Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 6, No. 2, February 2025, Page 499-507
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v6i2.7033

Machine Learning-Based GPS Spoofing Detection in UAV Networks: A Comparative Analysis of Anomaly Detection Models

Gregorius Airlangga

Information Systems Study Program, Atma Jaya Catholic University of Indonesia, Jakarta, Indonesia
Email: gregorius.airlangga@atmajaya.ac.id
Submitted: 21/02/2025; Accepted: 28/02/2025; Published: 28/02/2025

Abstract–The increasing reliance on Global Positioning System (GPS) technology in Unmanned Aerial Vehicles (UAVs) has exposed them to cybersecurity threats, particularly GPS spoofing attacks that manipulate location data. This study explores the effectiveness of various machine learning-based approaches in detecting GPS spoofing in UAV communication networks. Supervised classification models, unsupervised anomaly detection techniques, and deep learning-based autoencoders are evaluated to determine their capability in identifying spoofed signals. The dataset used for training and testing contains multi-dimensional UAV network parameters with labeled GPS spoofing instances. Experimental results indicate that traditional anomaly detection models, such as Isolation Forest, One-Class SVM, and Local Outlier Factor, struggle with detection accuracy and exhibit high false-positive rates. The autoencoder-based approach achieves the highest accuracy (91.20%) but has poor precision (3.97%) and recall (4.73%), highlighting limitations in threshold selection and anomaly classification. Computational complexity analysis reveals that deep learning models, despite their accuracy advantages, require significant computational resources, making them less feasible for real-time UAV applications. This study identifies critical challenges in GPS spoofing detection, including dataset bias, environmental variability, and model hyperparameter sensitivity.

Keywords: GPS Spoofing Detection; UAV Cybersecurity; Machine Learning Anomaly Detection; Deep Learning Autoencoders; UAV Communication Security

1. INTRODUCTION

Articles Unmanned Aerial Vehicles (UAVs), commonly known as drones, have significantly transformed various industries, including logistics, agriculture, disaster management, and surveillance [1]–[3]. These advancements have been primarily driven by the integration of wireless communication networks, Internet of Things (IoT) infrastructure, and artificial intelligence (AI) to enable autonomous decision-making and efficient navigation [4]–[6]. However, the increasing reliance on UAV communication networks has also made them susceptible to various cybersecurity threats, particularly GPS spoofing attacks, which manipulate satellite-based positioning data to mislead UAVs regarding their actual location [7]–[9]. This vulnerability presents a substantial risk in applications such as military reconnaissance, critical infrastructure monitoring, and autonomous delivery services, necessitating robust detection mechanisms to ensure the reliability and security of UAV operations [10]–[12]. GPS spoofing attacks involve transmitting counterfeit GPS signals to deceive UAVs into miscalculating their true position, potentially leading to mission failure or even hijacking scenarios [13]–[15]. Existing GPS spoofing detection techniques primarily rely on cryptographic solutions, anomaly-based heuristics, and machine learning algorithms [16]–[18]. For instance, cryptographic authentication mechanisms, such as GPS signal encryption and authentication keys, offer a first layer of defense [19]. However, these methods suffer from computational overhead and require significant infrastructure modifications. Additionally, anomaly-based techniques leveraging consistency checks between onboard sensors (e.g., inertial measurement units, barometric altimeters) and GPS readings provide a second layer of protection [20]. Despite their effectiveness, these approaches often fail to generalize across diverse UAV operating environments due to sensor drift and environmental noise [21].

Machine learning-based approaches have gained traction in recent years for detecting GPS spoofing attacks by analyzing network parameters, trajectory patterns, and radio signal anomalies. For example, a study proposed a signal feature-based GPS spoofing detection approach, SigFeaDet, utilizing machine learning techniques to analyze UAV signal characteristics, achieving high detection accuracy. Another research introduced a perception-data-based method, PerDet, which employs multiple sensor data and machine learning algorithms to detect GPS spoofing, demonstrating a detection rate of 99.69%[22]. However, these methods often require large labeled datasets and may suffer from adversarial robustness issues when attackers deliberately manipulate signal characteristics to evade detection. Deep learning models, particularly Convolutional Neural Networks (CNNs), have been employed to analyze time-series data from UAV sensors, identifying patterns indicative of spoofing. A study demonstrated that a 1D CNN could detect GPS spoofing attacks before position falsification occurs, making it suitable for small UAVs due to its lightweight implementation. Nonetheless, deep learning models require substantial training data and computational resources, which might be challenging for real-time deployment [23]. Signal Quality Monitoring (SQM) techniques assess the integrity of GPS signals by examining correlation functions for anomalies. Monitoring metrics such as the Automatic Gain Control (AGC) levels can reveal unexpected power increases associated with spoofing attempts. These methods can be integrated into existing receivers without additional hardware; however, their sensitivity to environmental

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 6, No. 2, February 2025, Page 499-507
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v6i2.7033

factors, such as multipath effects, can lead to false detections [24]. Software-Defined Radio (SDR) platforms offer flexibility in implementing and updating spoofing detection algorithms by enabling real-time analysis and mitigation of spoofing through processing raw signal data. While SDRs provide a versatile solution, they often demand high computational power and can be cost-prohibitive for widespread deployment in consumer-grade UAVs [35].

