Machine Learning-Based Intrusion Detection for UAV Swarm Networks

UMKC School of Computing and Engineering

Abdalrahman Bashir (bhbf73@umkc.edu), Qingli Zeng (zq6mw@umsystem.edu)

University of Missouri Kansas City, School of Science and Engineering

Introduction

- **Unmanned Aerial Vehicle(UAV):** UAVs are becoming increasingly important in various applications, such as surveillance, agriculture, and delivery services.
- **Problem Overview**: UAV swarm networks face significant security risks from cyber attacks, threatening their operational integrity[1].
- **Need for Intrusion Detection:** An effective IDS can enhance UAV network security by identifying and mitigating these network threats in real time.
- **Approach:** Simulate a UAV swarm network using NS3 with AODV routing and the BOID mobility model, introducing attacks such as black hole, flooding, and Sybil attacks.
- **Outcome:** Create a unique intrusion dataset and evaluate multiple machine learning algorithms for IDS, analyzing metrics like accuracy to determine performance.

Objectives

- **Develop a UAV Swarm Network Model:** Build a realistic simulation of UAV networks using NS3, employing AODV routing and the BOID mobility model.
- **Simulate Diverse Network Attacks:** Implement multiple attack scenarios, including black hole, flooding, and Sybil attacks, to replicate potential threats in UAV networks.
- **Create a Custom Intrusion Dataset:** Generate a dataset tailored to UAV network intrusions, capturing data from normal and attack scenarios.
- **Apply Machine Learning for Intrusion Detection:** Test and evaluate various machine learning algorithms to detect intrusions effectively within the UAV network.
- **Evaluate Model Performance:** Analyze key performance metrics such as accuracy, precision, recall, and F1-score to assess the effectiveness of each machine learning model in detecting network intrusions.

Methodology

1. UAV Swarm Networks Simulation

A. BFM: BOID Flocking Mobility Model

BOID model was introduced by Craig Reynolds[2], laid the foundational principles for simulating flocking behavior.

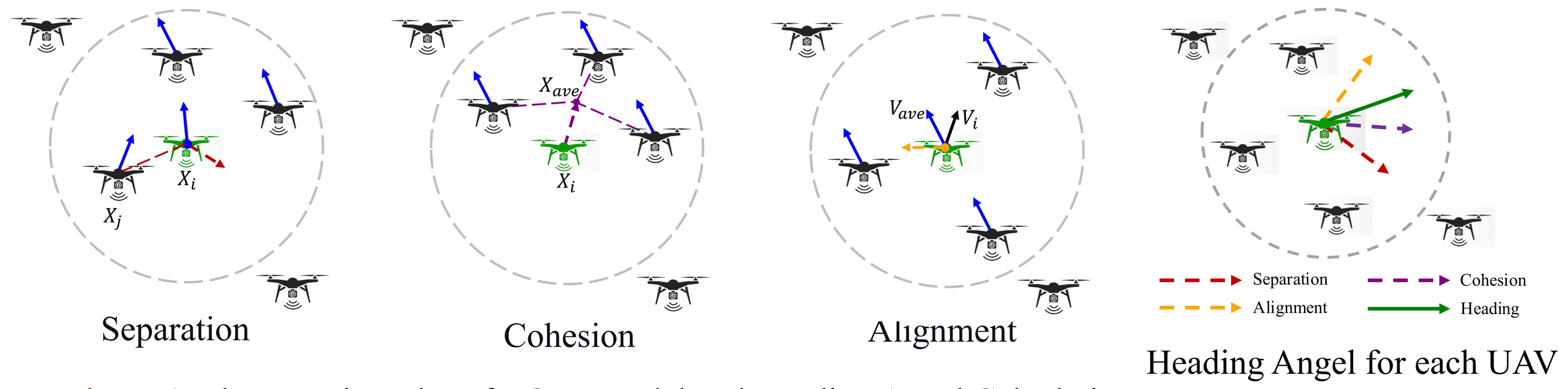

Figure 1. Three Basic Rules of BOID Model and Heading Angel Calculation

- **Separation** : Each UAV maintains a safe distance from its neighbors to prevent collisions.
- **Cohesion** : Each UAV moves towards the average position of its neighbors, allowing the swarm to stay together.
- **Alignment** : Each UAV matches its direction and speed with its neighboring UAVs to maintain the same trajectory.

