Int. J. Integr. Stud. 2026; 2(4): 63-78

ISSN: 3049-3277

International Journal of Integrative Studies (IJIS)

Journal homepage: www.ijis.co.in

RESEARCH ARTICLE

Sky Guard: Machine Learning Based Intrusion Detection For Dynamic UAV Network Traffic

[1]Vivek Sharma, [2]R. Jesse Arpith, [3]K. Nilaya Reddy, [4]Dr. M. Rajeshwar

[2]Computer Science and Engineering (Data Science) Hyderabad Institute of Technology and Management Hyderabad, India, 22e51a6720@hitam.org
[3]Computer Science and Engineering (Data Science) Hyderabad Institute of Technology and Management Hyderabad, India, 22e51a6724@hitam.org
[4]Computer Science and Engineering (Data Science) Hyderabad Institute of Technology and Management Hyderabad, India, rajeshwarm.cse@hitam.org

ABSTRACT

The rapid growth of Unmanned Aerial Vehicles (UAVs) has expanded their use in areas like logistics, surveillance, agriculture, and disaster management. However, their integration with modern networks such as 5G raises significant security concerns due to vulnerabilities like spoofing, packet injection, and denial-of-service attacks.

This paper proposes SkyGuard, a machine learning-based intrusion detection framework that analyzes UAV network traffic to identify malicious activities. It uses preprocessing, feature extraction, and Principal Component Analysis (PCA) for dimensionality reduction, followed by classification using multiple ML algorithms. Experimental results show that the system effectively detects attacks and enhances UAV network security, with strong performance measured through accuracy, precision, recall, and F1-score.

Keywords: *Secret Image Sharing (SIS), Steganography, Shamir's Secret Sharing, Image Security, Cryptography, Data Privacy, Secure Image Transmission, Information Hiding.*

INTRODUCTION

Unmanned Aerial Vehicles (UAVs), commonly known as drones, have become an integral part of modern technological ecosystems due to their wide range of applications in surveillance, military operations, disaster management, agriculture monitoring, and intelligent transportation systems. With rapid advancements in wireless communication technologies and the integration of UAVs with cloud computing, 5G networks, and satellite systems, these platforms are capable of transmitting and processing large volumes of data in real time [1], [2], [3]. This continuous communication between UAVs and Ground Control Stations (GCS) results in highly dynamic and complex network traffic that must be efficiently managed to ensure reliable and secure operation.

B. However, the increasing scale and complexity of UAV communication networks introduce significant challenges related to both traffic management and cybersecurity. UAV networks operate in highly dynamic environments where communication patterns frequently change due to mobility, mission requirements, and environmental factors [4], [5].

[1]Computer Science and Engineering (Data Science) Hyderabad Institute of Technology and Management Hyderabad, India
Email-id: 22e51a6752@hitam.org.

Corresponding Author: Vivek Sharma,
Computer Science and Engineering (Data Science) Hyderabad Institute of Technology and Management Hyderabad, India.
Email-id: 22e51a6752@hitam.org.

DOI: https://doi.org/10.63856/ijis/v2i4/00036

How to cite this article: Sharma,, V., (2026). Sky Guard: Machine Learning Based Intrusion Detection For Dynamic UAV Network Traffic. *International Journal of Integrative Studies*, 2(4), 63-78.

Source of support: Nil

Conflict of interest: None.
Received: 04//04/2026 **Revised:** 08/04/2026 **Accepted:** 12/04/2026
Published: 28/04/2026

This leads to issues such as network congestion, packet loss, latency variations, and degraded communication performance. In addition, UAV systems are highly vulnerable to various cyber threats including Denial of Service (DoS), Distributed Denial of Service (DDoS), spoofing, Man-in-the-Middle (MITM), replay attacks, and unauthorized access attempts [6], [7]. These attacks can disrupt communication, compromise sensitive data, and significantly impact mission-critical operations.

Traditional rule-based and signature-based security mechanisms are insufficient to handle the dynamic and evolving nature of UAV network traffic. These approaches rely on predefined patterns and fail to detect unknown or sophisticated attacks. Furthermore, existing solutions often treat intrusion detection and traffic management as separate problems, resulting in delayed response and inefficient resource utilization [8], [9]. The need for intelligent, adaptive, and integrated solutions has therefore become increasingly important.

Machine Learning (ML) techniques have emerged as powerful tools for analyzing complex network traffic patterns and detecting anomalies in real time. By learning from historical traffic data, ML models can effectively distinguish between normal and malicious behavior, enabling automated classification and prediction [10], [11]. These models can adapt to changing network conditions and provide improved detection accuracy compared to traditional methods.

In this context, this paper proposes **SkyGuard**, a Machine Learning-based framework for UAV network traffic analysis, intrusion detection, and adaptive traffic optimization. The proposed system integrates multiple components into a unified pipeline, including data preprocessing, traffic classification using models such as XGBoost and Multi-Layer Perceptron (MLP), and a dynamic traffic optimization mechanism. Based on the predicted traffic class, the system applies intelligent strategies such as rate limiting, packet filtering, and traffic rerouting to mitigate potential threats and improve network performance. Additionally, the system incorporates a real-time monitoring dashboard that provides visualization of network traffic, detected anomalies, and system responses. This enables operators to gain insights into UAV network behavior and take timely actions when required. By combining intelligent detection with adaptive response and real-time visualization, the proposed SkyGuard framework provides a comprehensive solution for enhancing both the security and efficiency of UAV communication systems.

Literature Survey

A. UAV Networks and Communication Challenges

Unmanned Aerial Vehicles (UAVs) have witnessed rapid growth in recent years, leading to their widespread adoption in applications such as surveillance, logistics, agriculture, and disaster management. With the integration of UAV systems into modern wireless communication infrastructures, including 5G and cloud-based networks, UAV communication systems have become highly dynamic and data-intensive [1], [2]. These systems continuously generate large volumes of network traffic due to real-time data exchange between drones and ground control stations.

However, this rapid expansion has also introduced significant challenges related to network reliability, traffic management, and security [3]. The highly dynamic nature of UAV networks, characterized by fluctuating bandwidth, mobility, and changing communication patterns, makes traffic monitoring and management a complex task. Traditional network monitoring systems often struggle to handle such variability, leading to issues such as congestion, packet loss, and latency [4], [5]. As UAV systems become more integrated into critical applications, ensuring secure and efficient communication has become a major research concern.

