Interceptação de Comunicação de Drones com HackRF PortaPack H2+: Análise de Contra-Inteligência com GPS Spoofing e Jamming de Sinais

Carlos Henrique*, Daniel Pinheiro†, Francisco Gandala‡, Lucas Arruda§, Pedro Saraiva¶
*carlosbatista@discente.ufg.br, †danpinheiro_o@discente.ufg.br,
‡gandala@discente.ufg.br, §lucas_arruda@discente.ufg.br,
¶pedro.saraiva@discente.ufg.br

***Resumo*—Este trabalho examina as possibilidades de interceptação e neutralização de drones através do uso do dispositivo HackRF PortaPack H2+, focando em técnicas avançadas de contra-inteligência como GPS spoofing e jamming de sinais de controle. Tais métodos permitem explorar e expor vulnerabilidades presentes em drones, especialmente em contextos onde a segurança e a privacidade são comprometidas por atividades não autorizadas. Por meio de experimentos controlados, este estudo avalia a eficácia das técnicas de spoofing e jamming no desvio ou interrupção dos sinais de navegação, contribuindo para a prevenção de riscos em áreas sensíveis.**

***Index Terms*—Drone, HackRF, Fourier, GPS spoofing, Jamming.**

I. Introdução e Revisão Bibliográfica

A. Problema

A crescente acessibilidade e versatilidade dos drones comerciais traz benefícios significativos para diversas áreas, porém, também amplia a exposição a potenciais usos mal-intencionados, como vigilância não autorizada, invasão de privacidade e até mesmo ameaças à segurança pública [4]. Diante dessa realidade, a interceptação de comunicações de drones se apresenta como uma medida de segurança crucial, especialmente em zonas sensíveis. O presente estudo explora como o HackRF PortaPack H2+ pode ser utilizado como uma ferramenta para mitigar tais riscos, aplicando técnicas de GPS spoofing e jamming de sinais de controle. Com isso, busca-se examinar as vulnerabilidades dos sistemas de navegação e controle de drones, destacando as implicações de segurança e privacidade no uso civil de radiofrequência para neutralizar tais dispositivos.

B. Literatura

Diversos estudos têm investigado as vulnerabilidades dos sistemas de drones e as formas de mitigação de riscos associados. Tippenhauer *et al.* [1] analisaram os requisitos para ataques de GPS spoofing, destacando a facilidade de implementação dessas técnicas. Humphreys [2] discutiu os riscos de segurança associados à navegação por satélite em drones civis. Shuai *et al.* [3] exploraram métodos de detecção e prevenção de interferência em drones. Puri [4] apresentou uma visão geral sobre veículos aéreos não tripulados e suas aplicações. Além disso, Baldini *et al.* [5] examinaram o uso de SDRs (Software Defined Radios) para segurança em drones.

C. Dataset

O conjunto de dados utilizado neste estudo inclui sinais de radiofrequência (RF) capturados de drones comerciais operando em contextos controlados. As amostras abrangem frequências de GPS (1,57542 GHz para L1) e sinais de controle típicos utilizados em bandas ISM (2,4 GHz e 5,8 GHz). A coleta de dados foi realizada utilizando o HackRF PortaPack H2+, permitindo uma análise detalhada dos padrões de comunicação e dos efeitos das interferências aplicadas.

D. Métodos

Para a execução dos experimentos, foram implementadas técnicas de GPS spoofing com o objetivo de manipular o sistema de navegação dos drones, desviando sua rota de maneira controlada. Paralelamente, utilizou-se o método de jamming de sinais de controle para bloquear a comunicação entre o operador e o drone, comprometendo sua capacidade de resposta. O HackRF PortaPack H2+ serviu como dispositivo central de interferência, configurado para transmitir sinais específicos capazes de enganar ou sobrecarregar os receptores dos drones.

E. Avaliação

A eficácia das técnicas aplicadas foi medida através de métricas como o tempo de resposta do drone à interferência, a distância de desvio causada pelo GPS spoofing e a taxa de sucesso na interrupção dos sinais de controle. Benchmarks específicos para sistemas de interferência em drones foram utilizados como referência, e matrizes de confusão foram elaboradas para avaliar a precisão e a acurácia dos métodos empregados.

II. Fundamentação Teórica

A manipulação de sinais de radiofrequência (RF) requer um entendimento profundo dos princípios de comunicação

sem fio e processamento de sinais, além de conhecimento dos princípios de funcionamento e comunicação de drones comerciais.

