

# Estratégias de Jamming e Spoofing para Aplicações Anti-Drones

Autor: Alferes-Aluno de Transmissões Younes Zidane, Academia Militar, Lisboa, Portugal - [zidane.y@exercito.pt](mailto:zidane.y@exercito.pt)

Dissertação de Mestrado (Master of Science) em Engenharia Electrotécnica Militar com especialização em Telecomunicações

Orientação do Prof. (Ph.D), José Silvestre Serra da Silva, da Academia Militar, e a coorientação do Professor Auxiliar Gonçalo Nunes Gomes Tavares, do Instituto Superior Técnico

**Resumo** - Este artigo investiga o desenvolvimento e a avaliação de técnicas de empastelamento (*jamming*) e de falsificação de sinais (*spoofing*) para perturbar os sistemas de comunicação e de navegação de Veículos Aéreos Não Tripulados (VANTs) em zonas restritas. Utilizando a tecnologia de *Software Defined Radio* (SDR), foi desenvolvido um sistema adaptável para neutralizar os drones, perturbando os seus sinais de controlo e serviços de geolocalização. Testes experimentais em drones comerciais demonstraram a eficácia do empastelamento por radiofrequência (RF) na interrupção do controlo e da transmissão de imagens, enquanto o *spoofing* emitiu com sucesso sinais falsos do *Global Navigation Satellite System* (GNSS) e interferiu com o comportamento dos drones.

## Introdução

Os VANTs desenvolveram-se rapidamente e são atualmente utilizados em sectores como da fotografia, cartografia e entregas [1]. As preocupações com a segurança, especialmente devido a conflitos recentes, alimentaram o interesse em tecnologias contra drones [1]. Estes sistemas, que detetam drones utilizando sinais de rádio e radar, têm como objetivo evitar acidentes e ameaças como o terrorismo. No entanto, a integração de sistemas de combate a drones em ambientes críticos apresenta desafios, incluindo questões regulamentares, técnicas e de custos [2].

## Contextualização

### A. Normas de Comunicação para os VANTs

O sistema de comunicação de um VANT inclui quatro ligações principais: Navegação, Rádio Controlo (RC), Telemetria e Vídeo. A ligação de navegação utiliza um recetor GNSS para fornecer dados de posição e velocidade, enquanto a ligação RC transmite comandos do operador com baixa latência. A telemetria envia informações sobre o estado do drone, e a ligação de vídeo transmite imagens da câmara ao controlador [3]. O Wi-Fi, amplamente utilizado, é uma tecnologia proeminente para comunicação entre a estação terrestre e o drone, operando nas bandas de 2,4 GHz (2400–2500 MHz) e 5 GHz (5725–5925 MHz), conforme as normas IEEE 802.11 [4,5].

1) Modulação e Protocolos dos VANTs: As ligações RC, telemetria e de vídeo usam canais RF, como o Wi-Fi, sendo a transmissão de vídeo predominantemente baseada em *Orthogonal Frequency-Division Multiplexing* (OFDM) [3,6]. Técnicas de modulação como *Frequency-Hopping Spread Spectrum* (FHSS), *Direct Sequence Spread Spectrum* (DSSS) e OFDM são comuns em drones. A telemetria na banda de 2,4 GHz usa OFDM e DSSS, enquanto na banda de 5 GHz é dominada por OFDM [6,7].

2) Fundamentos do GNSS: Os sistemas GNSS, como GPS, GLONASS, Galileo e BeiDou [8], operam na banda L, permitindo a navegação por meio do cálculo do tempo de viagem do sinal e da posição do satélite. Esses sinais incluem uma portadora em frequência RF e códigos de ruído pseudo-aleatório, como os códigos C/A e P do GPS. Essenciais para drones comerciais, suportam funções como *return-to-home* em caso de perda de sinal. Na UE, GPS e Galileo operam de forma interoperável, com o GPS utilizando as bandas L1 (1575,42 MHz), L2 (1227,60 MHz) e L5 (1176,45 MHz) [9].