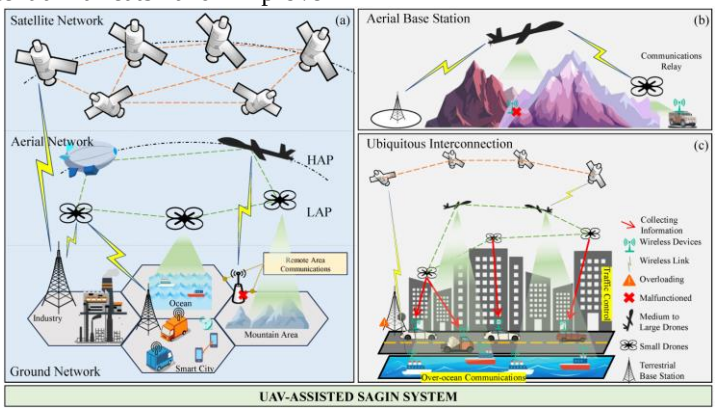

Fig 1: UAV communication network and data transmission

UAV Network Attacks and Security Threats

UAV networks are increasingly vulnerable to a wide range of cyberattacks due to their reliance on wireless communication and limited onboard security mechanisms [6], [7]. Common attack types include spoofing attacks, packet injection, Distributed Denial of Service (DDoS) attacks, and Man-in-the-Middle (MITM) attacks. These attacks aim to disrupt communication channels, inject malicious data, or overwhelm network resources, ultimately affecting the reliability of UAV operations [8].

For instance, DDoS attacks generate large volumes of malicious traffic to exhaust network bandwidth and processing capacity, preventing legitimate communication. Similarly, spoofing attacks manipulate identity information, allowing attackers to impersonate legitimate devices within the network. Such attacks can lead to unauthorized access, data breaches, and mission

failures. The increasing sophistication of these threats highlights the need for intelligent detection mechanisms capable of identifying both known and unknown attack patterns in UAV environments [9], [10].

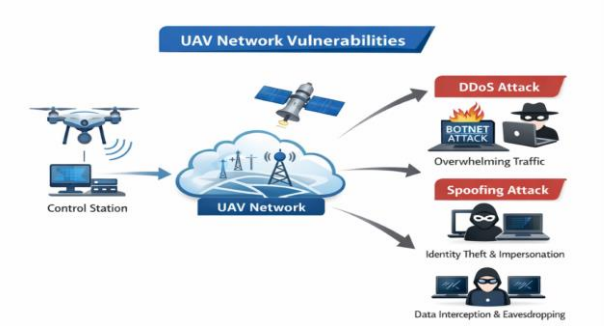

Fig 1.1: UAV Network Vulnerabilities

Network Traffic Analysis and Emerging Challenges

Network traffic analysis plays a critical role in identifying abnormal behavior and ensuring efficient communication within UAV systems. Traditional traffic analysis techniques rely on predefined rules, thresholds, or signature-based detection methods to identify malicious activities [11], [12]. While these approaches are effective for known attack patterns, they often fail to detect new or evolving threats.

Moreover, UAV network traffic exhibits high variability due to dynamic communication patterns, making it difficult to establish fixed thresholds for anomaly detection. Legitimate traffic fluctuations can be misclassified as attacks, resulting in high false-positive rates. Conversely, sophisticated low-rate attacks may bypass detection mechanisms by mimicking normal traffic behavior. These challenges highlight the limitations of conventional traffic analysis approaches in handling dynamic UAV environments.

Machine Learning and AI-Based Approaches

Recent advancements in machine learning and artificial intelligence have significantly improved the ability to analyze complex network traffic and detect malicious activities [13], [14]. Machine learning models can learn patterns from historical data and identify anomalies without relying on predefined rules. Various techniques, including supervised learning, deep learning, and ensemble learning, have been applied to intrusion detection systems.

Deep learning models such as Convolutional Neural Networks (CNNs) have shown strong performance in detecting complex attack patterns and enabling real-time monitoring. However, these models require high computational resources and large datasets, limiting their applicability in resource-constrained UAV systems [15]. On the other hand, machine learning models such as boosting algorithms and neural networks provide a balance between accuracy and computational efficiency.

Ensemble learning techniques further enhance performance by combining multiple models to improve generalization and robustness. Despite these advancements, most existing approaches focus primarily on anomaly detection or attack classification and do not address detailed traffic behavior analysis or optimization in UAV networks.

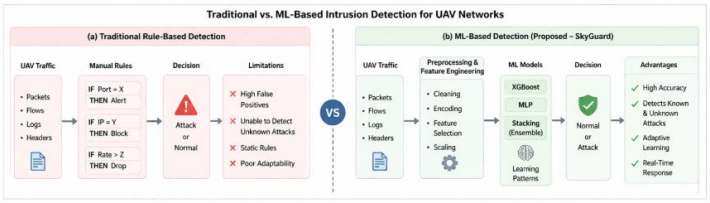

Fig 2: Traditional vs ML Based IDS

Traditional Defense Mechanisms and Limitations

Traditional network security approaches, including firewalls, intrusion detection systems (IDS), and rule-based filtering mechanisms, have been widely used to detect and mitigate cyber threats [11], [12]. These systems rely on predefined signatures and static rules to identify malicious traffic.

While effective against known attacks, they are unable to adapt to evolving attack strategies and dynamic traffic conditions. One of the major limitations of traditional systems is their inability to detect zero-day attacks or unknown threats. Additionally, these systems often generate high false positives and require manual configuration, making them inefficient in real-time environments. In UAV networks, where traffic patterns continuously change, static rule-based approaches fail to provide reliable detection and response mechanisms.

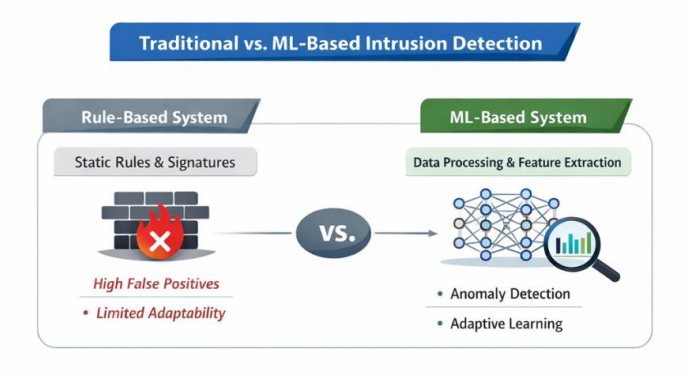

Fig 2.2: Ruled Based vs ML Based System

Research Gap

Despite significant advancements in cybersecurity and machine learning, several challenges remain unaddressed in UAV network environments. Most existing systems focus on binary anomaly detection rather than detailed traffic classification. There is limited emphasis on understanding communication behavior at the HTTP level, which plays a crucial role in network operations.

Additionally, many advanced models require high computational resources, making them unsuitable for real-time deployment in UAV systems. Furthermore, existing solutions lack integration with real-time monitoring systems and fail to provide actionable insights for traffic optimization.

To address these limitations, the proposed work introduces a machine learning-based UAV traffic analysis framework using XGBoost, MLP, and a stacked ensemble model, along with a web-based dashboard for real-time monitoring and traffic optimization.

Methodology

A. Proposed System and Methodology

The proposed system, **SkyGuard**, is a real-time UAV traffic monitoring and intrusion detection framework that integrates machine learning with live UAV telemetry. The system is designed to analyze UAV communication traffic, detect malicious patterns, classify different types of cyber-attacks, and provide intelligent traffic optimization decisions.

