AI-based Attack Detection Techniques for UAV Systems

Done by: Abdullah Almekhyal Supervisor: Dr. Noura Aljeri
Computer Science Department, College of Science, Kuwait University

ملتقى
الأمن السيبراني
الخليجي
قطر 2-3 أكتوبر 2024

Introduction

Unmanned Aerial Vehicles (UAVs), such as RQ-4 Global Hawk, MQ-9 Reaper, Bayraktar TB2 and HESA Shahed 136, have revolutionized modern warfare, surveillance, and logistics, offering critical value to military operations, economies, and societies worldwide. However, UAVs remain vulnerable to significant security threats. The most common attacks on UAVs systems include cyber hijacking, spoofing, jamming, high power microwave, electromagnetic gun, high energy laser and physical attack [1]. As UAVs become more integral to national defense and infrastructure, addressing these security issues is essential to ensure safe and reliable operations.

Problem Statement

We identify two primary security concerns regarding UAVs, either the UAV acts as an attacker on foreign territory, requiring countermeasures, or it becomes the target of an attack itself. Our focus is on the latter – attacks directed at the UAV (Table 1). The two main types of attacks that can compromise the communication network are:

- ○ **Spoofing:** GPS spoofing devices emit false signals to the target drone, replacing its original communication signals used for navigation. This allows the attacker to gain control over the drone
- ○ **Jamming:** Jamming devices, which can be either stationary or mobile, emit large amounts of RF energy towards the drone, disabling its control system. Depending on the type of jamming, one of the following scenarios may occur:
  - ▪ The drone is forced to crash to the ground in a controlled manner.
  - ▪ The drone is redirected toward its launch site.
  - ▪ The drone crashes to the ground uncontrollably.
  - ▪ The drone flies randomly and uncontrollably.

Table 1

Type of attacks	Counter measures
GPS-Jamming	-Activating GPS-deficient autonomous navigation -The utilization of extra sensors for backup navigation. -Using IDS based on ML to Identify sensor-based threats.
GPS-spoofing	-The use of GPS signal authentication techniques. -Spoofing anomalous variations in signal strength that point to the start of a spoofing attack.
Cyber Hijacking	-GPS-based flight pattern recognition and statistical analysis techniques, such as position estimation methods based on the onboard Inertial Measurement Unit (IMU), are employed

Our objective is to evaluate the performance of different AI-based models in detecting an attack on UAV using historical flight data. Almost all available datasets include information on GPS coordinates, altitude, Remote Control, accelerometer, among others.

Dataset

TLM Fusion data[3]

Labels	0 (normal)	1 (GPS)	2 (accelerometer)	3 (engine)	4 (RC)
TLM [1]	6567	1823	1863	1449	551

UAV data attack [4]
(sample movement comparison in figure 1)

Type of attack	benign	Malicious
Spoofing	3124	498
Jamming	4985	1460

Abstract

Over the past few years, we have witnessed a surge in Unmanned Aerial Vehicles (UAVs) technologies used in various applications such as commercial, military and industry. Nowadays, UAVs can cover many of the military critical services such as navigation, secure communication, and reconnaissance [2]. However, security aspects are one of the most critical issues in UAVs due to unreliable communications. In this poster, we evaluate AI-based attack detection techniques and report their performance in terms of accuracy and precision over different datasets.