## B. *Spoofing* de Radiofrequências

O *spoofing* envolve o envio de comunicações fraudulentas que aparentam vir de uma fonte confiável, com o objetivo de enganar o destinatário. No caso de sinais GPS, é possível induzir recetores a aceitar dados de localização falsificados, comprometendo a integridade da informação baseada na localização [10]. As *No Fly Zones* (NFZ), áreas onde o voo de determinadas aeronaves é proibido, são estabelecidas por entidades militares ou governamentais para mitigar ameaças, especialmente em áreas de conflito ou eventos de grande visibilidade. A violação dessas zonas por *spoofing* pode levar à aterragem automática ou impedir a decolagem de drones afetados [11].

## C. *Jamming* de Radiofrequências

O empastelamento de RF interrompe a comunicação entre um drone e o operador, afetando a sua capacidade de receber instruções. Os sinais GNSS são particularmente vulneráveis devido à sua fraqueza, e os bloqueadores de GPS podem impedir as funções de *return-to-home*, conduzindo a avarias ou colisões. As principais técnicas de interferência de RF incluem [3,7]:

- *Barrage Jamming*: O ruído de banda larga reduz o rácio sinal-ruído (SNR), aumentando as taxas de erro e diminuindo a capacidade do canal.
- *Sweep Jamming*: Um sinal de banda estreita varre as frequências, simulando os efeitos de interferência de barragem em altas taxas de varredura.
- *Follower Jamming*: Acompanha as alterações de frequência nos sistemas FHSS para bloquear as frequências recentemente seleccionadas.

## Conceção do Sistema e Metodologia

### A. *Hardware e Software*

O sistema inclui um computador portátil, o ADALM-PLUTO para modulação e transmissão (32 MHz a 3,8 GHz, -4 dBm a 0 dBm), um amplificador WYDZ-PA-1G-3GHz-1W (30 dB de ganho, 1 W), e antenas otimizadas: YAGI WIFI para 2,4 GHz e outra de 1,5 GHz. Os drones testados operam em 2,4 GHz e 5,8 GHz, com o Autel Evo Nano+ usando também 5,150-5,250 GHz e o Husban Zino Mini Pro com backup 4G. O *software* usado incluiu GNU Radio (3.10.1.1) no Ubuntu 24.04.1 LTS e *Visual Studio Code* para ajustar *scripts Python*.

### B. Metodologia

1) *Barrage Jamming* do GNSS: O GNU Radio foi usado para desenvolver *scripts* de interferência em sinais GNSS, com destaque para o *barrage jamming* (Figura 1). Essa técnica envolve a transmissão contínua de ruído de alta potência no espectro GNSS. O aumento do nível de ruído compromete a receção dos sinais legítimos, causando perda de precisão ou funcionalidade posicional nos recetores GNSS dos drones.

