Detecting Spoofing and GPS Jamming in UAVs: Multiclass Approach to Attack Diagnosis

Isadora Garcia Ferrão
University of São Paulo
isadoraferrao@usp.br

Leandro Marcos da Silva
University of São Paulo
leandro.marcos@usp.br

Daniel Bonilla
Czech Technical University
bonildan@fel.cvut.cz

David Espes
Université de Bretagne Occidentale
david.espes@univ-brest.fr

Catherine Dezan
Université de Bretagne Occidentale
dezan@univ-brest.fr

Kalinka Castelo Branco
University of São Paulo
kalinka@icmc.usp.br

Abstract

As Unmanned Aerial Vehicles (UAVs) become increasingly popular and affordable, it is essential to ensure their safe operation, especially around critical devices such as the aircraft's Global Positioning System (GPS). GPS plays an indispensable role in aviation systems. This study presents an efficient multiclass detection method to identify GPS attacks on UAVs, focusing on differentiating between spoofing and jamming attacks. The proposed approach outperforms existing methods. The results obtained in this study contribute to increasing the security of UAVs and provide valuable information for developing robust detection systems to combat evolving threats in the UAV domain.

Keywords: Smart Detection, Unmanned Aerial Vehicles, Detection Attacks, GPS Attacks, Security Failure.

1. Introduction

In recent years, there has been exponential growth in the Unmanned Aerial Vehicle (UAV) market, driven by the emergence of several innovative technologies (Li et al., 2019). These technological advances have been instrumental in driving profitability, reducing bottlenecks in business processes, and driving growth in the UAV market.

With the persistent increase in the use of UAVs in various applications and knowing the seriousness that a single failure can cause, it is crucial to protect these aircraft from external threats that could compromise their integrity and operations. UAVs often operate over wireless networks such as Wi-Fi or cellular networks, and just like any connected device, UAVs have vulnerabilities in their software or firmware (Dey et al., 2018). Hackers can exploit these vulnerabilities to compromise the security of the UAV or the network it is connected to. Several threats can be faced, such as signal interference, physical obstructions, attempted cyber attacks, network congestion, or interference from nearby devices. Furthermore, UAVs connected to the network can be targeted by hackers seeking unauthorized access to control the UAV or obtain confidential information transmitted over the network (Yaacoub et al., 2020).

One of the most essential parts of a UAV is its Global Positioning System (GPS) (Perez-Grau et al., 2018). Despite the widespread use of GPS, the system is not secure (Ferrão, da Silva, et al., 2020; Ferrão, Pigatto, et al., 2020). The civilian signal is not encrypted, meaning anyone can disguise and tamper with GPS signals to achieve their goals. UAVs are very vulnerable to GPS spoofing attacks, in which the attacker sends a more powerful signal than the legitimate signal so that the UAV's GPS signal receiver locks onto the malicious forged GPS signal. Exploit a GPS vulnerability on a UAV is relatively easy, given the nature of these positioning systems (Ferrão, da Silva, et al., 2020; Ferrão, n.d.). An attacker with proper technical knowledge can disrupt the GPS signals, causing the UAV to receive false location information.

In this context, we propose a multiclass detection of GPS attacks on UAVs. Our method is highly efficient in detecting GPS spoofing and jamming attacks, and shows promising results, especially compared to other jamming and spoofing detection mechanisms available in the literature. The results demonstrated that our solution works best using a large dataset, trained on a small fraction corresponding to the usual UAV flight strategies and the troubled flight.

URI: https://hdl.handle.net/10125/106440
978-0-9981331-7-1

1.1. Our contribution

This study presents the development of an advanced multiclass detection method to address the growing concerns surrounding GPS attacks on UAVs. Unlike existing methods, which often focus on single-class detection or use traditional machine learning models in isolation, this study presents a comprehensive approach that combines several well-established machine learning algorithms to accurately differentiate between two types of GPS attacks, such as spoofing and jamming. By harnessing the synergistic power of different models, the proposed method achieves improved levels of accuracy and precision, outperforming previous techniques in the same problem domain. In addition, we can synthesize this work with three main contributions to the scientific community:

- Development of an efficient multiclass approach for detecting GPS attacks on UAVs, where our detection approach can differentiate and identify spoofing and jamming attacks;
- Share the dataset and information processing to be reproduced and compared by the scientific community;
- Compared to existing mechanisms, the results showed that the proposed outperforms other jamming and spoofing detection mechanisms found in the literature.

The rest of this text is organized as follows. In Section 3, related works are presented. In Section 2, the background of this study is presented, as well as the main stages of development is presented in the Section 4. In Section 5, the main results obtained are presented. In Section 6, it is possible to visualize the conclusions of the tests, and finally, in Section 7, the general conclusions of this study are presented.