Despite these advancements, there remains a gap in developing an anomaly detection framework specifically tailored for GPS spoofing in UAV networks. Existing works focus either on GPS signal analysis or general network anomaly detection, but few have examined GPS spoofing detection as an isolated problem within drone communication networks. Given the unique operational constraints and security challenges in UAV environments, a dedicated study focusing solely on GPS spoofing detection within UAV communication networks is warranted.

The primary objective of this research is to develop an effective GPS spoofing detection model based on machine learning techniques. Unlike previous studies that consider multiple attack vectors, our study isolates GPS spoofing attacks to evaluate their impact comprehensively. We utilize a publicly available dataset, the Drone Communication and Network Anomaly Detection Dataset, which contains multi-dimensional network features and labeled attack instances. Our key contributions include identifying critical UAV communication features indicative of GPS spoofing attacks, applying dimensionality reduction and feature selection techniques to enhance model efficiency, implementing a range of traditional and deep learning models including Isolation Forest, One-Class SVM, and an autoencoder-based neural network to classify GPS spoofing anomalies, conducting extensive experiments using 10-fold cross-validation to benchmark detection performance across different models using accuracy, precision, recall, F1-score, and ROC-AUC, and providing a comparative assessment of various anomaly detection techniques to determine the most effective approach for detecting GPS spoofing attacks. The remainder of this paper is structured as follows. Section 2 provides a detailed literature review of existing GPS spoofing detection techniques, highlighting their strengths and limitations. Section 3 describes the dataset, preprocessing steps, and feature selection methodology. In this section we also present the machine learning models implemented for GPS spoofing detection, along with the experimental setup. Section 4 discusses the evaluation metrics and comparative analysis of model performance. Finally, Section 5 concludes the study with key findings and future research directions.

2. RESEARCH METHODOLOGY

As presented in the figure 1, the activity diagram represents the end-to-end pipeline for detecting GPS spoofing in UAV communication networks using machine learning models. It illustrates the major steps in data preprocessing, feature selection, model training, evaluation, and deployment while ensuring that the process remains efficient and adaptable. The dataset utilized in this study is derived from a publicly available Drone Communication and Network Anomaly Detection Dataset, which consists of multi-dimensional network features recorded over time and can be downloaded from [25]. The dataset spans a period from November 2019 to December 2024, capturing various drone communication parameters, GPS data, network statistics, and multi-label indicators for different network anomalies. The dataset includes a total of 44,016 samples, each characterized by 26 input features alongside 8 multi-label target variables. Among these labels, the primary focus of this study is on GPS spoofing detection, represented by the binary class variable $y \in 0,1$, where $y = 1$ indicates a detected GPS spoofing attack, while $y = 0$ corresponds to normal communication behavior.

2.1 Preprocessing Steps

Preprocessing is a crucial step in ensuring data quality and improving model performance. The first stage involves handling missing values, which are present in several features such as signal strength, packet loss rate, and altitude. Missing values are imputed using a combination of mean imputation for continuous variables and mode imputation for categorical attributes, defined as (1).

$$X_{i,j} = \frac{1}{n}\sum_{k=1}^{n} X_{k,j} \quad (1)$$

For numerical attributes, where $X_{i,j}$ represents the imputed value for the j-th feature of the i-th sample. Categorical values are imputed using the most frequent class mode as presented in (2).

$$X_{i,j}^{*} = \arg\max_{v} P\left(X_j = v\right) \quad (2)$$

Normalization is applied to scale the features to a standard range to prevent features with large numerical ranges from dominating the model training process. Standardization is performed using the Z-score normalization given by (3).

$$X'_{i,j} = \frac{X_{i,j} - \mu_j}{\sigma_j} \quad (3)$$

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 6, No. 2, February 2025, Page 499-507
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v6i2.7033

Where μ_j and σ_j are the mean and standard deviation of feature j, respectively. This ensures that all features are scaled to a distribution with zero mean and unit variance, which helps neural networks converge efficiently during training. To address class imbalance, synthetic data augmentation techniques are employed using the Synthetic Minority Over-sampling Technique (SMOTE). The minority class instances are artificially increased by generating synthetic samples based on the k-nearest neighbors (KNN) approach. For each minority class instance, new samples are generated using (4).

$$x^{new} = x_i + \lambda(x_{kn} - x_i) \quad (4)$$

Where x_i is a minority class instance, x_{kn} is its randomly chosen k-nearest neighbor, and λ is a random number between 0 and 1.