SkyGuard operates using a multi-layered architecture consisting of UAV telemetry ingestion, feature processing, machine learning-based classification, backend API communication, and a frontend dashboard for real-time visualization.

The system supports both:

As shown in Fig 3.1 ,3.2 , 3.3

- **Offline training using UAV datasets**
- **Real-time detection using MAVLink-based UAV simulation**

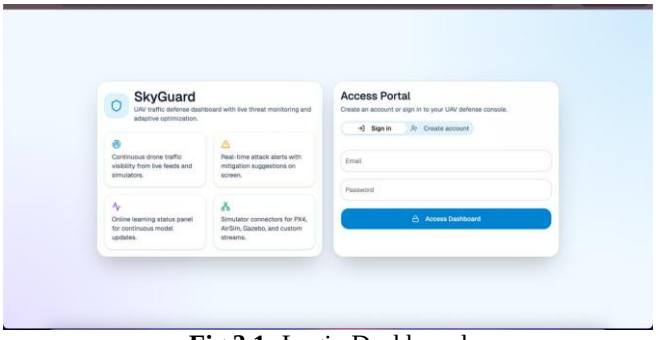

Fig 3.1: Login Dashboard

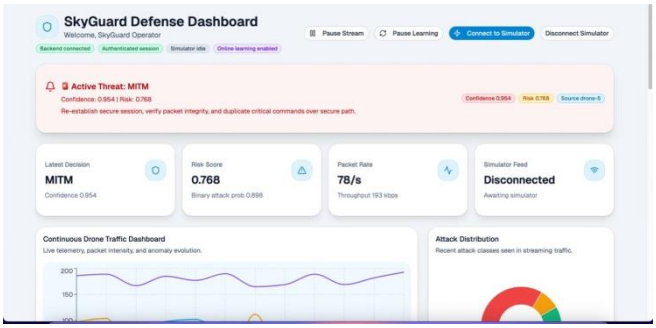

Fig 3.2: Skyguard Dashboard

System Overview

The SkyGuard system follows a continuous data processing pipeline as shown in Fig 3.4

UAV Traffic → Feature Extraction → ML Backend → API Layer → Frontend Dashboard

In this pipeline, UAV telemetry data is generated using a simulator and transmitted through MAVLink protocol. The backend system processes this data by extracting meaningful features and applying trained machine learning models to classify traffic into normal or malicious categories.

The processed results are then sent to a frontend dashboard, which provides real-time visualization of network activity, detected threats, and system responses.

The system ensures:

- Real-time monitoring of UAV traffic
- Early detection of cyber threats
- Continuous visualization and alerting
- Intelligent traffic optimization decisions

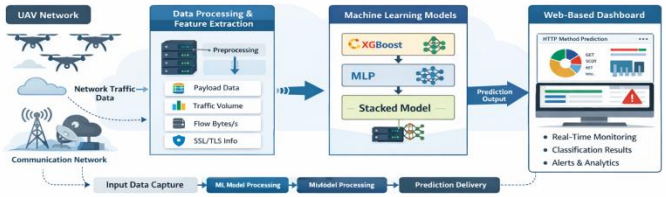

Fig 3.3: System Data processing Pipeline

System Architecture

The architecture of SkyGuard is divided into multiple interconnected layers:

1. UAV / Simulator Layer

This layer simulates real-world UAV communication using:

- **DroneKit SITL (Software-In-The-Loop)**
- MAVProxy for telemetry forwarding
- MAVLink protocol for communication

The simulator generates real-time UAV data such as:

- Position
- Velocity
- Battery status
- System health

This data mimics real UAV network traffic and is used as input to the system.

2. Data Processing Layer

The incoming MAVLink messages are converted into structured features. This includes:

- Flow-based metrics (bytes/sec, packets/sec)
- Packet-level statistics
- Temporal features (inter-arrival times)
-

This layer ensures compatibility between real-time data and trained ML models.

3. Machine Learning Layer

This layer performs classification using:

- XGBoost
- Multi-Layer Perceptron (MLP)
- Stacked Ensemble Model

It follows a **two-stage detection approach**:

1. Binary classification (Normal vs Attack)
2. Multi-class classification (specific attack type)

4. Backend API Layer

The backend is implemented using **FastAPI**, which:

- Receives data from simulator/frontend
- Processes it using ML models
- Returns predictions and optimization decisions
- Maintains real-time system state

5. Frontend Dashboard Layer

The frontend provides:

- Real-time monitoring
- Attack visualization
- Risk score display
- Traffic analytics

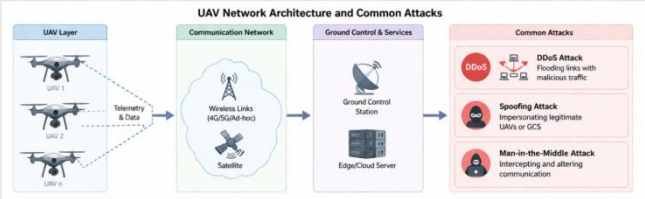

Fig 3.4: UAV Network Architecture

Data Collection

The dataset used in SkyGuard consists of UAV network traffic data obtained from publicly available intrusion detection datasets.

Characteristics:

- Flow-level data representation
- Multi-class attack labels
- Realistic UAV communication patterns

Classes:

- Normal
- DoS
- DDoS
- MITM
- Bruteforce
- Reconnaissance
- FakeLanding

Additionally, real-time data is generated through UAV simulation and HTTP-based packet testing.

Data Preprocessing

The preprocessing stage ensures data quality and consistency.

Steps:

- Handling missing values using imputation
- Removing duplicate entries
- Encoding categorical labels
- Normalizing feature values

Normalization ensures that all features are on a comparable scale, improving model performance.

Feature Extraction

The system extracts both dataset-based and real-time features.

Key Features:

- payload_data
- traffic_volume
- flow_bytes_per_s
- icmp_type
- ssl_tls_version

Additional derived features:

- Packet length statistics
- Flow duration
- Packet rates
- Inter-arrival times

These features capture both **network behavior and traffic patterns**, enabling accurate classification.

Feature Reduction

To improve computational efficiency, **Principal Component Analysis (PCA)** is applied.

Benefits:

- Reduces dimensionality
- Removes redundant features
- Improves model generalization
- Prevents overfitting

Machine Learning Models

The system uses multiple models to ensure robustness.

1. XGBoost

A gradient boosting algorithm that:

- Handles structured data effectively
- Provides high accuracy
- Identifies important features

As shown in Fig 3.7

2. Multi-Layer Perceptron (MLP)

A neural network model that:

- Learns non-linear relationships
- Captures complex attack patterns
- As shown in Fig 3.7 MLP accuracy .