2. Background

GPS spoofing is considered one of the most recurring threats to UAVs (Ferrão, da Silva, et al., 2020). The principle behind the GPS spoofing attack is sending fake UAV geographic coordinates to the control system. This procedure tricks the aircraft's system into believing it is in a different location than its actual position. As a result, it is possible to hijack the vehicle or gain complete access to its system (Ferrão, da Silva, et al., 2020). There are GPS spoofers that create false GPS signals to trick receivers into thinking that they are in a different location or at other times. For example, the spoofer described in (FakeGPS, 2020), an application for Android phones that falsifies the position by rewriting the location. In this case, the Fake GPS Location app is used to analyze whether the aircraft was vulnerable to this attack and to collect data from the UAV for the following two tests, computer simulations. This scenario is illustrated in Figure 1.

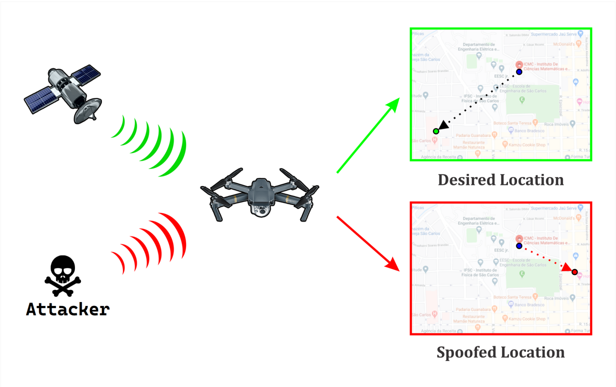

Figure 1. GPS spoofing attack.

GPS jamming is a form of attack that compromises GPS by purposely transmitting jamming signals in the same frequency spectrum used by GPS satellites to send their positioning signals. These jamming signals are designed to be more powerful than legitimate GPS signals, causing GPS receivers to be unable to decode the legitimate GPS signal. This scenario is illustrated in Figure 2.

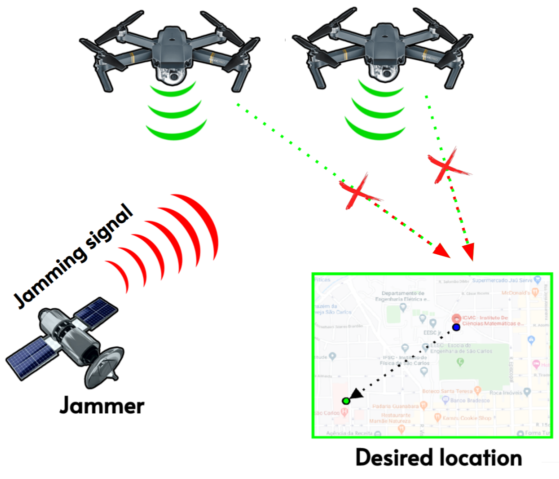

Figure 2. GPS jamming attack.

In jamming, different practices are used to carry out the attack, including using specific devices known as GPS jammers, responsible for radiating high-power interference signals at frequencies close to those used by GPS. Successful jamming can seriously compromise the operational capability of a UAV, from a temporary decrease in positioning quality to a complete loss of signal, resulting in loss of control.

3. Related works

The ability of an avionics architecture to automatically detect imminent aircraft failure at an early stage, where costly and possibly catastrophic system failures can be avoided, provides greater vehicle reliability (Ferrão et al., 2023). Detecting and correcting GPS failures or attacks in advance is essential to ensure the integrity of the UAV, as if a GPS attack is successful, it can induce the UAV to receive false location information, resulting in route deviations, collisions, or even in the total loss of control of the UAV.

The techniques for detecting GPS attacks on UAVs in the literature are focused on identifying and mitigating the effects of attacks that aim to compromise the accuracy and reliability of GPS systems on UAVs. In (Titouna et al., 2020), the authors propose an anomaly-based detection approach, which compares GPS data with a model of expected behavior. One of the strengths of this type of detection is its design to operate in real-time, allowing immediate detection of faults during UAV operations. However, this technique has issues with dependency. If the training data is insufficient or does not adequately represent all possible failures, the algorithm's ability to detect these failures is compromised.

In (Liu et al., 2022), the authors use the Kalman filter method to estimate the actual position of the UAV based on data from GPS and other sensors. This allowed the detection of discrepancies between the GPS information and the position the filter estimated, indicating possible attacks. The authors obtained good results, mainly in efficiently filtering out noisy information. This allowed the detection to be faster and more accurate when compared to other techniques. Despite the promising results obtained by the authors, the performance of the Kalman filter depends on a precise mathematical model of the system. If the model is incorrect or incomplete, the filter may not be able to detect failures correctly. Furthermore, the Kalman filter is more suitable for detecting faults that can be modeled and estimated using linear equations. More complex failures, which involve non-linear relationships or depend on external factors that are difficult to model, may not be easily detected by the Kalman filter.

Encryption and authentication are also considered GPS and vehicle (Zhi et al., 2020) protection measures. These techniques aim to guarantee the authenticity and integrity of the GPS signals, avoiding the interference of false or unauthorized signals (Sharma et al., 2019). However, these techniques are currently not widely used on UAVs because of the complexity and cost associated with implementing encryption systems on UAVs. Encryption requires solid cryptographic algorithms, keys, and secure communication protocols. Integrating these elements into a UAV system can require significant resources in terms of hardware, software, and cybersecurity expertise. Furthermore, encryption introduces computational overhead, which can affect the performance and efficiency of UAVs, especially those with limited computational resources (Khan et al., 2021). In addition, implementing encryption techniques on UAVs requires adopting security standards and coordinating with other methods to ensure compatibility and secure communication. This can be challenging, especially in scenarios where different organizations or agencies operate UAVs with different levels of security and encryption.