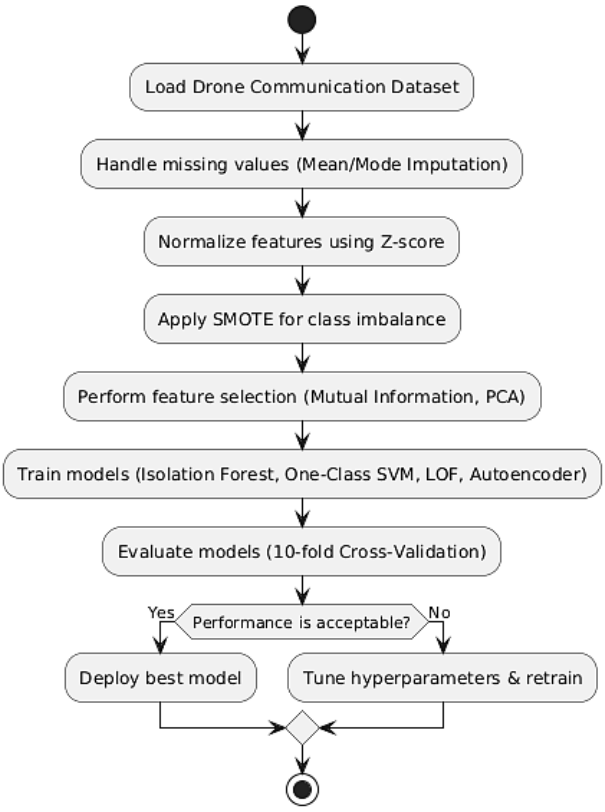

Figure 1. Research Methodology

2.2 Feature Selection Methodology

Feature selection is performed to enhance the model's interpretability and computational efficiency. The dataset contains redundant and non-informative features, which are removed through mutual information and principal component analysis (PCA). Mutual information is calculated for each feature X_j concerning the target variable y using the entropy formulation (5).

$$I(X_j; y) = H(y) - H(y|X_j) \quad (5)$$

Where $H(y)$ is the entropy of the target and $H(y|X_j)$ is the conditional entropy given feature X_j. Features with the lowest mutual information scores are discarded. PCA is used to project the high-dimensional feature space onto a lower-dimensional subspace while retaining maximum variance. Given the original feature matrix X, the covariance matrix is computed as presented in (6).

$$\Sigma = \frac{1}{n} X^T X \quad (6)$$

The principal components are extracted by solving the eigenvalue decomposition problem as presented in (7).

$$\Sigma v = \lambda v \quad (7)$$

Where v represents the eigenvectors and λ are the eigenvalues. The top k eigenvectors corresponding to the largest eigenvalues are selected to form the projection matrix V_k, and the reduced feature representation is given by (8).

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 6, No. 2, February 2025, Page 499-507
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v6i2.7033

$$X_{reduced} = XV_k \quad (8)$$

This transformation significantly reduces computational complexity while preserving the most informative patterns in the data. Through this comprehensive preprocessing and feature selection approach, the dataset is refined to maximize model performance and robustness. By integrating missing value imputation, normalization, synthetic data augmentation, and dimensionality reduction, the dataset is optimally structured for machine learning-based GPS spoofing detection.

2.3 Machine Learning Models and Evaluation

The study focuses on machine learning models specifically designed for GPS spoofing detection. The models utilized in the experiment include Isolation Forest, One-Class SVM, Local Outlier Factors and Autoencoders. These models are chosen for their ability to detect anomalies in UAV communication patterns by leveraging supervised and unsupervised learning techniques. Isolation Forest is an unsupervised anomaly detection algorithm that operates based on the principle of isolating outliers through recursive partitioning. Unlike traditional density-based methods, which rely on estimating data distribution, Isolation Forest explicitly isolates anomalies by randomly selecting features and splitting data points along random thresholds. This method is particularly effective for anomaly detection because anomalies tend to be more susceptible to isolation, requiring fewer splits compared to normal data points.

Given a dataset ($X = \{x_1, x_2, \dots, x_n\}$) with (n) samples and (d) features, Isolation Forest constructs a collection of isolation trees, denoted as ($T = \{T_1, T_2, \dots, T_t\}$), where (t) represents the number of trees in the forest. Each tree is built by recursively partitioning the data until a stopping criterion is met, such as reaching a predefined depth limit or when a single instance remains in a partition. The splitting process is performed by randomly selecting a feature (x_j) and choosing a threshold (θ) uniformly within the range of (x_j), such that $\theta \sim \text{Uniform}(\min(x_j), \max(x_j))$. At each step, data points are separated, forming partitions that continue until isolation is achieved. The depth at which a data point is isolated corresponds to its path length ($h(x)$), which represents the number of splits required to isolate (x) in a tree. Since anomalies are expected to reside in sparser regions of the feature space, they tend to have shorter path lengths compared to normal points. The anomaly score for a given instance (x) is computed as $s(x) = 2^{-\frac{E(h(x))}{c(n)}}$ where ($E(h(x))$) represents the average path length of (x) across all trees, and ($c(n)$) is a normalizing factor defined as $c(n) = 2H(n-1) - \frac{2(n-1)}{n}$ where ($H(n)$) is the harmonic number given by $H(n) = \sum_{i=1}^{n} \frac{1}{i}$ The anomaly score ($s(x)$) falls within the range ([0,1]), where higher values indicate a higher likelihood of being an anomaly. A predefined threshold (τ) is applied to classify anomalies.

One of the key advantages of Isolation Forest is its robustness against high-dimensional data since it does not require explicit density estimation. Additionally, the random partitioning process ensures that the algorithm remains effective without assuming any prior distribution of the data. However, a potential limitation is its sensitivity to the number of trees and the choice of the anomaly threshold (τ), which may require tuning based on specific datasets. Isolation Forest is particularly well-suited for GPS spoofing detection due to its ability to isolate anomalies in UAV communication patterns. Given the stochastic nature of GPS spoofing attacks, the algorithm efficiently distinguishes normal UAV signals from anomalous behaviors by identifying features that deviate from typical communication distributions. By leveraging recursive partitioning, Isolation Forest provides a computationally efficient and scalable approach for real-time anomaly detection in UAV security applications.

Local Outlier Factor (LOF) is an unsupervised anomaly detection algorithm that measures the relative density of a data point compared to its neighbors. Unlike global anomaly detection techniques that assume uniform distribution, LOF is particularly effective in identifying local anomalies where the density of a sample deviates significantly from its surrounding neighborhood.

