







Evaluation of Machine Learning Models for Attack Detection in Unmanned Aerial Vehicle Networks

AHMET FARUK GÖRMÜŞ¹ , SERKAN GÖNEN^{1,*} , ABDULSAMET HAŞILOĞLU¹ , ERCAN NURCAN YILMAZ² 

¹*Department of Computer Engineering, Istanbul Gelisim University, Istanbul, Turkey.*

²*Department of Electrical Electronics Engineering, Gazi University, Ankara, Turkey.*

Received: 17-10-2024 • Accepted: 27-11-2024

ABSTRACT. Nowadays, unmanned aerial vehicles (UAVs) are increasingly utilized in various civil and military applications, highlighting the growing need for robust security in UAV networks. Cyberattacks on these networks can lead to operational disruptions and the loss of critical information. This study evaluates five machine learning models—Random Forest (RF), CatBoost, XGBoost, AdaBoost, and Artificial Neural Networks (ANN)—for detecting attacks on UAV networks using the CICIOT2023 (Canadian Institute for Cybersecurity Internet of Things 2023) dataset. Performance metrics such as accuracy, precision, sensitivity, and F1 score were used to assess these models. Among them, CatBoost demonstrated superior performance, achieving the highest accuracy and the fastest prediction time of 6.487 seconds, making it particularly advantageous for real-time attack detection. This study underscores the effectiveness of CatBoost in both accuracy and efficiency, positioning it as an ideal choice for enhancing UAV network security. The findings contribute to addressing cybersecurity vulnerabilities in UAV networks and support the development of more secure network infrastructures.

2020 AMS Classification: 97R70

Keywords: UAV networks, cyber attack, attack detection, CICIOT2023 dataset, performance evaluation, security vulnerabilities.

1. INTRODUCTION

Unmanned aerial vehicles (UAVs) are rapidly becoming widespread in civil and military areas, and the importance of ensuring the security of UAV networks is increasing. UAVs are used in various critical missions such as military reconnaissance, border security, firefighting, agriculture, and logistics. This widespread use makes UAVs vulnerable to cyber attacks and can lead to operational disruptions and loss of sensitive information. Ensuring the security of UAV networks is possible by detecting and preventing such attacks. However, the dynamic and complex nature of UAVs makes traditional security measures inadequate. In particular, the constant exchange of data between UAVs and control centers increases the risk of attackers blocking and manipulating this traffic. Therefore, machine learning techniques emerge as an effective solution in attack detection and prevention processes.

As seen in Figure 1, the UAV network attack and detection model is shown. Within the scope of this model, the detection of attacks against UAV networks was evaluated using the CICIOT2023 dataset. CICIOT2023 is a comprehensive dataset that includes various attack types and contains many attack scenarios and normal traffic data samples.

*Corresponding Author

Email addresses: afgormus@gelisim.edu.tr (A.F. Görmüş), *sgonen@gelisim.edu.tr (S. Gönen), ahasiloglu@gelisim.edu.tr (A. Haşiloğlu), enyilmaz@gazi.edu.tr (E.N. Yılmaz)