Machine learning is the technique that has received the most effort from researchers for GPS fault detection UAVs. According to (Cohen et al., 2021), machine learning and artificial intelligence provide more accurate self-diagnostics to help anticipate a problem and report it before an error is noticed, as well as provide recommendations for repairs and thus reduce costs. Furthermore, according to (Cohen et al., 2021), data analytics and predictive maintenance allow you to detect a failure long before it occurs and provide recommendations to ensure repairs are carried out when needed, resulting in less downtime and reduced operating costs.

In some works found in the literature (Aissou et al., 2021), the authors use a technique with supervised learning algorithms to distinguish between genuine GPS signals and falsified or interfered signals. These classifiers are trained on labeled data, where it is known whether the GPS signal is legitimate or the result of an attack. Based on this training, the classifier can classify new GPS signals and identify whether they are reliable or suspicious. However, most authors only consider an attack or a specific GPS problem. When dealing with GPS attacks, it is essential to have a system that can recognize both known and emerging and unknown attacks, considering different types of possible attacks.

4. Method development stages

In this section, we explore GPS attacks in detail and how they can compromise the security of UAVs. Additionally, we discuss using machine learning algorithms as an effective approach to detecting these attacks. We will also present the process we implemented, highlighting its steps and methodology.

For this study, we used a multiclass system to detect GPS attacks on UAVs. These vehicles are exposed to an environment with several factors that can create vulnerabilities and possible intrusions, allowing unauthorized access by malicious people. Therefore, it is essential to detect different types of problems. Our system can identify and differentiate two main classes of UAV attacks: GPS spoofing and jamming.

Therefore, we present an intelligent method of detecting GPS attacks on UAVs using a multiclass system. Six stages are necessary to develop such a system: (1) Identify the type of attack to be detected and the types of attacks related to this failure; (2) Determine the dataset; (3) Pre-process the dataset; (4) Select the machine learning models; (5) Define the evaluation metrics; and (6) Train the model.

4.1. Stage 01: Identify the type of failure

Due to the significance and frequency of attacks that affect GPS systems, our research focused on detecting these attacks. The main objective of this study was to create an intelligent detection system capable of identifying and signaling the occurrence of attacks that affect GPS systems. In this regard, GPS spoofing and jamming are the most common attacks targeting UAVs. Therefore, the validation of our system was carried out through tests of spoofing attacks and jamming.

4.2. Stage 02: Dataset

For test, we used a dataset that contains a wide range of representative attacks that can be targeted at UAVs, including GPS spoofing attacks, GPS jamming, and other types of cyberattacks. The data contained in the database covers several categories, such as communication signals, control information, images captured by UAVs, data from onboard sensors, and other relevant metadata (Whelan et al., 2020).

The database contains information about the communication signals exchanged between the UAV and the controller, such as frequency data, amplitude, modulation, and other parameters related to data transmission. In addition, information about the control commands sent to the UAV, such as speed, altitude, and heading information, is recorded. Different data on images and videos are also available to provide valuable visual information about the behavior of the UAV, its trajectory, and selected targets, among other details. Among the sensor data, data from the position, inertial sensors, and proximity sensors, among others, are recorded. Finally, in addition to raw data, the database includes metadata such as the datetime of the attack, geographic location, and weather conditions.

Furthermore, data were collected in controlled environments, where different types of attacks were tested to provide a realistic representation of the threats faced by UAVs in the real world.

The dataset used in this study consists of logs from a benign flight and logs with GPS spoofing and jamming. Keysight's EXG N5172B signal generator was used to provide actual coordinates as a location in Shanghai, China. Jamming was done by transmitting white Gaussian noise using HackRF, with an amplitude of 0.3 and a gain of -48dB. For GPS spoofing, a Great Scott Gadgets HackRF software-defined radio was used with the GPS-SDR-SIM tool (https://github.com/osqzss/GPS-sdr-sim) to broadcast 30.286502, 120.032669. Our tests consisted of 1 UAV, 6,078 samples of benign flights, 498 samples with GPS spoofing attacks, and 1,460 with jamming attacks.

During the training of the detection module, two different types of data were used, namely flights with and without failures. Failed flights comprised the following characteristics: Minimum flight duration: 62.0 seconds; Average flight duration: 114.4 seconds; Average flight time: 116.0 seconds; and Maximum flight duration: 156.0 seconds. Flawless flights were constructed with the following information: Minimum flight duration: 26.0 seconds; Average flight duration: 55.3 seconds; Average flight duration: 57.0 seconds; and Maximum flight duration: 89.0 seconds.

We separate the dependent features from the independent variables, i.e., the variables we will use to predict the dependent variables. We then split the data into a training and test set. The training set was used to train the model, while the test set was used to evaluate the model's performance.

4.3. Stage 03: Pre-process the dataset

Data organization was crucial in building our UAV detection multiclass system, as we ensured the data was clean and correctly organized before applying machine learning algorithms.