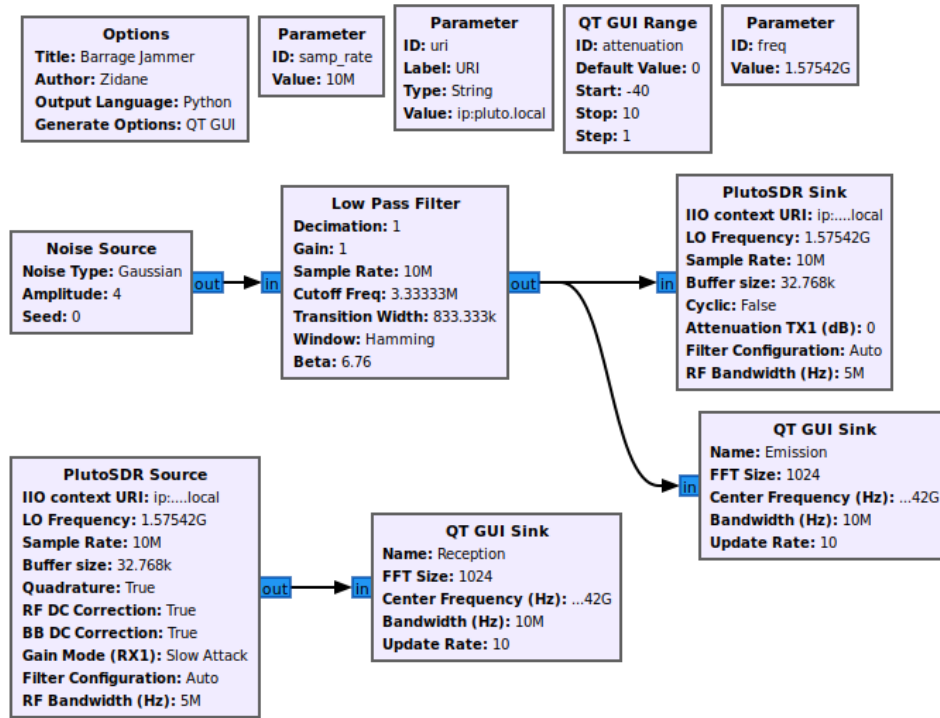


Figura 1: Script utilizado para implementar *Barrage jamming* no GNSS

O *script* utiliza uma taxa de amostragem de 10 MHz e gera ruído gaussiano. Um filtro passa-baixo limita a largura de banda a 3,333 MHz, focando na banda GPS L1, com frequência de corte correspondente ente a um terço da taxa de amostragem. O bloco *PlutoSDR Source* captura sinais na frequência GPS L1, enquanto o *PlutoSDR Source* transmite o ruído filtrado na mesma frequência e taxa de amostragem.

2) *BPSK Jamming do GNSS*: A interferência com conhecimento de protocolos imita e sobrepõe o sinal original, otimizando a relação potência-largura de banda. Em sistemas GPS, que usam modulação BPSK, esta técnica gera um sinal interferente que replica a modulação, levando o recetor a interpretar o sinal interferente como legítimo. A Figura 2 apresenta o script GNU Radio desenvolvido para esta implementação.

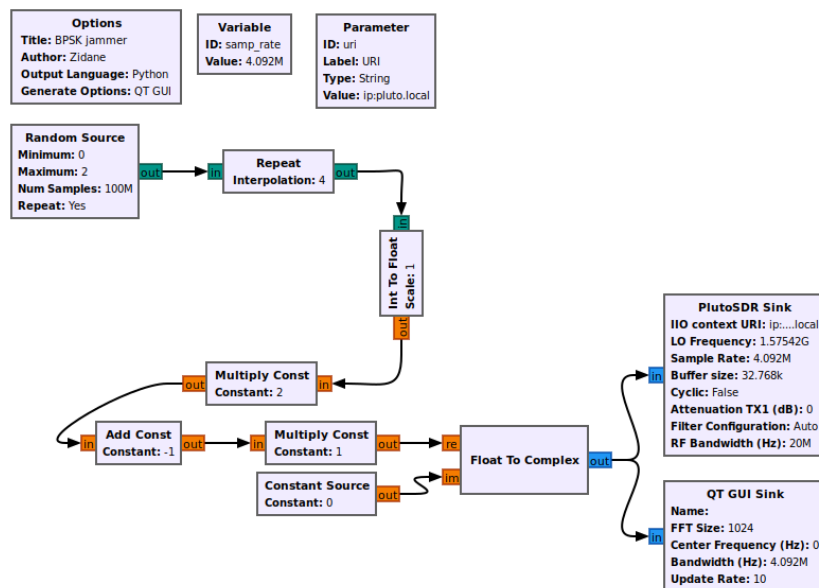


Figura 2: *Script* utilizado para implementar BPSK *jamming* no GNSS

O *script* gera uma sequência de bits aleatórios à taxa de 1,023 Mbit/s, correspondente à taxa de chip do GPS, com período de amostragem de 100 M. Um fator de interpolação de 4 ajusta a taxa de amostragem para 4,092 MHz, garantindo compatibilidade com o PlutoSDR Sink. Os bits são então mapeados para uma constelação BPSK representando +1 e -1. O PlutoSDR Sink transmite o sinal BPSK modulado na frequência central GPS L1, com buffer de 32,768 ks, transmissão não cíclica e atenuação TX1 ajustada para 0 dB.

