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

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, XGBoost, SVM, 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 drones, são 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 e 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 [A. Faria1 et al. 2018]. Sendo os não criptografados mais suscetíveis a ataques conhecidos como *Spoofing* de GPS [Srinivasan S e Sathyadevan 2023].

O ataque de *spoofing* de GPS é caracterizado por um atacante que faz uso de antenas terrestres emitindo sinais falsos. [Jafarnia-Jahromi, Broumandan e Nielsen 2012] Estes ataques são classificados em: simples, intermediários e sofisticados [Aissou et al. 2021].

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 sofisticadas de *spoofing* podem causar disrupção no funcionamento do VANT, portanto são necessários métodos robustos e adaptativos [İşleyen e Bahtiyar 2024]. Nesse contexto algoritmos de 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 e Bahtiyar 2024].

Neste trabalho será feita a reimplementação dos algoritmos *RandomForest* e *XGBoost* e seus respectivos experimentos do artigo [Aissou et al. 2021], com o objetivo de comparar esses algoritmos com outros que não são baseados em árvore, sendo eles: *Support Vector Machines* (SVM), *K-NN*, *Gaussian Naive Bayes* e *Extremely Randomized Trees*.

2. Trabalhos relacionados

Diversos estudos recentes tem utilizado aprendizado de máquina para detecção de ataques de *spoofing* de GPS. Podemos mencionar algumas abordagens utilizadas:

- **Redes neurais profundas (DNN):** Extração de padrões complexos em séries temporais dos sinais GNSS. [İşleyen e Bahtiyar 2024]
- **Máquinas de vetores de suporte (SVM):**
  Abordagem teve como objetivo a 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 através dos erros obtidos das diferenças posicionais, permitindo que o sistema detecte inconsistências que poderiam indicar um ataque de *spoofing* de GPS. [Panice et al. 2017]
- **Redes neurais convolucionais (CNN):** Em comparação aos modelos tradicionais de aprendizagem de máquina, os de aprendizagem profunda obtiveram alta acurácia na detecção dos ataques de *spoofing*. A grande vantagem desses modelos baseados em aprendizagem profunda, é pelo fato de aprenderem automaticamente a extraírem as *features* sem precisarem de intervenção humana. Além de se adaptarem melhor a *datasets* mais complexos. [Sun et al. 2023]
- **Aprendizagem supervisionada (Baseado em Árvores):** Aissou et al. (2021) utilizou os seguintes modelos baseados em árvores: Random Forest, Gradient Boost, XGBoost e LightGBM para fazer um comparativo de qual seria melhor na detecção dos ataques de *spoofing* de GPS. Sendo que o XGBoost obteve a melhor acurácia (95,52%).
- **IA Generativa:** Abordagem que em comparação com outros modelos de aprendizagem de máquina, se destacou pela eficácia na deteção dos ataques de *spoofing* e *jamming*. [El alami e Rawat 2024]

3. Delimitação e Escopo

O artigo [Aissou et al. 2021] não cita o *dataset* usado para o treinamento dos modelos, então para as análises decorrentes deste artigo será utilizado o *Mendeley Data* [Aissou 2022], que foi disponibilizado pelos autores do artigo. Esse *dataset* é uma versão simplificada, pois é representada em duas dimensões. Esses dados foram gerados de sinais GPS autênticos e contém aproximadamente 500,000 dados.

Nas próximas seções se estabelecerá a execução do trabalho. Na seção 4, 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 5. Finalmente, nossas conclusões sobre o trabalho serão expostos na seção 6.

4. Metodologia

A metodologia adotada e os passos seguidos foram inspirados no artigo de [Aissou et al. 2021], que implementou os algoritmos baseados em árvore: *Random Forest*, *Gradient Boost*, *XGBoost*, e *LightGBM* com o objetivo de explorar os dados obtidos.

Será realizada a reimplementação dos algoritmos (i) *Random Forest* e (ii) *XGBoost*, ambos obtiveram o pior e melhor desempenho, respectivamente, ponderando as métricas de tempo de execução e uso de memória, no comparativo dos modelos baseados em árvore. Ambos algoritmos serão comparados com outros modelos que não são baseados em árvore, sendo eles: (iii) SVM, (iv) *K-NN* e (v) *Gaussian Naive Bayes*.