First, the dataset was organized through the Google Colab (Bisong and Bisong, 2019) platform. Colab is a convenient platform for importing datasets, training classifiers, and evaluating models. The platform allows users to run code on Google's cloud servers, providing access to powerful hardware such as Graphics Processing Units (GPUs) and Tensor Processing Units (TPUs), regardless of the user's machine specifications. This feature allows for more efficient and effective processing of large datasets and complex machine learning models.

Second, the dataset cleaning and pre-processing process was carried out. Raw data that contained missing information, inconsistencies, or redundancies that could affect the performance of our model were cleaned up. This included removing unnecessary columns, filling in missing values, fixing inconsistencies, and normalizing values. When addressing missing values, records with incomplete or missing attributes were examined. A systematic approach was adopted, involving statistical techniques such as mean imputation for continuous features and mode imputation for categorical attributes. The specifics of this process resulted in the successful recovery of a substantial proportion of the dataset, minimizing the impact of missing values. Quantitatively, this pre-processing step led to the removal of approximately 5% of incomplete records, resulting in a cleaner and more comprehensive dataset. Furthermore, the feature selection process led to removing redundant attributes, streamlining the input space for subsequent modeling phases. Regarding feature selection, a judicious strategy was employed to increase model efficiency by removing redundant or irrelevant attributes. This step involved carefully considering domain knowledge and techniques such as correlation analysis to determine feature relevance.

Third, an imbalance between the classes was observed. This could lead to a biased detection model and compromise its effectiveness. As referenced in the (Tran et al., 2022) study, the oversampling technique involved increasing the number of samples in the minority class (attacks) by replicating the existing samples. This means that the minority class samples were duplicated so that the minority class had a more significant number of samples similar to the majority class (benign flight). This oversampling technique helped to even out the class imbalance and allowed the model to train in a more balanced way. In addition, the undersampling technique was also considered, as mentioned in the study (Freeman et al., 2012). This technique involves randomly reducing the number of samples from the majority class to make it more balanced against the minority class. However, according to the results obtained, this technique was less effective than oversampling and was not used during the training of the final model.

4.4. Stage 04: Machine learning models

A comprehensive evaluation was performed in selecting appropriate machine learning models, considering several criteria to ensure the most effective choices. We considered performance features, effectiveness, interpretability, training and test speed, and capacity to handle eclectic data types during model choice. To ensure the best possible results, we initially chose a set of algorithms, including Support Vector Machine (SVM) (Noble, 2006), Multi-Layer Perceptron (MLP) (Taud and Mas, 2018), Decision Tree (DT) (Osei-Bryson, 2004), Random Forest (RF) (Segal and Xiao, 2011), and Gradient Boosting (GB) (Guelman, 2012). These algorithms have a well-established reputation for their usefulness in classification and anomaly detection tasks in different domains. Likewise, they demonstrated strong performance on datasets with many attributes and dimensions.

In addition to the algorithms above, we incorporated two advanced techniques: Extreme Gradient Boosting (XGBoost) (T. Chen et al., 2015), and Light Gradient Boosting Machine (LGBM) (Su, 2020). These newer variants of gradient boosting algorithms are particularly notable due to their faster training speed and improved efficiency when dealing with large-scale datasets that contain a substantial volume of records. This quality aligns with the demands of UAV GPS attack detection, where the ability to process vast datasets efficiently is crucial.

By incorporating this diverse range of algorithms, we intend to leverage their unique strengths and capabilities to optimize GPS attack detection. Each algorithm contributes advantages, such as improved accuracy, adaptability to different data types, and handling complex patterns and relationships in the dataset. Collectively, the selection process considered a wide range of factors, emphasizing not only performance but also the ability of the algorithms to seamlessly handle the complexities of detecting GPS attacks on UAVs.

4.5. Stage 05: Evaluation metrics of the classifier

The evaluation metrics of the classifier stage are essential to ensure that the UAV attack detection system is evaluated properly and effectively. For this, we selected metrics that can provide an overview of our method's performance and helped identify possible areas for improvement. The chosen metrics were: Accuracy (P. Chen et al., 2021); Processing Time; Precision (Goutte and Gaussier, 2005); Recall (Yacouby and Axman, 2020); and F1-score (Goutte and Gaussier, 2005). The weighted average was also considered for each algorithm (Emrouznejad and Marra, 2014).

Precision was determined as it provides a general measure of the model's correctness in identifying positive and negative instances. In the context of UAV attack detection, accurately identifying attacks, including spoofing and jamming, is paramount to ensure the security and integrity of UAV operations. Training time was also determined to measure how quickly a model is ready to detect threats. Therefore, measuring the time spent by each algorithm provides insights into its computational efficiency, aiding in the selection of models that can quickly analyze incoming data streams and make decisions timely. Accuracy is highly relevant in the domain of UAV attack detection. It quantifies the proportion of correctly identified attacks among all instances predicted to be attacks. High accuracy is crucial to avoid false positives, as misidentifying benign flights as attacks can lead to unnecessary interruptions or interventions, impacting UAV operations. Recall was also determined to be an essential metric to identify the proportion of real attacks correctly detected by the model. In the context of UAVs, a high recall rate is crucial to ensure that real attacks are not missed, minimizing the risk of UAVs being compromised by malicious activity. The F1-score balances accuracy and recall, making it a comprehensive metric for evaluating model performance. As detecting UAV attacks requires accurate identification and a minimum of false negatives, the F1-score is a valuable indicator of a model's ability to maintain this balance. Finally, the weighted average was determined by considering the overall performance of each algorithm, accounting for the impact of different metrics. This is especially important in the UAV domain, where achieving a complete detection system requires a holistic perspective that incorporates multiple aspects of performance.

