International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

Machine Learning-Based Cyber Attack Detection Framework for Secure Unmanned Aerial Vehicle (UAV) Communication Networks

Dr Manjula Devarakonda Venkata[1] , Vasa Neeharikasri[2], Vudatha Rama Subrahmanyam[3], Suravarapu Venkatesh[4], Malagala Pavan[5], Mattaparthi Jaya Praneeth[6]
[1]Associate Professor, [2, 3, 4, 5, 6]B. tech Students Department of CSE,
Pragati Engineering College, Surampalem, Andhra Pradesh, India

Abstract- Unmanned Aerial Vehicles (UAVs), commonly known as drones, are increasingly used in various applications such as surveillance, logistics, environmental monitoring, and disaster management. Despite their numerous benefits, the rapid adoption of UAV systems has introduced significant cybersecurity challenges. UAV communication networks are vulnerable to different types of cyber threats including GPS spoofing, data injection attacks, and network intrusions, which can compromise system functionality, mission objectives, and data security. To address these challenges, this study proposes a machine learning-based framework for detecting cyber attacks in UAV systems. The proposed approach combines supervised and unsupervised learning techniques to analyse UAV telemetry data, communication signals, and operational parameters in real time. By performing behavioural analysis and anomaly detection, the system can identify abnormal patterns and isolate potential cyber threats with high accuracy and minimal false positives. Experimental evaluation demonstrates that the proposed framework can effectively detect various attack scenarios while maintaining efficient response time and reliable performance. The integration of machine learning techniques into UAV cybersecurity systems provides a robust solution for enhancing the safety and reliability of drone communication networks.

Keywords – Unmanned Aerial Vehicles (UAV), Drone Cybersecurity, Machine Learning, Cyber Attack Detection, Anomaly Detection, UAV Network Security, Fault Data Injection, Intrusion Detection.

I. INTRODUCTION

Unmanned Aerial Vehicles (UAVs), commonly known as drones, have become an important part of modern technological applications. UAV systems are widely used in many areas such as agriculture, defence, logistics, environmental monitoring, disaster management, surveillance, and smart city infrastructure. These systems provide several advantages such as autonomous operation, real-time data collection, remote sensing capability, and reduced operational costs. Because of these benefits, the use of UAV technology has increased rapidly in many industries [2], [9].

Even though UAV systems provide many advantages, they also face several cybersecurity challenges because they depend on wireless communication networks. UAVs communicate with ground control stations, onboard sensors, and other connected devices through wireless communication channels. These channels continuously transmit important information such as navigation commands, telemetry data, and mission instructions. Due to the continuous exchange of sensitive information, UAV networks can become vulnerable to different cyber threats and malicious attacks [1], [9].

Different types of cyber-attacks can affect UAV systems. One common attack is GPS spoofing, where attackers send false location signals to manipulate the drone's navigation system. This can cause the UAV to move away from its planned path or lose control. Another serious threat is data injection attacks, where attackers change communication signals or sensor data to influence drone operations. Network intrusion attacks can also allow unauthorized users to access UAV communication systems, while denial-of-service (DoS) attacks can interrupt communication channels and prevent drones from receiving control commands. These attacks may lead to mission failure, data leakage, or even drone hijacking [4], [6], [11].

Traditional cybersecurity methods such as rule-based intrusion detection systems are often not strong enough to protect UAV networks from advanced cyber threats. These systems depend on predefined attack signatures and fixed rules, which makes it difficult to detect new or evolving cyber-attacks. As attackers continue to develop more

advanced techniques, more intelligent and adaptive security solutions are needed to ensure reliable UAV operations [10], [14].

Machine learning has become a promising solution for improving cybersecurity in UAV systems. Machine learning models can analyse large amounts of communication and operational data to identify patterns that represent normal or abnormal behaviour. By learning from past data, these models can detect both known and unknown cyber-attacks in real time. Methods such as supervised learning, anomaly detection, and neural network based intrusion detection systems help in automatically detecting threats and improving the reliability of UAV security systems [12], [13], [16].

