Explainable AI–Driven Intrusion Detection System for UAV Networks Against Replay and DoS Attacks

Odinachi U. Nwankwo, Simeon Okechukwu Ajakwe*, Dong-Seong Kim, Jae Min Lee
Department of IT Convergence, Kumoh National Institute of Technology, Gumi, South Korea
*ICT Convergence Research Centre Kumoh National Institute of Technology, Gumi, South Korea
{odinachi, simeon.ajakwe, dskim, ljmpaul}@kumoh.ac.kr

***Abstract*—Unmanned Aerial Vehicles (UAVs) are increasingly deployed in tactical and civilian missions, yet remain vulnerable to stealthy replay and denial-of-service (DoS) attacks. This paper presents a lightweight intrusion detection framework that integrates explainable artificial intelligence (XAI) for UAV network security. Using a cyber-physical UAV dataset and the WSN-DS benchmark, we applied feature pruning, class balancing with SMOTE, and trained Decision Tree and Random Forest classifiers. The proposed system achieved 99.4% accuracy, with near-perfect precision, recall, and F1-scores for replay and DoS detection. To ensure transparency, SHAP and LIME were incorporated for global and local interpretability. Results demonstrate that the framework is highly accurate, interpretable, and suitable for edge deployment in resource-constrained UAV environments.**

***Index Terms*—UAV, Replay Attack, Denial of Service Attack, explainable AI**

I. INTRODUCTION

UAVs (drones) are cyber-physical systems whose safety relies on integrity and timeliness of sensor and control messages exchanged across wireless links. A replay attack captures legitimate packets and re-injects them later, thereby making the system believe stale (but valid) measurements are current, a stealthy attack that can destabilize control loops without requiring the adversary to understand system dynamics. Replay attacks are especially attractive to adversaries because they often do not require breaking cryptography, simply reusing previously captured traffic can be sufficient. Recent literature highlights replay attacks across IoT, industrial control systems, vehicular networks, and UAVs, and proposes detection and mitigation strategies ranging from active watermarking and probing signals to purely data-driven detection [1] [2] [3] [4]. Fig. 1 illustrates the replay attack scenario in UAV networks, establishing the threat context for this study.

In a study conducted in [5], replay attacks were investigated, targeting Semiconductor Equipment Communication Standard/Generic Equipment Model communications to compromise operation-based control systems in industrial environments. A detection mechanism was implemented using a simulated replay attack on Semiconductor Equipment Communication Standard/Generic Equipment Model communication, focusing on identifying and preventing the malicious retransmission of captured and recorded control messages. The research was carried out in the domain of industrial control system cybersecurity, emphasizing the protection of Internet Protocol-based communication in manufacturing and automation processes.The study addressed replay attacks effectively within Semiconductor Equipment Communication Standard-/Generic Equipment Model communication; however, it did not extend its applicability to drone networks, where mobility, wireless communication, and resource constraints introduce distinct vulnerabilities. Furthermore, the work lacked integration of Visual Explainable Artificial Intelligence (VXAI) and Quantitative Explainable Artificial Intelligence (QXAI), thereby limiting transparency and interpretability of the detection mechanism, which are critical for trust and operational validation in safety-critical domains like unmanned aerial vehicle (UAV) networks.

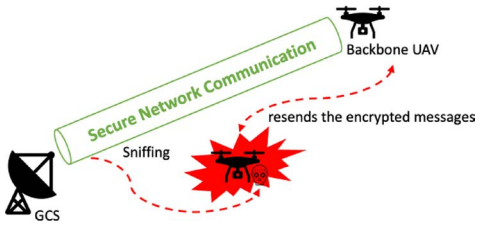

Fig. 1: This figure illustrates a replay attack scenario in UAV networks, where a malicious UAV intercepts and later resends encrypted messages to deceive the Backbone UAV. [2]

In a research conducted in [6], stealthy replay attacks were addressed, which are a form of deception attack in cyber-physical systems (CPS) where previously recorded legitimate data are maliciously re-injected into the system to degrade performance without requiring system knowledge. A data-driven detection approach was employed, utilizing moving window subspace identification to model the system in real time, an output coding strategy to transform replay attacks into detectable additive attacks, and an H-infinity filter to estimate states robustly in the presence of noise and modeling errors. The research was carried out in the domain of cyber-physical systems security, with applications demonstrated on both linear motor and nonlinear robotic systems. The study addressed stealthy replay attacks in CPS but did not consider UAV