4.6. Stage 06: Train the model

A crucial consideration worth mentioning is adopting the multiclass approach in our method. In this sense, our tests contemplated scenarios involving GPS spoofing and jamming, and benign flights. The intention was to verify that the system could identify irregularities and properly differentiate and classify the type of attack detected.

During the training stage, we feed the system a part of the dataset to learn to recognize patterns and features of the different attacks. Then, during the test stage, we used another piece of data to assess the system's ability to detect GPS attacks accurately.

The K-fold validation, a widely used technique for evaluating the effectiveness of machine learning models on datasets, was implemented. This technique is advantageous when evaluating a model's generalizability on new data, as it involves dividing the dataset into k folds, with each fold being used once as a test set and the others $k-1$ folds being used as a training set (Raschka, 2018). The k-fold was used in our system to evaluate the model's effectiveness in detecting different types of UAV attacks after balancing the classes. The dataset was divided into 10 folds, with 9 for training and the remaining fold for test. This division was repeated 10 times, with each fold being used as a test set once. The k-fold can be described in Equation 1, where k is the number of folds, L_i is the performance metric, e.g., accuracy, precision, or recall, calculated for the fold i, and the average is taken over the k folds.

$$k - fold = \frac{1}{k} \sum_{i=1}^{k} L(i) \tag{1}$$

The dataset used in this study provides various attack scenarios, allowing our system to be tested under realistic and challenging conditions. The results of this stage will be detailed in the results section of this study, where evaluation metrics will be presented, such as accuracy, precision, recall, and F1-score. In addition, deeper analyses will be carried out, such as identifying the best and worst classified attacks by our model.

5. Results

This section presents the tests performed on our UAV GPS attack detection system using data from safe flights and flights with attacks. For this approach, we employ multiclass classifiers to identify different types of attacks in real-time. We performed tests with several classification algorithms and data pre-processing techniques to evaluate the system's effectiveness.

The effectiveness of our technique is proven through extensive tests in the Google Colab performed using a dataset that includes benign flights, and flights with GPS spoofing and jamming attacks. By employing the multiclass concept, our model could detect GPS attacks with impressive accuracy, ranging between 92% and 98%. These results demonstrate the high level of accuracy and effectiveness of our model in identifying GPS attacks on UAVs. Our results showed that, on average, our system could detect and respond to a GPS attack in 0.238 seconds after 50 detection iterations. This speed of response is crucial as it allows corrective measures to be promptly taken to protect the UAV against the adverse consequences of the attack.

The high accuracy achieved by our model results from training it on a diverse and representative dataset, as well as using advanced machine learning algorithms such as Logistic Regression and Gradient Boosting. Furthermore, properly selecting relevant features and careful data pre-processing contributed to the model's effectiveness in detecting GPS spoofing attacks. The following section will present the individual results of each model trained in our multiclass system.

Table 1 presents all the accuracies obtained from the models trained using our multi-class system. Based on these results, we can observe that the Logistic Regression, Random Forest, XGBoost, and LightGBM techniques present higher accuracies, surpassing 0.98, indicating good data classification performance. The SVM and MLP techniques also show good accuracy, but a little lower than the previously mentioned ones. On the other hand, the Gradient Boosting technique has the most insufficient accuracy, reaching 0.78146. This indicates that this model may not be as efficient in detecting GPS attacks on UAVs.

Table 1. Comparison of accuracies.

Technique	**Accuracy (%)**
SVM	95.72
MLP	92.57
Logistic Regression	98.08
Decision Tree	92.52
Random Forest	**98.14**
Gradient Boosting	78.14
XGBoost	97.91
LightGBM	98.08

In Figure 3, it is possible to visualize a density graph showing the accuracy distribution of the different techniques used. The graph shows that most techniques have high precision, with values concentrated around 0.78 to 0.98. However, the Gradient Boosting technique presents a wider and asymmetric distribution, indicating more significant variability in the results.

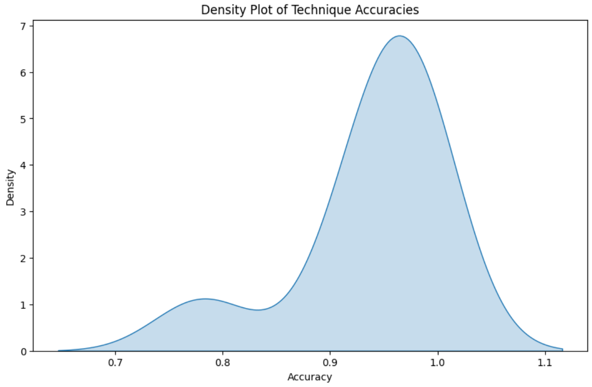

Figure 3. Distribution of the density.