Os drones comerciais utilizam RF entre 2,4 GHz e 5,8 GHz para comunicar com a central de controle (controle remoto) e transferir comandos e informações. Também é utilizado o GPS/GNSS para mapeamento da posição geográfica do drone.

O GPS spoofing baseia-se na transmissão de sinais falsos que imitam os sinais legítimos de satélites GPS, enganando o receptor do drone [1]. Já o jamming de sinais consiste em emitir sinais de interferência na mesma frequência dos sinais de controle, reduzindo a relação sinal-ruído e tornando a comunicação ineficaz [2].

O HackRF PortaPack H2+ é um transceptor SDR capaz de transmitir e receber sinais em uma ampla faixa de frequências (1 MHz a 6 GHz), permitindo a implementação dessas técnicas. O processamento dos sinais coletados e a geração dos sinais de interferência envolvem transformadas de Fourier e modulações específicas, sendo essencial o uso de algoritmos eficientes para garantir a eficácia das operações.

A. Recursos Relevantes

- **Mayhem Firmware no GitHub**: Firmware customizado para o HackRF PortaPack H2+ que amplia suas capacidades [6].
- **GPS-SDR-SIM no GitHub**: Software para gerar arquivos de sinais GPS que podem ser transmitidos pelo HackRF [7].
- **PothosSDR**: Software que permite transmitir arquivos do computador para o HackRF PortaPack [8].
- **Dados GNSS da NASA**: Repositório com arquivos de dados geo-espaciais gerados pela NASA, úteis para gerar sinais GPS precisos [9].
- **Vídeos Explicativos**:
  - https://www.youtube.com/watch?v=n-icyyWVHTUIntrodução ao GPS Spoofing e SDR
  - https://www.youtube.com/watch?v=3NWn5cQM7q4Spoofing GPS na Prática
  - https://www.youtube.com/watch?v=qPhGBFBj4PYExemplos Adicionais de Spoofing

III. Metodologia

A. GPS Spoofing

1) **Preparação do Ambiente**: Baixar o firmware Mayhem no HackRF PortaPack H2+. No computador, instalar o PothosSDR e o GPS-SDR-SIM, além de obter os dados geo-espaciais disponibilizados pela NASA.
2) **Geração do Sinal GPS Falso**: Executar o GPS-SDR-SIM fornecendo a latitude e longitude desejadas para o desvio do GPS e os dados geo-espaciais da NASA. Será gerado um arquivo chamado `gpssim.bin`.
3) **Transmissão do Sinal Spoofing**: Conectar o HackRF PortaPack H2+ ao computador via USB e ativar o modo HackRF. Utilizando o PothosSDR, executar o `hackrf_transfer` com o arquivo `gpssim.bin`. O dispositivo emitirá ondas com a localização escolhida, afetando dispositivos GPS próximos.

B. Wi-Fi Jamming

1) **Análise da Rede Wi-Fi**: Instalar o programa `wavemon` no computador e conectar-se à rede Wi-Fi alvo. Utilizar o `wavemon` para coletar informações como faixa de frequência e largura de banda.
2) **Configuração do HackRF**: Conectar o amplificador ao HackRF antes da antena e sua respectiva fonte de energia. No HackRF, selecionar "Transmit"e depois "Jamming". Carregar as frequências próximas às coletadas pelo `wavemon`.
3) **Execução do Jamming**: Ajustar a frequência exata da rede no campo "Center"e a largura de banda no campo "Width". Iniciar o Wi-Fi jamming pressionando "Start".
4) **Observação dos Efeitos**: Monitorar a queda da rede e o impacto na comunicação do drone.

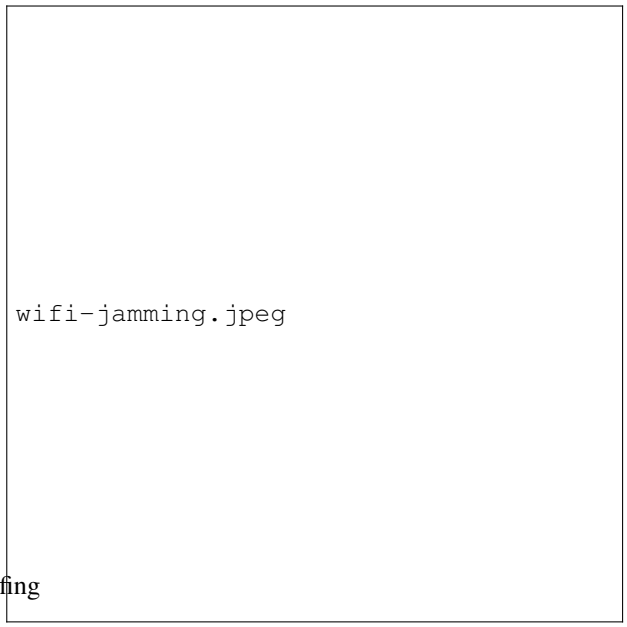

Figura 1. Fluxograma do processo de Wi-Fi Jamming.

