Explainable Agnostic Machine Learning Model for GPS Spoofing Attack Detection in UAV Network

Odinachi U. Nwankwo, Hope L. Nakayiza, Simeon O. Ajakwe, Dong-Seong Kim, Jae Min Lee
Department of IT Convergence, Kumoh National Institute of Technology, Gumi, South Korea
{odinachi, hopeleticia, simeon.ajakwe, dskim, ljmpaul}@kumoh.ac.kr

***Abstract*—The growing reliance on Global Positioning System (GPS) technology for Unmanned Aerial Vehicle (UAV) navigation exposes vulnerabilities to spoofing attacks, which transmit counterfeit signals causing loss of control or mission failure. This paper proposes a Decision Tree-based framework to detect GPS spoofing in real-time. By extracting features from GPS signals and UAV telemetry, the model effectively differentiates between legitimate and malicious signals. Experiment on AV-GPS dataset show high detection accuracy of 93.34%.The results demonstrate decision trees as lightweight tools to enhance UAV security against sophisticated GPS spoofing, supporting safer use in civilian and military contexts.**

***Index Terms*—Cyber-Attack Detection, GPS Spoofing Attacks, Internet of Drones, Unmanned Aerial Vehicles.**

I. INTRODUCTION

The widespread use of drones in military and civilian sectors depends on Global Navigation Satellite Systems (GNSS) like GPS for accurate navigation. However, GPS signals' unencrypted nature makes drones vulnerable to spoofing attacks, where counterfeit signals transmitted via software-defined radios mislead drones into false positions, risking mission failure and asset loss. Notable incidents, such as a U.S. military drone spoofing linked to the Iranian Army, illustrate this threat [1].

UAVs, key elements of the Internet of Drones (IoD) [2], have transformed various fields due to their mobility and autonomy [3], yet their reliance on GPS and wireless communication exposes critical vulnerabilities [4]. GPS spoofing manipulates UAV positioning, causing mission disruption, as depicted in Fig.1, where the UAV is deceived to follow a false path. This vulnerability necessitates machine learning (ML)-based intrusion detection systems (IDS) at ground control stations by training an ML model to detect anomalies [5], namely, simplistic, intermediate, and sophisticated spoofing attacks. This study proposes an explainable decision tree-based IDS for real-time detection of GPS spoofing attacks in an operational UAV environment.

II. SYSTEM METHODOLOGY

The study leverages the GPS spoofing detection dataset [6], consisting of normal, simplistic, intermediate, and sophisticated GPS spoofing attack types. The dataset has 158,170 samples from static and moving vehicles. It includes 13 features such as Satellite ID, Carrier Doppler, Pseudo-range, Receiver Time, Carrier Phase, Early/Late/Prompt Correlator magnitudes, Prompt in-phase/quadrature components. The proposed GPS spoofing detection framework for UAVs follows a structured approach as detailed below.

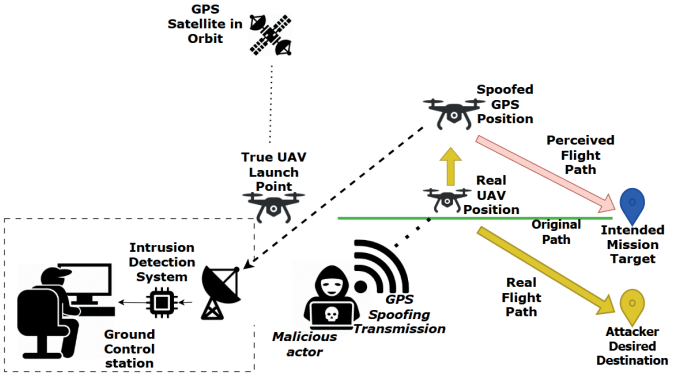

Fig. 1. A GPS spoofing attack architecture targeting UAVs, highlighting the vulnerability of navigation systems and the need for robust IDS mechanisms

A. Dataset Definition

Let the dataset be defined as:

$$\mathcal{D} = \{(X_i, y_i)\}_{i=1}^{N}, \tag{1}$$

where $X_i \in \mathbb{R}^d$ denotes the GPS and telemetry feature vector of dimension d, and $y_i \in \{0, 1, 2, 3\}$ indicates the class label representing spoofing attack types or normal signals.