The technique that achieved the highest accuracy in detecting GPS attacks on UAVs was Random Forest, with a value of 0.98148. Random Forest is a machine learning algorithm that combines several individual decision trees to make predictions. Some of the specific reasons within the context of detecting GPS attacks on UAVs that can explain the high accuracy of Random Forest may be that this technique combines several decision trees trained on different random samples of the dataset. This is beneficial for detecting GPS attacks, as each tree can learn to identify specific patterns related to spoofing or jamming attacks. Combining predictions from multiple trees allows Random Forest to capture a wide range of features and gain a more comprehensive view of potential attacks. Also, by training each tree on a random sample of the training dataset, the Random Forest reduces the risk of overfitting. These learning patterns need to be more specific and relevant to the training set. This is especially important in an attack detection scenario, where the model must generalize well to data not seen during training.

Table 2 compares the training times of the different techniques used in the GPS attack detection system in UAVs. Each method is evaluated based on the time in seconds required to perform the classification process, considering the average of 50 rounds of execution.

Based on these results, we can observe that the SVM and MLP techniques present the lowest training times, below 1 second. This indicates that these techniques are faster to classify data than other techniques. In contrast, the XGBoost and Gradient Boosting techniques present the highest execution times, with 8.27324 seconds and 5.674 seconds, respectively. The Logistic Regression, Decision Tree, and LightGBM techniques have intermediate execution times, varying between 1 and 3 seconds.

Table 2. Comparison of training times.

Technique	**Time (in seconds)**
SVM	0.97
MLP	**0.96**
Logistic Regression	3.13
Decision Tree	1.28
Random Forest	1.16
Gradient Boosting	5.67
XGBoost	8.27
LightGBM	3.42

The fastest model in terms of training time was the MLP, with a running time of 0.96719 seconds. One of the reasons that can justify this result is that MLP is a type of artificial neural network with a simple and computationally efficient architecture. It is composed of several layers of interconnected neurons, where each neuron performs a simple mathematical function. This simplicity contributes to faster data processing, which is particularly relevant in detecting GPS attacks on UAVs, where speed in data analysis is essential. Furthermore, compared to other more complex algorithms, such as Gradient Boosting, XGBoost, and LightGBM, MLP generally has a lower model complexity. This means MLP has fewer parameters to adjust and fewer computational steps to perform during training and inference. This lower complexity can result in a faster training time.

Table 3 presents the accuracy, F1-score, and recall results for each technique used in the GPS attack detection system on UAVs. The model that achieved the highest accuracy was the Logistic Regression, with a value of 0.98. This indicates that the proportion of correct predictions for the positive class, i.e., GPS attacks, is high. The MLP also had a high accuracy of 0.91, demonstrating the ability to make accurate predictions.

Regarding the F1-score, a metric that considers both accuracy and recall, the best-performing technique was the Decision Tree, with a value of 0.97. This indicates a good balance between accuracy and recall. In the case of a recall, which measures the proportion of correctly classified positive examples, it was Random Forest's turn to obtain a significant value of 0.98. This means that Random Forest correctly identifies all positive models of GPS attacks. Gradient Boosting, XGBoost, and LightGBM techniques have lower accuracy, F1-score, and recall values.

Table 3. Comparison of precision, F1-score, and recall.

Technique	Precision	F1-score	Recall
SVM	0.41	0.58	**1.00**
MLP	0.91	0.91	0.94
Log. Regression	**0.98**	**0.98**	0.99
Decision Tree	0.93	0.97	0.97
Random Forest	**0.98**	**0.98**	0.98
GB	0.78	0.81	0.63
XGBoost	**0.98**	**0.98**	0.99
LightGBM	**0.98**	**0.98**	0.99

The presented results show that Logistic Regression and Random Forest are techniques that achieved good accuracy and recall in detecting GPS attacks on UAVs. Logistic Regression is a linear classification model that uses the logistic function to estimate the probability of an instance belonging to a given class. It can effectively detect GPS attacks on UAVs by learning patterns and relationships between the input data and the GPS attack class. Furthermore, Logistic Regression has the advantage of providing interpretability of the results, which can be helpful in analysis and decision-making. On the other hand, Random Forest is an algorithm combining several individual decision trees to make predictions. Combining multiple decision trees in a voting process allows the Random Forest to reduce the overfitting effect, improving model generalization. This technique is suitable for detecting GPS attacks on UAVs, as it can capture different characteristics and patterns present in the input data, contributing to more accurate performance.

Decision Tree excelled in F1-score and can effectively detect GPS attacks on UAVs as it can create a hierarchical decision structure based on the relevant features to classify the instances correctly. This approach can balance accuracy and recall, accurately detecting both GPS attacks and non-attacked cases.

In summary, the techniques that stood out in the table above are Logistic Regression, Random Forest, and Decision Tree - they present characteristics and capabilities relevant to the GPS attack detection system in UAVs. They can learn patterns, capture different features, and make decisions based on the input data, contributing to accurate and reliable detection of GPS attacks. Choosing the most suitable technique will depend on the system's specific needs and the metrics considered most relevant for detecting GPS attacks on UAVs.