3) *Spoofing* do GNSS: Um ataque de *spoofing* foi realizado utilizando o simulador GPS-SDR-SIM, com o objetivo de manipular a posição de um recetor alvo. Este simulador gera sinais realistas que, ao serem convertidos em RF pelo SDR, tornam-se adequados para experimentos de *spoofing*. O GPS-SDR-SIM permite configurar trajetórias específicas através de ficheiros. Nesta investigação, sinais GPS simulados foram transmitidos pelo SDR com uma taxa de amostragem de movimento de 10 Hz, garantindo precisão na simulação de movimentos.

4) *Barrage jamming* de RC e Vídeo: O *script* implementado no *Barrage jamming* do GNSS foi ajustado para interferir em sinais RC e de vídeo na banda de 2,4 GHz. A largura de banda foi configurada para 20 MHz, largura de banda máxima do SDR, com amplitude do ruído definida em 2, garantindo interferência forte sem saturar o dispositivo. No entanto, estes parâmetros não cobrem toda a banda de 2,4 GHz (80 MHz), o que levou à necessidade de modificações no código *Python* gerado pelo GNU Radio para estender a cobertura a toda a banda. A frequência de `iio_pluto_sink_0` foi ajustada para utilizar este parâmetro. As variáveis `start_frequency` (2,405 GHz) e `stop_frequency` (2,475 GHz) foram definidas. A função `update_frequency` foi configurada para atualizar a frequência a cada 5 segundos.

Drones que operam na banda de 2,4 GHz frequentemente utilizam a tecnologia FHSS, que altera aleatoriamente as frequências de operação. Para interromper essa comunicação, foi desenvolvida uma nova estratégia de *jamming*. Na função `main`, foi definida uma lista de frequências centrais, incluindo [2,41 GHz, 2,425 GHz, 2,44 GHz, 2,455 GHz, 2,47 GHz]. A função `update_frequency` foi modificada para usar o módulo `random`, permitindo que, em vez de incrementar as frequências sequencialmente, ela selecione aleatoriamente uma frequência da lista predefinida.

## Resultados e Discussão

### A. *Jamming* e *Spoofing* do GNSS

Os testes práticos desta implementação foram realizados no Campo Militar de Santa Margarida, durante o exercício ARTEX24. Durante os testes, a posição tanto do operador quanto do *jammer* foi mantida fixa. Para avaliar as implementações, foi utilizado um Analisador de Sinal/Espectro Rohde & Schwarz FSV30. Além disso, a potência de saída no terminal do amplificador foi medida para estimar a eficácia potencial do ataque, empregando um atenuador de 30 dB para proteger o equipamento durante as medições.

1) *Barrage Jamming* do GNSS: A Figura 3 apresenta o espectro do sinal com a frequência de corte definida como um terço da taxa de amostragem (SR/3).

