

# Análise comparativa de métricas de avaliação em modelos de aprendizado de máquina na detecção de ataques de spoofing de GPS

Ana Carla Rodrigues<sup>1</sup>, Jessica Fileto<sup>1</sup>

<sup>1</sup> Centro de Matemática, Computação e Cognição  
Universidade Federal do ABC (UFABC)  
Av. dos Estados, 5001 – 09210-580 – Santo André – SP – Brasil

{carla.rodrigues, jessica.fileto}@ufabc.edu.br

**Resumo.** *O Veículo Aéreo Não Tripulado (VANT), comumente conhecido como drone, é uma plataforma que está revolucionando indústrias ao redor do mundo, oferecendo soluções de alta flexibilidade e riscos reduzidos. O Global Positioning System (GPS) fornece ao VANT navegação precisa, rastreamento e voo autônomo. Os VANTs podem sofrer ataques de spoofing nas coordenadas de GPS, comprometendo a segurança da informação e demonstrando que a precisão na análise dos dados são cruciais na tomada de decisões. A inteligência artificial pode ser uma aliada na detecção destes ataques através de técnicas sofisticadas, reduzindo a quantidade de falsos alarmes e fornecendo informações confiáveis por meio do aprendizado de máquina que exerce papel fundamental na classificação destes ataques. A proposta deste projeto é realizar uma análise comparativa das métricas de avaliação dos seguintes modelos de aprendizado de máquina: Random Forest, Naive Bayes, K-NN, Gaussian Naive Bayes e Extremely Randomized Trees, visando identificar aquele que melhor equilibre a detecção correta de spoofing e viabilidade de implementação do modelo.*

## 1. Introdução

Os veículos aéreos não tripulados (VANTS), também conhecidos como drone, é um tipo de tecnologia fundamental tanto em áreas civis quanto militares. Seu uso reduz a exposição humana a tarefas repetitivas, de longa duração e em alguns casos, de alto risco [Brasil 2025]. Desempenham papel importante nas seguintes áreas: gerenciamento de desastres, vigilância aérea, fotografia aérea de rastreamento, pesquisa e resgate, monitoramento de gado, dentre outros. [Titouna and Naït-Abdesselam 2021]

Por serem operados de maneira autônoma e remota suas coordenadas são essenciais para o sucesso de suas missões, para isso são usados sinais de Sistema Global de Navegação por Satélite (GNSS), sendo o mais conhecido o *Global Positioning System* (GPS), esses sinais podem ser criptografados ou não [de A. Faria1 et al. 2018]. Sendo os não criptografados mais suscetíveis a ataques conhecidos como *Spoofing* de GPS [Srinivasan S and Sathyadevan 2023].

Para garantir um voo seguro do VANT é essencial ter medidas para detecção dos ataques de *Spoofing de GPS*. A identificação precisa desses ataques é extremamente importante, pois técnicas avançadas de *spoofing* podem causar disrupção no funcionamento do VANT, portanto são necessários métodos robustos e adaptativos

[İşleyen and Bahtiyar 2024]. Nesse contexto algoritmos com aprendizado de máquina tem se mostrado promissores, pois são capazes de analisar grandes volumetrias de dados, identificando padrões e anomalias. Tais abordagens oferecem uma resposta robusta e adaptativa a essas ameaças contribuindo para as operações dos VANTs [İşleyen and Bahtiyar 2024].

Diversos estudos recentes tem utilizado essa abordagem para detecção de *spoofing* de GPS. Podemos mencionar algumas abordagens utilizadas:

- **Redes neurais profundas (DNN):** Extração de padrões complexos em séries temporais dos sinais GNSS [İşleyen and Bahtiyar 2024].
- **Máquinas de vetores de suporte (SVM):** Abordagem foi centrada na identificação de discrepâncias entre as posições determinadas pelos sinais de GPS e aquelas medidas pelo sistema de navegação inercial (INS). Especificamente, o modelo SVM foi treinado nos valores de erro gerados a partir dessas diferenças posicionais, permitindo que o sistema detecte inconsistências que poderiam indicar um ataque de *spoofing* de GPS. [Panice et al. 2017]
- **IA Generativa:** Abordagem que em comparação com outros modelos de aprendizagem de máquina, se destacou pela eficácia na detecção dos ataques de *spoofing* e *jamming* [El alami and Rawat 2024].