Given a dataset ($X = \{x_1, x_2, \dots, x_n\}$), LOF assigns an anomaly score to each data point based on its local reachability density (LRD). The LRD is computed using the k-nearest neighbors (k-NN) distance, which quantifies how densely a point is clustered relative to its neighbors. The k-distance of a point(x_i), denoted as ($d_k(x_i)$), is defined as the distance to its (k)-th nearest neighbor $d_k(x_i) = \max_{x_j \in N_k(x_i)} d(x_i, x_j)$ where ($N_k(x_i)$) represents the set of (k)-nearest neighbors of (x_i), and ($d(x_i, x_j)$) is the Euclidean distance between (x_i) and (x_j). The reachability distance between two points (x_i) and (x_j) is then given by $\text{reach-dist}_k(x_i, x_j) = \max\left(d_k(x_j), d(x_i, x_j)\right)$ which ensures that no point is closer than its (k)-distance neighbor. The local reachability density (LRD) of a point (x_i) is then computed as $\text{LRD}_k(x_i) = \frac{k}{\sum_{x_j \in N_k(x_i)} \text{reach-dist}_k(x_i, x_j)}$ where a lower LRD value indicates lower density around (x_i), suggesting an anomaly. The final Local Outlier Factor (LOF) score for (x_i) is defined as $\text{LOF}_k(x_i) = \frac{\sum_{x_j \in N_k(x_i)} \frac{\text{LRD}_k(x_j)}{\text{LRD}_k(x_i)}}{|N_k(x_i)|}$. A higher LOF score indicates a lower-density region compared to its neighbors, meaning that the point is more likely to be an anomaly.

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 6, No. 2, February 2025, Page 499-507
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v6i2.7033

Autoencoders are a class of neural networks used for unsupervised learning, particularly for dimensionality reduction and anomaly detection. The fundamental idea behind an autoencoder is to learn a compressed representation of input data while being able to reconstruct the original input with minimal error. Anomalies are detected based on high reconstruction errors, which indicate deviations from learned normal patterns. Given an input data point ($x \in R^n$), an autoencoder consists of two main components. The first component is an encoder function ($g: R^n \to R^d$), which maps input data to a lower-dimensional latent space representation $z = g(x) = f(W_e x + b_e)$ where (W_e) and (b_e) are the weight matrix and bias for the encoder, and ($f(\cdot)$) is a non-linear activation function such as ReLU or Sigmoid. The second component is a decoder function ($h: R^d \to R^n$), which reconstructs the original input from the latent representation $\hat{x} = h(z) = f(W_d z + b_d)$ where (W_d) and (b_d) are the weights and bias for the decoder. The network is trained by minimizing the reconstruction loss, typically measured using the Mean Squared Error (MSE) $\mathcal{L}(x, \hat{x}) = \frac{1}{n}\sum_{i=1}^{n}(x_i - \hat{x_i})^2$ where (x_i) is the original input and ($\hat{x_i}$) is the reconstructed output. During inference, the reconstruction error ($\mathcal{E}(x)$) is computed, and an anomaly score is assigned as $s(x) = \mathcal{E}(x) = \left|\left|x - \hat{x}\right|\right|^2$.

The Support Vector Machine (SVM) classifier constructs an optimal hyperplane to separate normal and spoofing instances. The objective function for SVM is given as (9).

$$\min_{w,b} \quad \frac{1}{2}\left|\left|w\right|\right|^2 \quad \text{subject to} \quad y_i(w^T x_i + b) \geq 1, \quad \forall i \tag{9}$$

Where represents the weight vector, is the bias term, and is the label of sample. The model is trained using a radial basis function (RBF) kernel to capture non-linear patterns in the dataset. For anomaly detection, the Isolation Forest and One-Class SVM models are used. Isolation Forest identifies GPS spoofing by partitioning the dataset into randomly selected splits and measuring the depth of isolation for each instance. The anomaly score for a given sample is computed as (10).

$$S(X_i) = 2^{-\frac{E\left(h(X_i)\right)}{c(N)}} \tag{10}$$

Where is the expected path length and is an adjustment factor based on the dataset size. Higher anomaly scores indicate potential GPS spoofing attacks. One-Class SVM is an unsupervised model that teaches the decision boundary around normal data points and classifies outliers as spoofing attacks. The model solves the following optimization problem by using (11).

$$\min_{w,\xi,\rho} \quad \frac{1}{2}\left|\left|w\right|\right|^2 + \frac{1}{\nu N}\sum_{i=1}^{N}\xi_i - \tag{11}$$

Subject to, where is a parameter controlling the proportion of anomalies detected. Training and validation are conducted using 10-fold cross-validation to ensure model robustness. The dataset is divided into 10 subsets. At each iteration, one subset is reserved for validation while the remaining nine subsets are used for training. The final performance is computed as the average across all folds as presented in (12).

$$\text{Performance} = \frac{1}{10}\sum_{k=1}^{10} M(D_k) \tag{12}$$

Where represents the evaluation metric for the -th fold. The performance metrics used include accuracy, precision, recall, F1-score, and ROC-AUC, ensuring a comprehensive assessment of model effectiveness in detecting GPS spoofing attacks.