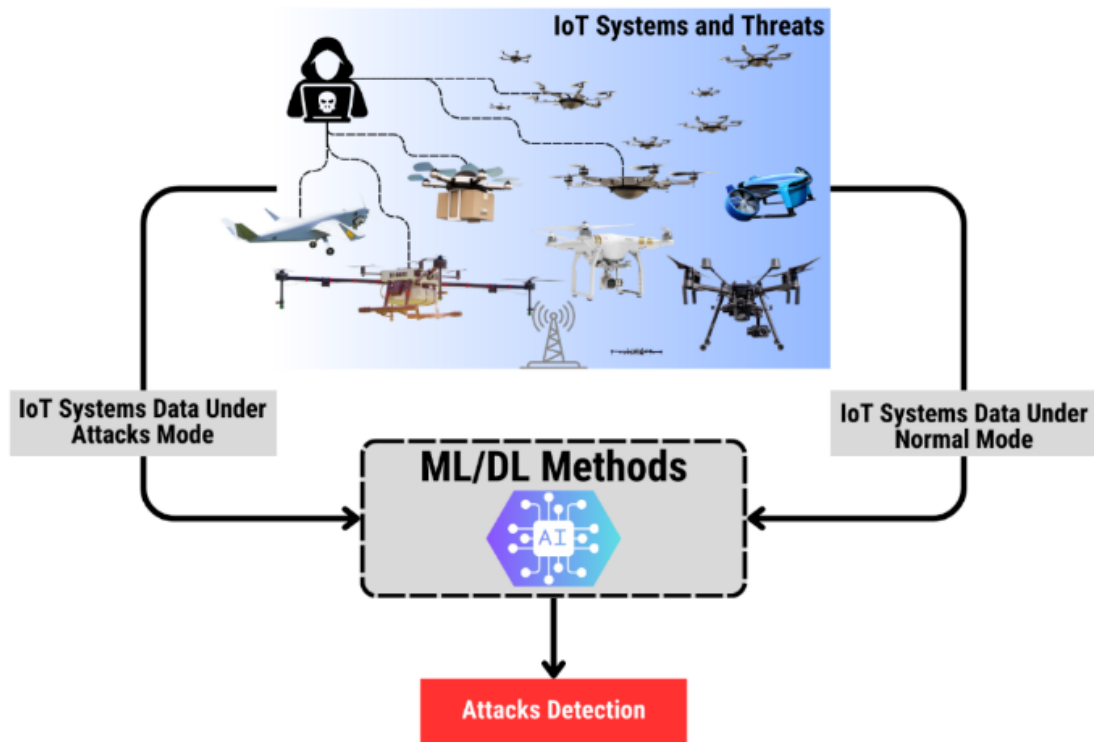


FIGURE 1. UAV Network Cyber Attack and Detection Model

It usually contains network traffic features, packet data, timestamps and labels corresponding to different attack types. This rich dataset provides an ideal source for training and testing attack detection models. The study aims to determine the most effective method in attack detection and aims to do this by comparing the performances of different algorithms. The evaluated algorithms include RFC, CatBoost, XGBoost, AdaBoost and ANN. Each model was analyzed using performance metrics such as accuracy, precision, specificity and F1 score. Comparison of model performances helped to identify methods that effectively detect certain types of attacks. This study focuses on the use of machine learning models for detecting cyber attacks in UAV networks and compares the performance of different algorithms. The findings provide valuable information for securing UAV networks and aim to contribute to advances in network architectures for improved security. The results will help determine the most effective machine learning techniques that can be used to protect UAV networks and guide the development of future security measures.

This research evaluates how effective machine learning models are in detecting cyber threats in unmanned aerial vehicle (UAV) networks. It finds that the CatBoost algorithm outperforms all other models due to its high accuracy rates and fast prediction times, which can be used to develop real-time systems to detect threats in UAV network environments. The study provides a starting point for further research on securing such networks, while also filling in the gaps missed by previous methods, as it demonstrates how well AI (Artificial Intelligence) techniques can be applied to detect and mitigate security weaknesses found in such areas.

The structure of this paper follows a methodical review of machine learning algorithms designed for intrusion detection in UAV networks. To contextualize the problem, the introduction first discusses why securing drones against hackers is becoming increasingly important. This is followed by a comprehensive review of relevant literature materials, where the weaknesses and strengths among the various studies conducted to date are clearly outlined. Next comes the data collection methods section, which provides information about the datasets used in this process and the steps taken to preprocess these input values before feeding them to the different ML models discussed next. The results section provides detailed analysis on the performances of the different algorithms used in this experiment, highlighting the advantages associated with using the CatBoost algorithm over others.

The findings from our research highlight the value of using machine learning models to detect cyberattacks on UAV networks. In particular, among all the algorithms considered, CatBoost has been shown to deliver better results – higher accuracy rates and faster predictions are its strengths; moreover, Catboost takes only 6.487 seconds to make a prediction, making it perfect for real-time attack detection on UAV systems. These results contribute significantly to reducing cybersecurity vulnerabilities, making catboost an ideal choice when protecting drone networks.

2. LITERATURE REVIEW

In the literature, Unmanned Aerial Vehicle (UAV) networks have been extensively covered in terms of cyber attacks. Researchers have studied in detail the various applications of UAVs and the security threats encountered in these areas [1, 2]. This section reviews the attacks on UAV networks and the methods used to detect these attacks.

Cyberattacks on UAV networks typically target UAVs' control systems, communication networks, and sensors [3]. These attacks can take various forms, including device control, data manipulation, denial of service (DoS), and distributed denial of service (DDoS). In particular, attacks aimed at taking control of UAVs can lead to serious security and privacy violations. Such attacks can prevent UAVs from performing their operational missions and can result in the theft of critical information [4, 5].

Many methods and models have been developed to detect cyber attacks, such as Intrusion Detection Systems (IDS). These methods are generally divided into two main categories: anomaly detection and signature-based detection. Signature-based detection methods detect attacks using signatures that describe known attack patterns. However, these methods may be inadequate in detecting attacks that have not been seen before [6].

Anomaly detection methods aim to detect abnormal behaviors by learning normal network traffic patterns. These methods are developed using machine learning and artificial intelligence techniques. Models such as Convolutional Neural Networks (CNN) are widely used for anomaly detection. These models are trained on large datasets and accurately detect anomalies and attack patterns in network traffic [7].

The CICIOT2023 dataset is a comprehensive dataset that includes various cyberattacks on IoT networks and normal network traffic. This dataset provides a suitable resource for training and evaluating machine learning models by covering different types of attacks and normal network traffic. This dataset, which includes various features and labels, has a wide range of applications in intrusion detection studies [8].

Various deep learning and machine learning-based intrusion detection systems have been developed to enhance network security for UAVs by detecting anomalies using models such as CNN and RNN [9]. Machine learning plays a crucial role in improving security for flying vehicles, including UAVs, through cyberattack detection, predictive maintenance, and anomaly detection [10]. Another study focused on 6G networks for UAVs successfully demonstrated the detection of threats like jamming and GPS spoofing using machine learning models [11]. Additionally, the use of meta-heuristic approaches, such as CNN-BiLSTM models, has improved both the speed and accuracy of UAV security measures [12]. Collaborative deep learning-based intrusion detection systems have also been developed, showing high success in detecting real-time attacks [13]. A comparative assessment of four different deep learning models for detecting GPS spoofing attacks revealed that the Convolutional Auto-Encoder was the most effective [14]. Lightweight machine learning-based detection systems, developed with the limited resources of UAVs in mind, offer high accuracy with low computational cost [15]. A deep learning review on UAV detection highlights the challenges of detecting UAVs using radar, acoustics, and visual data, while proposing future research directions [16]. Finally, Trojan attacks on deep learning-based navigation systems present a significant threat to UAVs, and robust security measures are required to defend against these types of attacks [17]. This literature review provides an overview of the methods used to detect cyber attacks in UAV networks and forms the basis of this study by introducing the CICIOT2023 dataset. The study aims to compare the performance of different machine learning models in detecting attacks in UAV networks by evaluating the existing approaches in the literature.