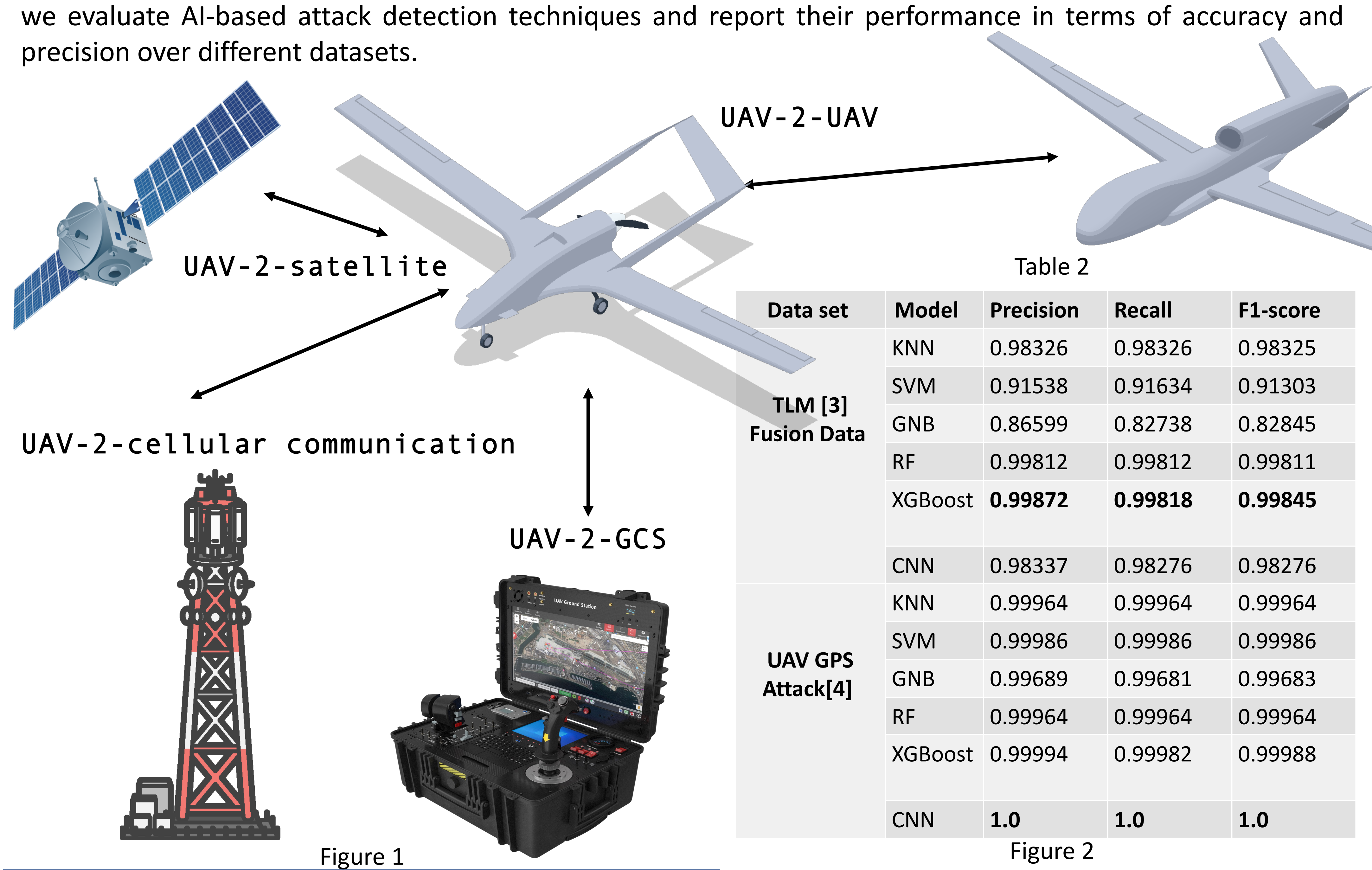


Figure 1

Sample of drone's movement projections (Benign vs Malicious)