3. RESULT AND DISCUSSION

3.1 Experimental Results and Analysis

The experimental results provide an insightful evaluation of different machine learning models for GPS spoofing detection in UAV communication networks. The primary objective of this analysis is to assess the strengths and limitations of various anomaly detection techniques and determine their efficacy in identifying GPS spoofing attacks. The models considered in this study include Isolation Forest, One-Class SVM, Local Outlier Factor, and an autoencoder-based deep learning approach. As presented in the table 1, the evaluation metrics used for comparison include accuracy, precision, recall, F1-score, which collectively provide a comprehensive understanding of model performance. The Isolation Forest algorithm achieved an accuracy of 67.55%, indicating that it correctly classified approximately two-thirds of the test samples. However, its precision was 41.39%, suggesting that while it identified spoofing cases, a significant portion of its positive predictions were incorrect. The recall score of 14.10% reveals a critical limitation, as the model failed to identify the majority of actual GPS spoofing attacks. The low F1-score of 20.64% further emphasizes the trade-off between precision and recall, indicating that the model struggles to maintain an optimal balance between false positives and false negatives. The ROC-AUC score of 52.59% suggests that the model performs slightly better than a random classifier but does not provide a strong discriminatory power for identifying GPS spoofing.

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 6, No. 2, February 2025, Page 499-507
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v6i2.7033

Table 1. Performance Results

Model	Accuracy	Precision	Recall	F1 Score	ROC-AUC
Isolation Forest	0,675506	0,413892	0,141036	0,206435	52.59%
One-Class SVM	0,519751	0,326392	0,536065	0,403205	51.97%
Local Outlier Factor	0,588222	0,263334	0,195631	0,222335	53.61%
AutoEncoder	0,912011	0,039735	0,047368	0,043217	52.46%

The One-Class SVM model exhibited significantly lower accuracy at 51.97%, indicating that its classification performance was close to random. However, it achieved the highest recall among the models at 53.61%, meaning it was able to detect more actual spoofing instances compared to Isolation Forest. This improvement in recall came at the cost of precision, which dropped to 32.63%, indicating a higher false positive rate. The F1-score of 40.32% reflects a moderate balance between precision and recall, though the model's reliability remains limited. The ROC-AUC score of 52.46% suggests that the model does not significantly outperform a random guess, reinforcing the need for additional optimization or feature engineering to enhance its performance. The Local Outlier Factor model demonstrated an intermediate accuracy of 58.82%, positioning itself between Isolation Forest and One-Class SVM. However, its precision was the lowest at 26.33%, meaning that a substantial portion of its identified anomalies were false positives. The recall value of 19.56% was also low, indicating that it struggled to detect actual GPS spoofing cases effectively. The F1-score of 22.23% confirms that the model does not maintain an effective balance between precision and recall. The ROC-AUC score of 47.81% suggests that the Local Outlier Factor method performed worse than the other models, highlighting its inefficacy for GPS spoofing detection in UAV networks.

The deep learning-based autoencoder model demonstrated a significantly higher accuracy of 91.20%, suggesting that it was able to learn normal UAV communication patterns effectively. However, its precision was extremely low at 3.97%, indicating that only a small fraction of its positive classifications were actually GPS spoofing cases. The recall value of 4.74% further illustrates its inability to correctly identify the majority of spoofing attacks, resulting in an F1-score of 4.32%. These results highlight a fundamental issue with the autoencoder, as its high accuracy is misleading due to the imbalanced nature of the dataset. The model tends to classify most samples as normal, leading to a high false negative rate and rendering it ineffective for real-world GPS spoofing detection applications. The findings from these results indicate that traditional anomaly detection models such as Isolation Forest, One-Class SVM, and Local Outlier Factor struggle to provide robust and reliable GPS spoofing detection. Although One-Class SVM achieves the highest recall, its low precision makes it impractical for real-world deployment where false alarms need to be minimized. The autoencoder model, despite its high accuracy, fails to effectively detect GPS spoofing due to its bias toward normal classification. The poor recall and precision metrics across all models suggest that GPS spoofing is a highly complex anomaly that requires more sophisticated techniques, such as ensemble learning, hybrid models, or enhanced feature engineering, to improve detection accuracy. The key limitations identified in these models include their inability to generalize well to rare GPS spoofing events, the high rate of false positives and false negatives, and the challenges associated with class imbalance.

The effectiveness of a model in detecting GPS spoofing is not solely determined by classification accuracy, precision, recall, and F1-score but also by its computational efficiency. The time complexity and space complexity of each model play a crucial role in real-time UAV communication networks where computational resources are often limited. The Isolation Forest algorithm, which constructs a set of decision trees to isolate anomalies, has a time complexity of $O(t{\cdot}n \log n)$, where t represents the number of trees and n is the number of samples. The logarithmic term arises due to the binary splitting process within each tree. Although Isolation Forest exhibits relatively fast training and inference times due to its tree-based architecture, its performance in detecting GPS spoofing was suboptimal, with a recall of only 14.10%. The algorithm requires storing multiple trees, leading to a space complexity of O(t·n), which can become a bottleneck in environments with memory constraints. The One-Class SVM, a kernel-based anomaly detection method, operates with a worst-case time complexity of $O(n^2)$ when using the radial basis function (RBF) kernel. This quadratic complexity results from the need to compute the pairwise similarity between all data points during training, making it computationally expensive, especially for large datasets. The space complexity of One-Class SVM is also $O(n^2)$ due to the requirement of storing the entire kernel matrix. Although it achieved the highest recall at 53.61%, its computational cost makes it impractical for real-time UAV operations. Additionally, the presence of false positives in its predictions further reduces its reliability in real-world applications.