3. MATERIALS AND METHODS

This section will explain in detail the dataset, machine learning models used, and data processing steps used to detect attacks on UAV networks. The aim of the study is to determine the most effective method by comparing the performance of different machine learning algorithms in detecting attacks.

3.1. CICIOT2023 Dataset and Its Features. The CICIOT2023 dataset is a comprehensive dataset created for research and development in the field of Internet of Things (IoT) security. Containing network traffic data from various IoT devices, this dataset provides a unique resource for security analysis. CICIOT2023 divides the data into two main categories: normal and malicious traffic. This allows researchers to investigate vulnerabilities and attack vectors related to IoT devices. The dataset covers a wide range of attack types and their impact on network traffic. It also provides labeled data for the development and testing of data mining and machine learning algorithms. This provides an ideal platform for improving the accuracy and effectiveness of security solutions.

Using this dataset, various attack scenarios in UAV networks were investigated, which is shown in Figure 2. The investigation of these attack scenarios aimed to identify vulnerabilities and potential attack vectors in UAV networks. As seen in Figure 2, the types of attacks applied vary according to the characteristics of the dataset. Therefore, different combinations of attack types can lead to different datasets. Updating the security of the dataset according to modern attack types is critical for data security. In this study, new strategies and solutions were developed to increase the security of UAV networks using the CICIOT2023 dataset [18].

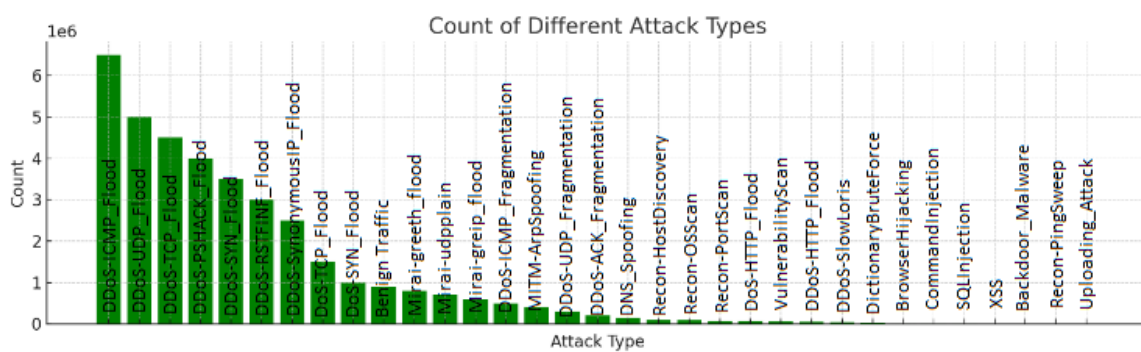


FIGURE 2. Characteristics of Attack Classes in the Dataset

3.2. Machine Learning Models Used. Five different machine learning models are used for intrusion detection in the study. These models are Random Forest Classifier (RFC), Categorical Boosting (CatBoost), Extreme Gradient Boosting (XGBoost), Adaptive Boosting (AdaBoost) and Artificial Neural Network (ANN). RFC is an ensemble method that combines multiple decision trees. Ensemble methods are a technique that allows multiple machine learning models to be used together. CatBoost is a gradient boosting model that automatically processes categorical variables. XGBoost is a gradient boosting library that works fast and scalably on large datasets. AdaBoost is a meta-learning algorithm that combines weak classifiers to form a strong classifier. Inspired by biological neural networks, ANN is a deep learning model that can learn complex structures. Each of these models offers different advantages to increase the performance of intrusion detection [19].

3.3. Data Preprocessing and Feature Selection. The dataset was preprocessed for training and evaluation of the models. The study addressed the class imbalance issue in the dataset through the application of the Synthetic Minority Over-sampling Technique (SMOTE), a widely used method for enhancing dataset balance. SMOTE generates synthetic examples for underrepresented classes by interpolating existing data points within the minority class. This approach effectively increases the number of samples in these classes, ensuring that they are better represented during model training.

In the context of the CICIOT2023 dataset, which contained a wide range of attack types with varying frequencies, SMOTE was particularly instrumental in reducing the bias toward majority classes, such as normal traffic or common attacks like DoS. By applying SMOTE, the dataset achieved a more equitable distribution of classes, enabling the machine learning models to generalize more effectively and improve their detection capabilities across all attack types. This preprocessing step was critical for ensuring the robustness of the proposed models, as it minimized the risk of overfitting to the majority classes and enhanced the reliability of the performance metrics, such as accuracy, F1 score, and recall, especially for minority attack classes. The balanced dataset thus supported a comprehensive evaluation of model effectiveness in real-world cybersecurity scenarios. The preprocessing steps applied are as follows:

1) Data Cleaning: Identifying and correcting erroneous or missing data in the dataset. Removing erroneous data is important for the proper functioning of the dataset.

2) Feature Selection: Since redundant features can affect the processing speed, selecting relevant features is important to reduce the computational time. In addition, selecting appropriate features makes the model more understandable and applicable.

3) Data Standardization: Ensuring that the data in the dataset conforms to a certain format or units. Standardizing the data ensures that different formats from various sources are harmonized.