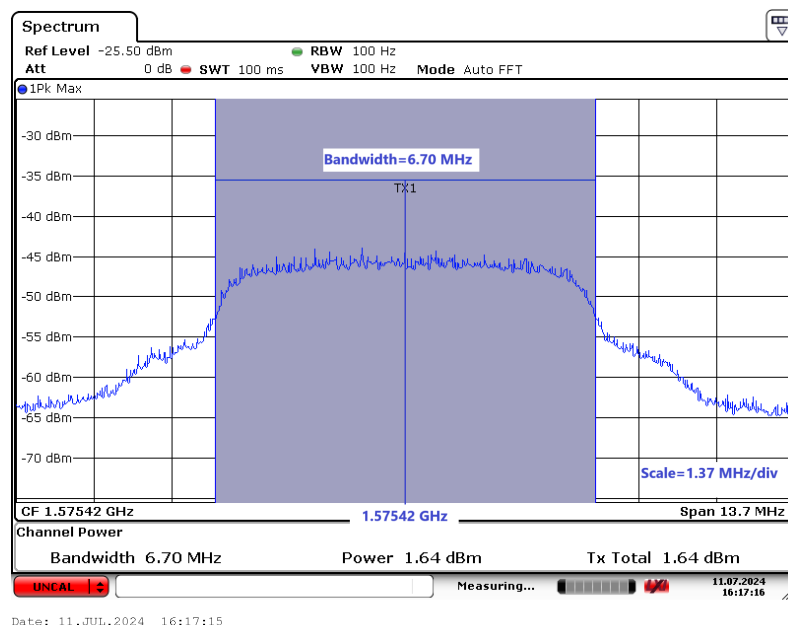


Figura 3: Espectro do sinal de *Barrage Jamming* de GNSS ( $f_c=SR/3$ )

Considerando a atenuação de 30 dB, somada à potência obtida de 1,64 dBm, obtemos 31,6 dBm, com uma Potência Isotrópica Radiada Eficaz (EIRP) de 43,6 dBm quando conectada a uma antena Yagi de 12 dBi.

Os resultados de interferência apresentados na Tabela 1 foram promissores. A distância (D) entre o *jammer* e o drone foi variada, com o jammer fixo enquanto o drone se movia para avaliar a eficácia do jamming. O sinal verde de *checkmark* indica sucesso total no *jamming*, resultando em uma interrupção de 100% na recepção do sinal de geolocalização, tornando o drone incapaz de receber qualquer informação de satélite. O "X" a vermelho representa uma tentativa de *jamming* falhada, onde a recepção do sinal de geolocalização não foi completamente interrompida.

| Drone/Distance (D)   | 80 m | 100 m | 120 m | 130 m | 140 m |
|----------------------|------|-------|-------|-------|-------|
| DJI Mini 3           | ✓    | ✓     | ✓     | ✗     | ✗     |
| DJI Mini 3 Pro       | ✓    | ✓     | ✓     | ✗     | ✗     |
| Autel Evo Nano+      | ✓    | ✓     | ✓     | ✓     | ✗     |
| Husban Zino Mini Pro | ✓    | ✓     | ✓     | ✓     | ✓     |
| ZLL SG 108           | ✓    | ✓     | ✓     | ✓     | ✓     |

TABELA 1- Efetividade do *Barrage jamming* de GNSS a diferentes distâncias entre o jammer e o drone

A eficácia do *jamming* foi avaliada verificando se o drone conseguia se conectar aos satélites apesar da interferência. A principal consequência do *jamming* do GNSS foi a falha na função *return-to-home*. Sem essa função, o drone perde a capacidade de determinar sua localização e pode se perder, especialmente quando controlado à distância e sem contato visual. Diferentes modelos de drones reagiram de maneira distinta ao *jamming*: os modelos DJI e Husban perderam a conexão com os satélites, mas permaneceram no estado comandado pelo último sinal recebido. Já os modelos Autel e ZLL responderam de forma mais segura, realizando imediatamente um procedimento de aterragem, mitigando riscos associados ao *jamming*.

2) BPSK *Jamming* do GNSS: O espectro do sinal transmitido para a implementação do BPSK *jamming* está ilustrado na Figura 4.