The Local Outlier Factor algorithm operates with a time complexity of $O(n^2)$ due to the need to compute k-nearest neighbors for each data point. This makes it one of the slowest methods in the study, especially when handling high-dimensional data. Its space complexity is $O(n)$, as it only stores the dataset and nearest neighbor distances. Despite having a moderate accuracy of 58.82%, its recall and precision were both poor, indicating that the computational cost did not translate into improved anomaly detection capabilities. This reinforces the observation that purely distance-based approaches may not be well-suited for detecting GPS spoofing attacks.

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 6, No. 2, February 2025, Page 499-507
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v6i2.7033

The autoencoder-based deep learning approach exhibits a different computational profile. The training time complexity of an autoencoder with *L* layers and n input features can be approximated as $O(L \cdot n^2)$ per epoch, assuming fully connected layers. The inference time complexity is $O(L \cdot n)$, making it more efficient for real-time detection once trained. The space complexity is determined by the number of trainable parameters, given by $O(n^2)$ for dense layers, which can be memory-intensive. Despite achieving the highest accuracy at 91.20%, the autoencoder failed to provide meaningful recall and precision values, suggesting that it primarily learned the distribution of normal communication patterns but struggled with rare GPS spoofing anomalies. This phenomenon is a common limitation of unsupervised deep learning models when applied to highly imbalanced datasets. In terms of practical deployment, real-time GPS spoofing detection requires a balance between accuracy and computational efficiency. Isolation Forest offers a compromise by providing relatively fast inference times and moderate memory requirements, though its low recall limits its effectiveness. One-Class SVM and Local Outlier Factor, while computationally expensive, did not provide sufficient detection performance to justify their use in UAV environments. The autoencoder, despite its deep learning capabilities, was ineffective due to class imbalance issues, highlighting the need for additional techniques such as data augmentation, adversarial training, or hybrid modeling approaches.

3.2 Threats to Validity

Ensuring the validity of our findings is a crucial aspect of this study, as it directly impacts the reliability and applicability of the proposed GPS spoofing detection framework in UAV communication networks. Several factors may influence the study's outcomes, and these must be carefully considered to assess the robustness of our approach. We categorize potential threats to validity into four main areas: internal validity, external validity, construct validity, and statistical conclusion validity. Internal validity pertains to factors within the study that could introduce biases or inaccuracies in the results. One significant concern is the quality of the dataset and preprocessing methods. The dataset is derived from a publicly available UAV anomaly detection dataset, which may contain inherent biases in terms of how spoofing events were recorded. While missing values are handled using mean and mode imputation, these techniques assume that missing data are randomly distributed, which may not always be the case. Additionally, standardization methods such as Z-score normalization assume normal distributions across features, which may not reflect the true nature of UAV communication data. Another potential issue lies in the feature selection process. Although mutual information and principal component analysis (PCA) improve computational efficiency by reducing dimensionality, there is a risk that important yet subtle indicators of GPS spoofing are removed. PCA, in particular, assumes linear relationships between features, which may not fully capture complex interactions in UAV communication patterns. Furthermore, the dataset exhibits a significant class imbalance, with normal UAV communication instances vastly outnumbering GPS spoofing occurrences. To mitigate this, we applied the Synthetic Minority Over-sampling Technique (SMOTE) to generate additional samples of the minority class. However, SMOTE generates synthetic instances based on existing data points, which may lead to models overfitting to artificial patterns rather than genuine spoofing behaviors. Lastly, the effectiveness of machine learning models depends on optimal hyperparameter selection. Models such as Isolation Forest and One-Class SVM require tuning parameters like the contamination rate and kernel selection. Suboptimal configurations could lead to excessive false positives or false negatives, reducing the practical applicability of the model.

External validity refers to the extent to which our findings generalize to different UAV communication environments, datasets, and real-world applications. A primary concern is whether the dataset sufficiently captures the full range of GPS spoofing techniques that could be encountered in operational UAV networks. While the dataset spans from November 2019 to December 2024, it may not comprehensively represent emerging spoofing strategies that adversaries could develop in the future. Additionally, the dataset is collected under specific UAV network conditions, which may not be reflective of military, commercial, or emergency response drone operations that operate in diverse environments. Another critical consideration is the practicality of deploying our proposed models in real-world UAV applications. The study assumes that UAVs operate in relatively stable communication environments, yet in practice, real-world UAV networks are subject to external disruptions such as atmospheric interference, GPS signal obstructions, and intentional jamming. These factors could significantly affect the model's detection capabilities. Furthermore, while this study focuses exclusively on GPS spoofing detection, UAV networks face multiple cybersecurity threats, including jamming, protocol-based attacks, and packet injection. The models trained here may not generalize well to detect these broader anomalies, potentially limiting their usefulness in a more comprehensive UAV security framework.

