MACHINE LEARNING AND UAVS

Nikitha Rajagopalan, Salma Aboelmagd, Dr. Abdulrahman Takiddin

FSU | FLORIDA STATE UNIVERSITY
FSU UNDERGRADUATE RESEARCH OPPORTUNITY PROGRAM
CENTER FOR UNDERGRADUATE RESEARCH & ACADEMIC ENGAGEMENT

ABSTRACT

Unmanned Aerial Vehicles (UAVs) are increasingly used for applications such as package delivery and crop monitoring, but their growing use also increases exposure to cyber and physical attacks. While intrusion detection systems (IDS) monitor UAV inputs to detect cyber intrusions, most research focuses only on the cyber layer and overlooks resulting physical effects. This study investigates how machine learning can improve UAV security by detecting cyber-physical attacks. Using Python libraries including pandas, scikit-learn, and TensorFlow, shallow and deep learning models were trained on a publicly available UAV physical dataset and evaluated using benign flight data. Results show that deep learning models can better capture complex patterns and anomalies compared to traditional approaches, enabling earlier detection of malicious behavior. Improving UAV attack detection is critical as drones are increasingly used in emergency response, delivery systems, and environmental monitoring. Integrating advanced machine learning techniques can enhance the safety, reliability, and autonomy of UAV operations in dynamic environments.

INTRODUCTION

- Unmanned Aerial Vehicles (UAVs) are widely used in defense, agriculture, logistics, surveillance, and real-time data collection to improve efficiency and reduce costs.
- Despite their benefits, UAVs are vulnerable to cyber threats such as GPS spoofing, network intrusion, false data injection, and denial-of-service attacks, which can cause hijacking, data loss, and mission failure.

Machine Learning (ML) strengthens UAV cybersecurity by:

- Detecting anomalies in sensor and communication data
- Identifying emerging attack patterns
- Enabling real-time threat detection and response
- The rise in sophisticated UAV cyberattacks underscores the need for intelligent, real-time intrusion detection systems, especially for mission-critical operations.
- Objective: Evaluate machine learning models using UAV telemetry data to detect and classify cyber-physical attacks.

Our objective is to investigate the effect of machine learning algorithms on UAV systems.

METHODS

How Data was collected:

Dataset:

- Used a dataset containing UAV telemetry and cyber-physical measurements collected during normal operation and multiple attack scenarios.
- Features include flight dynamics, motion states, control inputs, sensor readings, position, orientation, and velocity data. Target labels represent normal behavior and different attack types.

Preprocessing

- Removed null/constant columns, applied median imputation, label encoding, and feature standardization. Generated sliding-window sequences for temporal models and split data into stratified training and testing sets.

Models implemented

- Traditional ML: Logistic Regression, Decision Tree, Random Forest, Gradient Boosting, SGD
- Deep Learning: CNN for spatial feature extraction and LSTM/GRU for temporal attack pattern detection

Evaluation Metrics

- Models were compared using accuracy, precision, recall, and F1-score to assess overall performance, false alarm reduction, and attack detection capability.

RESULTS

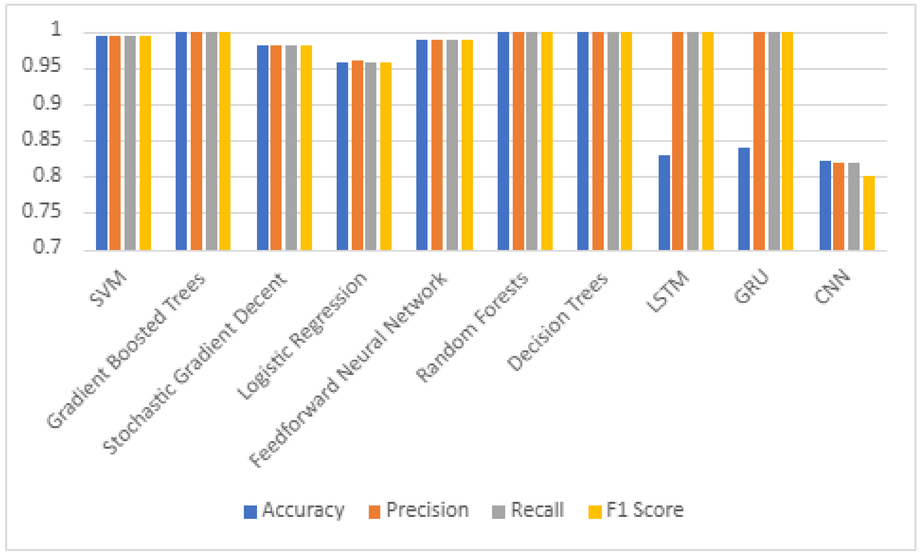

Figure 1: Graph showing the accuracy, precision, recall, and F1 score of each model tested

DISCUSSION

- Study Focus: Evaluated machine learning and deep learning models for detecting cyber-physical attacks in UAV telemetry data.
- Traditional ML Performance: Decision Tree, Random Forest, Logistic Regression, and Gradient Boosting provided strong baseline results, with ensemble models outperforming single-tree approaches.
- Best Traditional Model: Random Forest showed particularly strong performance by capturing nonlinear relationships in telemetry features.
- Deep Learning Advantages:
- CNN: Captured spatial relationships between features
- LSTM & GRU: Modeled temporal attack patterns in sequential data
- Efficiency Insight: GRU achieved performance similar to LSTM with fewer parameters, making it more suitable for real-time detection systems.
- Overall Finding: Temporal modeling improves attack detection accuracy, though deep learning approaches require greater computational resources.

CONCLUSION

- Key Result: Machine learning and deep learning models can effectively detect cyber-physical attacks in UAV systems using telemetry and sensor data.
- Model Performance:
- Random Forest provides a strong and interpretable baseline.
- CNNs and recurrent networks (LSTM/GRU) improve detection by capturing complex feature relationships and temporal patterns.
- Best Balance: GRU offers a strong trade-off between accuracy and computational efficiency, making it suitable for real-time UAV intrusion detection.
- Implication: Temporal feature modeling is critical for improving cyber-physical attack detection and strengthening UAV system security.
- Future Work: Focus on real-time deployment, model compression for edge devices, and testing under adversarial conditions to improve robustness.

REFERENCES