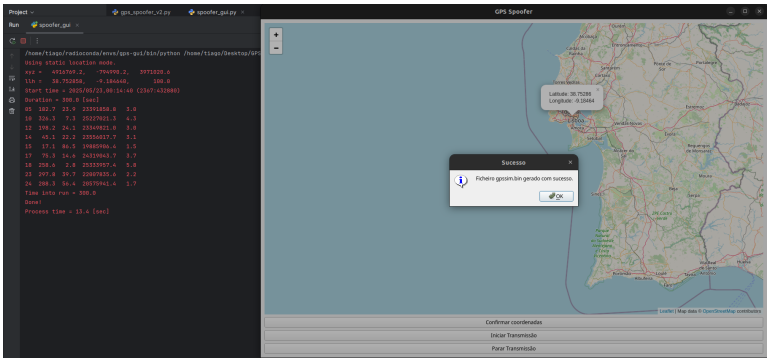
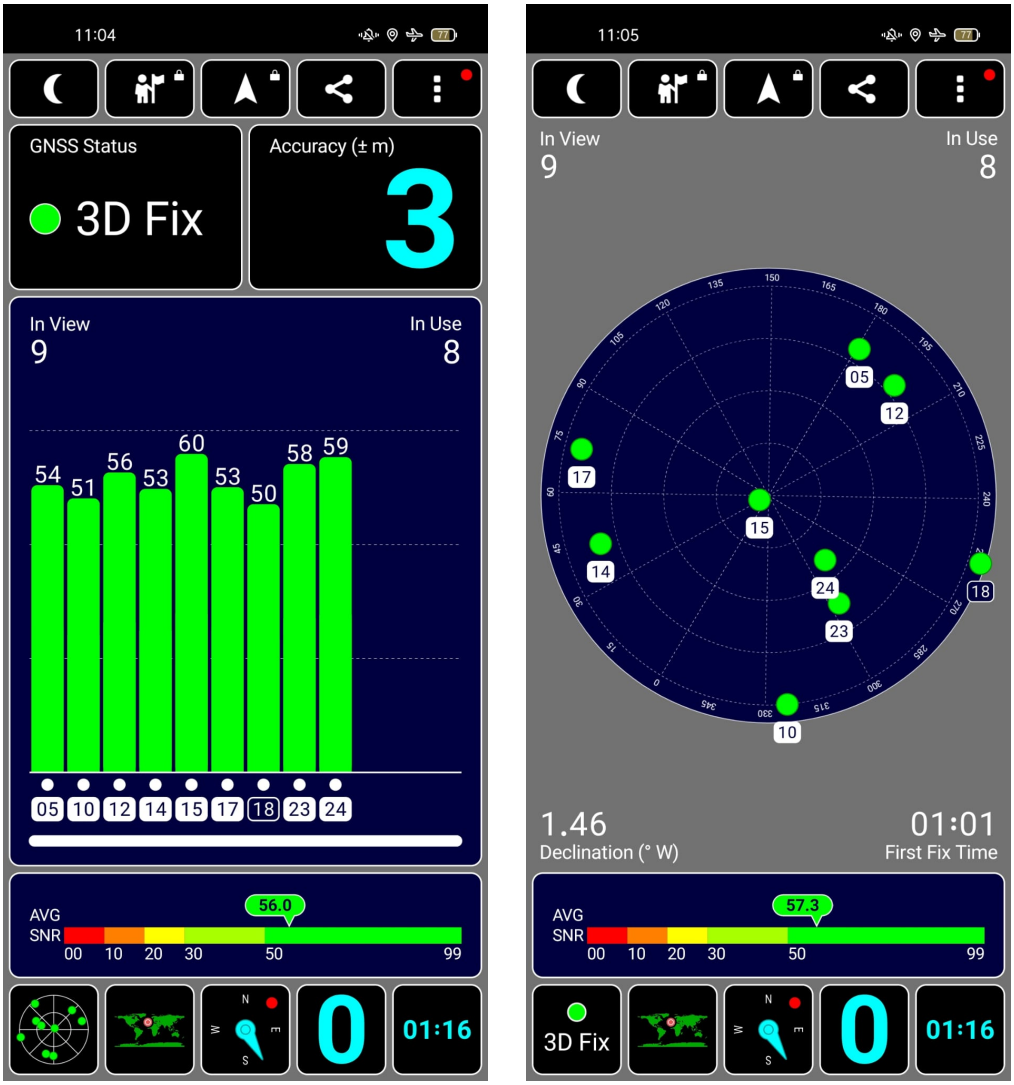


