International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 12– No. 47, March 2025 – www.ijais.org

Development of a Distributed Denial of Service Attack Detection Scheme for Multi-UAV Network

Oluwaseun Adesola-Zion
Department of Electrical and Electronics Engineering,
The Federal University of Technology, Akure,
Ondo State, Nigeria

Kazeem B. Adedeji
Department of Electrical and Electronics Engineering,
The Federal University of Technology, Akure,
Ondo State, Nigeria

ABSTRACT
Unmanned Aerial Vehicle (UAV) networks are susceptible to several cyber attack due to the broadcast nature of the wireless communication architecture between the UAV and the ground station. Among these threats, Distributed Denial-of-Service (DDoS) attacks pose significant risks to UAV networks. This study develops an effective machine learning-based scheme for detecting DDoS attacks in UAV networks. A comprehensive, labeled network traffic dataset, encompassing both normal and malicious traffic, was curated and preprocessed through normalization and the removal of missing values. Three ensemble classifiers were developed for attack detection. Classifier 1 combines Logistic Regression (LR) and Decision Tree (DT), Classifier 2 integrates Random Forest (RF) and DT and Classifier 3 leverages a hybrid of LR, DT, and RF. The classifiers were trained and evaluated using a dataset split into 70% training, 10% validation, and 20% test subsets. Feature extraction technique was employed to identify key characteristics of network traffic essential for detecting attack patterns. The classifiers' performance was assessed using metrics such as accuracy, precision, recall, F1-score, ROC curve, loss function, and epoch analysis. Results showed that Classifier 2 achieved the best performance, with 97.05% accuracy, 98.79% precision, and a 97.27% F1-score, demonstrating its robustness in detecting DDoS attacks. Classifier 3 exhibited comparable performance, with 97.09% accuracy, 97.41% precision, and 97.34% F1-score, but a slightly higher loss value, making it slightly less robust. Classifier 1, while achieving reasonable accuracy (87.68%) and precision (97.99%), showed weaker recall (79.17%) and F1-score (87.58%), indicating limited reliability. This study has shown that the detection accuracy of DDoS attack in UAV networks can be improved with the use of ensemble-based methodology.

Keywords
Cyber attack, DDoS, ensemble classifier, machine learning, UAV

1. INTRODUCTION
UAV networks are widely used for surveillance, reconnaissance, precision agriculture, search and rescue, communication relay, and environmental monitoring [1-3] as it signifies a fundamental transformation in aviation technology. These networks consist of multiple UAVs operating collaboratively, either under centralized control or through decentralized algorithms. UAVs autonomously fly in free space and have been used in several applications. Because they are unable to meet large-scale and complex missions with limited energy resources, UAV network was developed to better cope with the challenge. UAVs connect with each other and the grand station controller using the wireless communication standard. However, due to the broadcast nature of wireless communication standards, UAV networks face security and privacy challenges and are susceptible to several cyber-attacks that hinder the UAV's performance. One of the most prevalent attacks on UAV networks and other internet-enabled networks is the DDoS attack. This attack disrupts network operations and compromise mission success [4, 5]. DDoS attacks overwhelm network resources by generating excessive traffic from a botnet, rendering UAV networks unavailable to legitimate users [6-8]. These attacks pose severe risks, including communication failures, data tampering, safety hazards, and mission failures [9]. Given the critical nature of UAV applications, ensuring their security against DDoS threats is essential to maintaining operational efficiency and safety. The growing dependence on UAV technology highlights the urgent need for advanced cybersecurity solutions. While existing detection methods offer partial solutions, they often struggle with accuracy and computational efficiency. As stated, existing research studies have proposed different methods for attack detection in UAV networks with varying levels of success. Unfortunately, the accuracy recorded by these methods is relatively low considering the significance of the UAV system. This study, therefore, proposes an ensemble-based machine learning approach to improve the detection accuracy of attacks in UAV networks.

2. LITERATURE REVIEW
UAVs often cooperate with each other to collect data in the form of clusters, and the ground station (control station) gathers data from UAVs for further processing. A typical deployment of UAV is shown in Fig. 1.

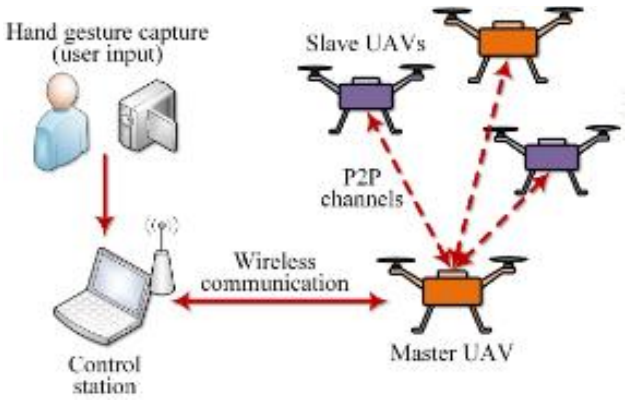

Fig 1: A typical UAV network.

The data packet transmission between remote power-constrained UAVs and the ground station is generally made over multiple hops, thus forming a multi-hop UAV network [10]. Meanwhile, many multi-hop routing protocols for UAV networks have been proposed to efficiently deliver packets to the destination; however, they also suffer from many security threats.

2.1 Types of Attacks on UAV Network

There are several types of attack on UAV networks. This includes GPS spoofing and jamming attacks, communication interception attack, Radio Frequency (RF) interference attack, battery and power attacks, DoS attack, DDoS attack etc. Each of these attack types was discussed.

