

Detection of DDoS Attacks in UAV Communication Networks Using Machine Learning Models

Gregorius Airlangga

Information Systems Study Program, Universitas Katolik Indonesia Atma Jaya, Indonesia
gregorius.airlangga@atmajaya.ac.id

Abstract

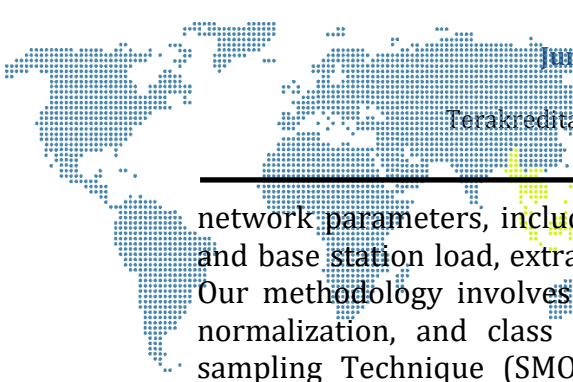
The increasing adoption of unmanned aerial vehicle (UAV) communication networks has introduced new cybersecurity challenges, particularly in detecting and mitigating distributed denial-of-service (DDoS) attacks. This study evaluates the effectiveness of multiple machine learning models, including Random Forest, Gradient Boosting, XGBoost, Logistic Regression, and Support Vector Machine (SVM), for DDoS attack detection in UAV networks. The dataset, derived from a simulated UAV communication network, incorporates key network parameters such as signal strength, packet loss rate, round-trip time, and base station load. Data preprocessing steps, including feature selection, normalization, and synthetic minority over-sampling (SMOTE), were applied to enhance model performance. Among the evaluated models, Random Forest demonstrated the highest classification accuracy with an F1-score of 0.839 and an AUC score of 0.912, outperforming other models in precision-recall trade-offs. Gradient Boosting and XGBoost exhibited moderate classification ability, whereas Logistic Regression and SVM struggled with capturing complex network patterns. The results highlight the effectiveness of ensemble learning in intrusion detection for UAV networks. This study provides valuable insights into optimizing machine learning-based intrusion detection systems and paves the way for further advancements in UAV cybersecurity. Future work will focus on integrating additional feature engineering techniques and validating models on real-time network traffic datasets.

Keywords: UAV Communication Security, DDoS Attack Detection, Machine Learning Models, Random Forest Classification, Cybersecurity in UAV Networks

1. INTRODUCTION

The rapid expansion of unmanned aerial vehicle (UAV) networks has led to transformative applications in various domains, including logistics, surveillance, disaster response, and communication infrastructure [1]–[3]. However, the integration of UAVs into critical network infrastructures exposes them to numerous cybersecurity threats, particularly distributed denial-of-service (DDoS) attacks [4]–[6]. DDoS attacks aim to disrupt network availability by overwhelming UAV communication channels with excessive traffic, rendering essential operations inoperable [7]–[9]. The dynamic nature of drone-to-drone (D2D) and drone-to-base station (D2BS) communication further amplifies the complexity of mitigating such threats, as traditional intrusion detection methods often fail to adapt to evolving attack patterns in real time [7], [10], [11].

Existing research on UAV network security has primarily focused on encryption-based defenses, anomaly detection mechanisms, and adaptive routing strategies to mitigate cyber threats [12]–[14]. While these approaches have demonstrated varying degrees of effectiveness, machine learning-based intrusion detection systems (IDS) have emerged as a promising alternative for real-time attack detection and mitigation [15]–[17]. This study investigates the effectiveness of multiple machine learning model for DDoS attacks detection in UAV communication networks. We employ a dataset comprising multi-dimensional



network parameters, including signal strength, packet loss rate, round-trip time, and base station load, extracted from a simulated drone communication network. Our methodology involves preprocessing the dataset through feature selection, normalization, and class imbalance handling using Synthetic Minority Over-sampling Technique (SMOTE). We implement a deep neural network (DNN) alongside multiple classical machine learning models, including Random Forest, Gradient Boosting, XGBoost, Logistic Regression, and Support Vector Machine (SVM), to benchmark classification performance. The models are evaluated based on their ability to accurately classify DDoS attack instances, using performance metrics such as F1-score, precision, recall, and area under the receiver operating characteristic curve (AUC-ROC).

Despite the significant advancements in machine learning-driven network security, existing approaches often struggle with generalization across dynamic UAV network conditions. Conventional intrusion detection systems frequently rely on manually crafted features, limiting adaptability to emerging attack vectors. Furthermore, prior studies on UAV security predominantly focus on static network environments, overlooking the implications of mobility, fluctuating transmission power, and latency variations in real-world UAV networks. Our study addresses these limitations by introducing a comprehensive evaluation framework that integrates feature selection, imbalanced data handling, and multi-model comparison to enhance DDoS detection accuracy.