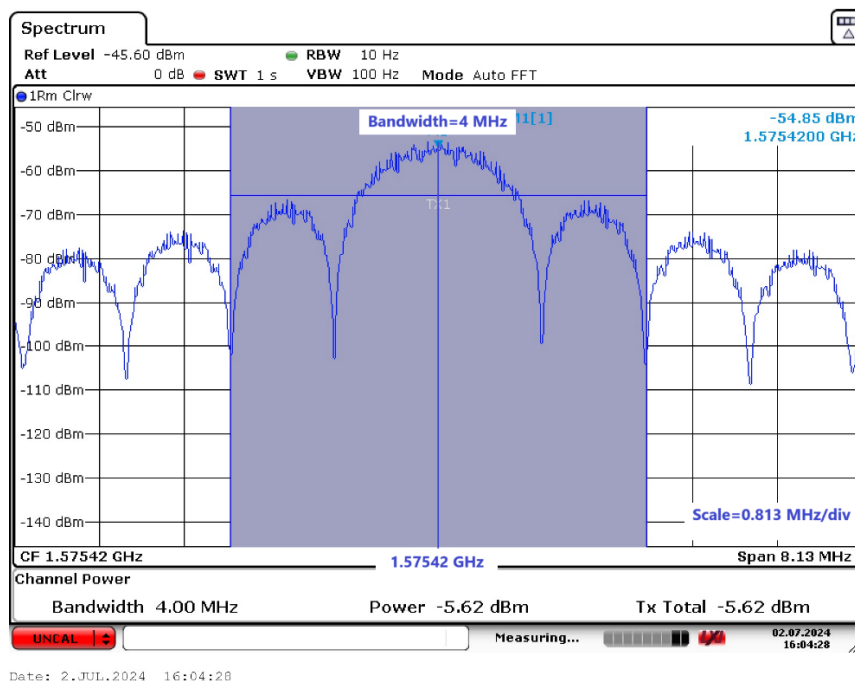


Figura 4: Espectro do sinal de BPSK *jamming* no GNSS

A potência de saída medida foi de -5,6 dBm. Considerando o ganho do amplificador (30 dB) e o ganho da antena (12 dBi), o EIRP total calculado foi de aproximadamente 36,4 dBm. A Tabela 2 apresenta os resultados da eficácia do *jamming*, com a distância (D) representando a separação entre o *jammer* e o drone.

| Drone/Distance (D)   | 80 m | 100 m | 120 m | 130 m | 140 m |
|----------------------|------|-------|-------|-------|-------|
| DJI Mini 3           | ✓    | ✓     | ✓     | ✓     | ✗     |
| DJI Mini 3 Pro       | ✓    | ✓     | ✓     | ✓     | ✗     |
| Autel Evo Nano+      | ✓    | ✓     | ✓     | ✓     | ✗     |
| Husban Zino Mini Pro | ✓    | ✓     | ✓     | ✓     | ✓     |
| ZLL SG 108           | ✓    | ✓     | ✓     | ✓     | ✓     |

TABELA 2 - Efetividade do BPSK *jamming* de GNSS a diferentes distâncias entre o *jamming* e o drone

A modulação BPSK demonstra maior eficiência do que o *barrage jamming* para GNSS, especialmente em distâncias maiores e com menor potência, devido a dois fatores principais: a densidade de potência dos sinais BPSK concentra energia em uma faixa de frequência estreita, alinhada com as utilizadas pelos sistemas GNSS, e a semelhança de modulação com os sinais GNSS, o que dificulta a distinção entre sinais legítimos e sinais de *jamming* pelos receptores.

3) Spoofing do GNSS: Foi simulado um ataque de spoofing com SDR transmitindo dados geoespaciais falsos. O primeiro método foi o spoofing estático para uma posição aleatória (Tóquio, Japão), sem afetar o comportamento do drone. Em seguida, foi realizado spoofing estático para uma NFZ (Aeroporto Francisco Sá Carneiro, Porto, Portugal), impactando os drones DJI, que ativaram medidas de proteção, como avisos e contagem regressiva para o pouso automático.

O *spoofing* dinâmico com variação de altitude, utilizando um arquivo CSV com 3000 pontos, gerou comportamentos erráticos nos drones ZLL SG 108 e Autel Evo Nano+, enquanto os DJI mantiveram estabilidade. No *spoofing* dinâmico para uma NFZ com altitude zero, os drones tentaram pousar prematuramente, aumentando os riscos de colisão. O *jamming* combinado com sinais falsificados foi eficaz contra os drones DJI.