Figura 16: Espectro de frequências do sinal transmitido.

O último teste correspondeu à verificação do sistema de forma integrada. O sinal transmitido foi captado por um dispositivo *Android*, com recurso à aplicação GPS Test App.

A figura 17 mostra os resultados obtidos durante este teste. O dispositivo foi capaz de adquirir e fixar posição com um nível de precisão de 3 metros (±3 m), tendo conseguido identificar 9 satélites em simultâneo, todos com valores elevados de razão sinal-ruído (SNR), sendo o valor médio de 56,5 dB-Hz. Estes níveis de SNR são compatíveis com sinais GNSS reais e demonstram que a simulação foi bem-sucedida em termos de potência e fidelidade espectral.

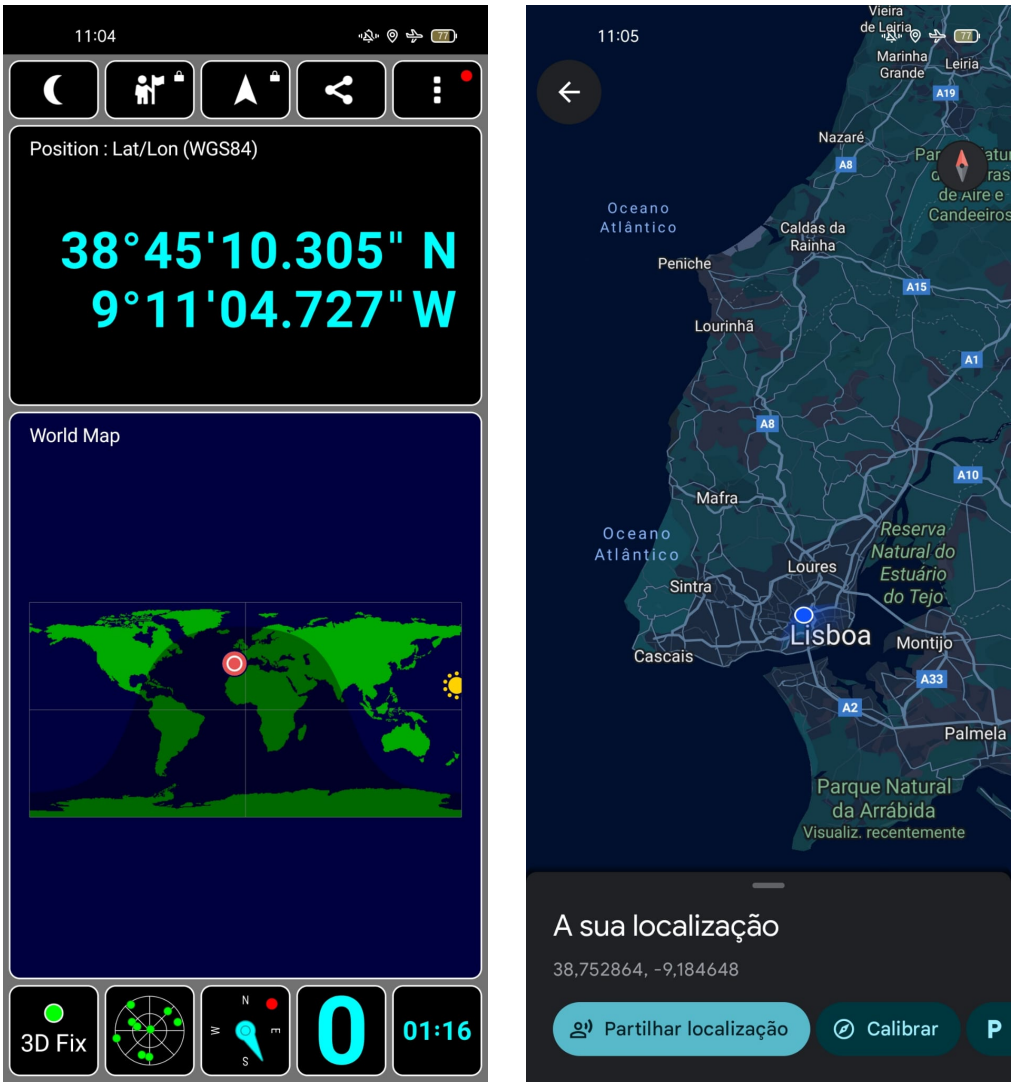


(a) Informações sobre o sinal e os diferentes satélites.

(b) Distribuição dos satélites.

Figura 17: Estado do recetor GPS durante a simulação.

Além disso, a localização registada pelo dispositivo, tal como está representado na figura 18, correspondeu ao ponto previsto pelo sinal simulado, com coordenadas centradas na posição previamente definida na configuração do emissor (38°45'09.891"N, 9°11'04.850"W). A presença de um 3D Fix indica que o recetor conseguiu obter informação suficiente de pelo menos quatro satélites, permitindo calcular a posição horizontal, mas também a altitude, validando assim o funcionamento tridimensional do sistema.



(a) 3D Fix da posição final.

(b) Posição final vista no google maps.

Figura 18: Posição Final.

4.3 Análise Crítica dos Resultados

A análise dos resultados obtidos permitiu aferir o grau de eficácia e fiabilidade da aplicação desenvolvida, tanto do ponto de vista funcional como operacional. Através da execução dos testes descritos anteriormente, foram recolhidas evidências empíricas que sustentam uma avaliação crítica do desempenho da solução implementada.