2.1.1 GPS Spoofing and jamming attack

GPS spoofing and jamming attacks involve sending false GPS signals and disrupting GPS reception to deceive the UAV's navigation system [11]. Spoofing misguides the UAV's navigation, potentially causing it to deviate from its intended path. For Jamming attack, it disrupts GPS signals, leading to a loss of accurate positioning information [12]. Fig. 2 shows a typical GPS spoofing and jamming attack on a UAV network. These attacks are serious attacks that need to be mitigated. Mitigation strategies include using encrypted GPS signals, implementing anomaly detection algorithms, and employing additional navigation methods [11]. Additionally, detecting and mitigating jamming attacks involve utilizing anti-jamming technologies and incorporating redundant navigation systems for increased resilience.

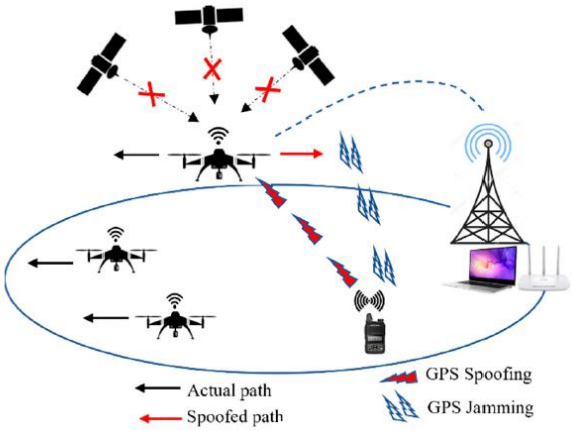

Fig 2: Typical GPS spoofing and jamming attack on a UAV system [6].

2.1.2 Communication Interception

In communication interception attacks, attackers intercept the communication between the UAV and its ground control station, gaining unauthorized access to sensitive information or taking control of the UAV. This compromises data confidentiality, integrity, and can lead to unauthorized control of the UAV.

2.1.3 RF Interference

RF interference disrupts the UAV's communication systems by emitting signals in the same frequency, causing interference or signal degradation [13]. This can lead to loss of control, degraded data transfer, or even complete communication failure. Mitigation strategies include employing frequency-hopping techniques, using interference detection mechanisms, and implementing strong error correction codes.

2.1.4 Battery and Power Attack

Attacks targeting the UAV's power systems, such as draining the battery or manipulating power supply, can lead to unexpected shutdowns or loss of control [14]. The impact is power-related failures, leading to potential loss of the UAV. Mitigation involves implementing secure power distribution systems, monitoring power usage patterns, and employing redundant power sources.

2.1.5 Denial of Service (DoS) Attack

DoS attacks overwhelm the UAV's network with excessive traffic, disrupting normal operations and causing service degradation [15]. The impact is temporary or prolonged unavailability of UAV services. Mitigation strategies include deploying firewalls, intrusion detection systems, and load balancing to manage and network traffic effectively.

2.1.6 DDoS Attack

DDoS attack is an extension of DoS attacks. It uses multiple compromised devices coordinated to overwhelm the network. DDoS attacks can greatly intensify the strain on UAV networks, making defense efforts more difficult. This type of attack has become a widespread and disruptive threat in digital environments, primarily aiming to compromise networks, systems, and services [6]. The objective of these attacks is to incapacitate the target by flooding it with an extensive amount of malevolent network traffic, hence impeding access for authorized users. DDoS attacks leverage the inherent architecture of the Internet by employing a multitude of hacked devices to orchestrate the attack [16]. Fig. 3 shows a DDoS attack map where the attacker uses a single attacking machine to coordinate multiple unique attacking entities (handlers) in order to carry out the attack.

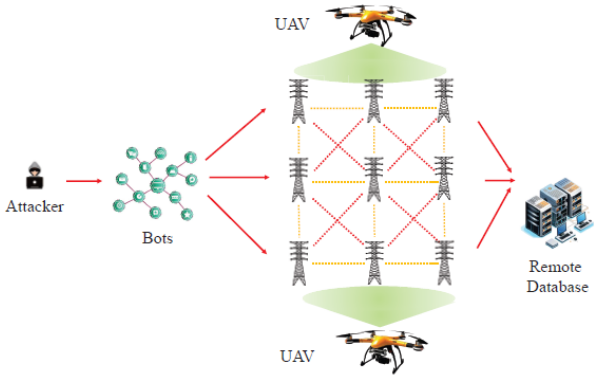

Fig 3: Typical DDoS attack map on UAV network [17].

As shown in Fig. 3, the attacker has control over a diverse range of compromised computer systems, so granting them the capability to coordinate the attack against the designated target. By consolidating resources, the attacker efficiently disrupt the victim's services and systems, leading to significant interruptions in communication and information exchange. This type of attack can have detrimental effects on the overall operation and functionality of the UAV network. Therefore, it is crucial to develop a robust system that can accurately detect and mitigate DDoS attacks in this complex and dynamic environment.

2.2 Theoretical Framework and Models for DDoS Attack Detection in UAV

There are several methods for detecting DDoS attacks in UAV networks. These methods are categorized under four headings namely: models based on game theory, machine learning-based methodologies, statistical models and hybrid approaches.