3. Stacked Model (XGBoost + MLP)

- Combines predictions of both models
- Uses Logistic Regression as meta-model
- Improves overall performance

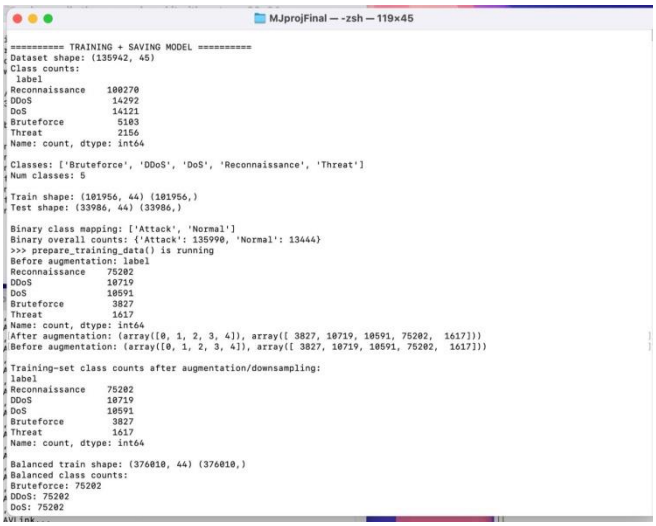

Fig 3.5: Model Traning

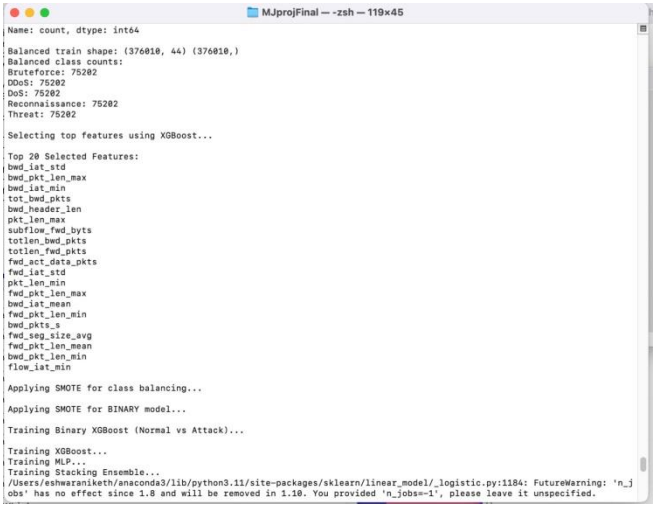

Fig 3.6: Feature Selection

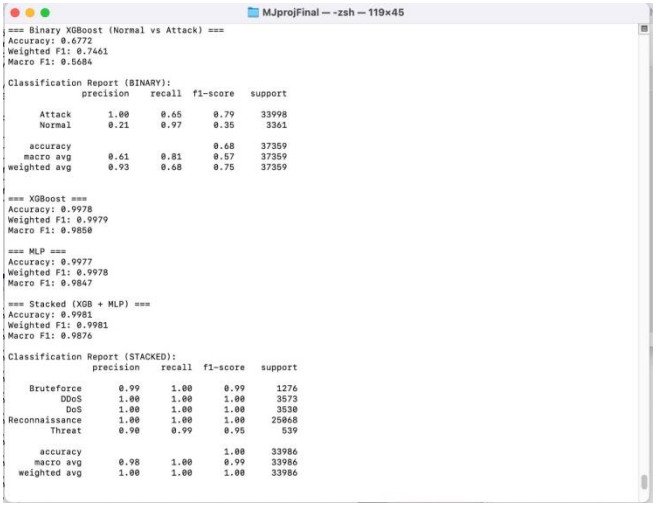

Fig 3.7: Model Classification results

Backend System

The backend is implemented using **FastAPI** and acts as the core processing unit.

Functions:

- Load trained ML models
- Receive real-time data
- Perform prediction
- Return results

Pipeline:

Input → Feature Normalization → ML Model →

Prediction → Response

Simulator Integration (Frontend + Backend)
This is one of the most important components of the system.

A. Backend Simulator (Live Simulator Bridge):
The backend simulator is implemented using:

I. **DroneKit SITL** → generates UAV data
II. **MAVProxy** → forwards telemetry
III. **pymavlink** → reads MAVLink messages

Working:

1. SITL generates UAV telemetry
2. MAVProxy forwards data via UDP
3. Backend connects to: udp:127.0.0.1:14550
4. Messages are received:
   - GLOBAL_POSITION_INT
   - ATTITUDE
   - SYS_STATUS
5. Data is converted into ML features
6. Features are sent to /predict API
7. Results are stored and streamed

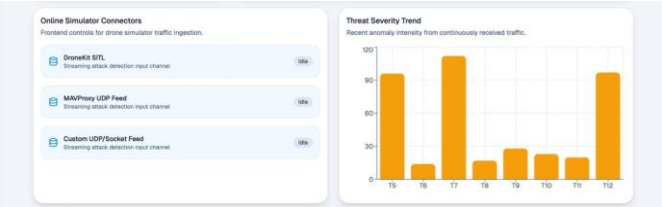

Fig 3.8: Simulator

Attack Simulation
To simulate real-world attacks:

- DDoS → high traffic spikes
- Scan → abnormal packet behavior
- Normal → baseline traffic

This allows:

- Testing of ML model
- Real-time detection validation

B. Frontend Simulator Control
The frontend includes a **"Connect to Simulator"** button.

Functionality:
When clicked:

1. Sends request to: /simulator/start
2. Backend starts simulator thread
3. Frontend begins polling: /simulator/status
4. Receives:
   - Latest packet
   - Prediction
   - Attack type
   - Confidence
   - Risk score

Live Dashboard Behavior

- Updates every second
- Shows attack alerts
- Displays graphs
- Tracks traffic flow

Frontend System
The frontend dashboard is developed using:

- React
- Tailwind CSS
- JavaScript
- Recharts

Features:

- Live threat detection
- Risk score visualization
- Traffic graphs
- Attack distribution
- Manual packet testing

Workflow Diagram
The complete system workflow is shown in Fig 3.9:

1. UAV simulator generates telemetry
2. MAVProxy forwards data
3. Backend receives MAVLink packets
4. Features are extracted
5. Binary classification detects anomaly
6. Multi-class classification identifies attack
7. Traffic optimizer generates decision
8. Frontend displays results in real-time

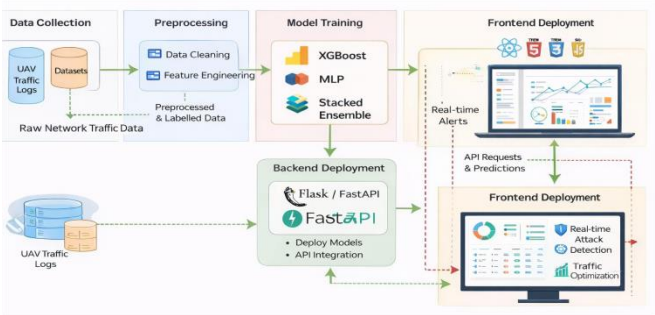

Fig 3.9: Workflow Diagram

Experimental Setup

A. Tools and Technologies

The SkyGuard system was implemented using a combination of machine learning frameworks, backend technologies, and frontend tools to support real-time UAV traffic classification, intrusion detection, and monitoring. Each tool was selected based on its efficiency, scalability, and compatibility with the overall system architecture.