As respostas ao *spoofing* dinâmico variaram: os DJI Mini 3 e Mini 3 Pro mantiveram estabilidade no voo estacionário, mas perderam o controle em movimento, ativando o pouso automático. O Autel Evo Nano+ ficou instável, subindo descontroladamente antes de pousar de forma errática. O Husban Zino Mini Pro perdeu o controle em movimento, colidindo sem iniciar o pouso automático, e o ZLL SG 108 teve

## B. Barrage Jamming de RC e Vídeo

A eficácia do *jamming* foi avaliada por meio de testes realizados em diferentes locais, como o Campo Militar de Santa Margarida e a Academia Militar de Amadora. Para garantir a precisão, a distância entre o operador e o drone foi significativamente maior que a distância entre o *jammer* e o drone, permitindo que o *jamming* interferisse efetivamente na comunicação. O *jammer* foi posicionado a 6 metros do drone, garantindo um sinal de *jamming* forte o suficiente para impactar o GNSS do VANT. A distância entre o operador e o drone (denotada como D) foi variada durante os testes para avaliar como o *jamming* afetava o controle do drone. A análise de espectro, ilustrada na Figura 5, mostra os padrões de emissão para as duas implementações de *barrage jamming*: uma varredura ampla da banda de 2,4 GHz e a mudança aleatória de frequências.

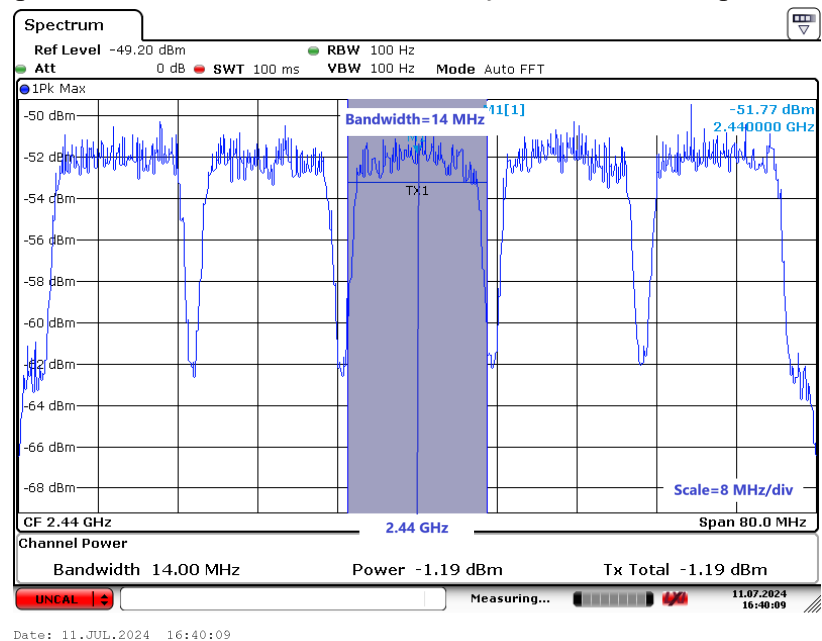


Figura 5: Espectro do sinal de Barrage Jamming na banda 2.4 GHz

A série de cálculos foi realizada para estimar a intensidade do sinal na saída da antena do sistema. O sinal de saída inicial no amplificador foi medido em -1,2 dBm. Considerando a atenuação de 30 dB do atenuador e o ganho de 18 dBi da antena Yagi, a EIRP na saída da antena foi calculada em aproximadamente 46,8 dBm. A Tabela 3 reúne os resultados.

| Drone/Distance (D)   | 30 m | 50 m | 80 m | 100 m | 120 m |
|----------------------|------|------|------|-------|-------|
| DJI Mini 3           | X    | X    | X    | X     | ✓     |
| DJI Mini 3 Pro       | X    | X    | X    | X     | ✓     |
| Autel Evo Nano+      | X    | ✓    | ✓    | ✓     | ✓     |
| Husban Zino Mini Pro | X    | X    | X    | X     | X     |
| ZLL SG 108           | ✓    | ✓    | ✓    | ✓     | ✓     |

TABELA 3- Efetividade do Barrage jamming de RC e vídeo a diferentes distâncias entre o operador e o drone.