B. BMR: BOID Mobility-Based Routing

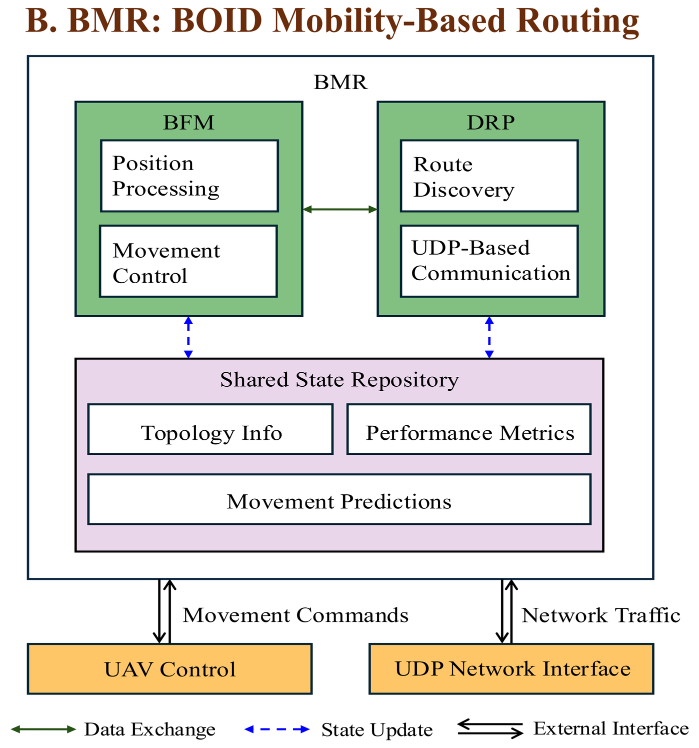

Figure 2. UAVs Swarm Network Architecture

C. Simulation Configuration

Parameters	Value
Network Simulator	NS-3.24
Operation System	Ubuntu 20.04
Wireless Standard	IEEE 802.11ac
Routing Protocol	AODV
UAV Mobility Model	BOID Model
Traffic Type	UDP
Transmission Range	100 meters
Transmission Power	20 dBm
Channel Model	Nakagami
Programming Language	C++, Python

Table I. Simulation Configuration

2. Attacks Simulation and Dataset

Type of Attacks	Normal Traffic	Black Hole	Sybil	Flooding	Legitimate AODV Traffic	Total
Number of Samples	5749	9064	972	1233	25777	42795

