

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

Ana Carla Rodrigues¹, Jessica Fileto¹

¹ 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, Bagged Decision Trees 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. O uso de drones reduzem 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]

Esses sistemas possuem designs versáteis para atender diversas necessidades. Esses dispositivos carregam dados cruciais para seus usuários, devido ao seu longo alcance, para a realização de diversos trabalhos. [Khan et al. 2022].

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]. Sinais militares possuem criptografia, enquanto os que são de uso civil não possuem mecanismos de proteção. Com isso ocorre a extrema vulnerabilidade a diversos tipos de ataques, principalmente os conhecidos como *Spoofing de GPS*. [Srinivasan S and Sathyadevan 2023].

O tipo de ataque analisado nesse artigo é o *spoofing*. Ele é caracterizado por uma técnica de ataque na qual o agressor faz uso de antenas terrestres emitindo sinais falsos de localização [Jafarnia-Jahromi et al. 2012]. Esse tipo de ação pode resultar em: danos materiais e o acesso indevido aos dados do usuário, conforme relatado em diversos incidentes mundialmente. [G1 2022b, G1 2022a, BandNews 2022, Paraná 2022, Veja 2022, Hambling 2020, Aviation 2022]

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 interrupção no funcionamento do VANT. Portanto são necessários métodos robustos e adaptativos. [İşleyen and Bahtiyar 2024]

Algoritmos com aprendizado de máquina tem se mostrado promissores, pois são capazes de analisar dados e detectar anomalias que podem causar interrupção 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 volumes 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, tradução nossa].

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 o *HEAD* contém aproximadamente 500,000 dados, que serão reduzidos a uma quantidade considerável. Portanto, os resultados do trabalho ficarão limitados a este *dataset*. O *8d00d81* (feat: metodologia) 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, os ataques do tipo *spoofing* podem ser classificados em: simples, intermediários e sofisticados. O *8d00d81* (feat: metodologia)

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 30%

para testes. E será aplicada a técnica de pré processamento *Principal Component Analysis* (PCA) para melhorar a precisão dos resultados final, 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].

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.
- Aviation, A. (2022). Electromagnetic interference behind darling harbour drone crash. Disponível em: <https://australianaviation.com.au/2022/06/electromagnetic-interference-behind-darling-harbour-drone-crash/>. Acesso em: 24 jul. 2025.
- BandNews (2022). Cinco acidentes causados por drones são registrados no oeste. Disponível em: <https://bandnewsfmcuitiba.com/cinco-acidentes-causados-por-drones-sao-registrados-no-oeste/>. Acesso em: 24 jul. 2025.
- 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. Faria¹, L., de Melo Silvestre¹, C. A., Correia¹, M. A. F., and Roso, N. A. (2018). Gps jamming signals propagation in free-space, urban and suburban environments. *Journal Aerospaceal Tecnology Managment*.
- G1 (2022a). Drone cai em cima de mulher durante show de luan santana na expogrande. Disponível em: <https://g1.globo.com/pop-arte/noticia/2022/05/02/drone-cai-em-cima-de-mulher-durante-show-de-luan-santana-na-expogrande.ghtml>. Acesso em: 24 jul. 2025.
- G1 (2022b). Mulher é atingida por drone durante show e precisa passar por cirurgia no df. Disponível em: <https://g1.globo.com/df/distrito-federal/noticia/2022/07/26/mulher-e-atingida-por-drone-durante-show-e-precisa-passar-por-cirurgia-no-df.ghtml>.
- Hambling, D. (2020). Investigation finds gps interference caused uk survey drone crash. Disponível em: <https://www.forbes.com/sites/davidhambling/2020/08/10/investigation-finds-gps-interference-caused-uk-survey-drone-crash/?sh=57b389bd534a>. Acesso em: 24 jul. 2025.
- 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.
- Jafarnia-Jahromi, A., Broumandan, A., and Nielsen, J. and Lachapelle, G. (2012). Gps vulnerability to spoofing threats and a review of antispooing techniques. *International Journal of Navigation and Observation*.

- Khan, A., Gupta, S., and Gupta, S. K. (2022). Emerging uav technology for disaster detection, mitigation, response, and preparedness. *Journal of fields robotics*.
- Paraná, B. (2022). Copel registra cinco acidentes com rede elétrica pelo uso de drones pulverizadores no paraná. Disponível em: <https://www.bemparana.com.br/noticias/parana/copel-registra-cinco-acidentes-com-rede-eletrica-pelo-uso-de-drones-pulverizadores-no-parana/>. Acesso em: 24 jul. 2025.
- 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.
- Veja (2022). Drone da fab que ajudava no monitoramento cai no rio grande do sul. Disponível em: <https://veja.abril.com.br/tecnologia/drone-da-fab-que-ajudava-no-monitoramento-cai-no-rio-grande-do-sul/>. Acesso em: 24 jul. 2025.