A análise dos testes revelou desempenho semelhante entre os drones DJI, com operação estável até 40 metros, quando surgiram leves interferências. A partir de 85 metros, a conexão foi afetada, com falhas na transmissão de vídeo e atrasos nas manobras, culminando em perda total de conexão a 120 metros. O Autel Evo Nano+ mostrou maior vulnerabilidade, sendo neutralizado a partir de 50 metros. O Husban Zino Mini Pro foi imune ao *jamming* devido à possibilidade de alternar para comunicação 4G. Já o ZLL SG 108, sem interface visual, foi o mais afetado, tornando-se incontrolável a apenas 30 metros.

## Conclusão

Este estudo focou no desenvolvimento de contramedidas de *jamming* para neutralizar os sistemas de comunicação de drones, com ênfase em proteger áreas sensíveis e infraestruturas. O sistema baseado em SDR mostrou-se eficaz, combinando *jamming* em barragem e técnicas como o *jamming* BPSK para interferência GNSS, adaptando-se aos desafios dos VANTs modernos.

Os testes realizados, tanto em ambientes controlados quanto em campo, demonstraram a eficácia do sistema. O *jamming* em barragem foi eficiente para interromper controle e transmissões de vídeo, embora o Husban Zino Mini Pro, com comunicação 4G, tenha revelado limitações. O *jamming* BPSK foi superior em precisão e alcance para interferir na navegação GNSS. O spoofing dinâmico, combinado com zonas de exclusão aérea e manipulação de altitude, provou ser eficaz para forçar pousos ou induzir comportamentos erráticos.

Em resumo, a pesquisa apresenta uma solução adaptável e de baixo custo para *jamming* e *spoofing* de drones, fornecendo uma base sólida para proteger infraestruturas críticas contra atividades não autorizadas de VANTs.

## Bibliografia

- [1] D. Zmyslowski, P. Skokowski, and J. Kelner, "Anti-drone Sensors, Effectors, and Systems-A Concise Overview." *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, vol. 17, no. 2, p. 455–461, 2023.
- [2] G. Abro, S. Zulkifli, R. Masood, V. Asirvadam, and A. Laouiti, "Comprehensive Review of UAV Detection, Security, and Communication Advancements to Prevent Threats," *Drones*, vol. 6, no. 10, p. 284, 2022.
- [3] D. J. Rozenbeek, "Evaluation of Drone Neutralization Methods using Radio Jamming and Spoofing Techniques," Ph.D. dissertation, KTH Royal Institute of Technology, 2020. [Online]. Available: <https://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-279557>.
- [4] M. A. Jasim, H. Shakhathreh, N. Siasi, A. H. Sawalmeh, A. Aldalbahi, and A. Al-Fuqaha, "A Survey on Spectrum Management for Unmanned Aerial Vehicles (UAVs)," *IEEE Access*, vol. 10, p. 11443–11499, 2022.
- [5] S. I. Han, "Survey on UAV Deployment and Trajectory in Wireless Communication Networks: Applications and Challenges," *Information*, vol. 13, no. 8, p. 389, 2022.
- [6] D. Torrieri, *Direct-Sequence Systems*. Springer International Publishing, 2021, p. 81–150.
- [7] O. Simon and T. Gotthans, "A Survey on the Use of Deep Learning Techniques for UAV Jamming and Deception," *Electronics*, vol. 11, no. 19, p. 3025, 2022.
- [8] EU Agency for the Space Programme, "What is GNSS," <https://www.euspa.europa.eu/eu-space-programme/galileo/what-gnss>, accessed: 2024-08-23.
- [9] Navipedia, "GPS Signal Plan," [https://gssc.esa.int/navipedia/index.php/GPS\\_Signal\\_Plan](https://gssc.esa.int/navipedia/index.php/GPS_Signal_Plan), accessed: 2024-08-24.
- [10] R. Ferreira, J. Gaspar, P. Sebastião, and N. Souto, "A Software Defined Radio Based Anti-UAV Mobile System with Jamming and Spoofing Capabilities," *Sensors*, vol. 22, no. 4, p. 1487, 2022.
- [11] D. Drones, "FIX No Fly Zone, won't takeoff, DJI Drones," 2024, accessed: 2024-08-28. [Online]. Available: <https://www.youtube.com/watch?v=nm5YdxXKV3E>.