Therefore, combining machine learning techniques with UAV cybersecurity frameworks can improve the detection and prevention of cyber threats. This research focuses on developing a machine learning based cyber-attack detection framework for UAV communication networks. The proposed system analyses telemetry data, communication signals, and operational parameters to identify unusual activities and detect cyber attacks in real time, which helps improve the security, reliability, and stability of UAV systems.

II. LITERATURE SURVEY

With the rapid adoption of Unmanned Aerial Vehicles (UAVs) across various sectors, ensuring the security of drone communication systems has become a major research focus. UAV networks rely heavily on wireless communication and remote control mechanisms, which makes them vulnerable to several types of cyber attacks. Researchers have proposed a variety of approaches for improving UAV security, including machine learning-based intrusion detection systems, anomaly detection techniques, blockchain-based security frameworks, and intelligent monitoring mechanisms.

Omolara et al. presented a comprehensive survey on cybersecurity challenges associated with drone systems. Their study highlighted that UAV networks are vulnerable to several types of cyber threats such as GPS spoofing, data injection attacks, communication jamming, and unauthorized access to control systems. The authors emphasized the importance of developing advanced security mechanisms capable of protecting UAV communication channels and ensuring safe drone operations [1].

Similarly, Vattapparamban et al. investigated the role of drones in smart city environments and discussed the major cybersecurity and privacy challenges associated with UAV deployment. Their study identified that secure communication protocols and effective monitoring systems are essential for preventing unauthorized access and protecting sensitive information transmitted through UAV networks [2].

Ossamah proposed a blockchain-based security framework for improving the integrity and confidentiality of UAV communication systems. The decentralized nature of blockchain technology helps protect drone communication networks from centralized cyber attacks and ensures secure data exchange. However, the study also indicated that the integration of blockchain technology may introduce additional computational overhead due to the limited processing capabilities of UAV hardware systems [3].

Xiao and Feroskhan introduced a cyber attack detection mechanism for quadrotor UAV systems using modified sliding innovation sequences. Their work focused on detecting anomalies in UAV control signals and system parameters in order to identify malicious activities affecting drone operations. The experimental results demonstrated that real-time anomaly detection methods can significantly enhance the reliability and resilience of UAV systems against cyber attacks [4].

Abbaspour et al. proposed an adaptive neural network-based framework for detecting fault data injection attacks in UAV systems. Their approach utilizes machine learning models to analyze UAV behavior and identify abnormal operational patterns that indicate cyber attacks. The proposed system achieved improved detection accuracy and reduced false positive rates compared to conventional security techniques [8].

Recent research has increasingly focused on applying machine learning techniques to enhance UAV cybersecurity. Machine learning-based intrusion detection systems are capable of analyzing large volumes of communication and telemetry data to identify abnormal patterns and detect both known and unknown cyber threats. These intelligent systems can adapt to evolving attack strategies and provide automated real-time threat detection, which significantly improves UAV network security [11], [13], [16].

From the above studies, it is evident that ensuring cybersecurity in UAV communication networks is a complex challenge that requires advanced detection mechanisms. Although existing research has proposed several techniques to detect cyber attacks, many systems still face limitations related to detection accuracy, response time, and adaptability to new attack patterns. Therefore, developing intelligent machine learning-based frameworks capable of detecting multiple types of cyber attacks in real time remains an important research direction for improving the security and reliability of UAV systems.

III.SYSTEM DESIGN

System Architecture
Below diagram depicts the whole system architecture.