4) Data Splitting: Splitting the dataset into training and test sets according to a certain ratio is an important step.

5) Data Balancing: Increasing the number of classes with fewer examples in the dataset. Figure 3 shows the process of applying SMOTE to the features of the attack classes. The Ordered Boosting technique addresses target leakage, effectively mitigating overfitting, while its symmetric tree structures facilitate faster predictions and efficient memory usage.

In this study, the feature selection process played a critical role in optimizing the performance of the machine learning models. While the preprocessing steps included data cleaning, standardization, and balancing, the specific methods used for feature selection could benefit from further elaboration. To ensure computational efficiency and improve model interpretability, employing techniques such as Recursive Feature Elimination (RFE) or mutual information-based selection would have provided a more transparent approach to identifying the most impactful features.

Additionally, leveraging models like Random Forest (RF) or CatBoost, which inherently compute feature importance, could offer valuable insights. RF determines feature importance based on Gini impurity reduction across its decision trees, while CatBoost evaluates importance within its boosting framework. Such metrics would allow for a more robust ranking of features, directly linking their relevance to the detection of specific cyberattack patterns. For instance, features such as Packet Size, Bytes Sent, Protocol Type, and Service are likely to have high importance due to their strong association with network anomalies like DDoS attacks. Reporting these rankings and their impact on model performance would enhance the transparency and credibility of the feature selection process, providing greater clarity on how these features contribute to detecting UAV network intrusions.

The CICIOT2023 dataset [22], utilized in this study, consists of a comprehensive collection of 1,050,000 instances, with 50,000 samples allocated for testing and 1,000,000 samples for training. The dataset includes 28 features that capture various aspects of network traffic, such as packet size, time intervals, protocol types, and service details. Key features include Protocol Type, indicating the communication protocol (e.g., TCP, UDP, ICMP), Service, specifying the targeted service (e.g., HTTP, DNS), Duration of the connection, Packet Count, representing the number of packets transmitted, Bytes Sent, indicating the total data transferred, Flag Status, detailing network packet flags, and Timestamp, providing temporal information. The data is labeled with Attack Label, distinguishing between benign and malicious activities. Malicious traffic is further categorized into specific attack types, including Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), Data Manipulation, Command Injection, and GPS Spoofing. To address class imbalances, the Synthetic Minority Over-sampling Technique (SMOTE) was applied, particularly for underrepresented attack categories, ensuring that the machine learning models could generalize effectively. This dataset offers a rich and diverse resource for evaluating intrusion detection systems and is pivotal in advancing cybersecurity measures in UAV networks.

3.4. Creating and Training the Model. In this study, as seen in Figure 4, intrusion detection was performed on network traffic using artificial intelligence algorithms. The network traffic data recorded by the system was analyzed with various artificial intelligence algorithms. The intrusion detection model consists of four stages. In the first stage, the data obtained from the network traffic was subjected to preprocessing steps to create a suitable dataset. The dataset was divided into 10-millisecond segments before being loaded into the model to increase the accuracy of the algorithms. In the second stage, the prepared dataset was trained with 50,000 data points and tested with more than 1,000,000 data points. Various artificial intelligence algorithms such as RFC, CatBoost, XGBoost, AdaBoost and ANN were used in this process. In the third stage, visualization techniques were used to better analyze the results of the artificial intelligence algorithms. These techniques provided a clearer analysis of the algorithm performance. In the final evaluation phase, the CatBoost algorithm was selected for intrusion detection, as it showed the highest accuracy, F1 score, recall, precision and time values across all attack types. It was also registered for use with real-time data.

3.5. Model Selection and Rationale. The selection of machine learning models such as CatBoost, ANN, and RF for this study was guided by their specific advantages in handling diverse and complex datasets, as well as their proven

effectiveness in similar contexts. CatBoost was chosen for its robust handling of categorical data without the need for extensive preprocessing, as it natively supports categorical features through its gradient boosting framework. Its use of Ordered Boosting and symmetric trees minimizes overfitting and ensures high accuracy and efficiency, which are critical for real-time applications like UAV intrusion detection. Studies have consistently highlighted its superiority in scenarios with categorical and imbalanced data.

Artificial Neural Networks (ANNs) were included due to their ability to model complex non-linear relationships in data. Their flexibility makes them ideal for capturing intricate attack patterns in UAV network traffic. ANN's structure allows it to generalize well in detecting a wide range of cyberattacks, as demonstrated in prior work on anomaly detection and predictive maintenance in UAV systems. Random Forest (RF) was selected for its interpretability and ensemble nature, combining multiple decision trees to reduce variance and improve prediction stability. It is particularly effective for datasets with mixed data types and has a strong track record in intrusion detection tasks. RF also provides insights into feature importance, aiding interpretability.

These models complement each other, offering a balance of speed, accuracy, and robustness to effectively address the challenges of UAV network security.

