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], **Jhossett Longobardi**[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,stalinn.longobardi}@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

2. Justificativa

Os veículos aéreos não tripulados (VANTs), popularmente conhecidos como drones são amplamente utilizados, tanto no âmbito civil, quanto no militar. [Capitán et al. 2019]

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]

O GPS é o que torna os VANTs autônomos e capazes de concluir de maneira automatizada as diferentes tarefas a que são atribuídos. Estas informações são cruciais para seu desempenho e locomoção correta. A comunicação dos VANTs civis, diferente dos militares, utiliza comunicação desencriptada e não autenticada. Como este dispositivo depende primariamente de dados de localização de GPS, ele fica extremamente vulnerável a diversos tipos de ataques, principalmente os conhecidos como *Spoofing de GPS*. [Srinivasan S and Sathyadevan 2023, Titouna and Naït-Abdesselam 2021]

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

3. Objetivos

O *dataset* foi tomado da base de dados do *Mendeley Data* [Aissou 2022]; esses dados foram gerados de sinais GPS autenticas e contem aproximadamente 500,000 dados. Então, os resultados do trabalho ficam limitados à esse *dataset*.

Nas proximas seções se estabelece a execução do trabalho. Na seção 2, fazemos nossa proposta de mudança ao trabalho de [Aissou et al. 2021], discutindo a metodologia e modelos de aprendizado de maquina a serem implementados. Logo, os resultados e discusões são apresentados na seção 3. Finalmente, nossas conclusões sobre o trabalho são expostas na seção 4.

4. Proposta de mudança (Metodologia)

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.

5. Proposta de mudança (Metodologia)

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.

Capitán, C., Castaño, Á. R., Capitán, J., and Ollero, A. (2019). A framework to handle threats for UAS operating in the U-space. In *2019 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED UAS)*, pages 1–8.

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.

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.