IV. Resultados e Conclusões

A. Jamming com Drone Wi-Fi

Utilizou-se um drone Wi-Fi modelo Tello. Foram realizados dois experimentos visando comprometer o funcionamento e a comunicação do drone com o controlador. Em ambos os experimentos, os componentes principais foram: dispositivo de controle, drone e o HackRF (com amplificador e antena).

1) Experimento 1: **Procedimento**: Conectou-se um dispositivo de controle à rede Wi-Fi do drone e executou-se um script de controle autônomo (ver Código A).

```
// script_exp1.py
tello.takeoff()
```

```
for i in range(10):
    tello.move_forward(100)
    sleep(2)
    tello.move_left(100)
    sleep(2)
    tello.move_back(100)
    sleep(2)
    tello.move_right(100)
```

Objetivo: Testar o funcionamento do Wi-Fi jamming e sua efetividade prática.

Resultado Esperado: Paralisação do drone e perda de conexão com o controlador.

Resultados Obtidos:

- **Quantidade de Testes**: 8
- **Quantidade de Sucessos**: 8
- **Taxa de Sucesso**: 100%

Observações: O drone perdeu completamente o controle em todos os testes, confirmando a eficácia do jamming.

2) Experimento 2: **Procedimento**: O drone foi controlado manualmente por um operador enquanto o Wi-Fi jamming era ativado a diferentes distâncias.

Objetivo: Testar o alcance efetivo do Wi-Fi jamming.

Resultados Obtidos:

Tabela I
RESULTADOS DO EXPERIMENTO DE ALCANCE

Distância (metros)	Resultado
5	Perda total do controle
10	Perda total do controle
15	Perda total do controle
20	Perda parcial do controle
25	Pouca ou nenhuma influência

Observações: O jamming foi efetivo até cerca de 20 metros, com perda total do controle do drone até 15 metros.

V. REFERÊNCIAS

REFERÊNCIAS

[1] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Čapkun, "On the requirements for successful GPS spoofing attacks," *Proceedings of the 18th ACM conference on Computer and communications security*, pp. 75–86, 2011.

[2] T. E. Humphreys, "Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing," *Subcommittee on Oversight, Investigations, and Management, US House of Representatives*, 2012.

[3] J. Shuai, J. Wang, and Y. Wang, "Drone remote control jamming and anti-jamming techniques: A review," *IEEE Access*, vol. 6, pp. 19873–19883, 2018.

[4] A. Puri, "A survey of unmanned aerial vehicles (UAV) for traffic surveillance," *Department of Computer Science and Engineering, University of South Florida*, 2005.

[5] G. Baldini, R. Garello, and M. Sterbini, "A survey of techniques for remote control and localization of civilian drones," *IEEE Aerospace and Electronic Systems Magazine*, vol. 32, no. 4, pp. 90–103, 2017.

[6] PortaPack Mayhem Firmware. Disponível em: https://github.com/portapack-mayhem/mayhem-firmware. Acesso em: 05 out. 2023.

[7] GPS-SDR-SIM. Disponível em: https://github.com/osqzss/gps-sdr-sim. Acesso em: 05 out. 2023.

[8] PothosSDR. Disponível em: https://downloads.myriadrf.org/builds/PothosSDR/. Acesso em: 05 out. 2023.

[9] NASA GNSS Data. Disponível em: https://cddis.nasa.gov/archive/gnss/data/daily/2024/brdc/. Acesso em: 05 out. 2023.

APÊNDICE A
CÓDIGO UTILIZADO

```
// script_exp1.py
tello.takeoff()

for i in range(10):
    tello.move_forward(100)
    sleep(2)
    tello.move_left(100)
    sleep(2)
    tello.move_back(100)
    sleep(2)
    tello.move_right(100)
```

APÊNDICE B
VÍDEOS DOS EXPERIMENTOS

Os vídeos dos experimentos estão disponíveis nos seguintes links:

- **Experimento 1**: https://github.com/user-attachments/assets/3188c650-e0a4-4602-9faf-05b1b073d194
- **Experimento 2**: https://github.com/user-attachments/assets/8778b3dc-ce72-46a1-808c-f0a888b8dc92