The key contributions of this research are as follows: (1) a novel dataset preprocessing pipeline optimized for UAV-based network anomaly detection, incorporating domain-specific feature engineering and class imbalance correction; (2) an extensive comparative analysis of machine learning models for detecting DDoS attacks in UAV networks; and (3) an assessment of model generalization under varying network conditions, ensuring robustness in practical UAV deployment scenarios. The results provide valuable insights into the applicability of data-driven security mechanisms for UAV networks, offering a foundation for future research on adaptive threat mitigation strategies. The remainder of this paper is structured as follows. Section 2 details the proposed methodology, including dataset preparation, feature selection, model training, and evaluation metrics. Section 3 presents experimental results and a comparative analysis of model performance. Additionally, we discuss the implications of our findings and potential future research directions. Finally, Section 4 concludes the study with key takeaways and recommendations for enhancing UAV network security against evolving cyber threats.

2. RESEARCH METHODOLOGY

The methodology for detecting DDoS attacks in UAV communication networks involves dataset preparation, feature selection, model training, and evaluation. The dataset consists of multi-dimensional network parameters, including signal strength, packet loss rate, round-trip time, and base station load and can be downloaded in [18]. To ensure the integrity of the dataset, preprocessing is applied by removing irrelevant features such as timestamps and drone

identification, extracting latitude and longitude from GPS coordinates, encoding categorical features using label encoding, and handling missing values through mean imputation. Each categorical feature (X_c) is transformed into numerical form using (1).

$$X'_c = \text{LabelEncoder}(X_c) \quad (1)$$

while numerical features (X_n) are normalized using standardization using (2).

$$X'_n = \frac{X_n - \mu}{\sigma} \quad (2)$$

where (μ) is the mean and (σ) is the standard deviation of each feature. Given that DDoS attacks are rare events, the dataset exhibits class imbalance, which is corrected using the Synthetic Minority Over-sampling Technique (SMOTE). The new synthetic instances (X_{new}) are generated using (3).

$$X_{\text{new}} = X_{\text{minority}} + \lambda(X_{\text{nearest}} - X_{\text{minority}}) \quad (3)$$

where ($\lambda \sim U(0,1)$) is a randomly selected weight, (X_{minority}) is a randomly chosen sample from the minority class, and (X_{nearest}) is one of its k-nearest neighbors. The resampled dataset is then partitioned into training and testing sets such (4).

$$(X_{\text{train}}, y_{\text{train}}), (X_{\text{test}}, y_{\text{test}}) = \text{TrainTestSplit}(X, y, \text{test_size} = 0.2) \quad (4)$$

ensuring that both normal and attack instances are proportionally represented. Feature selection is performed to identify the most informative attributes for classification. Random Forest Feature Importance (RFI) measures the significance of each feature (X_i) by evaluating its contribution to reducing entropy in the classification task. The importance score is computed as (5).

$$I(X_i) = \sum_{t \in T} p_t \cdot \Delta H_t \quad (5)$$

where (p_t) is the probability of reaching a particular node in a decision tree, (ΔH_t) is the entropy reduction achieved by splitting on (X_i), and (T) is the ensemble of decision trees. Additionally, mutual information (MI) quantifies the dependency between each feature and the target variable using (6).

$$I(X_i; Y) = \sum_{x \in X_i} \sum_{y \in Y} P(x, y) \log \frac{P(x, y)}{P(x)P(y)} \quad (6)$$

where ($P(x, y)$) represents the joint probability distribution of (X_i) and (Y), and ($P(x)$), ($P(y)$) denote their marginal distributions. The top features based on RFI and MI scores are selected for training. The Random Forest model aggregates predictions across multiple decision trees such that the final prediction is given by (7).

$$\hat{y} = \frac{1}{T} \sum_{t=1}^T h_t(x) \quad (7)$$

where $(h_i(x))$ represents the prediction from an individual tree. The Gradient Boosting model iteratively refines predictions using (8).

$$F_m(x) = F_{m-1}(x) + \gamma_m h_m(x) \quad (8)$$

where (γ_m) is the learning rate. The XGBoost classifier optimizes a loss function as presented as (9).

$$l(\theta) = \sum_i l(y_i, \hat{y}_i) + \sum_j \Omega(f_j) \quad (9)$$

where $(\Omega(f_j))$ is a regularization term controlling model complexity. The SVM classifier finds an optimal decision boundary by using (10).

$$\min \frac{1}{2} |\mathbf{w}|^2 + C \sum_i \max(0, 1 - y_i(\mathbf{w}^T x_i + b)) \quad (10)$$

where (\mathbf{w}) represents the weight vector and (C) is the penalty parameter for misclassification. Each model is trained using 5-fold cross-validation. To evaluate model performance, multiple metrics are used. Accuracy is computed as (11).