6. Discussion

Considering all comparison metrics, including accuracy, trainning time, accuracy, F1-score, and recall, we can conclude that Random Forest is the most suitable technique for detecting GPS attacks on UAVs. It had high accuracy (0.98148), good precision (0.98), F1-score (0.98), and recall (0.98). Furthermore, Random Forest can handle correlations between features and reduce the overfitting effect. While other techniques, such as Logistic Regression, have shown similar results on some metrics, Random Forest stands out for its ability to combine multiple decision trees and provide robust detection of GPS attacks on UAVs. In addition, it also showed a balanced performance between accuracy and recall.

It is important to emphasize that the choice of the most appropriate technique will depend on the specific needs and restrictions of the GPS attack detection system in UAVs and the availability of computational resources. Therefore, it is recommended to consider all the metrics and characteristics of the techniques before making a final choice.

Our multiclass system is more precise than the references (Du et al., 2017; Tlili et al., 2022). Furthermore, based on the same flaws and dataset, our multiclass model for UAV GPS attack detection achieved a remarkable accuracy of 98%, compared to the recent study published in 2022 (Tlili et al., 2022), which achieved an accuracy of 95%. The difference in performance can be attributed to several factors, such as the applied model and the adopted methodological approach.

7. Conclusion

The results of this study contribute to advances in the field of GPS attack detection on UAVs. The accuracy achieved by the evaluated techniques demonstrates their ability to identify different types of GPS attacks successfully. This is critical to ensuring the security and reliability of UAVs in GPS-dependent applications.

Furthermore, the comparative analysis between the techniques provided valuable information about their advantages and limitations regarding performance and computational efficiency. These insights can assist researchers and developers in choosing the most appropriate technique for their needs and resource constraints. In summary, the main results of this study are: Random Forest was identified as the most accurate technique, with an accuracy of 98.15% in detecting GPS attacks on UAVs; MLP was the fastest algorithm, with an average trainning time of 0.96719 seconds, and the Logistic Regression, Random Forest, and Decision Tree techniques consistently performed on the precision, F1-score, and recall metrics.

To promote transparency and replicability of the results obtained in this study, we share the dataset used and details on information processing, available at: https://github.com/IsadoraFerrao/Faults-DataSet/tree/main/Attacks. Our intention in making this information available allows the scientific community to reproduce and compare the results, contributing to the validation and advancement of knowledge in this area. By sharing the dataset and the methods employed, we encourage collaboration and exchanging ideas among researchers, strengthening the scientific base and promoting future improvements in detecting GPS attacks on UAVs.

References

Aissou, G., Slimane, H. O., Benouadah, S., & Kaabouch, N. (2021). Tree-based supervised machine learning models for detecting gps spoofing attacks on uas. *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 0649–0653.

Bisong, E., & Bisong, E. (2019). Google colaboratory. *Building machine learning and deep learning models on google cloud platform: a comprehensive guide for beginners*, 59–64.

Chen, P., Ye, J., Chen, G., Zhao, J., & Heng, P.-A. (2021). Robustness of accuracy metric and its inspirations in learning with noisy labels. *Proceedings of the AAAI Conference on Artificial Intelligence*, *35*(13), 11451–11461.

Chen, T., He, T., Benesty, M., Khotilovich, V., Tang, Y., Cho, H., Chen, K., Mitchell, R., Cano, I., Zhou, T., et al. (2015). Xgboost: Extreme gradient boosting. *R package version 0.4-2*, *1*(4), 1–4.

Cohen, A. P., Shaheen, S. A., & Farrar, E. M. (2021). Urban air mobility: History, ecosystem, market potential, and challenges. *IEEE Transactions on Intelligent Transportation Systems*, *22*(9), 6074–6087. https://doi.org/10.1109/TITS.2021.3082767

Dey, V., Pudi, V., Chattopadhyay, A., & Elovici, Y. (2018). Security vulnerabilities of unmanned aerial vehicles and countermeasures: An experimental study. *2018 31st international conference on VLSI design and 2018 17th international conference on embedded systems (VLSID)*, 398–403.

Du, M., Li, F., Zheng, G., & Srikumar, V. (2017). Deeplog: Anomaly detection and diagnosis from system logs through deep learning. *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security*, 1285–1298.

Emrouznejad, A., & Marra, M. (2014). Ordered weighted averaging operators 1988–2014: A citation-based literature survey. *International Journal of Intelligent Systems*, *29*(11), 994–1014.

FakeGPS. (2020). Fake gps location. https://play.google.com/store/apps/details?id=com.lexa.fakegps&hl=pt_BR

Ferrão, I. G., da Silva, S. A., Pigatto, D. F., & Branco, K. R. (2020). Gps spoofing: Detecting gps fraud in unmanned aerial vehicles. *2020 Latin American Robotics Symposium (LARS), 2020 Brazilian Symposium on Robotics (SBR) and 2020 Workshop on Robotics in Education (WRE)*, 1–6.