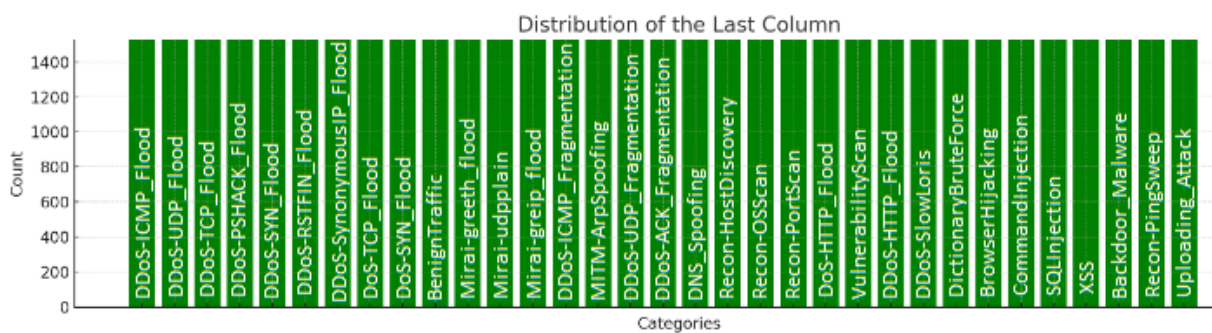


FIGURE 3. Illustrates the cloned features of attack classes in the dataset for training.

3.6. CatBoost Algorithm. The CatBoost algorithm is a gradient boosting method based on decision trees, specifically optimized for working with categorical data. This algorithm is a modern machine learning technique that can provide faster and higher accuracy rates compared to other boosting methods. CatBoost uses categorical data directly and eliminates the need to convert them to numerical values, simplifying the data preprocessing process and improving model performance. One of the main advantages of CatBoost is that it uses unique techniques to prevent overfitting, thus reducing the risk of overfitting. In addition, the CatBoost algorithm builds each decision tree based on training data and successively adds new decision trees to reduce errors in the data. This process of reducing errors gradually improves the model's prediction accuracy. By using symmetric trees, CatBoost speeds up the training process and increases the generalization ability of the model. The speed and efficiency of the algorithm, the ability to produce fast results on large data sets due to low computational requirements, its mathematically simple and understandable structure, and the ability to achieve high accuracy rates, especially with categorical data, are among its advantages [20].

3.7. Creating and Training the Model. This section focuses on the second stage where attack analyses are performed and the packets transferred to the expert system are processed using machine learning and artificial intelligence algorithms. The packets captured in the expert system used for intrusion detection are labeled as both 33 different attack types and normal network packets. This classification process is introduced to the expert system. After the completion of the classification stage, 50,000 data points are used to train various artificial intelligence algorithms and more than 1,000,000 data points are used for testing and the obtained results are analyzed. The accuracy of the decision tree can be examined based on this data. At this stage, the packets classified and labeled by the expert system are analyzed using various artificial intelligence algorithms. In general, parameters such as F1 score, recall, precision and accuracy are emphasized in classification type studies. However, in cyber security, it is of great importance to quickly detect cyber attacks according to attack classes. Therefore, the testing process applied after the training stage is very important for the study. In addition, the shortness of the testing period is as critical as the accuracy rate. When the values in Table 1 are examined, it is observed that the accuracy rates of the algorithms are similar.

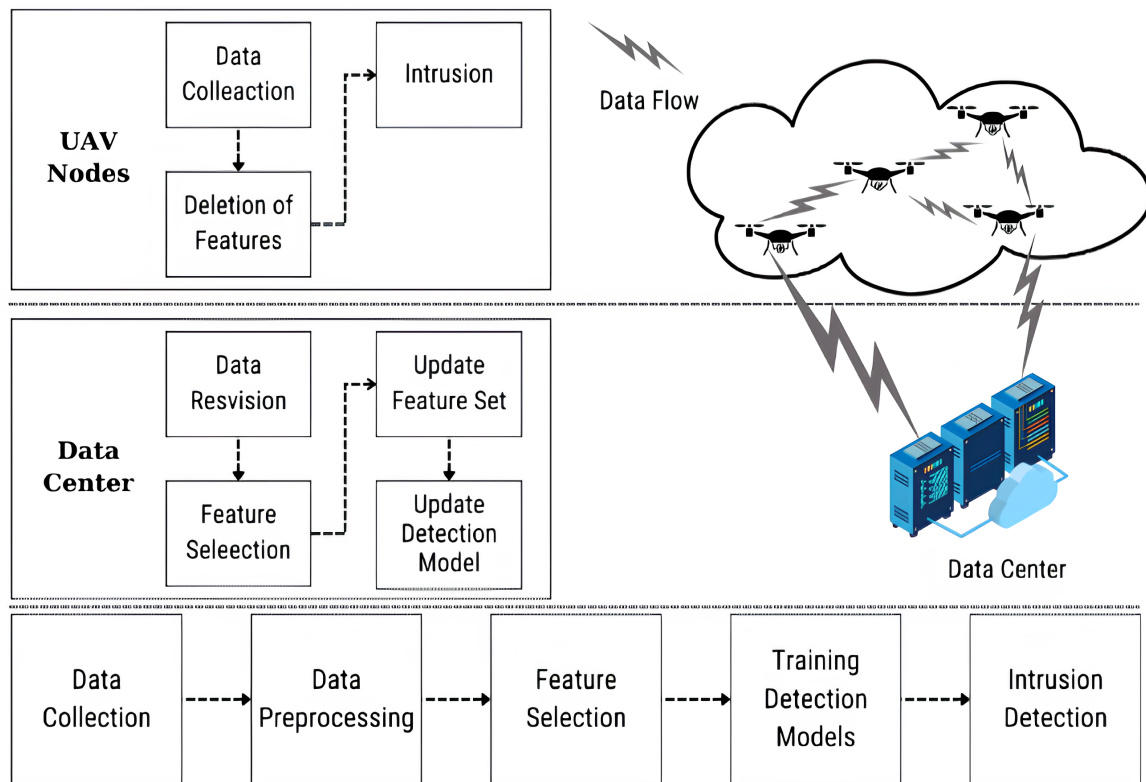


FIGURE 4. Data and model training stages of the CatBoost algorithm.