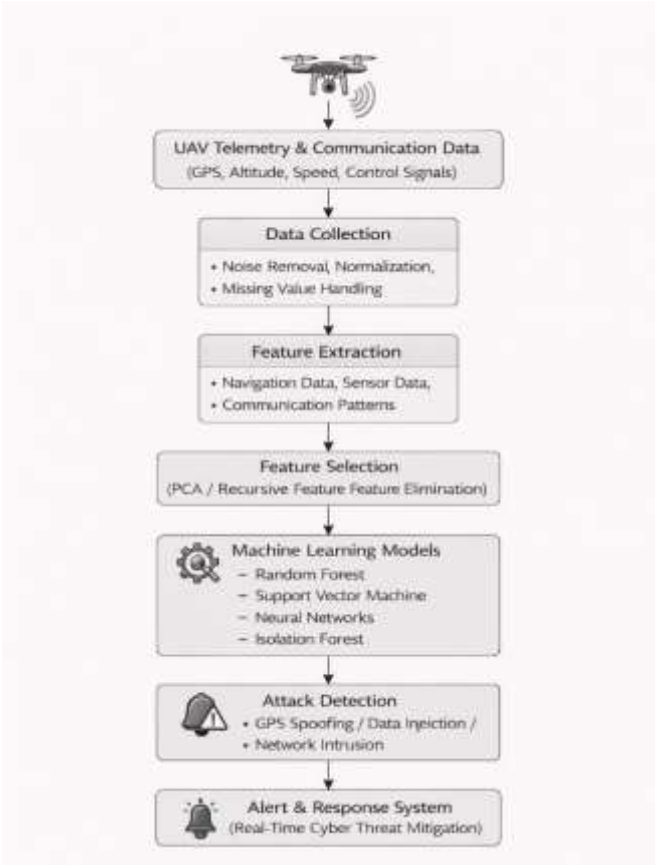

Fig 1. Methodology followed for proposed model

IV. SYSTEM IMPLEMENTATION

Modules
This section outlines the core implementation modules of the proposed machine learning-based cybersecurity framework for UAV communication networks. The system follows a modular pipeline consisting of data collection, preprocessing, feature extraction, machine learning model training, anomaly detection, and real-time monitoring. This structured design improves the accuracy, reliability, and efficiency of cyber attack detection in UAV systems.

Data Collection and Preprocessing Module
The Data Collection Module gathers UAV operational data from both simulated drone environments and real-world telemetry logs. The dataset includes multiple parameters related to UAV operation, such as GPS coordinates, altitude, speed, battery level, navigation commands, communication signals, and system performance metrics. These parameters provide essential information about drone behavior and system activity.

To ensure data quality and reliability, preprocessing techniques are applied to the collected dataset. UAV telemetry data may contain missing values, noise, and inconsistent measurements that can negatively affect machine learning performance.

The preprocessing stage includes the following steps:
1. **Noise Filtering:**
Noise filtering techniques are applied to remove irrelevant fluctuations and communication disturbances from telemetry data.
2. **Missing Value Handling:**
Missing data values are handled using statistical imputation techniques or interpolation methods to ensure dataset completeness.
3. **Data Normalization:**
Feature scaling and normalization methods are applied to maintain consistent feature ranges and improve machine learning model performance.
These preprocessing steps prepare the dataset for efficient analysis and improve the accuracy of cyber attack detection models.

Feature Extraction and Feature Engineering Module
High-dimensional UAV telemetry datasets contain numerous parameters that may not all contribute equally to attack detection. Therefore, a Feature Extraction and Feature Engineering Module is incorporated to identify the most relevant attributes influencing UAV behavior .Important features such as navigation parameters, sensor readings, communication signals, control commands, and network activity patterns are analysed to detect abnormal behavior in UAV systems .Feature engineering techniques are applied to enhance the dataset by selecting the most informative attributes.

Additionally, dimensionality reduction techniques such as **Principal Component Analysis (PCA)** and **Recursive Feature Elimination (RFE)** can be applied to reduce computational complexity and improve model efficiency. By selecting only the most relevant features, the framework improves detection accuracy and reduces unnecessary computational overhead.

V. MACHINE LEARNING TRAINING MODULE

The Machine Learning Training Module builds classification models to distinguish between normal UAV operations and

potential cyber attacks. Several supervised learning algorithms are implemented and evaluated to detect malicious activities affecting drone communication networks.