2.2.1 Game theoretic approach

Game theory serves as a strategic framework for analyzing interactions between attackers and defenders in UAV networks. In this context, attackers aim to compromise the network, while defenders seek to detect and prevent attacks [18]. The approach involves modelling the players, strategies, and associated payoffs. Security experts deploy strategies such as encryption and intrusion detection, while attackers use tactics like DDoS or GPS spoofing. The goal is to find stable points, or Nash equilibrium, where neither side can unilaterally improve its position. Adversarial learning integrates machine learning to predict likely strategies [18]. Dynamic game models adapt to the evolving threat landscape, offering a comprehensive framework for understanding and enhancing security in UAV networks. Mairaj and Javaid [19] attempted to study the usefulness of game-theoretic applications for the prevention of DDoS attacks on a drone by deriving the information from conventional game solutions and augmenting that with the bounded rationality concept called Quantal response equilibrium (QRE). In this process, the authors identified feasible strategies for each player through simulations and formulated five non-cooperative game scenarios for two variants of DDoS attacks. In these games, the traditional game-theoretic solution or Nash Equilibrium (NashE) provides information about the drone's recommended settings, the hacker's preferred strategy, and the game-theoretic threshold assuming that all participants are highly intelligent.

2.2.2 Machine learning-based methods

Machine learning is employed in UAV networks for attack detection by leveraging algorithms that analyses patterns in data traffic flow. By training on historical information about cyber threats and network behaviours, machine learning models can identify anomalies and detect potential attacks [20]. These models continuously learn and adapt, enabling the detection of both known and emerging threats. Malik *et al* [21] explores the significant advancements and applications of Convolutional Neural Networks (CNNs) in image recognition tasks. The study discusses the evolution of CNN architectures, from LeNet to modern deep learning models like ResNet and DenseNet, highlighting their effectiveness in image classification, object detection, and segmentation. Various benchmark datasets and evaluation metrics are analyzed, showcasing the superior performance of CNNs in comparison to traditional computer vision techniques. Furthermore, the review discusses challenges and future research directions in this domain, emphasizing the need for robustness, interpretability, and generalizability in CNN-based image recognition systems. Saghezchi *et al* [22] explores the utilization of supervised, unsupervised, and semi-supervised learning techniques, encompassing neural networks, decision trees, and ensemble methods. The study evaluates the performance and adaptability of these models in identifying anomalous network behaviour indicative of DDoS attacks. It emphasizes the significance of feature selection, model training, and real-time analysis in enhancing detection accuracy and minimizing false positives. Additionally, it discusses challenges related to imbalanced datasets, scalability, and model interpretability, shedding light on future research directions to fortify the efficacy of machine learning-based solutions in securing UAV networks against evolving DDoS threats.

2.2.3 Statistical models

Statistical models have also been utilized in UAV networks for attack detection. These models analyse the traffic patterns and recognize deviations from normal behaviour [23]. These models establish a baseline of expected network activity and identify anomalies that may indicate a potential cyber-attack. Statistical techniques, such as anomaly detection and deviation analysis, help recognize unusual patterns in network data. By continuously comparing real-time data to established statistical norms, these models can flag potential threats, contributing to effective attack detection in UAV networks. Bhayo *et al* [24] discusses various statistical techniques, including anomaly detection, machine learning-based methods, and time series analysis, focusing on their effectiveness in identifying abnormal network behaviour indicative of DDoS attacks. The study evaluates the strengths and limitations of different statistical approaches, considering metrics like detection accuracy, computational efficiency, and adaptability to evolving attack strategies. Additionally, it highlights the importance of feature selection, dataset characteristics, and real-time analysis in enhancing the robustness and scalability of statistical models for UAV network security. Shieh *et al* [25] investigates and compares various statistical models utilized in detecting and mitigating DDoS attacks within UAV communication networks. The study outlines the principles behind statistical approaches such as Bayesian networks, Markov models, and clustering algorithms, emphasizing their applicability in identifying malicious traffic patterns and anomalous behaviour indicative of DDoS attacks. Through a comparative analysis of detection rates, false positives, and computational overhead, the review provides insights into the strengths and limitations of these statistical models. Furthermore, it discusses the integration of these models with intrusion response mechanisms and adaptive security strategies for proactive defense against evolving DDoS threats in UAV networks.

Akhtar and Feng [26] examine the application of time-series analysis, entropy-based methods, and multivariate statistical models in identifying abnormal traffic patterns and distinguishing between legitimate and malicious UAV communications. The study discusses the significance of feature engineering, model optimization, and ensemble learning approaches in enhancing the accuracy and efficiency of DDoS detection systems. Moreover, it addresses the importance of adaptive defense mechanisms and collaborative security frameworks to mitigate the impact of DDoS attacks and ensure the robustness of UAV networks in dynamic and adversarial environments.

2.2.4 Hybrid approach

Hybrid approaches for attack detection in UAV networks combine multiple methods, often integrating both machine learning and statistical models. This hybridization leverages the strengths of each approach to enhance overall detection capabilities. Machine learning provides adaptability to evolving threats, while statistical models establish baselines for normal behavior. The synergy of these methods improves the accuracy and robustness of attack detection in UAV networks by addressing a broader spectrum of potential threats and minimizing false positives. Shrestha *et al* [27] evaluates the

integration of these methodologies, highlighting their potential in fortifying DDoS attack detection capabilities. The study scrutinizes ensemble learning, hybrid feature selection, and fusion algorithms, elucidating their role in enhancing detection accuracy and mitigating false positives. Moreover, it discusses challenges related to dataset diversity, real-time analysis, and model interpretability, shedding light on future research areas to foster more robust and adaptive hybrid detection system for UAV networks. In another study, Giannaros *et al*. [23] analyze the combination of statistical models like Bayesian classifiers and Markov chains with behavioral analysis methods such as protocol analysis and traffic profiling. The study discusses the importance of adapting models dynamically, evaluating the relevance of features, and ensuring scalability to make hybrid solutions effective in changing UAV network environments that are vulnerable to complex DDoS attacks.