Table 1. Model Comparison.

Model	Accuracy Score	Recall Score	Precision Score	F1 Score	Training Time (s)	Test Time (s)
RFC	0.986050	0.986050	0.989801	0.987567	25.089776	26.329253
CatBoost	0.980467	0.980467	0.986566	0.982895	58.325107	6.487063
XGBoost	0.990174	0.990174	0.992309	0.991075	28.288238	279.035625
AdaBoost	0.402281	0.402281	0.429845	0.307580	18.431036	212.139942
ANN	0.825719	0.825719	0.838950	0.815586	37.430356	191.186571

However, when focusing on the test period, it is clear that the CatBoost algorithm detects attacks faster and with higher success rates than other algorithms. Therefore, although some algorithms have high accuracy rates, the algorithms with shorter test periods and lower accuracy rates compared to other algorithms can be selected as the most successful algorithms. In this context, it was decided to use the CatBoost algorithm in the expert system.

Figure 5 shows a heat map of the confusion matrix used to evaluate the performance of a classification model.

The horizontal axis of the matrix represents the predicted classes, and the vertical axis represents the true classes. Each cell in the matrix shows the number of instances for which a given true class was predicted as a given class. The color scale on the right side of the matrix represents the density of the cell values; dark blue indicates high match counts, and light colors indicate low match counts.

The cells on the diagonal of the matrix represent instances correctly classified by the model, meaning that the predicted class matches the true class. In contrast, the cells off the diagonal represent misclassifications, where the predicted class does not match the true class. The heat map visually shows the accuracy of the model’s predictions for each class, highlighting which classes are predicted more accurately and which are frequently predicted incorrectly. In addition, the confusion matrix provides information about the types of errors the model makes. For example, it can reveal whether the model consistently confuses certain classes with each other. This information is critical for understanding the model’s strengths and weaknesses and for making further improvements. However, despite the

detailed information provided by the confusion matrix, a low evaluation score suggests that the overall performance of the model with real-world data is suboptimal. This discrepancy may indicate that the model is overfitting the training data or has difficulty generalizing to new, unseen data. Therefore, further research and optimization is needed to improve the robustness and effectiveness of the model. This may include techniques such as collecting more diverse training data, tuning hyperparameters, or using more sophisticated algorithms.

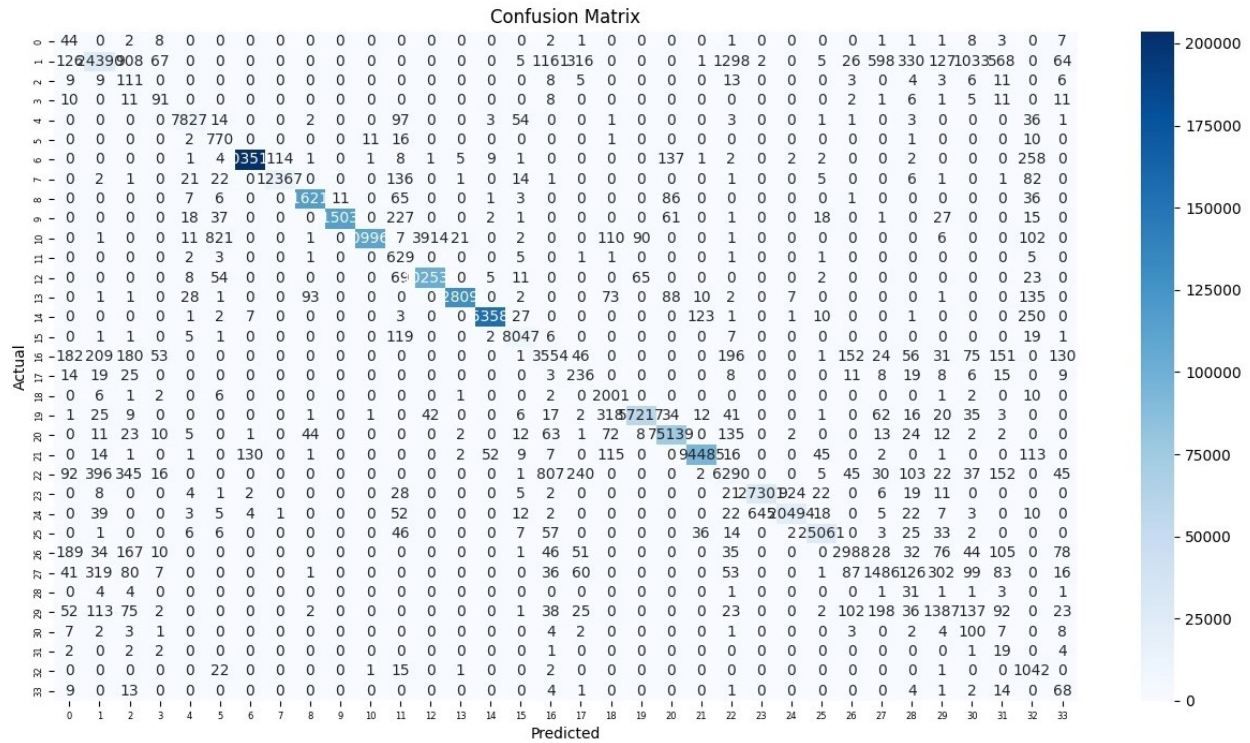


FIGURE 5. Confision Matrix of the Models.