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \quad (11)$$

where (TP) , (TN) , (FP) , and (FN) represent the counts of true positives, true negatives, false positives, and false negatives, respectively. Precision quantifies the fraction of correctly predicted DDoS attacks as presented as (12).

$$\text{Precision} = \frac{TP}{TP + FP} \quad (12)$$

while recall measures the fraction of actual attacks correctly detected as (13).

$$\text{Recall} = \frac{TP}{TP + FN} \quad (13)$$

F1-score provides a balanced measure of precision and recall using (14).

$$\text{F1-score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (14)$$

Additionally, the area under the receiver operating characteristic curve (AUC-ROC) evaluates the model's ability to distinguish between attack and normal instances by integrating the true positive rate (TPR) and false positive rate (FPR). The final model selection is based on optimizing these metrics to ensure robust and reliable DDoS detection in UAV networks.

3. RESULTS AND DISCUSSION

The performance of various machine learning models for detecting DDoS attacks in UAV communication networks is analyzed using multiple evaluation metrics, including precision, recall, F1-score, accuracy, and AUC-ROC. The Random

Forest classifier demonstrates the highest overall performance, achieving an F1-score of 0.84 for the minority class and an AUC score of 0.912. It maintains a balanced precision and recall, ensuring a reliable classification of both normal and attack instances. The recall of 0.89 for DDoS attacks indicates that this model effectively detects most attack instances, reducing false negatives. The cross-validation F1-score of 0.834 further supports its robustness and generalizability.

The Gradient Boosting model exhibits a lower overall performance compared to Random Forest, with an F1-score of 0.63 and an AUC score of 0.803. While it achieves a high recall of 0.92 for normal communication, it struggles with detecting DDoS attacks, as evidenced by the lower recall of 0.50 for the minority class. This suggests that Gradient Boosting is more conservative in classifying attacks, leading to an increased false negative rate. The XGBoost classifier performs better than Gradient Boosting but does not surpass Random Forest. It achieves an F1-score of 0.71 and an AUC score of 0.867. The recall of 0.58 for DDoS attacks suggests a trade-off between detection sensitivity and false alarms. While XGBoost is effective in reducing misclassification of normal traffic, it struggles with distinguishing attack patterns with high confidence.

The Logistic Regression model exhibits the weakest performance, with an F1-score of 0.58 and an AUC score of 0.519. The model achieves a recall of 0.66 for DDoS attacks but suffers from poor precision, leading to a high number of false positives. This indicates that a simple linear decision boundary is insufficient for accurately classifying complex network anomalies in UAV communication. The Support Vector Machine (SVM) achieves an F1-score of 0.67 and an AUC score of 0.636. While it performs better than Logistic Regression, it struggles to generalize effectively. The recall of 0.82 for attack instances suggests that SVM is effective at identifying DDoS attacks, but its low precision (0.57) leads to an increased false positive rate. This can result in unnecessary mitigation actions in real-world deployments.

A summary of model performance across multiple metrics is presented in the table 1. From this comparison, Random Forest emerges as the best-performing model, demonstrating the highest AUC score (0.912), F1-score (0.839), and cross-validation F1-score (0.834). These results indicate that Random Forest is the most reliable and robust model for detecting DDoS attacks in UAV networks. The ability to capture complex decision boundaries and handle high-dimensional feature spaces contributes to its superior performance.

Table 1. Machine Learning Performance

Model	AUC Score	CV F1 Score
Random Forest	0.912	0.834
Gradient Boosting	0.803	0.636
XGBoost	0.867	0.709
Logistic Regression	0.520	0.570
Support Vector Machine	0.636	0.665

The superior performance of Random Forest can be attributed to its ensemble learning mechanism, which reduces overfitting and improves

generalization. The model effectively balances precision and recall, minimizing both false positives and false negatives. This makes it a viable candidate for real-time deployment in UAV network security applications. Gradient Boosting and XGBoost, while competitive, show limitations in recall, suggesting that they may not be as effective in high-risk scenarios where attack detection is critical. The performance gap between Random Forest and XGBoost can be explained by the latter's sensitivity to hyperparameters and potential overfitting to minority class instances. Logistic Regression and SVM, being relatively simple models, fail to capture the non-linear decision boundaries present in the dataset. Their lower performance underscores the necessity of using more complex models for DDoS attack detection.