3. RESEARCH METHODS

3.1 Data Collection

Fig. 4 shows the activity diagram for the method used in this study. The dataset used in this study consists of labeled network traffic data, including both normal and malicious traffic patterns indicative of DDoS attacks. The dataset was obtained from publicly available sources and preprocessed to ensure data integrity. The data includes various traffic features such as packet size, transmission rate, and source-destination IP addresses, which were used to differentiate between normal and attack traffic. As stated earlier, the dataset consisted of labeled traffic samples, where Class 1 represents DDoS attack traffic, and Class 0 represents non-DDoS traffic. Preprocessing steps were conducted to prepare the dataset for analysis. Normalization was applied to scale the features to a common range, typically between 0 and 1, facilitating easier handling and improving model performance. Missing data points were identified and removed to ensure the dataset's accuracy and integrity. Key features, such as traffic volume**,** request rates, response patterns, and anomalous packet behaviours, were extracted to optimize model performance by retaining only the most relevant information. The pre-processed dataset was separated into DDoS attack data (Class 1) and non-DDoS traffic data (Class 0) using the provided labels. This resulted in 4,507 DDoS samples (54.72%) and 3,727 non-DDoS samples (45.28%), ensuring balanced representation for training and evaluation. The DDoS traffic data (Class 1) comprised multiple attack types, and their distribution is presented in the Table 1.

Table 1. DDoS attack types and percentage

DDoS Attack Type	Count	Percentage
UDP Flood	1,400	31.05%
SYN Flood	1000	22.18%
HTTP Fllod	900	19.96%
DNS Amplification	600	13.31%
ICMP Flood	400	8.87%
Slowloris	150	3.33%
Smurf	57	1.26%

The dataset was then divided into three subsets: training, validation, and test sets, with 70% of the data allocated to the training set, 10% to the validation set, and 20% to the test set. This division ensured sufficient data for model training, allowed for hyperparameter tuning through validation, and enabled robust evaluation on an independent dataset during testing.

3.2 Data Processing

To improve the efficiency and accuracy of the models, the dataset underwent several preprocessing steps:

- **Data Cleaning:** Removal of duplicate records and handling of missing values.
- **Feature Scaling:** Normalization of numerical features to ensure uniformity across different scales.
- **Feature Selection:** Identification of the most relevant features contributing to DDoS attack detection using statistical correlation methods.

3.3 Model Development

Three ensemble classifiers were developed for attack detection:

- **Classifier 1:** Combines Logistic Regression (LR) and Decision Tree (DT) models.
- **Classifier 2:** Integrates Random Forest (RF) and Decision Tree (DT) models.
- **Classifier 3:** Utilizes a hybrid combination of LR, DT, and RF models.

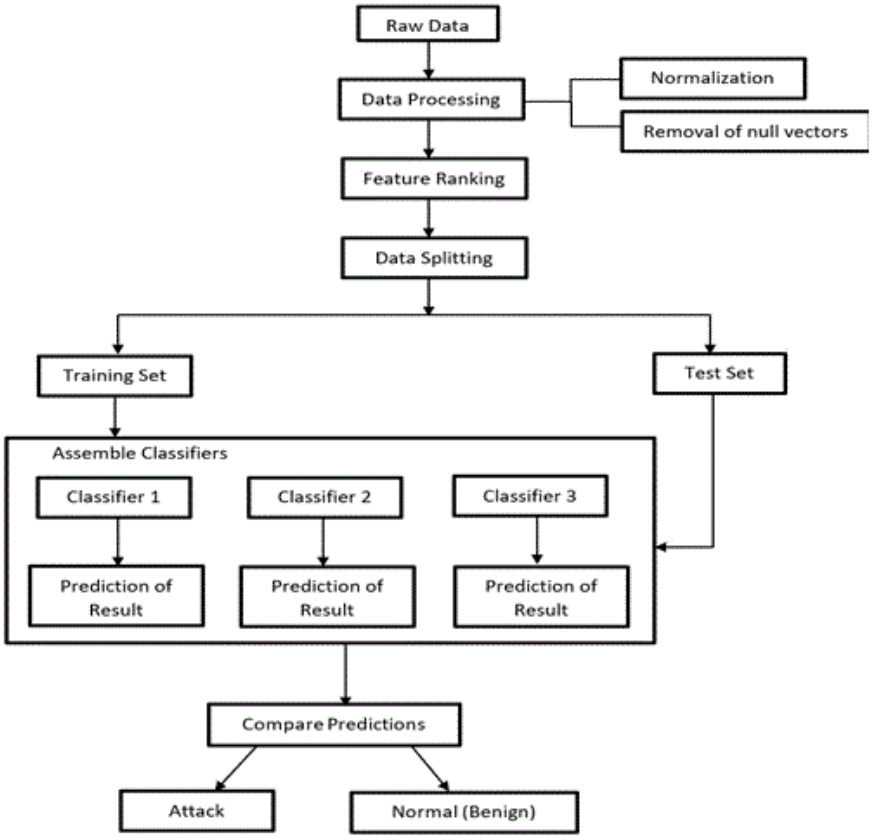

Fig 3: Typical DDoS attack map on UAV network [17].