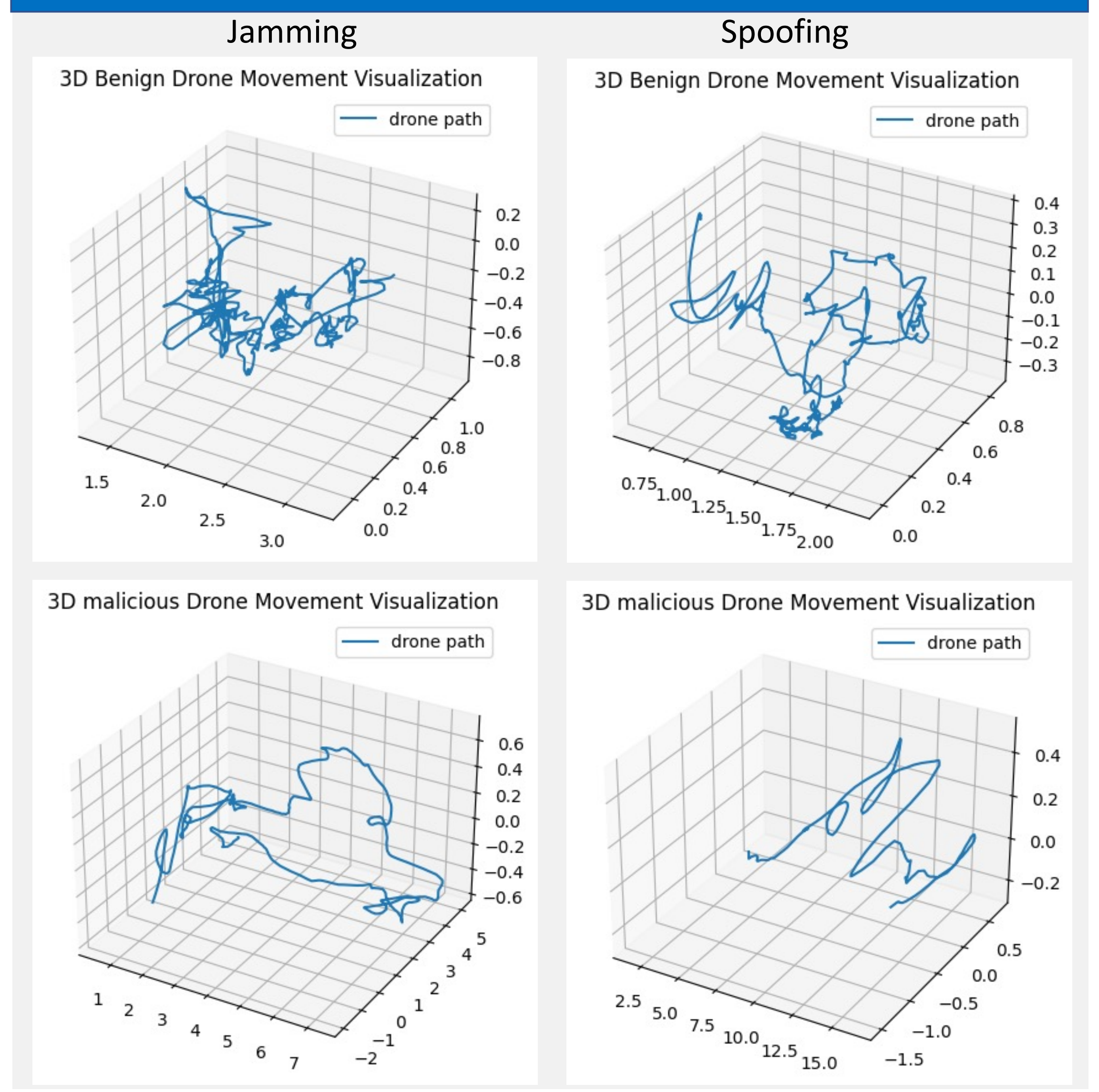