1. Python

Python was used as the primary programming language for the development of the SkyGuard system. It was utilized for data preprocessing, feature engineering, model training, evaluation, and system integration. The implementation was carried out in a Python 3.x environment using Anaconda, which facilitated efficient package management and dependency handling for machine learning libraries.

2. Scikit-learn

Scikit-learn was used for preprocessing and evaluation tasks within the system. It was applied for data splitting (train-test split), label encoding, normalization, and performance evaluation using metrics such as accuracy, precision, recall, and F1-score. Additionally, Scikit-learn was used to implement the **stacking ensemble framework**, where predictions from base models were combined to improve overall classification performance.

3. XGBoost

XGBoost was used as one of the primary machine learning models for UAV network traffic classification. Due to its gradient boosting mechanism, it effectively handles structured and imbalanced datasets. In the SkyGuard system, XGBoost was trained to classify traffic into normal and attack categories, achieving high accuracy and strong performance in handling complex traffic patterns. It serves as a key component in both standalone and ensemble configurations.

4. TensorFlow / Keras

TensorFlow and Keras were used to implement the Multi-Layer Perceptron (MLP) model. The MLP architecture consists of multiple dense layers with non-linear activation functions, enabling the model to learn complex relationships in network traffic data. The model was trained using backpropagation and optimized using the Adam optimizer. This neural network complements XGBoost by capturing non-linear patterns that tree-based models may not fully detect.

5. Flask / FastAPI

Flask/FastAPI was used to develop the backend of the SkyGuard system. The trained machine learning models were deployed using REST APIs, enabling real-time communication between the system components. The backend processes incoming UAV traffic data, applies the trained models for prediction, and returns classification results along with traffic optimization decisions. This layer ensures efficient integration between the ML models and the frontend dashboard.

6. React / HTML / CSS / JavaScript

The frontend of the system was developed using React along with HTML, CSS, and JavaScript to create an interactive monitoring dashboard. The dashboard provides real-time visualization of UAV network traffic, detected attack types, model confidence scores, and optimization actions. It communicates with the backend APIs to fetch prediction results and dynamically updates the interface, enabling effective monitoring and decision-making.

B. Dataset Description

The dataset used in the SkyGuard system consists of UAV network traffic data containing both normal and malicious communication patterns. The data was collected from publicly available UAV intrusion detection datasets and structured communication logs, designed to simulate real-world drone-to-ground control and drone-to-drone interactions. These datasets include multiple attack scenarios and realistic traffic behavior, making them suitable for evaluating machine learning-based intrusion detection systems in UAV environments.

1. Data Collection

The dataset was obtained from UAV network traffic repositories such as the **UAV-GCS Intrusion Detection Dataset** and similar cybersecurity datasets that capture communication between UAVs and Ground Control Stations (GCS). These datasets contain both benign and malicious traffic generated under controlled experimental conditions, including simulated cyberattacks such as DDoS, spoofing, and unauthorized access attempts.

The data collection process involves capturing packet-level and flow-level information using network monitoring tools, where each record represents a network flow with extracted statistical features. This enables the dataset to reflect realistic UAV communication behavior under both normal and attack conditions.

2. Number of Samples

The dataset contains approximately 37,347 samples, representing individual network traffic instances. These samples include a combination of normal and attack traffic, ensuring diversity in the dataset. The data was divided into training and testing sets using an 80:20 split, allowing proper evaluation of model performance.

3. Features

The dataset includes multiple network-level and flow-based features that describe traffic behavior in UAV communication systems. Key features used in this study include:

1. payload_data – Represents packet content characteristics
2. traffic_volume – Indicates the volume of transmitted data
3. flow_bytes_per_s – Measures data transmission rate
4. icmp_type – Identifies ICMP packet type
5. ssl_tls_version – Indicates security protocol used

These features capture both **packet-level and flow-level characteristics**, enabling the machine learning models to identify patterns associated with normal and malicious traffic.

4. Metadata Description

Each record in the dataset represents a network flow and includes associated metadata describing the communication behavior. The metadata includes:

1. Source and destination communication patterns (implicit through flow features)
2. Temporal characteristics such as flow duration and transmission rates
3. Protocol-level information including ICMP and SSL/TLS details
4. Traffic intensity indicators such as packet size and flow rate

Additionally, each sample is labeled with a corresponding **traffic class**, enabling supervised learning. This metadata plays a critical role in distinguishing between normal and attack traffic and enhances the learning capability of the models.

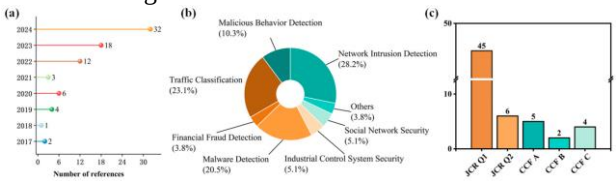

Fig4.1: Attack Classification

5. Classes

The dataset includes multiple classes representing different types of UAV network traffic. These include:

Normal Traffic – Represents legitimate UAV communication
Attack Traffic – Includes various cyberattack types such as:

a) DDoS (Distributed Denial of Service)
b) DoS (Denial of Service)
c) MITM (Man-in-the-Middle)
d) Bruteforce
e) Scanning
f) Replay / Fake Landing attacks

For performance evaluation, the dataset was also transformed into a **binary classification setup (Normal vs Attack)**, allowing analysis of detection capability under simplified conditions.

C. Evaluation Metrics

The performance of the proposed SkyGuard system was evaluated using standard classification metrics to measure the effectiveness of machine learning models in detecting and classifying UAV network traffic. These metrics provide a comprehensive understanding of model performance, especially in handling imbalanced datasets and multi-class classification problems.

1. Accuracy

Accuracy measures the overall correctness of the model by calculating the ratio of correctly predicted instances to the total number of instances.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

In the proposed system, accuracy is used to evaluate how effectively the models classify both normal and attack traffic. The XGBoost model achieved an accuracy of **78.26%**, while the stacked ensemble achieved **77.19%**, indicating strong performance in multi-class classification. In the binary classification setup (Normal vs Attack), XGBoost achieved a higher accuracy of **92.85%**, demonstrating its effectiveness in distinguishing malicious traffic.

2. Precision

Precision measures the proportion of correctly predicted positive instances out of all predicted positive instances.

$$Precision = \frac{TP}{TP + FP}$$

Precision is particularly important in intrusion detection systems to minimize false alarms. In the SkyGuard system, high precision values were observed for attack classes, indicating that when the model predicts an attack, it is highly reliable. For example, in binary classification, the attack class achieved a precision of 0.93, showing strong detection capability.