Ferrão, I. G., Pigatto, D. F., Fontes, J. V., Silva, N. B., Espes, D., Dezan, C., & Branco, K. R. (2020). Stuart: Resilient architecture to dynamically manage unmanned aerial vehicle networks under attack. *2020 IEEE Symposium on Computers and Communications (ISCC)*, 1–6.

Ferrão, I. G. (n.d.). *Resilient architecture to dynamically manage unmanned aerial vehicle networks under attack* (Doctoral dissertation). Universidade de São Paulo.

Ferrão, I. G., da Silva, L. M., da Silva, S. A., Dezan, C., Espes, D., & Branco, K. C. (2023). Intelligent diagnosis of engine failure in air vehicles using the alfa dataset. *2023 International Conference on Unmanned Aircraft Systems (ICUAS)*, 871–878.

Freeman, E. A., Moisen, G. G., & Frescino, T. S. (2012). Evaluating effectiveness of down-sampling for stratified designs and unbalanced prevalence in random forest models of tree species distributions in nevada. *Ecological modelling*, *233*, 1–10.

Goutte, C., & Gaussier, E. (2005). A probabilistic interpretation of precision, recall and f-score, with implication for evaluation. *Advances in Information Retrieval: 27th European Conference on IR Research, ECIR 2005, Santiago de Compostela, Spain, March 21-23, 2005. Proceedings 27*, 345–359.

Guelman, L. (2012). Gradient boosting trees for auto insurance loss cost modeling and prediction. *Expert Systems with Applications*, *39*(3), 3659–3667.

Khan, N. A., Jhanjhi, N., Brohi, S. N., Almazroi, A. A., & Almazroi, A. A. (2021). A secure communication protocol for unmanned aerial vehicles. *Computers, Materials and Continua*, *70*(1).

Li, B., Fei, Z., Zhang, Y., & Guizani, M. (2019). Secure uav communication networks over 5g. *IEEE Wireless Communications*, *26*(5), 114–120.

Liu, X., Ju, Y. T., Gao, Y. Z., & Li, C. Z. (2022). A fault-tolerant navigation method for multirotor uavs based on federal adaptive kalman filter. *Advances in Guidance, Navigation and Control: Proceedings of 2020 International Conference on Guidance, Navigation and Control, ICGNC 2020, Tianjin, China, October 23–25, 2020*, 1577–1588.

Noble, W. S. (2006). What is a support vector machine? *Nature biotechnology*, *24*(12), 1565–1567.

Osei-Bryson, K.-M. (2004). Evaluation of decision trees: A multi-criteria approach. *Computers & Operations Research*, *31*(11), 1933–1945.

Perez-Grau, F. J., Ragel, R., Caballero, F., Viguria, A., & Ollero, A. (2018). An architecture for robust uav navigation in gps-denied areas. *Journal of Field Robotics*, *35*(1), 121–145.

Raschka, S. (2018). Model evaluation, model selection, and algorithm selection in machine learning. *arXiv preprint arXiv:1811.12808*.

Segal, M., & Xiao, Y. (2011). Multivariate random forests. *Wiley interdisciplinary reviews: Data mining and knowledge discovery*, *1*(1), 80–87.

Sharma, D., Rashid, A., Gupta, S., & Gupta, S. K. (2019). A functional encryption technique in uav integrated hetnet: A proposed model. *Int. J. Simul.-Sci. Technol*, *20*, 7–1.

Su, Y. (2020). Prediction of air quality based on gradient boosting machine method. *2020 International Conference on Big Data and Informatization Education (ICBDIE)*, 395–397.

Taud, H., & Mas, J. (2018). Multilayer perceptron (mlp). *Geomatic approaches for modeling land change scenarios*, 451–455.

Titouna, C., Naït-Abdesselam, F., & Moungla, H. (2020). An online anomaly detection approach for unmanned aerial vehicles. *2020 International Wireless Communications and Mobile Computing (IWCMC)*, 469–474.

Tlili, F., Ayed, S., Fourati, L., & Ouni, B. (2022). Artificial intelligence based approach for fault and anomaly detection within uavs. https://doi.org/10.1007/978-3-030-99584-3_26

Tran, T., Le, U., & Shi, Y. (2022). An effective up-sampling approach for breast cancer prediction with imbalanced data: A machine learning model-based comparative analysis. *Plos one*, *17*(5), e0269135.

Whelan, J., Sangarapillai, T., Minawi, O., Almehmadi, A., & El-Khatib, K. (2020). Novelty-based intrusion detection of sensor attacks on unmanned aerial vehicles. *Proceedings of the 16th ACM symposium on QoS and security for wireless and mobile networks*, 23–28.

Yaacoub, J.-P., Noura, H., Salman, O., & Chehab, A. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet of Things*, *11*, 100218.

Yacouby, R., & Axman, D. (2020). Probabilistic extension of precision, recall, and f1 score for more thorough evaluation of classification models. *Proceedings of the first workshop on evaluation and comparison of NLP systems*, 79–91.

Zhi, Y., Fu, Z., Sun, X., & Yu, J. (2020). Security and privacy issues of uav: A survey. *Mobile Networks and Applications*, *25*, 95–101.