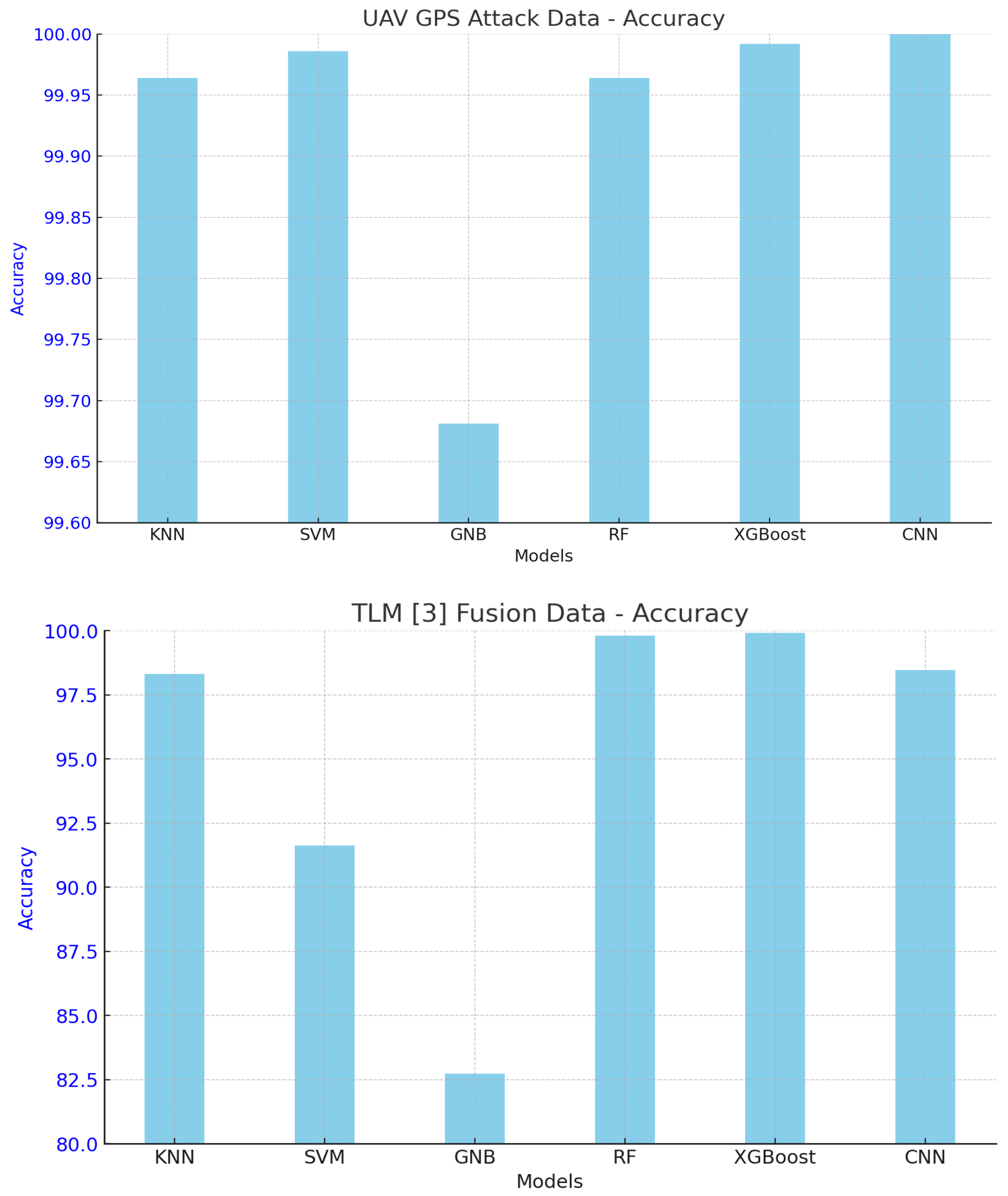