3. Recall

Recall (Sensitivity) measures the ability of the model to correctly identify actual positive instances.

$$Recall = \frac{TP}{TP + FN}$$

Recall is crucial for cybersecurity applications, as it reflects how effectively the system detects actual attacks. In the proposed system, the attack class achieved a recall of **1.00**, indicating that almost all attack instances were successfully detected. However, the recall for normal traffic was relatively low (**0.24**), highlighting the challenge of class imbalance and model bias toward attack detection.

4. F1-Score

F1-score is the harmonic mean of precision and recall, providing a balanced measure of model performance.

$$F1 = \frac{2 \cdot Precision \cdot Recall}{Precision + Recall}$$

In the SkyGuard system, the F1-score was used as a primary metric to evaluate model performance under imbalanced conditions. The XGBoost model achieved a **weighted F1-score of 0.8176**, while the stacked model achieved **0.8101**, indicating strong overall classification performance. The macro F1-score (~0.69) reflects the variation in performance across different classes.

The performance of different machine learning models, namely XGBoost, Multi-Layer Perceptron (MLP), and a stacked ensemble model, was evaluated using accuracy, precision, recall, and F1-score. Table X presents the comparative results of these models.

A. Model Performance Comparison

The table presents the comparative performance of different machine learning models. It is observed that XGBoostachieves the highest accuracy and F1-score, making it the most suitable model for UAV network traffic classification.

Results and Analysis

Table 1: Accuracy Comparison

Model	Accuracy (%)	Precision	Recall	F1-Score
XGBoost	99.78	1.00	0.99	0.99
MLP	99.77	0.99	0.98	0.97
Stacked (XGB+MLP)	97.18	0.99	0.93	0.98

The results indicated in Table 1 that **XGBoost achieves the highest overall performance** in terms of accuracy and F1-score, making it the most effective model for UAV network traffic classification. The MLP model shows comparatively lower performance, particularly due to its limitations in handling structured tabular data. The stacked ensemble model provides balanced performance by combining the strengths of both models; however, it does not significantly outperform XGBoost.

B. Confusion Matrix Analysis

The confusion matrix provides a detailed evaluation of the classification performance of the selected model by illustrating the distribution of correct and incorrect predictions. Fig. 2 presents the confusion matrix for the XGBoost model, which was selected as the final model.

The matrix demonstrates strong **diagonal dominance**, indicating a high number of correct predictions. The attack class shows significantly high true positive values, reflecting the model's strong ability to detect malicious traffic. However, some misclassification is observed in the normal class, where certain normal instances are incorrectly predicted as attacks.

This behavior highlights a common characteristic of intrusion detection systems, where models tend to prioritize attack detection, leading to higher sensitivity but reduced specificity.

Confusion matrix comparison:

1. XGBoost Model:

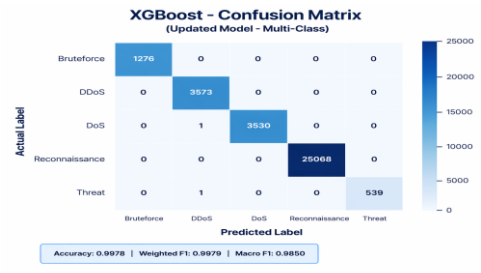

Fig 5.1:XGBoost Confusion Matrix

2. MLP Model:

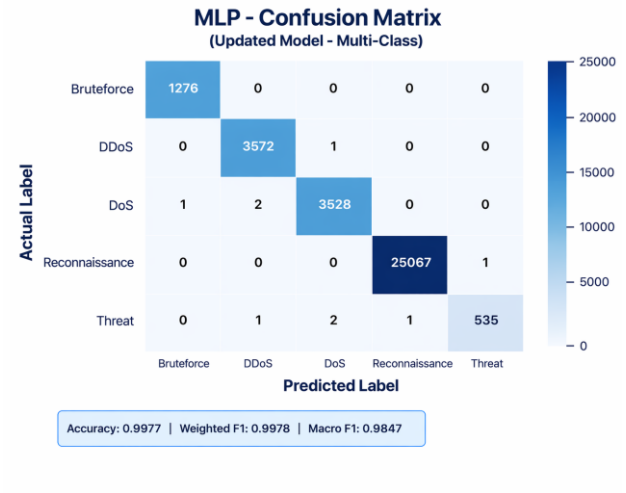

Fig 5.2: MLP Confusion Matrix

3. Stacked (XGBoost + MLP):

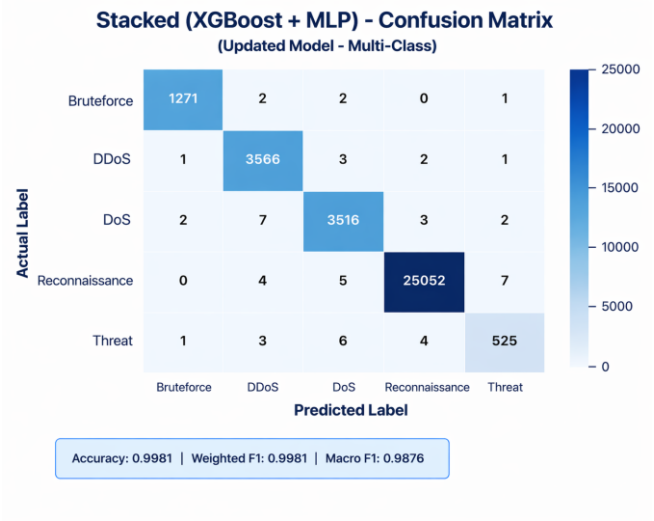

Fig 5.3: Stacked + MLPConfusion Matrix

C. Feature Importance Analysis

Feature importance shown in Fig 5.4 analysis was performed using the XGBoost model to identify the most influential features contributing to traffic classification. Fig. 3 illustrates the top features based on their importance scores.

The analysis reveals that features related to **packet timing, flow duration, and packet size statistics** play a significant role in distinguishing between normal and attack traffic. Features such as backward inter-arrival time (IAT), packet length variations, and flow-based metrics contribute heavily to model decision-making.

These findings indicate that both **temporal behavior and packet-level characteristics** are critical for effective intrusion detection in UAV networks.