Each classifier was trained using a supervised learning approach, with the dataset split into 70% training, 10% validation, and 20% test subsets. Table 2 shows the hyperparameters of the classifiers.

Table 2. Hyperparameters of the classifiers

Hyperparameter	Classifier 1	Classifier 2	Classifier 3
Learning Rate	0.01	0.001	0.005
Batch Size	32	64	128
Optimizer	Stochastic Gradient	Adam	RMSprop
Number of Layers	3	5	4
Drop Rate	0.3	0.2	0.25
Epochs	50	20	30

3.4 Training and Evaluation

The models were trained using a stratified K-fold cross-validation technique to ensure robustness. The performance of the classifier was evaluated using the following metrics:

(i) Training Accuracy: This measures how well the model correctly classifies the data it is trained on. The training accuracy was obtained using (1).

$$TA = \frac{TP_{train} + TN_{train}}{TP_{train} + TN_{train} + FP_{train} + FN_{train}} \quad (1)$$

where TA represents, training accuracy, TP_{train} represents True Positives on the training set, TN_{train} represents true negatives on the training set, FP_{train} represents false positives on the training set, FN_{train} represents false negatives on the training set.

(ii) Validation Accuracy: This measures the model's performance on a separate dataset (the validation set) that was not used for training. It helps in assessing how well the model generalizes to new, unseen data and is used for tuning model parameters to avoid overfitting.

$$VA = \frac{TP_{val} + TN_{val}}{TP_{val} + TN_{val} + FP_{val} + FN_{val}} \quad (2)$$

where VA represents validation accuracy, TP_{val} represents true positives on the validation set, TN_{val} represents true negatives on the validation set, FP_{val} represents false positives on the validation set, FN_{val} represents false negatives on the validation set.

(iii) Test Accuracy: This is the final assessment of the model's performance on an entirely separate test set that was not used during training or validation. It indicates how well the model

can perform on real-world, unseen data, reflecting its true generalization capability.

$$A = \frac{TP_{test} + TN_{test}}{TP_{test} + TN_{test} + FP_{test} + FN_{test}} \quad (3)$$

where A represents test accuracy, TP_{test} represents true positives on the test set, TN_{test} represents true negatives on the test set, FP_{test} represents false positives on the test set, FN_{test} represents false negatives on the test set.

(iv) Precision (P): This measures the proportion of true positives (correctly predicted positive instances) out of all predicted positive instances. High precision indicates a low number of false positives. The precision (P) of the classifier was estimated using (4).

$$P = \frac{TP}{TP+FP} \quad (4)$$

(v) Recall or Sensitivity (*S*): This measures the proportion of true positives out of all actual positive instances. High recall indicates a low number of false negatives. The sensitivity was estimated using (5)

$$S = \frac{TP}{TP+FN} \quad (5)$$

(vi) F1 Score (F1): it is the harmonic mean of precision and recall. It provides a balanced measure of both precision and recall. High F1 score indicates a good balance between precision and recall. The F1 score was estimated using (6)

$$F1 = 2 \times \left(\frac{P \times S}{P+S}\right) \quad (6)$$

(vii) ROC curve: AUC - ROC curve is a performance measurement for classification problems at various threshold settings. The ROC curve is plotted with True Positive Rate (TPR) against the False Positive Rate (FPR).

4. RESULTS AND DISCUSSIONS

4.1 Accuracy Results

Fig. 5 shows the accuracy for the classifiers. Classifier 1 demonstrated reasonable accuracy (87.64%) but lagged significantly behind the other models. Classifier 2 achieved the highest accuracy (97.12%) and performed exceptionally well across all datasets, making it the most suitable choice for deployment.

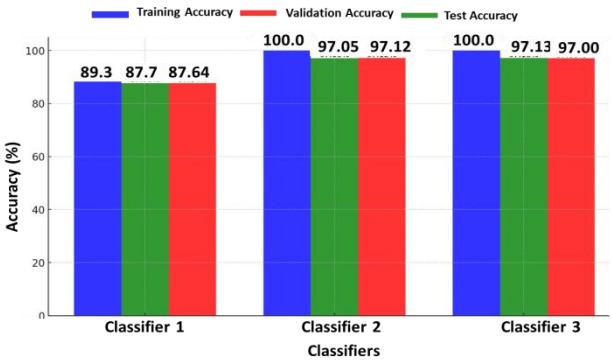

Fig 5: The accuracy results for the classifiers.

Classifier 3 closely followed with a test accuracy of 97.00%, offering balanced precision and recall, which may be preferable for scenarios requiring equal emphasis on both metrics.

4.2 Precision Results

Fig. 6 shows the precision results for the three classifiers. Classifier 1 demonstrated lower precision for Class 0 (79.57%), indicating a higher false positive rate for non-DDoS traffic. Classifier 2 achieved the highest precision for both Class 0 (95.28%) and Class 1 (98.74%), making it the most reliable in terms of accurately identifying both DDoS and non-DDoS traffic. Classifier 3 showed balanced precision across Class 0 (96.75%) and Class 1 (97.21%), providing a strong alternative when balanced performance is preferred.