4. DISCUSSION

In this study, various machine learning models used to detect cyber attacks in unmanned aerial vehicle (UAV) networks were comprehensively examined and compared. The algorithms used in the study include RFC, CatBoost, XGBoost, AdaBoost, and ANN. The results of the study provide important findings in determining the performance of different machine learning algorithms in the cyber attack detection process. While all algorithms generally exhibited high accuracy rates, significant differences were observed in the test times. In particular, the CatBoost algorithm showed superior performance compared to other algorithms in terms of accuracy rate and processing time. There are several important factors contributing to the success of CatBoost: Producing faster results in test times compared to other algorithms is an important advantage in UAV networks where real-time attack detection is critical. It has been particularly successful in achieving high accuracy rates when working with categorical data. Effective processing and analysis of various data encountered in UAV networks increases the efficiency of attack detection. The findings of the study emphasize that CatBoost generally outperforms other algorithms and therefore is an ideal choice for detecting attacks in UAV networks. These findings highlight the importance of using the CatBoost algorithm to secure UAV networks and detect cyber attacks quickly and effectively.

CatBoost demonstrates significant advantages beyond accuracy and processing time, establishing itself as a prominent algorithm in machine learning. Its ability to natively process categorical variables without extensive preprocessing

reduces complexity and minimizes information loss. Additionally, CatBoost achieves strong performance with minimal hyperparameter tuning and supports distributed training, ensuring scalability for large datasets. Features such as built-in cross-validation and interpretability tools further enhance its usability and transparency.

Several factors contribute to CatBoost's success, including its algorithmic innovations, robustness with categorical data, and versatility across diverse applications. However, it has certain limitations. CatBoost's memory consumption during training is higher compared to alternatives like LightGBM, and its training time may be slower on datasets with fewer categorical features. The relatively large model size can also be a disadvantage for deployment in resource-constrained environments. Furthermore, its ecosystem, while expanding, remains less mature than that of widely adopted algorithms like XGBoost.

Despite these challenges, CatBoost's strengths make it particularly well-suited for real-time applications. Its exemplary performance on the CICIOT2023 dataset highlights its efficacy in handling complex data, particularly in cybersecurity contexts, such as UAV network intrusion detection.

5. CONCLUSION

This study conducted an in-depth evaluation and comparison of various machine learning models to detect cyberattacks in unmanned aerial vehicle (UAV) networks, a critical area of research due to the increasing deployment of UAVs in both civilian and military applications. The models analyzed included Random Forest (RF), CatBoost, XGBoost, AdaBoost, and Artificial Neural Networks (ANN). The findings revealed that, while all models achieved high accuracy rates in attack detection, CatBoost demonstrated clear superiority. Its exceptional performance in terms of both accuracy and processing time makes it particularly well-suited for real-time applications where timely detection of cyberattacks is critical. Notably, CatBoost's ability to handle categorical data efficiently, coupled with its robust processing capabilities, ensures the effective analysis of complex UAV network traffic. These advantages underscore its potential as a cornerstone for enhancing UAV network security.

Despite these promising results, the study also highlighted several limitations. The dataset used, CICIOT2023, provides a rich set of labeled data covering various attack types. However, it does not encompass all possible attack scenarios, limiting its ability to represent the full spectrum of real-world UAV network dynamics. Furthermore, the performance of the machine learning models was found to depend heavily on the characteristics of the dataset, indicating the potential for variability when applied to different datasets or real-world scenarios. The results of this study remain largely theoretical and require further validation in real-time applications to establish their practical viability. In conclusion, this study represents a significant step forward in the use of machine learning for UAV network security. By demonstrating the effectiveness of CatBoost and other machine learning models, it provides a foundation for developing real-time, adaptive intrusion detection systems. These systems will not only secure UAV networks but also contribute to building resilient infrastructure capable of withstanding the rapidly evolving landscape of cybersecurity threats. The findings and insights gained from this study will serve as an important reference for future studies, guiding the development of advanced and robust security measures for UAV networks.

Future studies directions are clear and imperative. Expanding datasets like CICIOT2023 to include a broader and more diverse range of attack types is essential for developing more robust detection systems. Studies should also focus on identifying new machine learning algorithms and methods to enhance detection accuracy, computational efficiency, and generalizability. Developing hybrid models that combine the strengths of multiple algorithms offers another promising avenue for increasing detection performance. Additionally, the implementation and testing of these systems in real-world environments will be critical for validating their effectiveness and addressing practical challenges. Ensuring that such systems can adapt to evolving threats will play a vital role in securing UAV networks against future cyberattacks.

6. LIMITATION

The CICIOT2023 dataset used in this study covers a variety of attack scenarios targeting UAV networks, but it does not cover all possible attack types. The limitations of the dataset are due to the diversity of modeled attacks and the fact that it does not fully reflect the real-world dynamics of UAV networks. In addition, the performance of the machine learning algorithms used depends on the characteristics of the dataset, and different results may be obtained with different datasets. Although the superior performance of the CatBoost algorithm has been verified within the

scope of this study, similar results cannot be guaranteed in other applications and datasets. Finally, the results of the study remain at a theoretical level and further validation is required for real-time applications.

