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

Ana Carla Rodrigues[1], **Jessica Fileto**[1]

[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

Abstract. *Unmanned aerial systems (UAS), commonly known as drones, are transformative platforms that revolutionize industries around the world by offering highly flexible solutions with reduced operational risks. Although the Global Positioning System (GPS) enables precise navigation, tracking, and autonomous flight for UAS, these systems remain vulnerable to GPS spoofing attacks, which compromise data integrity and underscore the critical role of accurate data analysis in decision-making. Artificial intelligence can mitigate such attacks through sophisticated techniques, reducing false alarms and providing reliable threat classification via machine learning. This project proposes a comparative analysis of evaluation metrics in three machine learning models: Random Forest, Bagged Decision Trees and Extremely Randomized Trees, to identify the optimal approach to balance the accuracy of spoofing detection and the feasibility of model implementation.*

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 vôo 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) são conhecidos como aeronaves que operam sem piloto, sendo um tipo de tecnologia essencial em diversas áreas civis e militares. O uso de drones reduzem a exposição humana a tarefas repetitivas, de longa duração e em

alguns casos perigosas [Brasil 2025]. Alguns exemplos de uso são: 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, e para isso existem requerimentos para sua qualidade dentre eles estão: bateria, peso, tamanho e as coordenadas. 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 cumprimento de seus objetivos, 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 um atacante que faz uso de antenas terrestres emitindo sinais falsos de localização com o objetivo de direcionar o dispositivo em direção ao atacante [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]

> Como resultado, garantir a segurança cibernética [...] se tornou uma preocupação crucial [...]. Isso destaca a necessidade de extensas pesquisas na segurança cibernética [...] que se concentram na detecção e prevenção de ataques e falhas. [El alami and Rawat 2024, tradução nossa]

Para garantir um vôo 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]

Segundo Isleyen e Bahtiyar (2024, tradução nossa) “Os algoritmos de aprendizado de máquina podem analisar] grandes volumes de dados para identificar padrões e anomalias sutis que são indicativas de falsificação.”

O *dataset* que será tomado 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*.

Nas próximas seções se estabelecerá a execução do trabalho. Na seção 2, 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 3. Finalmente, nossas conclusões sobre o trabalho serão expostos na seção 4.

2. Metodologia (Proposta de mudança)

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

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://bandnewsfmcuritiba.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 Aerospacial Tecnology Managment*.

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.

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 antispoofing techniques. *International Journal of Navigation and Observation*.

Khan, A., Gupta, S., and Gupt, 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.