B. Feature Selection via Pearson Correlation Coefficient

For each feature dimension $X^{(j)}$, compute the Pearson Correlation Coefficient denoted as:

$$P_j = \text{PCC}(X^{(j)}), \tag{2}$$

where P_j measures the linear correlation between the feature $X^{(j)}$ against each of the 13 input features.

Features with correlation magnitude exceeding a threshold τ are selected to form the reduced feature set:

$$X' = \{X^{(j)} \mid |P_j| > \tau\}. \tag{3}$$

C. Data Balancing using SMOTE

To address class imbalance, the Synthetic Minority Oversampling Technique (SMOTE) is applied on the reduced dataset (X', y) to generate synthetic samples for minority classes:

$$\mathcal{D}' = \text{SMOTE}(X', y). \tag{4}$$

D. Train-Test Split

The balanced dataset $\mathcal{D}'$ is split into training and testing subsets, typically with an 80:20 ratio:

$$\mathcal{D}' = \mathcal{D}_{\text{train}} \cup \mathcal{D}_{\text{test}}, \quad |\mathcal{D}_{\text{train}}| = 0.8 \times |\mathcal{D}'|, \quad |\mathcal{D}_{\text{test}}| = 0.2 \times |\mathcal{D}'|. \tag{5}$$

E. Decision Tree Model Training

A Decision Tree classifier $\mathcal{M}$ is initialized and trained on the training dataset $\mathcal{D}_{\text{train}}$:

$$\mathcal{M} = \text{TrainDecisionTree}(\mathcal{D}_{\text{train}}). \tag{6}$$

The system methodology is summarized in Algorithm 1.

Algorithm 1 GPS Spoofing Attack Detection

Require: Dataset $\mathcal{D} = \{(X_i, y_i)\}_{i=1}^{N}$, where X_i are GPS and telemetry features, and $y_i \in \{0, 1, 2, 3\}$
Ensure: Trained model $\mathcal{M}$, predictions $\hat{y}$, accuracy A, and confusion matrix C
procedure SPOOFINGDETECTION($\mathcal{D}$)
Step 1: Feature Selection
Compute PCC on Xi
Select high-correlation features to obtain $X' \subseteq X$
Step 2: Data Balancing
Apply SMOTE on (X', y) to generate $\mathcal{D}'$
Step 3: Train-Test Split
Split $\mathcal{D}'$ into $\mathcal{D}_{\text{train}}$ (80%) and $\mathcal{D}_{\text{test}}$ (20%)
Step 4: Model Training
Initialize Decision Tree classifier $\mathcal{M}$
Train $\mathcal{M}$ on $\mathcal{D}_{\text{train}}$
Step 5: Evaluation
Predict labels $\hat{y} \leftarrow \mathcal{M}(X'_{\text{test}})$
Compute accuracy $A \leftarrow \text{Accuracy}(y_{\text{test}}, \hat{y})$
$C \leftarrow \text{ConfusionMatrix}(y_{\text{test}}, \hat{y})$
return $\mathcal{M}, \hat{y}, A, C$
end procedure

III. PERFORMANCE EVALUATION

The model was evaluated using the GPS Spoofing Detection on Autonomous Vehicles dataset [6], covering four classes: normal, simplistic, intermediate, and sophisticated spoofing attacks. The confusion matrix (Fig. 2) shows strong classification accuracy with high numbers of correct predictions across all classes. The SHAP plot in Fig. 3 shows that features PD and RX have the highest overall impact on model predictions across all four classes.

IV. CONCLUSION AND FUTURE WORK

This study proposed a GPS spoofing detection model to mitigate fake signals misdirecting UAV navigation. A real-time intrusion detection system using a decision tree was integrated into the Ground Control Station to detect and counter these attacks. Results from the confusion matrix show good detection accuracy. Future work aims to explore LIME for explainable AI and also to quantize the trained model.