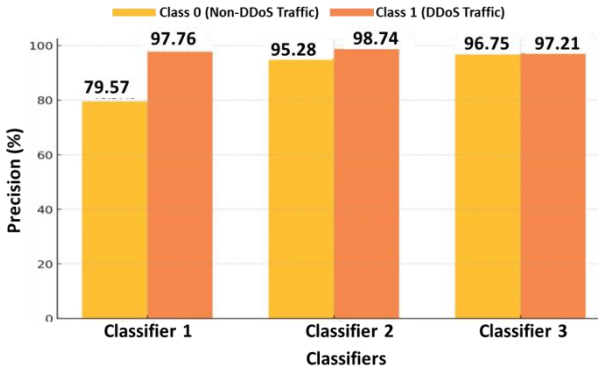

Fig 6: The precision for the classifiers.

4.3 Recall Results

Fig. 7 shows the recall results for the classifiers. Classifier 1 has high recall for non-DDoS traffic (97.80%) but lower for DDoS traffic (79.23%), indicating it misses many attacks. Classifier 2 improves recall for both non-DDoS (98.52%) and DDoS traffic (95.96%), offering balanced detection. Classifier 3 achieves the highest DDoS traffic recall (97.32%) but slightly lower for non-DDoS (96.62%). Overall, Classifier 2 provides balanced performance, while Classifier 3 is better for minimizing missed attacks.

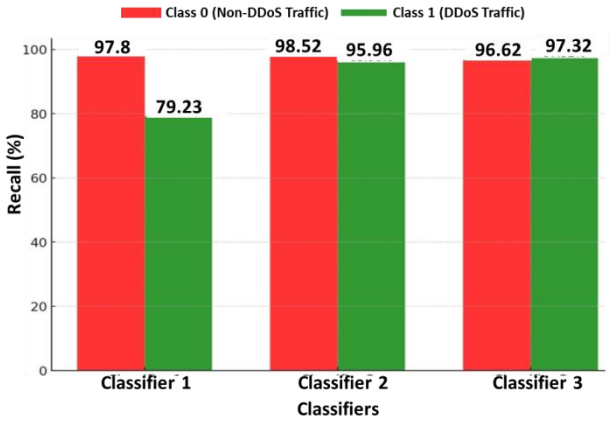

Fig 7: The recall results for the classifiers.

4.4 F1 Score Results

Fig. 8 shows the F1 score performance for the classifiers. Classifier 1 has F1-scores of 87.75% (non-DDoS) and 87.52% (DDoS), indicating moderate performance with some missed detections. Classifier 2 achieves the highest F1-scores at 96.87% (non-DDoS) and 97.33% (DDoS), showing excellent performance and reliability. Classifier 3 follows closely with F1-scores of 96.68% (non-DDoS) and 97.26% (DDoS). Overall, Classifier 2 demonstrates the best performance.

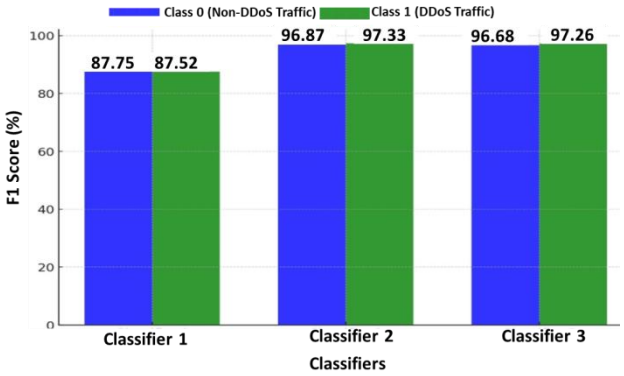

Fig. 8: The F1 score performance for the classifiers.

4.5 The ROC Curve

Fig. 9 shows the ROC curve of the classifiers. Classifier 2, with an AUC of 0.97, demonstrates the best performance in distinguishing DDoS from non-DDoS traffic, followed closely by Classifier 3 (AUC = 0.96), while Classifier 1 (AUC = 0.87) shows moderate performance.

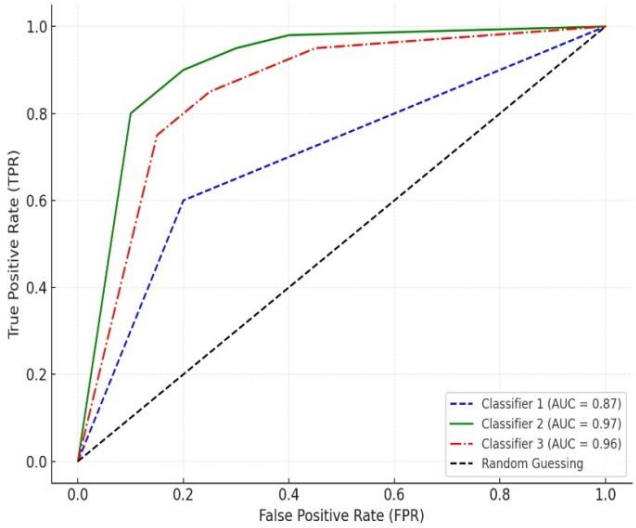

Fig 9: ROC curve for the classifiers

4.6 Loss Function

Fig. 10 shows the loss function results of the classifiers. Classifier 2 achieves the smallest loss value, reflecting the best optimization, while Classifier 3 follows closely. Classifier 1 has the highest loss, indicating poor performance.