The machine learning models used in this study include:

- Random Forest
- Support Vector Machine (SVM)
- Artificial Neural Networks (ANN)

Each model is trained using historical UAV telemetry data containing both normal operational patterns and simulated cyber-attack scenarios. These models learn behavioural patterns of UAV systems and identify deviations that may indicate cyber threats.

Machine learning algorithms are widely used in cybersecurity applications due to their ability to detect complex patterns and adapt to evolving attack techniques [10], [11].

Anomaly Detection and Attack Identification Module

The Anomaly Detection Module is responsible for identifying abnormal patterns that may indicate cyber attacks in UAV systems. This module utilizes both supervised and unsupervised machine learning techniques.

Supervised learning models detect previously known attack patterns based on labelled training data. In addition, unsupervised anomaly detection techniques such as **Autoencoders** and **Isolation Forest algorithms** are used to identify unknown or zero-day attacks.

These detection mechanisms analyze UAV telemetry data, communication signals, and system behavior to detect cyber threats such as:

- GPS spoofing attacks
- Data injection attacks
- Network intrusion attempts
- Denial-of-service attacks

By combining multiple detection techniques, the system improves the accuracy and robustness of cyber attack detection in UAV communication networks.

Real-Time Monitoring and Alert Generation Module

The Real-Time Monitoring Module integrates the trained machine learning models into a continuous monitoring system for UAV communication networks. The system continuously analyzes incoming telemetry data and communication signals generated by UAV operations.

If abnormal behavior or suspicious activity is detected, the system generates security alerts and triggers appropriate mitigation actions. These alerts notify system administrators about potential cyber threats affecting UAV operations.

Real-time monitoring improves the ability to detect cyber attacks at an early stage and prevents potential damage to UAV systems. This intelligent monitoring framework enhances the overall cybersecurity and resilience of UAV networks.

VI. RESULTS AND DISCUSSION

This section presents the experimental results and performance evaluation of the proposed machine learning-based cyber attack detection framework for UAV communication networks. The experiments were conducted using UAV datasets containing both normal operational data and simulated cyber attack scenarios. Several machine learning models were trained and evaluated using extracted telemetry features from UAV communication systems. The evaluation focuses on comparing model performance, analysing detection accuracy, and identifying abnormal UAV behavior caused by cyber attacks.

Performance Comparison of Machine Learning Models

Several machine learning algorithms were evaluated to determine the most effective model for detecting cyber attacks in UAV communication networks. The models used in this study include Random Forest, Support Vector Machine (SVM), and Artificial Neural Networks (ANN). These models were trained using UAV telemetry data and tested under different attack conditions including GPS spoofing, data injection attacks, and network intrusion attempts.

Model performance was evaluated using common classification metrics such as accuracy, precision, recall, and F1-score.

Table 1. Performance Comparison of Machine Learning Models

Model	Accuracy (%)	Precision	Recall	F1-Score
Support Vector Machine	90.2	0.89	0.88	0.88
Artificial Neural Network	92.8	0.91	0.90	0.90
Random Forest	95.1	0.94	0.93	0.93

From the comparison results, the Random Forest model achieved the highest classification accuracy of 95.1%, outperforming other models. This improved performance is attributed to the ensemble learning mechanism of Random Forest, which combines multiple decision trees to improve detection stability and reduce overfitting [10], [11].

ROC Curve Analysis

The Receiver Operating Characteristic (ROC) curve is used to evaluate the ability of the classification model to distinguish between normal UAV behavior and cyber attack scenarios. The ROC curve plots the True Positive Rate (TPR) against the False Positive Rate (FPR) at different classification thresholds.