7. FUTURE WORKS

Future studies should aim to expand the CICIOT2023 dataset to include a wider and more diverse set of attacks. In addition, research should be conducted to discover new algorithms and methods to improve the performance of machine learning models. The development of real-time intrusion detection systems and field testing of these systems will be important steps in improving the security of UAV networks. Validation of the performance of the models used in this study on different datasets and real-world scenarios should be the focus of future research to confirm their general applicability. Finally, integrating different machine learning algorithms and developing hybrid models can increase the accuracy and speed of intrusion detection.

CONFLICTS OF INTEREST

The authors declare that there are no conflicts of interest regarding the publication of this article.

AUTHORS CONTRIBUTION STATEMENT

All authors have read and agreed to the published version of the manuscript.

REFERENCES

- [1] Derhab, A., Cheikhrouhou, O., Allouch, A., Koubaa, A., Qureshi, B. et al., *Internet of drones security: Taxonomies, open issues, and future directions*, Vehicular Communications **39**(2023), 100552.
- [2] Durfey, N., Sajal, S., *A comprehensive survey: Cybersecurity challenges and futures of autonomous drones*, 2022 Intermountain Engineering, Technology and Computing (IETC), (2022), 1–7.
- [3] Gabrielsson, J., Bugeja, J., Vogel, B., *Hacking a commercial drone with open-source software: Exploring data privacy violations*, 2021 10th mediterranean conference on embedded computing (MECO), IEEE, 2(021), 1–5.
- [4] Galvan, J., Raja, A., Li, Y., Yuan, J., *Sensor data-driven uav anomaly detection using deep learning approach*, MILCOM 2021-2021 IEEE Military Communications Conference (MILCOM), IEEE, (2021), 589–594.
- [5] Jony, A.I., Arnob, A.K.B., *A long short-term memory based approach for detecting cyber attacks in iot using cic-iot2023 dataset*, Journal of Edge Computing **3**(1)(2024), 28–42.
- [6] Nayak, J., Naik, B., Dash, P.B., Vimal, S., Kadry, S., *Hybrid bayesian optimization hypertuned catboost approach for malicious access and anomaly detection in iot nomalyframework*, Sustainable Computing: Informatics and Systems, **36**(2022), 100805.
- [7] Neto, E.C.P., Dadkhah, S., Ferreira, R., Zohourian, A., Lu, R. et al., *Ciciot2023: A real-time dataset and benchmark for large-scale attacks in iot environment*, Sensors, **23**(13)(2023), 5941.
- [8] Noorwali, A., Javed, M.A., Khan, M.Z., *Efficient uav communications: Recent trends and challenges*, Computers, Materials & Continua, **67**(1)(2021).
- [9] Ahmad, W., Almaiah, M.A., Ali, A., Al-Shareeda, M.A., *Deep learning based network intrusion detection for unmanned aerial vehicle (uav)*, 2024 7th World Conference on Computing and Communication Technologies (WCCCT), IEEE, (2024), 31–36.
- [10] Alqahtani, H., Kumar, G., *Machine learning for enhancing transportation security: A comprehensive analysis of electric and flying vehicle systems*, Engineering Applications of Artificial Intelligence **129**(2024), 107667.
- [11] Alrefaei, F., *Machine learning for intrusion detection into unmanned aerial system 6g networks*, Doctoral dissertation, Embry-Riddle Aeronautical University, (2024).
- [12] Miao, S., Pan, Q., Zheng, D., *Unmanned aerial vehicle intrusion detection: Deep-meta-heuristic system*, Vehicular Communications, **46**(2024), 100726.
- [13] Hadi, H.J., Cao, Y., Li, S., Hu, Y., Wang, J. et al., *Real-time collaborative intrusion detection system in uav networks using deep learning*, IEEE Internet of Things Journal, (2024).
- [14] Khoei, T.T., Al Shamaileh, K., Devabhaktuni, V. K., Kaabouch, N., *A comparative assessment of unsupervised deep learning models for detecting gps spoofing attacks on unmanned aerial systems*, 2024 Integrated Communications, Navigation and Surveillance Conference (ICNS), IEEE, (2024), 1–10.
- [15] Wu, Y., Yang, L., Zhang, L., Nie, L., Zheng, L., *Intrusion detection for unmanned aerial vehicles security: A tiny machine learning model*, IEEE Internet of Things Journal, **11**(2024), 20970–20980.
- [16] Al-Iqubaydhi, N., Alenezi, A., Alanazi, T., Senyor, A., Alanezi, N. et al., *Deep learning for unmanned aerial vehicles detection: A review*, Computer Science Review, **51**(2024), 100614.
- [17] Mynuddin, M., Khan, S.U., Ahmari, R., Landivar, L., Mahmoud, M.N. et al., *Trojan attack and defense for deep learning based navigation systems of unmanned aerial vehicles*, IEEE Access, **12**(2024), 89887–89897
- [18] Omolara, A.E., Alawida, M., Abiodun, O.I., *Drone cybersecurity issues, solutions, trend insights and future perspectives: A survey*, Neural Computing and Applications, **35**(31)(2023), 23063–23101.

-
- [19] Sharifani, K., Amini, M., *Machine learning and deep learning: A review of methods and applications*, World Information Technology and Engineering Journal, **10**(07)(2023), 3897–3904.
- [20] Yahuza, M., Idris, M.Y.I., Ahmedy, I.B., Wahab, A.W.A., Nandy, T. et al., *Internet of drones security and privacy issues: Taxonomy and open challenges*, IEEE Access **9**(2021), 57243–57270.