ACKNOWLEDGEMENT

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the IITP grant funded by the Korea government(MSIT) (IITP-2025-RS-2020-II201612, 33%) and by Priority Research Centers Program through the NRF funded by the MEST(2018R1A6A1A03024003, 33%) and by the MSIT, Korea, under the ITRC support program(IITP-2025-RS-202400438430, 34%)

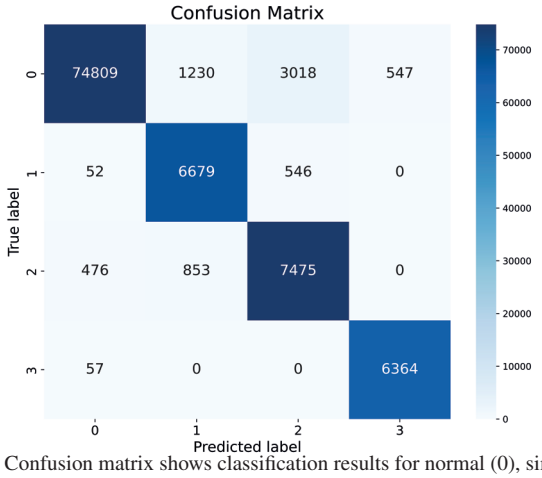

Fig. 2. Confusion matrix shows classification results for normal (0), simplistic (1), intermediate (2), and sophisticated (3) GPS spoofing attacks. It demonstrates a classification model performance with an overall accuracy of 93.34%. The macro-averaged precision, recall, and F1-score are 83.77%, 92.45%, and 87.61%, respectively, indicating strong generalization across all classes.

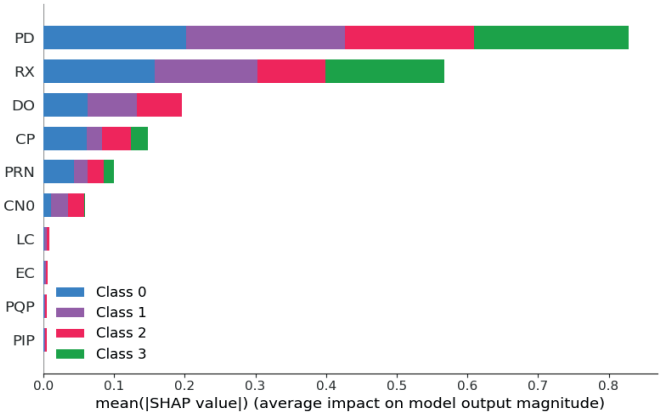

Fig. 3. SHAP summary plot shows top 10 features ranked by their mean absolute SHAP values across a 4-class classification model. Features PD and RX has highest overall influence, with mean SHAP values exceeding 0.8 and 0.5 respectively.

REFERENCES

[1] V. U. Ihekoronye, S. O. Ajakwe, J. M. Lee, and D.-S. Kim, "Droneguard: An explainable and efficient machine learning framework for intrusion detection in drone networks," *IEEE Internet of Things Journal*, vol. 12, no. 7, pp. 7708–7722, 2025.

[2] V. U. Ihekoronye, S. O. Ajakwe, D. Kim, and J. M. Lee, "Hierarchical intrusion detection system for secured military drone network: A perspicacious approach," in *MILCOM 2022 - 2022 IEEE Military Communications Conference (MILCOM)*, 2022, pp. 336–341.

[3] K. A. Tychola, K. Voulgaridis, and T. Lagkas, "Beyond flight: enhancing the internet of drones with blockchain technologies," *Drones*, vol. 8, no. 6, p. 219, 2024.

[4] K.-Y. Tsao, T. Girdler, and V. G. Vassilakis, "A survey of cyber security threats and solutions for uav communications and flying ad-hoc networks," *Ad Hoc Networks*, vol. 133, p. 102894, 2022.

[5] S. O. Ajakwe and D.-S. Kim, "Facets of security and safety problems and paradigms for smart aerial mobility and intelligent logistics," *IET Intelligent Transport Systems*, vol. 18, pp. 2827–2855, 2024.

[6] G. Aissou, S. Benouadah, H. E. ALAMI, and N. Kaabouch, "A dataset for gps spoofing detection on autonomous vehicles," 2022.