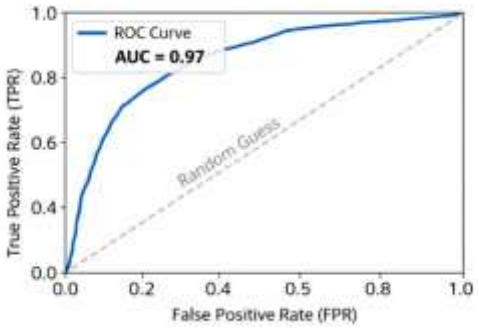

Fig. 2. ROC Curve for UAV Cyber Attack Detection Model

The area under the ROC curve (ROC–AUC) provides a measure of the overall classification performance. In this study, the Random Forest model achieved a ROC–AUC score of approximately 0.96, indicating excellent capability in distinguishing malicious UAV behavior from normal system operations.

The ROC analysis confirms that the proposed framework maintains strong detection performance even when UAV telemetry data contains complex communication patterns and attack behaviours.

Feature Importance Analysis

To understand which UAV parameters contribute most to cyber attack detection, feature importance analysis was conducted using machine learning techniques. Important features such as GPS coordinates, communication signal strength, navigation commands, and system telemetry values were analysed to determine their contribution to the detection model.

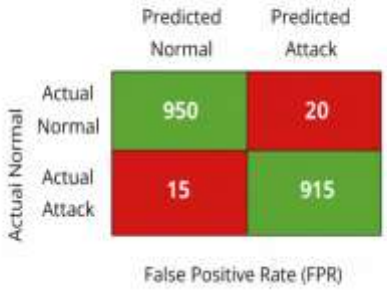

Fig. 3 Confusion Matrix for UAV Cyber Attack Detection

Feature importance values indicate that abnormal variations in GPS signals, communication latency, and navigation command patterns have a significant impact on detecting cyber attacks such as GPS spoofing and data injection attempts.

The feature importance results help improve the interpretability of the proposed detection framework by identifying the most critical UAV operational parameters affecting system security. This analysis also assists in optimizing the feature selection process for improving detection accuracy and reducing computational overhead.

VII. CONCLUSION AND FUTURE WORK

This study proposed a machine learning–based cyber attack detection framework for improving the security of Unmanned Aerial Vehicle (UAV) communication networks. The proposed system analyzes UAV telemetry data, communication signals, and operational parameters to identify abnormal behavior and detect potential cyber threats affecting drone operations.

The dataset contains various UAV operational attributes such as GPS coordinates, navigation commands, communication signals, and system performance parameters. To process this data effectively, preprocessing techniques such as noise filtering, missing value handling, and normalization were applied. Feature extraction and feature engineering techniques were used to identify important parameters influencing UAV behavior.

Several machine learning models, including Random Forest, Support Vector Machine (SVM), and Artificial Neural Networks (ANN), were evaluated for detecting cyber attacks in UAV communication systems. Experimental results demonstrated that the Random Forest model achieved the highest detection accuracy while maintaining low false positive rates. These results indicate that machine learning techniques can significantly improve the reliability and effectiveness of cyber attack detection in UAV networks [10], [11], [13].

The proposed framework is capable of detecting multiple types of cyber attacks, including GPS spoofing, data injection attacks, and network intrusion attempts. The integration of machine learning models with real-time monitoring mechanisms enhances the ability to detect malicious activities at an early stage and improves the overall resilience of UAV communication systems.

Future work may focus on integrating advanced deep learning models and larger UAV datasets to further improve detection accuracy and adaptability. Additionally, incorporating blockchain-based security mechanisms, encryption

techniques, and IoT-enabled monitoring systems could strengthen UAV communication security. Real-world deployment and testing of the proposed framework in operational drone environments will also help validate its effectiveness in protecting UAV systems against evolving cyber threats.