Table 2

Data set	Model	Precision	Recall	F1-score
TLM [3] Fusion Data	KNN	0.98326	0.98326	0.98325
	SVM	0.91538	0.91634	0.91303
	GNB	0.86599	0.82738	0.82845
	RF	0.99812	0.99812	0.99811
	XGBoost	**0.99872**	**0.99818**	**0.99845**
	CNN	0.98337	0.98276	0.98276
UAV GPS Attack[4]	KNN	0.99964	0.99964	0.99964
	SVM	0.99986	0.99986	0.99986
	GNB	0.99689	0.99681	0.99683
	RF	0.99964	0.99964	0.99964
	XGBoost	0.99994	0.99982	0.99988
	CNN	**1.0**	**1.0**	**1.0**

Figure 2

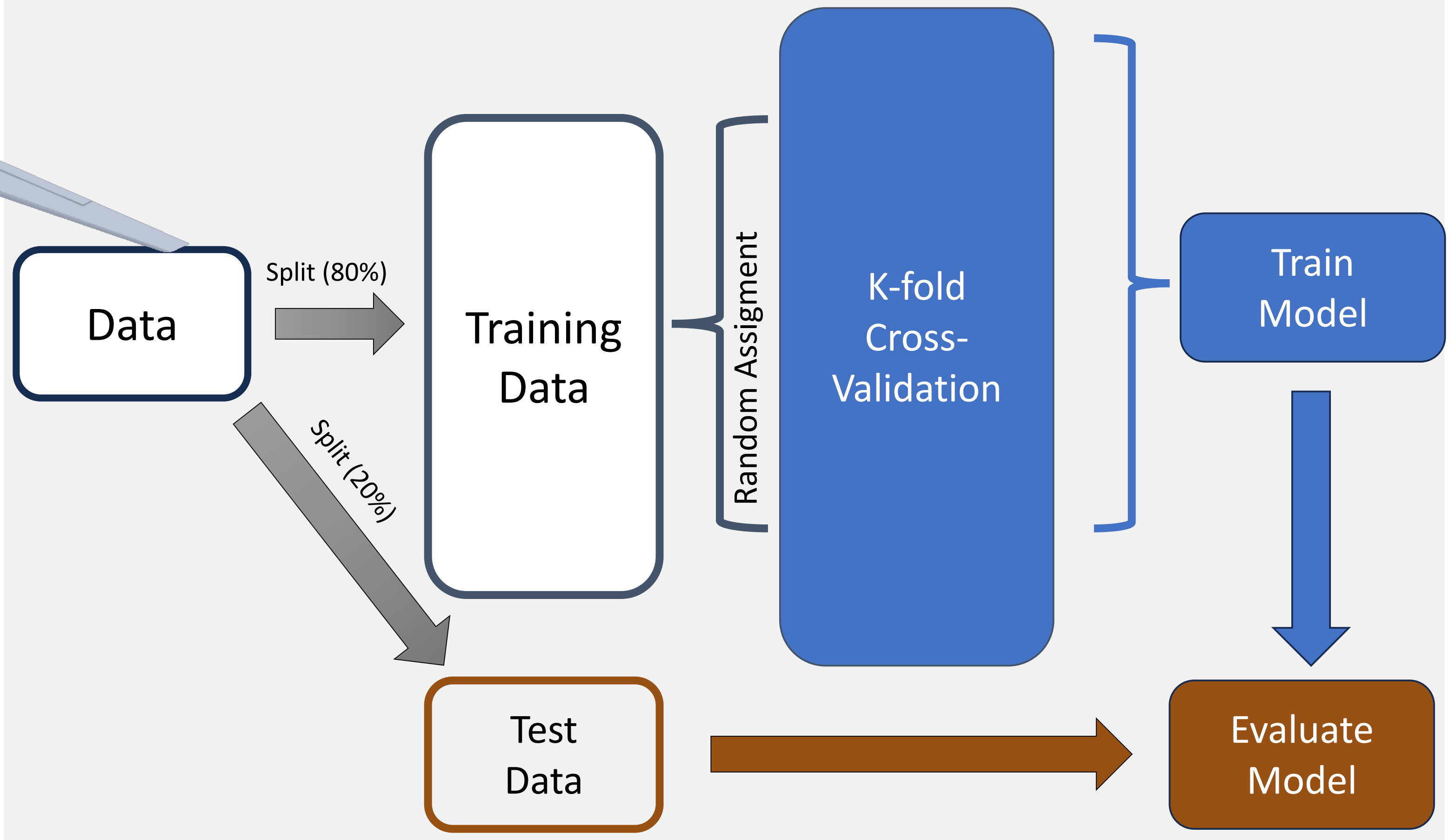


References:

[1] Jean-Paul Yaacoub et.al. (2020), Security analysis of drones systems: Attacks, limitations, and recommendations
[2] Syed Agha Hassnain Mohsan, et.al.(2023), Unmanned aerial vehicles (UAVs): practical aspects, applications, open challenges, security issues, and future trends
[3] https://www.kaggle.com/datasets/luyucwnu/tlmuav-anomaly-detection-datasets
[4] https://ieee-dataport.org/open-access/uav-attack-dataset
[5] Nader Al-lQubaydhi et.al. (2024), Deep learning for unmanned aerial vehicles detection: A review

Methodology

We applied various AI-based models to predict the type of attack a UAV might encounter. To evaluate the accuracy of these models, we used k-fold cross-validation [5]. The models compared include Convolutional Neural Networks (CNN), Support Vector Machines (SVM), K-Nearest Neighbors (KNN), Extreme Gradient Boosting (XGBoost), Random Forest (RF), and Gaussian Naïve Bayes (GNB). The models were implemented using Python libraries such as Scikit-learn and TensorFlow and were run in the Google Colab environment.



Results and Discussion

Testing on different datasets and reporting their accuracy (as seen in Figure 2), F1-socre, precision, and recall (as seen in Table 2).

- The results indicate that the Extreme Gradient Boosting (XCBoost) achieved the highest accuracy of 99.92%, outperforming other models, while CNN followed closely with 98.47% in the TLM Fusion dataset/ However, the Convolutional Neural Networks (CNN) showed perfect performance with 100% accuracy, outperforming other models in UAV GPS attack datasets that includes spoofing and jamming reports. .
- We also observed that unbalanced dataset impacted the model's performance, and using balancing techniques such as SMOTE help in producing accurate predictions that are not baised to a certain label.
- In terms of complexity, XGBoost tends to be more computationally efficient compared to CNN, especially when dealing with tabular data, while CNN requires significantly more processing power and memory due to its layered architecture, making it more suitable for tasks involving complex patterns or visual data.

Conclusion and Future Directions

This study demonstrated the effectiveness of AI-based techniques for UAV attack detection, with XGBoost and CNN models showing strong results across different datasets. Future work will explore real-world data collection, particularly in military and industrial settings, to improve detection capabilities in environments where data volatility and communication disruptions are common. Additionally, we aim to develop an online prediction system that adapts to the dynamic network conditions of UAV systems, ensuring that detection algorithms remain effective even during real-time network changes.