Os três testes realizados demonstraram que o sistema de simulação é funcional e eficaz. A interface gráfica possibilita o controlo em tempo real dos parâmetros de simulação; a transmissão é efetuada com fidelidade suficiente para emular um sinal GNSS real; e os dispositivos comerciais são capazes de detetar e posicionar-se com base nesse sinal.

Apesar do sucesso geral, alguns aspetos merecem atenção futura, nomeadamente, a presença de picos de ruído no espectro, os quais poderão comprometer a qualidade do sinal em ambientes mais ruidosos ou em cenários mais exigentes, como a simulação de múltiplas constelações.

Adicionalmente, os resultados obtidos revelaram-se promissores, uma vez que não foram detetados erros na geração dos ficheiros binários nem falhas na execução do fluxo de transmissão, evidenciando a robustez do sistema. O facto de os testes terem sido conduzidos em ambiente isolado e monitorizados com ajuda de um analisador de espectro, e com a aplicação GPS Test App, permitiu confirmar que a emissão decorreu dentro dos parâmetros previstos, sem sinais espúrios ou instabilidade de frequência.

Em síntese, os resultados obtidos comprovaram que a aplicação satisfaz os requisitos funcionais definidos, apresenta estabilidade em contexto de execução real e é capaz de produzir sinais sintéticos de navegação GPS coerentes e detetáveis. Estes resultados sustentam a viabilidade da abordagem adotada e a sua aplicabilidade futura em contextos de investigação e validação de sistemas de posicionamento.

5 Conclusões

O presente trabalho teve como principal objetivo o desenvolvimento e validação de um sistema capaz de simular sinais GPS de forma controlada, utilizando rádios definidos por software. Através da combinação de componentes como o GPS-SDR-SIM, GNU Radio, HackRF One e GPS Teste App, foi possível construir e testar uma plataforma funcional que permite a geração e emissão de sinais GNSS sintéticos.