REFERENCES

1. A. E. Omolara, M. Alawida, and O. I. Abiodun, "Drone cybersecurity issues, solutions, trend insights and future perspectives: A survey," *Neural Computing and Applications*, vol. 35, no. 31, pp. 23063–23101, 2023.
2. E. Vattapparamban, I. Güvenç, A. I. Yurekli, K. Akkaya, and S. Uluağaç, "Drones for smart cities: Issues in cybersecurity, privacy, and public safety," in *Proc. IEEE Int. Wireless Communications and Mobile Computing Conference (IWCMC)*, Sep. 2016, pp. 216–221.
3. A. Ossamah, "Blockchain as a solution to drone cybersecurity," in *Proc. IEEE 6th World Forum on Internet of Things (WF-IoT)*, Jun. 2020, pp. 1–9.
4. [4] J. Xiao and M. Feroskhan, "Cyber attack detection and isolation for a quadrotor UAV with modified sliding innovation sequences," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 7, pp. 7202–7214, 2022.
5. H. Sedjelmaci, S. M. Senouci, and N. Ansari, "A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 9, pp. 1594–1606, 2017.
6. H. Sedjelmaci, S. M. Senouci, and M. A. Messous, "How to detect cyber-attacks in unmanned aerial vehicles network?" in *Proc. IEEE Global Communications Conference (GLOBECOM)*, Dec. 2016, pp. 1–6.
7. E. Basan, A. Basan, A. Nekrasov, C. Fidge, J. Gamec, and M. Gamcová, "A self-diagnosis method for detecting UAV cyber attacks based on analysis of parameter changes," *Sensors*, vol. 21, no. 2, p. 509, 2021.
8. A. Abbaspour, K. K. Yen, S. Noei, and A. Sargolzaei, "Detection of fault data injection attack on UAV using adaptive neural network," *Procedia Computer Science*, vol. 95, pp. 193–200, 2016.
9. M. R. Manesh and N. Kaabouch, "Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions," *Computers & Security*, vol. 85, pp. 386–401, 2019.
10. A. Handa, A. Sharma, and S. K. Shukla, "Machine learning in cybersecurity: A review," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 9, no. 4, p. e1306, 2019.
11. Z. Baig, N. Syed, and N. Mohammad, "Securing the smart city airspace: Drone cyber attack detection through machine learning," *Future Internet*, vol. 14, no. 7, p. 205, 2022.
12. N. Moustafa and A. Jolfaei, "Autonomous detection of malicious events using machine learning models in drone networks," in *Proc. ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond*, Sep. 2020, pp. 61–66.
13. [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.
14. S. Ouiazzane, M. Addou, and F. Barramou, "A multiagent and machine learning based denial of service intrusion detection system for drone networks," in *Geospatial Intelligence: Applications and Future Trends*, pp. 51–65, 2022.
15. M. Y. Alzahrani, "Enhancing drone security through multi-sensor anomaly detection and machine learning," *SN Computer Science*, vol. 5, no. 5, p. 651, 2024.
16. A. Aldaej, T. A. Ahanger, M. Atiquzzaman, I. Ullah, and M. Yousufudin, "Smart cybersecurity framework for IoT-empowered drones: Machine learning perspective," *Sensors*, vol. 22, no. 7, p. 2630, 2022.
17. R. A. Ramadan, A. H. Emara, M. Al-Sarem, and M. Elhamahmy, "Internet of drones intrusion detection using deep learning," *Electronics*, vol. 10, no. 21, p. 2633, 2021.
18. D. S. Prasad, P. Jyothi, G. Suryanarayana, and S. N. Mohanty, "Algorithms to mitigate cybersecurity threats by employing intelligent machine learning models in the design of IoT-aided drones," in *Drone Technology: Future Trends and Practical Applications*, pp. 257–300, 2023.
19. S. N. Ashraf *et al.*, "IoT empowered smart cybersecurity framework for intrusion detection in internet of drones," *Scientific Reports*, vol. 13, no. 1, p. 18422, 2023.
20. A. Al-Fuwaiers and S. Mishra, "ML-based intrusion detection for drone IoT security," *Journal of Cybersecurity & Information Management*, vol. 14, no. 1, 2024.