Será incluído o modelo baseado em árvore conhecido como (vi) *Extremely randomized trees* que é um modelo melhorado do *Random Forest*, que se difere pelo fato que no *Extremely randomized trees* não existe a fase de *bagging* e no momento da separação dos nós, esta escolha é feita aleatoriamente [Geurts, Ernst e Wehenkel 2006].

Será feita a análise comparativa entre os algoritmos baseados em árvore e os demais algoritmos, com o objetivo de identificar aquele que melhor equilibre a detecção correta de *spoofing* e viabilidade de implementação do modelo. Também ocorrerá a análise entre os modelos baseados em árvore para averiguar se o *Extremely Randomized Trees* obtém um desempenho melhor que o *Random Forest*. O algoritmo *XGBoost* será mantido, pois obteve o melhor desempenho no artigo de [Aissou et al. 2021]. Portanto ele será usado como base para comparação com os demais algoritmos.

Para a avaliação do desempenho dos modelos será utilizada a biblioteca *PyCM* do Python, que é uma biblioteca de matriz de confusão multiclasse, que implementa diversas métricas de classificação. [Haghighi et al. 2018]

Serão analisadas a acurácia, precisão e a quantidade de falsos negativos. Além disso, será feita a análise do tempo de treinamento, predição e uso de memória de cada modelo, com o objetivo de identificar o mais viável para implementação em VANTs.

4.1. Divisão dos dados

A base será dividida em porções diferentes para testes e o treinamento do modelo, sendo 70% para treino e 30% para testes conforme realizado no artigo. [Aissou et al. 2021]

4.2. Matthews Correlation Coefficient (MCC)

O *Matthews Correlation Coefficient* (MCC) é uma métrica de avaliação de modelos de classificação binária, que posteriormente foi extrapolada para classificação multiclasse. [Jurman, Riccadonna e Furlanello 2012]

Neste trabalho será utilizado o MCC, juntamente com a acurácia para avaliar a eficácia dos modelos de aprendizado de máquina na detecção de ataques de *spoofing* de GPS.

4.3. Pré-Processamento dos dados

Será aplicada a técnica de pré processamento *Principal Component Analysis* (PCA) para melhorar a precisão dos resultados finais. Ela consiste em reduzir a dimensão do dataset para deixar apenas as informações mais relevantes, removendo assim as redundâncias [Zhang 2019]. Assim como serão utilizadas outras duas técnicas adicionais conhecidas como *Standard Scaler* para melhorar o desempenho do processamento [de Amorim, Cavalcanti e Cruz 2023] e o *Random Under Sampler* para reduzir o desbalanceamento das classes que dificultam o treinamento e a análise dos dados [de Amorim, Cavalcanti e Cruz 2023]. Essas técnicas são diferentes da usada no artigo de [Aissou et al. 2021] que se chama *Spearman Correlation Coefficient*.

4.4. Análise do desempenho

Para análisar a eficácia do algoritmo através dos dados disponíveis é necessário avaliar os comportamentos dos modelos e para isso serão utilizadas as seguintes métricas: (i) probabilidade de detecção, (ii) acurácia, (iii) probabilidade de detecção falsa, (iv) probabilidade de alarme falso, (v) taxa de erro, (vi) coeficiente MCC, (vii) F1 score, (viii) especificidade.

5. Resultados e discussões

Com base nos dados da Tabela 1 podemos avaliar o desempenho dos algoritmos utilizados para classificar ataques de *spoofing* aos VANTS.

5.1. Probabilidade de detecção

5.2. Acurácia

5.3. Probabilidade de detecção falsa

5.4. Probabilidade de alarme falso

5.5. Taxa de erro

5.6. Coeficiente MCC

5.7. F1 score

5.8. Especificidade

6. Conclusão

Referências

A. Faria1, Lester de et al. (2018). "GPS Jamming Signals Propagation in Free-Space, Urban and Suburban Environments". Em: *Journal Aerospacial Tecnology Managment*. DOI: 10.5028/jatm.v10.870.

Aissou, Ghilas (2022). *A DATASET for GPS Spoofing Detection on Unmanned Aerial System*. Mendeley Data, V3. DOI: 10.17632/z7dj3yyzt8.3.