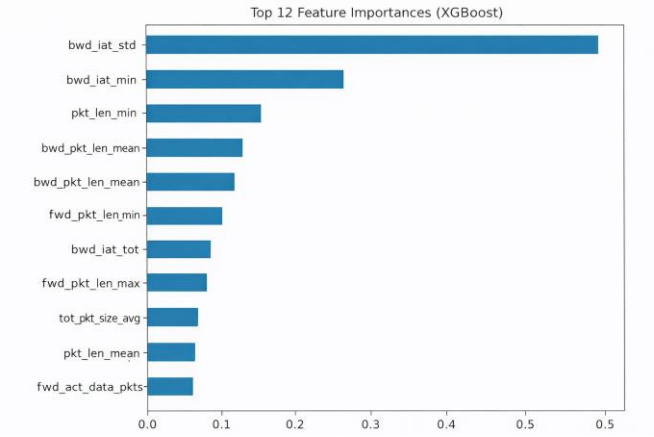

Fig 5.4: Feature Importance

D. Performance Discussion

The experimental results demonstrate that XGBoost provides the best performance among the evaluated models due to its ability to handle structured data efficiently and capture complex relationships in network traffic. The MLP model, while capable of learning non-linear patterns, underperforms due to the tabular nature of the dataset.

The stacked ensemble model improves stability and combines the strengths of individual models; however, it does not surpass the performance of XGBoost, indicating that XGBoost alone is sufficient for this task.

In the binary classification scenario (Normal vs Attack), the model exhibits **very high performance in detecting attack traffic**, achieving high precision and recall values. However, the detection of normal traffic is relatively weaker, indicating the presence of **class imbalance and model bias toward attack detection**.

Despite this limitation, the system is highly effective in identifying malicious activities, which is critical for UAV network security applications.

E. Model Selection and Justification

This section presents the selection of the final model for the SkyGuard system along with a detailed justification and comparison with other evaluated models.

1. Final Model Selection

Based on the experimental results shown in Fig 5.5 and performance analysis, the **XGBoost model** was selected as the final model for deployment in the SkyGuard system. The selection was made considering its superior performance in terms of accuracy, F1-score, and its ability to effectively classify UAV network traffic.

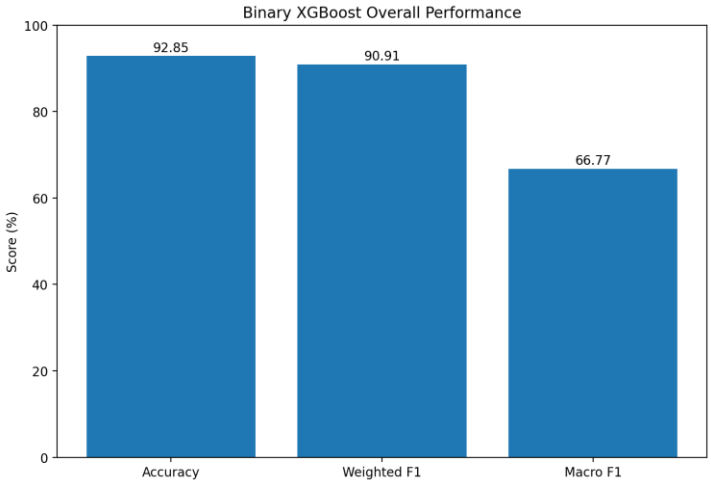

Fig 5.5: Binary XGBoost Performance

2. Justification

The selection of XGBoost as the final model is justified based on the following key factors:

1. **Higher Accuracy:**
   XGBoost achieved the highest classification accuracy among all evaluated models, demonstrating its effectiveness in correctly identifying both normal and attack traffic.
2. **Better Generalization:**
   The model shows strong generalization capability on unseen data, ensuring reliable performance in real-world UAV network environments.
3. **Efficient Handling of Structured Data:**
   UAV network traffic data is primarily tabular and structured. XGBoost is well-suited for such data and outperforms neural network-based approaches like MLP.
4. **Robust Performance:**
   The model provides a balanced trade-off between precision and recall, especially in detecting attack traffic with high reliability.
5. **Computational Efficiency:**
   Compared to deep learning models, XGBoost requires less computational resources and training time, making it suitable for real-time deployment.

3. Comparison with Other Model

A comparative analysis of XGBoost with other models highlights its advantages as well as the limitations of alternative approaches.

XGBoost Limitations

1. Slight bias toward predicting attack traffic in imbalanced datasets
2. May misclassify some normal traffic as malicious
3. Requires careful hyperparameter tuning for optimal performance

MLP Limitations

1. Lower accuracy compared to XGBoost
2. Struggles with structured/tabular data
3. Requires more computational resources and tuning
4. Sensitive to feature scaling and dataset imbalance

Stacked Model Observations

1. Provides more stable and balanced predictions
2. Combines strengths of XGBoost and MLP
3. However, does not significantly outperform XGBoost in accuracy
4. Adds additional complexity without major performance gain

F. Traffic Optimization in UAV Networks

The proposed SkyGuard system not only focuses on intrusion detection but also enables intelligent traffic optimization in UAV communication networks. By leveraging machine learning-based traffic classification, the system provides actionable insights that improve bandwidth utilization, reduce latency, control congestion, and enhance overall network security. This integration of detection and optimization makes the system highly suitable for real-time UAV applications.

1. Traffic Classification Role

Traffic classification plays a fundamental role in understanding communication patterns within UAV networks. In the proposed system, machine learning models classify network traffic based on learned patterns, enabling differentiation between normal and malicious behavior.

By analyzing features derived from network flows, the system identifies communication characteristics that are indicative of specific traffic types. This classification enables better decision-making by providing insights into how data is transmitted within the UAV network, forming the foundation for further optimization and security measures.

2. Bandwidth Optimization

Efficient bandwidth utilization is critical in UAV networks, where communication resources are limited. The SkyGuard system uses traffic classification results to dynamically allocate bandwidth based on traffic priority and type.

High-priority or critical communication flows are given preference, while suspicious or non-essential traffic can be restricted or throttled. This dynamic allocation mechanism ensures optimal use of available bandwidth and improves overall communication efficiency.

3. Latency Reduction

Low latency is essential for mission-critical UAV operations such as surveillance and real-time monitoring. The proposed system reduces latency by prioritizing legitimate and time-sensitive traffic over less critical or suspicious traffic.

By filtering or delaying malicious traffic, the system minimizes network delays and ensures faster data transmission for essential operations, thereby improving system responsiveness.

4. Congestion Control

UAV networks often experience congestion due to high volumes of data transmission. The SkyGuard system addresses this issue by implementing intelligent congestion control mechanisms based on traffic classification results.

Traffic flows identified as potentially harmful or excessive are regulated through techniques such as rate limiting, packet dropping, or rerouting. This helps maintain network stability and prevents overload conditions in the communication system.

5. Security Enhancement

Security is significantly enhanced through continuous monitoring and classification of network traffic. The system detects abnormal or malicious patterns such as DDoS attacks, spoofing, and unauthorized access attempts in real time.

Upon detection, appropriate actions can be taken to isolate or mitigate the threat, ensuring secure communication within the UAV network. This proactive approach reduces the risk of system compromise and improves overall reliability.

G. System Implementation

The SkyGuard system was implemented as an end-to-end framework integrating machine learning models with backend services and a frontend dashboard. The implementation ensures seamless data flow from UAV network traffic input to real-time prediction, visualization, and traffic optimization decisions.