Construct validity addresses whether the experimental design and evaluation metrics effectively capture the intended phenomenon. A key concern is the choice of evaluation metrics. While accuracy, precision, recall, F1-score, and ROC-AUC provide insights into model performance, they may not fully capture the challenges associated with anomaly detection in highly imbalanced datasets. A model that simply classifies all instances as normal would achieve high accuracy yet fail to detect spoofing events effectively. Precision and recall must be carefully balanced—high false positive rates may render the model impractical in real-world UAV operations, while low recall means that many actual GPS spoofing attacks could go undetected. Another concern is the interpretability of the models used. Deep learning models, such as autoencoders, operate as black-box systems,

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 6, No. 2, February 2025, Page 499-507
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v6i2.7033

making it difficult to determine which features contribute most to detecting spoofing attacks. This lack of interpretability poses a challenge in operational UAV security, where transparency in decision-making is essential. Additionally, the study assumes that the training data accurately represents real-world UAV network behavior. Given that adversarial spoofing methods are continuously evolving, models trained on historical data may not be effective in detecting novel GPS spoofing attacks that exhibit previously unseen characteristics.

Statistical conclusion validity pertains to the reliability and reproducibility of our findings. One potential limitation is the use of 10-fold cross-validation to evaluate model performance. While this method helps reduce variance, different train-test splits can lead to variations in results, particularly when dealing with an imbalanced dataset. Some training subsets may contain more distinguishable GPS spoofing instances than others, potentially inflating the model's performance. Additionally, machine learning models—especially anomaly detection algorithms—are highly sensitive to hyperparameter tuning. Small changes in parameters, such as the number of trees in Isolation Forest or the contamination rate in One-Class SVM, can significantly impact results, raising concerns about the reproducibility of reported performance metrics. Another critical issue is overfitting in deep learning models. The autoencoder achieved a notably high accuracy of 91.20%, yet its recall was only 4.74%, indicating that the model primarily learned normal UAV communication patterns but failed to generalize to GPS spoofing anomalies. This highlights the common limitation of unsupervised deep learning in highly imbalanced datasets, where models tend to focus on normal instances while struggling to detect rare attacks. Addressing this issue would require additional regularization techniques, adversarial training, or specialized anomaly detection strategies to improve model robustness.

To mitigate these threats to validity, several enhancements could be considered in future research. One promising approach is to move beyond traditional oversampling techniques like SMOTE and explore more sophisticated data augmentation strategies, such as Generative Adversarial Networks (GANs), to create more realistic synthetic GPS spoofing samples. Additionally, adversarial training could be incorporated to improve the model's resilience to evolving attack techniques. Another area for improvement lies in feature engineering—rather than relying solely on statistical methods such as PCA, future studies could integrate domain-specific knowledge to extract features that are more indicative of spoofing behavior. Expanding the dataset by incorporating real-world UAV communication data from multiple network environments would also improve external validity. Furthermore, enhancing model interpretability through post-hoc explainability methods such as SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-Agnostic Explanations) could help security analysts better understand model predictions, increasing trust in the system.

4. CONCLUSION

The study presents a comprehensive evaluation of machine learning models for GPS spoofing detection in UAV communication networks. The experimental results demonstrate significant variations in the performance of different anomaly detection approaches, highlighting the trade-offs between accuracy, recall, and computational efficiency. The models evaluated include Isolation Forest, One-Class SVM, Local Outlier Factor, and a deep learning-based autoencoder, each exhibiting distinct strengths and weaknesses in detecting GPS spoofing anomalies. The Isolation Forest model achieved a moderate accuracy of 67.55%, but its recall of only 14.10% indicates that it struggles to identify actual GPS spoofing instances. This limitation reduces its reliability for real-world applications, where the ability to detect spoofing events is critical. The One-Class SVM model showed improved recall at 53.61%, meaning it was able to detect more true positive cases. However, its lower accuracy and high false positive rate limited its overall effectiveness. The Local Outlier Factor model provided intermediate performance but was computationally expensive, requiring significant processing time without yielding superior detection results. The deep learning-based autoencoder achieved the highest accuracy at 91.20%, suggesting that it effectively learned normal UAV communication patterns. However, its precision and recall were exceptionally low, with an F1-score of just 4.32%. This result implies that while the model can reconstruct normal patterns, it fails to generalize well to rare GPS spoofing events. The imbalance in the dataset may have contributed to this issue, leading the autoencoder to classify most inputs as normal. A deeper computational analysis revealed that the models exhibit significant differences in time and space complexity. Isolation Forest and One-Class SVM demonstrated feasible computational efficiency but lacked the required recall for reliable GPS spoofing detection. The autoencoder, while computationally expensive, failed to effectively capture GPS spoofing patterns due to the imbalance in the dataset. This underscores the need for advanced feature selection and hybrid modeling approaches to enhance detection performance. The findings suggest that no single model can provide a perfect solution for GPS spoofing detection. Instead, a hybrid approach integrating the advantages of different models may yield improved detection accuracy while maintaining computational efficiency. Future research should explore ensemble methods that combine tree-based models with deep learning techniques to enhance robustness. Additionally, addressing dataset imbalance through synthetic data augmentation or adversarial training may further improve recall and reduce false negatives. In practical UAV applications, real-time GPS spoofing detection remains a challenging task due to the constraints on computational resources and the complexity of spoofing attacks. The implementation of lightweight yet

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 6, No. 2, February 2025, Page 499-507
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v6i2.7033

effective anomaly detection methods, potentially leveraging federated learning and edge computing architectures, could provide a viable path forward. The integration of domain-specific knowledge, such as UAV flight behavior patterns and signal integrity checks, could further enhance the detection framework. Future research should explore hybrid approaches that integrate multiple anomaly detection techniques, optimize computational efficiency, and improve the generalization of detection models. The findings contribute to the advancement of UAV cybersecurity by providing insights into machine learning-based GPS spoofing detection strategies and their potential applications in real-world UAV deployments.