Aissou, Ghilas et al. (2021). "Tree-based Supervised Machine Learning Models For Detecting GPS Spoofing Attacks on UAS". Em: *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pp. 0649–0653. DOI: 10.1109/UEMCON53757.2021.9666744.

Brasil, Dialogos Uniao Europeia (2025). *Estudo sobre a Indústria Brasileira e Europeia de Veículos aéreos não tripulados*. Rel. técn. Dialogos Uniao Europeia Brasil. DOI: https://www.gov.br/mdic/pt-br/images/publicacaoa_DRONES-20161130-20012017-web.pdf.

de Amorim, Lucas B.V., George D.C. Cavalcanti e Rafael M.O. Cruz (2023). "The choice of scaling technique matters for classification performance". Em: *Applied Soft Computing* 133, p. 109924. ISSN: 1568-4946. DOI: https://doi.org/10.1016/j.asoc.2022.109924. URL: https://www.sciencedirect.com/science/article/pii/S1568494622009735.

El alami, Hassan e Danda B. Rawat (2024). "DroneDefGANt: A Generative AI-Based Approach for Detecting UAS Attacks and Faults". Em: *ICC 2024 - IEEE International Conference on Communications*, pp. 1933–1938. DOI: 10.1109/ICC51166.2024.10622524. (Acesso em 23/07/2025).

Geurts, Pierre, Damien Ernst e Louis Wehenkel (2006). "Extremely Randomized Trees". Em: *Machine Learning* 63.1, pp. 3–42. ISSN: 0885-6125, 1573-0565. DOI: 10.1007/s10994-006-6226-1. URL: http://link.springer.com/10.1007/s10994-006-6226-1 (acesso em 06/08/2025).

Haghighi, Sepand et al. (2018). "PyCM: Multiclass confusion matrix library in Python". Em: *Journal of Open Source Software* 3.25, p. 729. DOI: 10.21105/joss.00729. URL: https://doi.org/10.21105/joss.00729.

İşleyen, Emre e Şerif Bahtiyar (2024). "GPS Spoofing Detection on Autonomous Vehicles with XGBoost". Em: *2024 9th International Conference on Computer Science and Engineering (UBMK)*, pp. 500–505. DOI: 10.1109/UBMK63289.2024.10773593. (Acesso em 23/07/2025).

Jafarnia-Jahromi, Ali, Ali Broumandan e Gérard Nielsen J.and Lachapelle (2012). "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques". Em: *International Journal of Navigation and Observation*. DOI: 10.1155/2012/127072.

Jurman, Giuseppe, Samantha Riccadonna e Cesare Furlanello (2012). "A Comparison of MCC and CEN Error Measures in Multi-Class Prediction". Em: *PLOS ONE* 7.8, pp. 1–8. DOI: 10.1371/journal.pone.0041882. URL: https://doi.org/10.1371/journal.pone.0041882.

Panice, G. et al. (2017). "A SVM-based detection approach for GPS spoofing attacks to UAV". Em: *2017 23rd International Conference on Automation and Computing (ICAC)*, pp. 1–11. DOI: 10.23919/IConAC.2017.8081999.

Srinivasan S, Prasanna e Shiju Sathyadevan (2023). "GPS Spoofing Detection in UAV Using Motion Processing Unit". Em: *2023 11th International Symposium on Digital Forensics and Security (ISDFS)*, pp. 1–4. DOI: 10.1109/ISDFS58141.2023.10131729. (Acesso em 23/07/2025).

Sun, Yichen et al. (2023). "A Deep-Learning-Based GPS Signal Spoofing Detection Method for Small UAVs". Em: *Drones* 7.6. ISSN: 2504-446X. DOI: 10.3390/drones7060370. URL: https://www.mdpi.com/2504-446X/7/6/370.

Titouna, Chafiq e Farid Naït-Abdesselam (2021). "A Lightweight Security Technique For Unmanned Aerial Vehicles Against GPS Spoofing Attack". Em: *2021 International Wireless Communications and Mobile Computing (IWCMC)*, pp. 819–824. DOI: 10.1109/IWCMC51323.2021.9498734. (Acesso em 23/07/2025).

Zhang, Jason Y. (2019). “Machine Learning With Feature Selection Using Principal Component Analysis for Malware Detection: A Case Study”. Em: *ArXiv* abs/1902.03639. URL: https://api.semanticscholar.org/CorpusID:60440676.