## 2. Delimitação e Escopo

O *dataset* que será utilizado como base de dados é o *Mendeley Data* [Aissou 2022], esses dados foram gerados de sinais GPS autênticos e contém aproximadamente 500,000 dados que logo serão reduzidos a uma quantidade considerável. Então, os resultados do trabalho ficarão limitados a este *dataset*. De acordo com o artigo de [Aissou et al. 2021], os ataques do tipo *spoofing* podem ser classificados em: simples, intermediários e sofisticados.

Nas próximas seções se estabelecerá a execução do trabalho. Na seção 3, faremos nossa proposta de mudança ao trabalho de [Aissou et al. 2021], discutindo a metodologia e modelos de aprendizado de máquina a serem implementados. Logo, os resultados e discussões serão apresentados na seção 4. Finalmente, nossas conclusões sobre o trabalho serão expostos na seção 5.

## 3. Metodologia (Proposta de mudança)

Para alcançar o objetivo deste estudo, esta seção detalha a abordagem proposta para a classificação de possíveis ataques de *spoofing* a sinais de GPS, avaliando o desempenho dos algoritmos: (i) Naive Bayes, (ii) K-NN, (iii) Extreme Random Forest, (iv) Random Forest e (v) Gaussian Naive Bayes.

A metodologia adotada e os passos seguidos foram inspirados no artigo de [Aissou et al. 2021], com o objetivo de explorar os dados obtidos. Serão analisados a acurácia, precisão e a quantidade de falsos negativos. Para isso a base será dividida em porções diferentes para testes e o treinamento do modelo, sendo 80% para treino e 20% para testes.

E será aplicada a técnica de pré processamento *Principal Component Analysis* (PCA) para melhorar a precisão dos resultados finais, ela consiste em reduzir as dimensões

do dataset para deixar apenas as informações mais importantes, removendo assim as redundâncias [IBM 2025]. Esse tipo de processamento ajuda algoritmos de aprendizagem de máquina, simplificando o processo de reconhecimento dos dados, essa técnica é diferente da usada no artigo de [Aissou et al. 2021] que se chama *Spearman Correlation Coefficient*.

## Referências

- Aissou, G. (2022). A DATASET for GPS Spoofing Detection on Unmanned Aerial System. Mendeley Data, V3.
- Aissou, G., Slimane, H. O., Benouadah, S., and Kaabouch, N. (2021). Tree-based supervised machine learning models for detecting gps spoofing attacks on uas. In *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pages 0649–0653.
- Brasil, D. U. E. (2025). Estudo sobre a indústria brasileira e europeia de veículos aéreos não tripulados. Technical report, Dialogos Uniao Europeia Brasil.
- de A. Faria<sup>1</sup>, L., de Melo Silvestre<sup>1</sup>, C. A., Correia<sup>1</sup>, M. A. F., and Roso, N. A. (2018). Gps jamming signals propagation in free-space, urban and suburban environments. *Journal Aerospace Technology Management*.
- El alami, H. and Rawat, D. B. (2024). DroneDefGANt: A Generative AI-Based Approach for Detecting UAS Attacks and Faults. In *ICC 2024 - IEEE International Conference on Communications*, pages 1933–1938.
- IBM (2025). What is principal component analysis (pca)?
- İşleyen, E. and Bahtiyar, Ş. (2024). GPS Spoofing Detection on Autonomous Vehicles with XGBoost. In *2024 9th International Conference on Computer Science and Engineering (UBMK)*, pages 500–505.
- Panice, G., Luongo, S., Gigante, G., Pascarella, D., Di Benedetto, C., Vozella, A., and Pescapè, A. (2017). A svm-based detection approach for gps spoofing attacks to uav. In *2017 23rd International Conference on Automation and Computing (ICAC)*, pages 1–11.
- Srinivasan S, P. and Sathyadevan, S. (2023). GPS Spoofing Detection in UAV Using Motion Processing Unit. In *2023 11th International Symposium on Digital Forensics and Security (ISDFS)*, pages 1–4.
- Titouna, C. and Naït-Abdesselam, F. (2021). A Lightweight Security Technique For Unmanned Aerial Vehicles Against GPS Spoofing Attack. In *2021 International Wireless Communications and Mobile Computing (IWCMC)*, pages 819–824.