REFERENCES

[1] O. M. Bushnaq, D. Mishra, E. Natalizio, and I. F. Akyildiz, "Unmanned aerial vehicles (UAVs) for disaster management," in *Nanotechnology-Based Smart Remote Sensing Networks for Disaster Prevention*, Elsevier, 2022, pp. 159–188.
[2] A. Rejeb, K. Rejeb, S. J. Simske, and H. Treiblmaier, "Drones for supply chain management and logistics: a review and research agenda," *Int. J. Logist. Res. Appl.*, vol. 26, no. 6, pp. 708–731, 2023.
[3] A. Khan, S. Gupta, and S. K. Gupta, "Multi-hazard disaster studies: Monitoring, detection, recovery, and management, based on emerging technologies and optimal techniques," *Int. J. disaster risk Reduct.*, vol. 47, p. 101642, 2020.
[4] A. Biswas and H.-C. Wang, "Autonomous vehicles enabled by the integration of IoT, edge intelligence, 5G, and blockchain," *Sensors*, vol. 23, no. 4, p. 1963, 2023.
[5] I. Ullah, I. U. Khan, M. Ouaissa, M. Ouaissa, and S. El Hajjami, *Future Communication Systems Using Artificial Intelligence, Internet of Things and Data Science*. CRC Press, 2024.
[6] B. Chander, S. Pal, D. De, and R. Buyya, "Artificial intelligence-based internet of things for industry 5.0," *Artif. Intell. internet things Syst.*, pp. 3–45, 2022.
[7] A. AlAbidy, A. Zaben, O. M. F. Abu-Sharkh, and H. A. Noman, "A Survey on AI-Based Detection Methods of GPS Spoofing Attacks on UAVs," in *2024 IEEE 12th International Conference on Intelligent Systems (IS)*, 2024, pp. 1–13.
[8] M. Kang, S. Park, and Y. Lee, "A Survey on Satellite Communication System Security," *Sensors*, vol. 24, no. 9, p. 2897, 2024.
[9] S. Salim, N. Moustafa, and M. Reisslein, "Cybersecurity of Satellite Communications Systems: A Comprehensive Survey of the Space, Ground, and Links Segments," *IEEE Commun. Surv. \& Tutorials*, 2024.
[10] T. M. Dorn, *US critical infrastructure: Its Importance and Vulnerabilities to Cyber and Unmanned Systems*. Page Publishing Inc, 2023.
[11] J. Greer IV, "MITRE Attack framework adaptation in UAV usage during surveillance and reconnaissance missions," 2024.
[12] I. Anagnostis, P. Kotzanikolaou, and C. Douligeris, "Understanding and Securing Unmanned Aerial Vehicle (UAV) Services: A Comprehensive Tutorial," *Authorea Prepr.*, 2024.
[13] P. Lin, K. Abney, B. DeBruhl, K. Abercromby, H. Danielson, and R. Jenkins, "Outer Space Cyberattacks: Generating Novel Scenarios to Avoid Surprise," *arXiv Prepr. arXiv2406.12041*, 2024.
[14] A. Giannaros *et al.*, "Autonomous vehicles: Sophisticated attacks, safety issues, challenges, open topics, blockchain, and future directions," *J. Cybersecurity Priv.*, vol. 3, no. 3, pp. 493–543, 2023.
[15] V. Varadharajan and N. Suri, "Security challenges when space merges with cyberspace," *Space Policy*, vol. 67, p. 101600, 2024.
[16] N. Jeffrey, Q. Tan, and J. R. Villar, "A review of anomaly detection strategies to detect threats to cyber-physical systems," *Electronics*, vol. 12, no. 15, p. 3283, 2023.
[17] M. M. Abrar, "Anomaly-Based Intrusion Detection System for Autonomous Vehicles," The University of Arizona, 2023.
[18] J. Nagarajan *et al.*, "Machine Learning based intrusion detection systems for connected autonomous vehicles: A survey," *Peer-to-Peer Netw. Appl.*, vol. 16, no. 5, pp. 2153–2185, 2023.
[19] C. V. S. Babu and A. Pal, "Enhancing Security for Unmanned Aircraft Systems in IoT Environments: Defense Mechanisms and Mitigation Strategies," *Unmanned Aircr. Syst.*, pp. 429–476, 2024.
[20] E. Balestrieri, P. Daponte, L. De Vito, F. Picariello, and I. Tudosa, "Sensors and measurements for UAV safety: An overview," *Sensors*, vol. 21, no. 24, p. 8253, 2021.
[21] A. K. Al Hwaitat *et al.*, "Overview of Mobile Attack Detection and Prevention Techniques Using Machine Learning.," *Int. J. Interact. Mob. Technol.*, vol. 18, no. 10, 2024.
[22] X. Wei, Y. Wang, and C. Sun, "PerDet: machine-learning-based UAV GPS spoofing detection using perception data," *Remote Sens.*, vol. 14, no. 19, p. 4925, 2022.
[23] M. M. H. Shuvo, S. K. Islam, J. Cheng, and B. I. Morshed, "Efficient acceleration of deep learning inference on resource-constrained edge devices: A review," *Proc. IEEE*, vol. 111, no. 1, pp. 42–91, 2022.
[24] J. Pavur, "Securing new space: on satellite cyber-security," University of Oxford, 2021.
[25] D. Engineer, "Drone Communication Dataset." 2024.