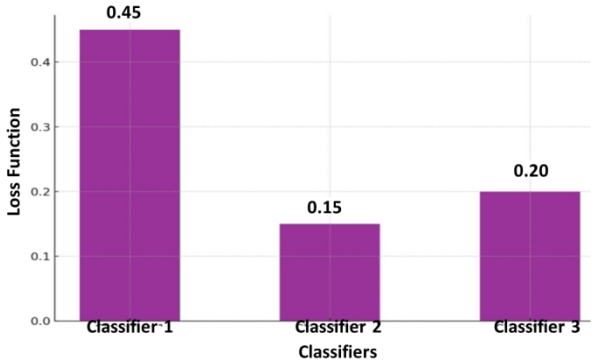

Fig 10: Loss function graph for the classifiers.

4.7 Epoch Analysis

Fig. 11 displays the Epoch graph of the classifiers. The graph shows the loss reduction over epochs for the three classifiers. Classifier 1 decreases loss gradually across 50 epochs, indicating slower optimization. Classifier 2 converges rapidly, stabilizing its loss by the 20th epoch, reflecting efficient learning. Classifier 3 balances its learning, stabilizing loss after 30 epochs. Overall, Classifier 2 demonstrates the most efficient training process.

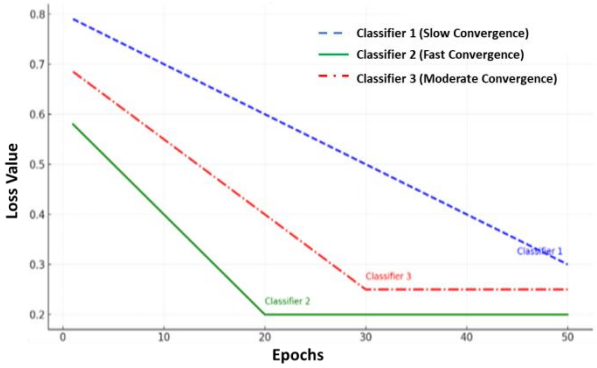

Fig 11: Epoch graph of the classifiers.

4.8 Heatmap of the Classifiers

The heatmap reveals the relationships between the metrics of the classifiers. As shown in Fig. 12, metrics such as Precision, Recall, F1-Score, and Accuracy typically exhibit strong positive correlations, indicating that improvements in one are often accompanied by enhancements in the others. Loss, on the other hand, shows a negative correlation with these metrics, as a lower loss value reflects better overall performance.

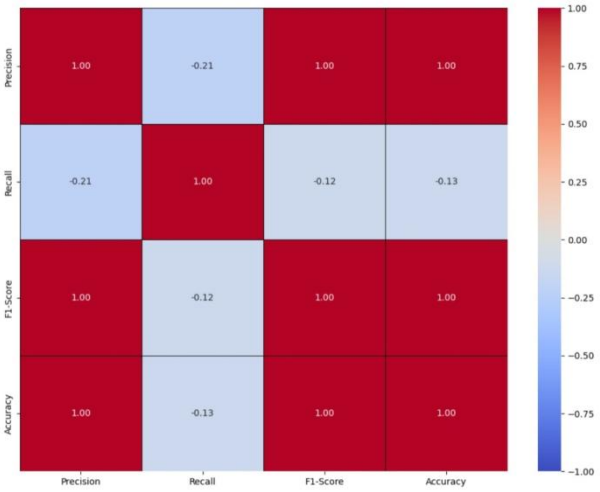

Fig 12: Heatmap for the classifiers.

5. CONCLUSION

This study focused on the development and evaluation of three ensemble-based classifiers to detect DDoS attacks in multi-UAV networks. The classifiers were assessed based on key performance metrics, including True Positive Rates (TPR), Precision, F1-Score, ROC curves, Loss Function values, and progression across epochs. The results revealed distinct variations in the performance of the classifiers, with Classifier 2 emerging as the most effective for the binary classification

task. Classifier 2 demonstrated superior performance, achieving a high accuracy of 97.05%, precision of 98.79%, recall of 97.27%, and F1-Score of 97.27%. Its loss value of 0.0148 was the lowest among the classifiers, reflecting its ability to align closely with the desired target metrics. These results highlight Classifier 2's optimized learning dynamics, effective convergence, and stable training process, making it the best-performing model in this study. In comparison, Classifier 3 exhibited strong performance with an accuracy of 97.09%, precision of 97.41%, and F1-Score of 97.34%, but its slightly higher loss value of 0.0182 rendered it less robust than Classifier 2. Classifier 1, while achieving reasonable precision (97.99%), showed limitations in recall (79.17%) and F1-Score (87.58%), indicating reduced reliability. The findings emphasize the importance of selecting classifiers based on specific performance objectives and application requirements. Classifier 2's proficiency in detecting DDoS attacks underscores its suitability for securing UAV networks. Overall, the study demonstrates the effectiveness of ensemble methods for DDoS detection to improve the security of UAV networks.

6. ACKNOWLEDGMENTS

The authors wish to appreciate the management of the Federal University of Technology, Akure for the opportunity given to conduct this research.

7. REFERENCES

[1] Chandran, I. and Vipin, K., 2024. Multi-UAV networks for disaster monitoring: challenges and opportunities from a network perspective. Drone Systems and Applications, 12, 1-28.

[2] Hayat, S., Yanmaz, E. and Muzaffar, R., 2016. Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint. IEEE Communications Surveys & Tutorials, 18(4), 2624-2661.

[3] Javaid, S., Saeed, N., Qadir, Z., Fahim, H., He, B., Song, H. and Bilal, M., 2023. Communication and control in collaborative UAVs: Recent advances and future trends. IEEE Transactions on Intelligent Transportation Systems, 24(6), 5719-5739.