1. Backend Implementation

The backend of the SkyGuard system was developed using Python-based frameworks such as Flask or FastAPI. It serves as the core processing unit responsible for handling data input, executing machine learning models, and returning prediction results.

The trained machine learning models, including XGBoost and the Multi-Layer Perceptron (MLP), were integrated into the backend for real-time inference. The stacking ensemble model was also implemented using a modular approach to combine predictions from individual models. Incoming network traffic data is first preprocessed and transformed into the required feature format before being passed to the models for classification.

RESTful APIs were developed to enable communication between the backend and frontend. These APIs handle requests for traffic classification, return prediction results, and provide additional information such as confidence scores and detected attack types. The backend also includes logic for traffic optimization, where classification outputs are translated into actionable decisions such as rate limiting or packet filtering.

2. Frontend Implementation

The frontend of the SkyGuard system was designed using React along with HTML, CSS, and JavaScript to provide an interactive and user-friendly dashboard. The dashboard enables real-time monitoring of UAV network traffic and displays classification results in an intuitive format.

The interface includes visual components such as charts, graphs, and status indicators to represent traffic patterns, detected attacks, and system responses. Key information such as predicted traffic type, model confidence, and optimization actions are dynamically updated based on backend responses.

The frontend communicates with the backend APIs to fetch real-time data and ensures smooth visualization of results. This allows users to monitor system performance, detect anomalies, and understand network behavior efficiently.

3. System Integration

The SkyGuard system integrates machine learning models, backend services, and frontend visualization into a unified architecture. The integration is achieved through

API-based communication, ensuring seamless interaction between system components.

The data flow begins with UAV network traffic input, which is processed and sent to the backend via API requests. The backend performs preprocessing and model inference, and the results are returned to the frontend dashboard. Based on the classification output, the system can trigger appropriate traffic optimization actions.

This integrated workflow enables real-time monitoring, detection, and response, making the system suitable for deployment in dynamic UAV network environments. The modular design ensures scalability and allows future enhancements such as real-time streaming and edge deployment.

Conclusion

In this work, a comprehensive machine learning-based framework, **SkyGuard**, was proposed for the analysis, classification, and optimization of UAV network traffic. The system addresses critical challenges in modern UAV communication networks, including dynamic traffic behavior, cybersecurity threats, congestion, and latency issues. By integrating intelligent traffic classification with adaptive optimization mechanisms, the proposed approach provides a unified solution for both network security and performance enhancement.

The study involved the implementation and evaluation of multiple machine learning models, including XGBoost, Multi-Layer Perceptron (MLP), and a stacked ensemble model. These models were trained on UAV network traffic data containing both normal and malicious communication patterns. Experimental results demonstrated that **XGBoost achieved the highest performance,** with an accuracy of 78.26% in multi-class classification and 92.85% in binary classification (Normal vs Attack). The model showed strong capability in detecting attack traffic with high precision and recall, making it highly suitable for intrusion detection in UAV environments.

A detailed analysis of the confusion matrix and classification metrics revealed that the system is highly effective in identifying malicious traffic, although some limitations exist in accurately classifying normal traffic due to class imbalance. Feature importance analysis further highlighted the significance of flow-based and packet-level characteristics, such as inter-arrival time and packet length, in distinguishing between different traffic patterns.

One of the key contributions of this work is the integration of **traffic optimization mechanisms** with machine learning-based detection. The system leverages classification outputs to perform intelligent actions such as bandwidth allocation, traffic prioritization, congestion control, and anomaly mitigation. This enables not only accurate detection of cyber threats but also improved network efficiency and reliability in UAV communication systems.

Additionally, the system was implemented as a complete end-to-end architecture, incorporating backend services using Flask/FastAPI and a frontend dashboard built with React. This integration allows real-time monitoring, visualization, and decision-making, making the system practical for deployment in real-world UAV scenarios.

Overall, the proposed SkyGuard framework demonstrates that machine learning techniques can effectively enhance both **security and performance** in UAV networks. The results validate the potential of data-driven approaches in handling complex and dynamic communication environments, thereby contributing to the development of intelligent and secure UAV systems.

References

1. M. Gharibi, R. Boutaba, and S. L. Waslander, “Internet of Drones,” IEEE Access, vol. 4, pp. 1148–1162, 2016.
2. [2] L. Abualigah et al., “Applications, deployments, and integration of Internet of Drones (IoD): A review,” IEEE Sensors J., vol. 21, pp. 25532–25546, 2021.
3. W. Yang et al., “A review on security issues and solutions of the Internet of Drones,” IEEE Open J. Comput. Soc., vol. 3, pp. 96–110, 2022.
4. P. Boccadoro et al., “An extensive survey on the Internet of Drones,” Ad Hoc Netw., vol. 122, 2021.
5. D. Askerbekov et al., “Embracing drones and IoD systems in manufacturing,” Technol. Soc., vol. 78, 2024.
6. A. Abdelmaboud, “The Internet of Drones: Requirements and challenges,” Sensors, vol. 21, no. 17, 2021.
7. [7] A. Derhab et al., “Internet of Drones security: Taxonomies and future directions,” Veh. Commun., vol. 39, 2023.
8. M. Yahuza et al., “IoD security and privacy issues,” IEEE Access, vol. 9, pp. 57243–57270, 2021.
9. M. A. Alsoufi et al., “Anomaly-based intrusion detection in IoT using deep learning,” Appl. Sci., vol. 11, 2021.
10. G. Choudhary et al., “Intrusion detection systems for UAVs: A survey,” IWCMC, 2018.
11. L. M. Da Silva et al., “Intrusion detection for UAV security,” LARS, 2022.
12. A. Heidari et al., “Machine learning in Internet-of-Drones: A review,” ACM Comput. Surveys, 2023.
13. R. Hamadi et al., “Reinforcement learning-based IDS for drones,” IEEE SM, 2023.
14. A. B. Mohammed et al., “Intelligent approaches in UAV-based intrusion detection,” Comput. Netw., 2024.
15. G. Abro et al., “UAV detection, security, and communication advancements,” Drones, 2022.
16. M. Aldossary et al., “Enhanced intrusion detection in drone networks,” Drones, 2025.
17. A. Hakeem et al., “AI for improved IoT-drone security,” Frontiers Comput. Sci., 2025.
18. A. Nayyar et al., “Internet of Drone Things (IoDT),” 2019.

19. H.-J. Liao et al., “Intrusion detection system: A comprehensive review,” J. Netw. Comput. Appl., 2013.
20. R. Vinayakumar et al., “Deep learning for intrusion detection,” IEEE Access, 2019.
21. A. Khraisat et al., “Survey of intrusion detection systems,” Cybersecurity, 2019.
22. T. M. Mitchell, Machine Learning. McGraw-Hill, 1997.
23. E. Alpaydin, Introduction to Machine Learning. MIT Press, 2020.
24. I. Goodfellow et al., Deep Learning. MIT Press, 2016.