Table II. Overview of the UAV Swarm Networks IDS Dataset

3. Machine Learning Based Intrusion Detection System

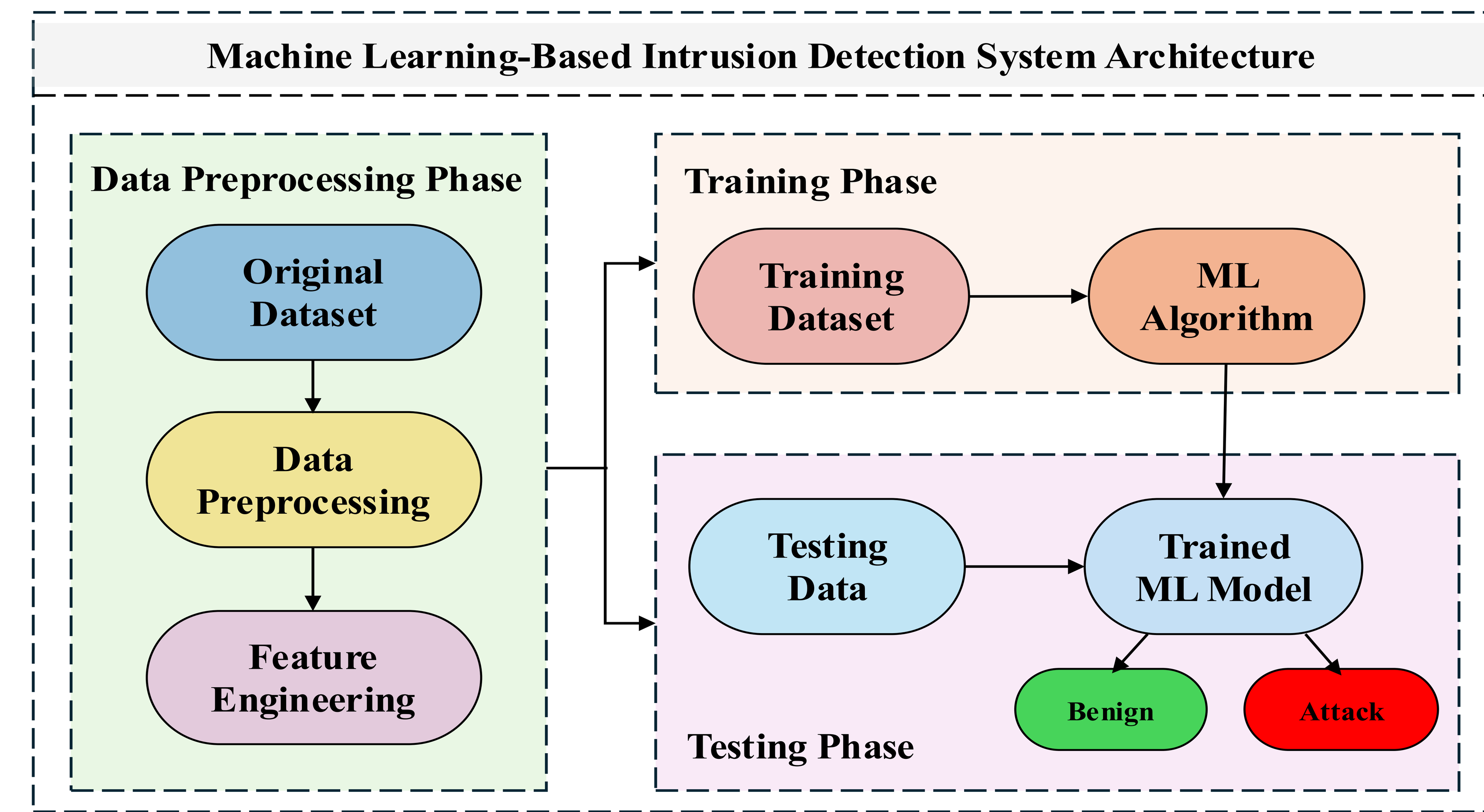

Figure 3. Machine Learning Based UAV Intrusion Detection System

- **Data Preprocessing:** Raw UAV data is cleaned, and features are extracted to enhance model readiness.
- **Training Phase:** ML algorithms are trained to recognize benign and attack patterns from labeled data.
- **Testing Phase:** The model is tested on new data to classify instances as benign or attack, enabling real-time detection [3].

Results

1. Performance Metrics

Acc: Accuracy measures the overall correctness of the intrusion detection model's predictions.

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

Rc: Recall measures the proportion of actual intrusions that are correctly identified by the model.

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

Pre: Precision measures the proportion of true positive predictions among all positive predictions made by the model.