O processo de desenvolvimento incidiu-se desde a análise inicial do problema e levantamento dos requisitos técnicos, passando pela configuração do ambiente de desenvolvimento e pela integração das ferramentas necessárias, até à implementação dos diferentes módulos do sistema. Iniciou-se com a criação e manipulação de ficheiros binários com o GPS-SDR-SIM, seguiu-se a construção do fluxo de transmissão em GNU Radio e a sua validação com o HackRF One como dispositivo emissor. Paralelamente, foi desenvolvida uma interface gráfica que permite ao utilizador interagir com o sistema de forma intuitiva, selecionando coordenadas e controlando a transmissão. Todo o processo culminou na integração dos componentes num sistema funcional completo, sujeito a um conjunto de testes em ambiente controlado para garantir a fiabilidade e a conformidade com os objetivos traçados.

A metodologia adotada contemplou uma abordagem estruturada de testes, que incluiu a avaliação individual dos módulos de geração e transmissão, a validação da interface gráfica desenvolvida e, finalmente, a execução de testes integrados em ambiente controlado. Os resultados demonstraram a eficácia do sistema na simulação de coordenadas arbitrárias, com recetores comerciais a interpretar os sinais como legítimos e a posicionar-se de acordo com a localização simulada.

A aplicação revelou-se robusta e fiável, com desempenho estável e ausência de erros críticos. No entanto, foram também identificadas oportunidades de melhoria, nomeadamente na mitigação de ruído espúrio no espectro de emissão e na potencial extensão para suporte a múltiplas constelações.

Em suma, o trabalho desenvolvido evidencia o potencial das tecnologias SDR para investigação e ensaio de sistemas GNSS, abrindo caminho para futuras aplicações em contextos de segurança, validação de recetores, análise de vulnerabilidades ou desenvolvimento de contra-medidas a ataques de *spoofing*. O cumprimento dos objetivos propostos e a solidez dos resultados obtidos comprovam a viabilidade da solução apresentada e a sua relevância no panorama atual da investigação em navegação por satélite.

Referências

[1] G. S. Gadgets, “Hackrf one - great scott gadgets.” [Online]. Available: https://greatscottgadgets.com/hackrf/one/

[2] Duncan-Parnell, “Difference between gps spoofing & jamming | duncan-parnell.” [Online]. Available: https://www.duncan-parnell.com/blog/109/what-s-the-difference-between-gps-spoofing-and-jamming-

[3] everythingRF, “What is the difference between gps jamming and spoofing? - everything rf.” [Online]. Available: https://www.everythingrf.com/community/what-is-the-difference-between-gps-jamming-and-spoofing

[4] N. I. of Standards and T. (NIST), “Time and frequency from a to z, g | nist.” [Online]. Available: https://www.nist.gov/pml/time-and-frequency-division/popular-links/time-frequency-z/time-and-frequency-z-g

[5] NovAtel, “What is gps? | novatel.” [Online]. Available: https://novatel.com/support/knowledge-and-learning/what-is-gps-gnss

[6] E. S. A. (ESA), “Gps signal plan - navipedia.” [Online]. Available: https://gssc.esa.int/navipedia/index.php/GPS_Signal_Plan

[7] P. S. University, “The navigation message | geog 862: Gps and gnss for geospatial professionals.” [Online]. Available: https://www.e-education.psu.edu/geog862/node/1734

[8] G. Radio, “About gnu radio.” [Online]. Available: https://www.gnuradio.org/about/

[9] T. Ebinuma, “Github - osqzss/gps-sdr-sim: Software-defined gps signal simulator.” [Online]. Available: https://github.com/osqzss/gps-sdr-sim

[10] N. CDDIS, “Cddis | | archive | gnss | data | daily | 2025 |.” [Online]. Available: https://cddis.nasa.gov/archive/gnss/data/daily/2025/brdc/

[11] Q. Company, “All classes | qt 5.15.” [Online]. Available: https://qthub.com/static/doc/qt5/qtdoc/classes.html#