4. CONCLUSION

This study analyzed the performance of multiple machine learning models for detecting DDoS attacks in UAV communication networks. Among the evaluated models, Random Forest demonstrated the highest classification performance, achieving superior accuracy, recall, and F1-score. The ensemble learning approach in Random Forest allowed it to effectively distinguish between normal and attack instances, making it the most suitable model for deployment in UAV network security applications. The results highlight the importance of selecting robust and adaptable models for real-time intrusion detection. While Gradient Boosting and XGBoost provided competitive results, they showed limitations in recall, leading to a higher false negative rate. Logistic Regression and SVM, on the other hand, struggled with capturing complex decision boundaries, resulting in lower predictive performance. Future research should focus on integrating deep learning-based approaches with ensemble models to enhance classification accuracy further. Additionally, expanding the dataset with real-time UAV network traffic and implementing adversarial robustness techniques could improve the reliability of DDoS detection systems in practical deployments. The insights gained from this study contribute to the ongoing advancements in UAV cybersecurity and anomaly detection methodologies.

REFERENCES

- [1] S. A. H. Mohsan, N. Q. H. Othman, Y. Li, M. H. Alsharif, and M. A. Khan, "Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends," *Intell. Serv. Robot.*, vol. 16, no. 1, pp. 109–137, 2023.
- [2] M. K. Banafaa *et al.*, "A comprehensive survey on 5G-and-beyond networks with UAVs: Applications, emerging technologies, regulatory aspects, research trends and challenges," *IEEE access*, vol. 12, pp. 7786–7826, 2024.
- [3] A. Khan, S. Gupta, and S. K. Gupta, "Emerging UAV technology for disaster detection, mitigation, response, and preparedness," *J. F. Robot.*, vol. 39, no. 6, pp. 905–955, 2022.
- [4] M. A. O. Rabah, H. Drid, Y. Medjadba, and M. Rahouti, "Detection and Mitigation of Distributed Denial of Service Attacks Using Ensemble Learning and Honeypots in a Novel SDN-UAV Network Architecture," *IEEE Access*, 2024.
- [5] Z. Wang *et al.*, "A survey on cybersecurity attacks and defenses for unmanned aerial

- systems," *J. Syst. Archit.*, vol. 138, p. 102870, 2023.
- [6] Z. Yu, Z. Wang, J. Yu, D. Liu, H. H. Song, and Z. Li, "Cybersecurity of unmanned aerial vehicles: A survey," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 39, no. 9, pp. 182–215, 2023.
- [7] O. Ceviz, S. Sen, and P. Sadioglu, "A survey of security in uavs and fanets: Issues, threats, analysis of attacks, and solutions," *IEEE Commun. Surv. & Tutorials*, 2024.
- [8] J. Greer IV, "MITRE Attack framework adaptation in UAV usage during surveillance and reconnaissance missions," 2024.
- [9] C. Abdulrazak, "Cybersecurity Threat Analysis And Attack Simulations For Unmanned Aerial Vehicle Networks," *arXiv Prepr. arXiv2404.16842*, 2024.
- [10] R. Shrestha, A. Omidkar, S. A. Roudi, R. Abbas, and S. Kim, "Machine-learning-enabled intrusion detection system for cellular connected UAV networks," *Electronics*, vol. 10, no. 13, p. 1549, 2021.
- [11] V. Hassija *et al.*, "Fast, reliable, and secure drone communication: A comprehensive survey," *IEEE Commun. Surv. & Tutorials*, vol. 23, no. 4, pp. 2802–2832, 2021.
- [12] X. Wang *et al.*, "A Survey on Security of UAV Swarm Networks: Attacks and Countermeasures," *ACM Comput. Surv.*, vol. 57, no. 3, pp. 1–37, 2024.
- [13] N. Malik, H. Sinha, and M. Dahiya, "Security in UAV ecosystem: An implementation perspective," *Sigma J. Eng. Nat. Sci.*, vol. 42, no. 6, pp. 1986–1994, 2024.
- [14] H. A. Khan, H. Khan, S. Ghafoor, and M. A. Khan, "A Survey on Security of Automatic Dependent Surveillance-Broadcast (ADS-B) Protocol: Challenges, Potential Solutions and Future Directions," *IEEE Commun. Surv. & Tutorials*, 2024.
- [15] A. Aldweesh, A. Derhab, and A. Z. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," *Knowledge-Based Syst.*, vol. 189, p. 105124, 2020.
- [16] H. Liu and B. Lang, "Machine learning and deep learning methods for intrusion detection systems: A survey," *Appl. Sci.*, vol. 9, no. 20, p. 4396, 2019.
- [17] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, "A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions," *Electronics*, vol. 9, no. 7, p. 1177, 2020.
- [18] D. Engineer, "Drone Communication and Network Anomaly Detection Dataset." 2024.