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

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

$$F1 = 2 \cdot \frac{Pre \times Rc}{Pre + F1}$$

2. Performance Evaluation

Method	Attacks	Pre(%)	Recall(%)	F1(%)	Overall Acc(%)
Random Forest	Black hole attacks	94%	91%	93%	**97%**
	Flooding Attacks	99%	96%	98%	
	Sybil Attack	99%	100%	99%	
	Normal Traffic	99%	100%	100%	
	Legitimate AODV Traffic	97%	98%	97%	
XGBOOST	Black hole attacks	95%	93%	94%	**97%**
	Flooding Attacks	99%	97%	98%	
	Sybil Attack	98%	100%	99%	
	Normal Traffic	100%	100%	100%	
	Legitimate AODV Traffic	98%	98%	98%	
CNN	Black hole attacks	93%	87%	90%	**93%**
	Flooding Attacks	55%	88%	67%	
	Sybil Attack	97%	15%	25%	
	Normal Traffic	92%	100%	96%	
	Legitimate AODV Traffic	96%	98%	97%	
DNN	Black hole attacks	95%	88%	91%	**94%**
	Flooding Attacks	54%	94%	69%	
	Sybil Attack	97%	15%	25%	
	Normal Traffic	94%	99%	96%	
	Legitimate AODV Traffic	96%	98%	97%	
LIGHTGBM	Black hole attacks	92%	92%	92%	**97%**
	Flooding Attacks	100%	97%	99%	
	Sybil Attack	98%	97%	97%	
	Normal Traffic	99%	100%	99%	
	Legitimate AODV Traffic	97%	97%	97%	

Table III. Machine Learning Algorithm Performance Evaluation

3. Analysis

- The high precision, recall, and F1-scores across most machine learning methods indicate that our dataset effectively captures distinctive patterns for both benign and attack traffic in UAV networks.
- Random Forest, XGBoost, and LightGBM achieved excellent overall accuracy, demonstrating their strong capability to handle the complex attack scenarios present in the dataset.
- Despite the challenging nature of certain attacks, such as Sybil and flooding, the consistent performance of several models highlights the quality and robustness of our dataset.
- These results validate our dataset as a reliable resource for training intrusion detection models and reinforce the potential of machine learning in enhancing UAV network security.

Discussion, Conclusion and Future Work

Discussion

- The proposed machine learning-based IDS demonstrates significant potential for enhancing the security of UAV swarm networks by effectively detecting various network attacks.
- Unlike traditional IDS systems, our model leverages a customized dataset and considers UAV-specific mobility patterns, making it highly adaptable and responsive to the unique challenges in UAV networks.
- This approach shows promise in reducing false alarms and improving detection rates, particularly in dynamic network environments like UAV swarms.

Conclusion

- Our study successfully developed an IDS capable of identifying black hole, flooding, and Sybil attacks within UAV networks with high accuracy.
- Key findings highlight that machine learning algorithms, when applied to a well-preprocessed UAV dataset, can provide robust intrusion detection in real-time.
- This work contributes to the field by addressing security vulnerabilities specific to UAV networks, ultimately helping to safeguard UAV applications in various sectors.

Future Work

- Further research could explore the integration of deep learning models to enhance detection accuracy and adapt to more complex attack patterns.
- Expanding the dataset with additional attack types and more diverse UAV network scenarios would improve model generalizability.
- Investigating real-world deployment and scalability of this IDS in large-scale UAV networks could bring us closer to practical, field-ready solutions.

References

[1] Gupta L, Jain R, Vaszkun G. Survey of important issues in UAV communication networks[J]. IEEE communications surveys & tutorials, 2015, 18(2): 1123-1152.

[2] Reynolds C W. Flocks, herds and schools: A distributed behavioral model[C]//Proceedings of the 14th annual conference on Computer graphics and interactive techniques. 1987: 25-34.

[3] Zeng Q, Nait-Abdesselam F. Leveraging Human-In-The-Loop Machine Learning and GAN-Synthesized Data for Intrusion Detection in Unmanned Aerial Vehicle Networks[C]//ICC 2024-IEEE International Conference on Communications. IEEE, 2024: 1557-1562.

Acknowledgments

Abdalrahman Bashir and Qingli Zeng contribute equally for this project. There is no funding source for this project.

GitHub Link

https://github.com/AbdalrahmanBashir/AI-based-intrusion-detection-system