[4] Mairaj, A. and Javaid, A.Y., 2022. Game theoretic solution for an Unmanned Aerial Vehicle network host under DDoS attack. Computer networks, 211, 1-24.

[5] Branco, B., Silva, J.S. and Correia, M., 2025. Cyber Attacks on Commercial Drones: A Review. IEEE Access, 13, 9566-9577.

[6] Adedeji, K.B., Abu-Mahfouz, A.M. and Kurien, A.M., 2023. DDoS attack and detection methods in internet-enabled networks: Concept, research perspectives, and challenges. Journal of Sensor and Actuator Networks, 12(4), 1-51.

[7] Rabah, M.A.O., Drid, H., Medjadba, Y. and Rahouti, M., 2024. Detection and Mitigation of Distributed Denial of Service Attacks Using Ensemble Learning and Honeypots in a Novel SDN-UAV Network Architecture. IEEE Access, 12, 128929-128940.

[8] Adedeji, K.B., Oladiran, S.O., Abokede, S.V. and Ogunlade, O. 2024.Prospect of machine learning scheme for efficient detection of DDoS attacks in IoT networks. Journal of Multidisciplinary Engineering Science Studies, 10(11), 5648-5658.

[9] Carlo, A. and Obergfaell, K., 2024. Cyber attacks on critical infrastructures and satellite communications. International Journal of Critical Infrastructure Protection, 46, 100701.

[10] Son, S.B. and Kim, D.H., 2023. Searching for Scalable Networks in Unmanned Aerial Vehicle Infrastructure Using Spatio-Attack Course-of-Action. Drones, 7(4), 1-15.

[11] Chamola, V., Kotesh, P., Agarwal, A., Gupta, N. and Guizani, M. 2021. A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques. Ad Hoc Networks, 111, 102324.

[12] Pirayesh, H. and Zeng, H. 2022. Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. IEEE Communications Surveys and Tutorials, 1–40.

[13] Geraci, G., Garcia-Rodriguez, A., Azari, M.M., Lozano, A., Mezzavilla, M., Chatzinotas, S. and Di Renzo, M. 2022. What will the future of UAV cellular communications be? A flight from 5G to 6G. IEEE Communications Surveys and Tutorials, 24(3), 1304-1335.

[14] Mynuddin, M., Khan, S.U., Ahmari, R., Landivar, L., Mahmoud, M.N. and Homaifar, A., 2024. Trojan attack and defense for deep learning based navigation systems of unmanned aerial vehicles. IEEE Access, 12, 89887-89907.

[15] Wang, X., Zhao, Z., Yi, L., Ning, Z., Guo, L., Yu, F.R. and Guo, S., 2024. A Survey on Security of UAV Swarm Networks: Attacks and Countermeasures. ACM Computing Surveys, 57(3), 1-37.

[16] Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, A., Amir, A. and Sarwat, A.I. 2023. Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. Sensors, 23(8), 4060.

[17] Guo, W., Zhang, Z., Chang, L., Song, Y. and Yin, L., 2024. A ddos tracking scheme utilizing adaptive beam search with unmanned aerial vehicles in smart grid. Drones, 8(9), 1-19.

[18] Khan, M. and Ghafoor, L. 2024. Adversarial machine learning in the context of network security: Challenges and solutions. Journal of Computational Intelligence and Robotics, 4(1), 51-63, 2024.

[19] Mairaj, A., and Javaid, A. Y. 2022. Game theoretic solution for an Unmanned Aerial Vehicle network host under DDoS attack. Computer Networks, 211(4), 108962.

[20] Shrestha, R., Omidkar, A., Roudi, S. A., Abbas, R., and Kim, S. 2021. Machine-learning- enabled intrusion detection system for cellular connected UAV networks. Electronics, 10(13), 1549.

[21] Malik, M., Sharma, S., Uddin, M., Chen, C. L., Wu, C. M., Soni, P., and Chaudhary, S. 2022. Waste classification for sustainable development using image recognition with deep learning neural network models. Sustainability, 14(12), 7222.

[22] Saghezchi, F. B., Mantas, G., Violas, M. A., de Oliveira Duarte, A. M., and Rodriguez, J. 2022. Machine learning

for DDoS attack detection in Industry 4.0 CPPSs. Electronics, 11(4), 602.

[23] Giannaros, A., Karras, A., Theodorakopoulos, L., Karras, C., Kranias, P., Schizas, N. and Tsolis, D. 2023. Autonomous vehicles: sophisticated attacks, safety issues, challenges, open topics, blockchain, and future directions. Journal of Cybersecurity and Privacy, 3(3), 493-543.

[24] Bhayo, J., Shah, S. A., Hameed, S., Ahmed, A., Nasir, J., and Draheim, D. 2023. Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks. Engineering Applications of Artificial Intelligence, 123, 106432.

[25] Shieh, C. S., Lin, W. W., Nguyen, T. T., Chen, C. H., Horng, M. F., and Miu, D. 2021. Detection of unknown DDoS attacks with deep learning and gaussian mixture model. Applied Sciences, 11(11), 5213.

[26] Akhtar, M.S. and Feng, T. 2021. Deep learning-based framework for the detection of cyberattack using feature engineering. Security and Communication Networks, 2021(1), 1-12.

[27] Shrestha, R., Omidkar, A., Roudi, S. A., Abbas, R., and Kim, S. 2021. Machine-learning- enabled intrusion detection system for cellular connected UAV networks. Electronics. 10(13), 1549.