TABLE I: Comparative Analysis of Existing Works and Proposed Approach

Work	Focus	Gap	Our Contribution
Al-Shareeda et al. (2022) [5]	Replay attack detection in Industry 4.0 (SECS/GEM).	Not UAV-specific, no XAI integration.	UAV-focused IDS with replay + DoS detection, XAI support.
Zhang et al. (2024) [6],	Data-driven replay attack detection in CPS.	No UAV context, lacks VXAI/QXAI.	UAV-tailored detection with SHAP & LIME for transparency.
Shen & Qin (2024) [7]	Replay + FDI attack detection in power grids.	Not UAV, no explainability.	UAV network IDS with explainable AI and blockchain logging.
Ihekoronye et al. (2022) [8]	IDS for Military UAV networks (DoS, Probe, U2R, R2L).	No replay attack detection, no XAI.	Extends coverage to replay + DoS with XAI interpretability.
Ihekoronye et al. (2025) [9]	DroneGuard: IDS for UAVs (GPS spoofing, DoS) with VXAI.	No replay attack, lacks QXAI.	Covers both replay & DoS; integrates VXAI & QXAI.
Proposed Work	UAV IDS using DT & RF with SHAP+LIME.	Fills gap of replay+DoS detection and explainability.	High-accuracy IDS (99.4%), XAI-based insights, blockchain evidence.

networks and lacked VXAI and QXAI, limiting applicability and interpretability.

In the study [7], replay attacks and false data injection attacks were addressed, both targeting supervisory control and data acquisition systems to disrupt power system operations by falsifying meter measurements. Random matrix theory was employed to detect hybrid attacks on static state estimation, differentiate false data injection attacks from replay attacks, and localize falsified measurements, with a singular value decomposition–convolutional neural network method used for classification and localization. The research was carried out in the domain of power system cybersecurity, with validation conducted on the Institute of Electrical and Electronics Engineers 14-bus system and Institute of Electrical and Electronics Engineers 57-bus system. The study effectively detected replay and false data injection attacks in SCADA-based power systems using random matrix theory and SVD–CNN, but it did not address UAV networks, and lacked VXAI and QXAI integration for interpretability and trust.

The paper "Hierarchical Intrusion Detection System for Secured Military Drone Network: A Perspicacious Approach" presents the design of a hierarchical anomaly-based Intrusion Detection System (IDS) tailored for military Internet of Drones (M-IoD) networks. An optimized Random Forest classifier was developed using Randomized Search Cross-Validation (RSCV) for hyperparameter tuning, ensuring lightweight computation suitable for drones with limited energy and payload capacity. The Pearson Correlation Coefficient (PCC) was applied for feature selection, reducing complexity while maintaining detection accuracy. The proposed IDS was validated with the NSL-KDD dataset, achieving a high F1-score of 96.38%, low mean squared error (0.13), and efficient training time (749 ms), outperforming several state-of-the-art machine learning models in detecting Denial of Service (DoS), Probe, User-to-Root (U2R), and Root-to-Local (R2L) attacks [8]. The IDS showed strong results on NSL-KDD for DoS, Probe, U2R, and R2L attacks, but it was not tested on real UAV data, did not address replay attacks, and lacked VXAI and QXAI for interpretability.

In prior research, a lightweight and explainable intrusion detection framework, DroneGuard, was proposed to enhance the security of drone networks. The framework was designed to mitigate two critical threats, namely Global Positioning System (GPS) spoofing attacks and Denial of Service (DoS) attacks, through the application of supervised machine learning models. To improve the interpretability of the system, Shapley Additive Explanations (SHAP) were incorporated, enabling visualization of feature contributions and fostering transparency and trust in the decision-making process of the model [9]. This study did not address replay attack. Also, it only covered visual explainable artificial intelligence (VXAI) but did not cover quantitative explainable artificial intelligence (QXAI).

This work will include the following contributions:

- An intrusion detection system was developed for UAV networks, capable of effectively detecting replay and denial-of-service (DoS) attacks through Decision Tree and Random Forest classifiers demonstrating strong performance metrics on cyber-physical UAV and WSN-DS datasets.
- Comprehensive explainability and forensic transparency were provided by integrating SHAP and LIME methods for both global and local interpretability, with all detected threats immutably recorded using blockchain technology to ensure traceability and tamper-resistant evidence.
- A performance comparison of classifiers was done using WSN-DS dataset to investigate the best performing classifier of which Random Forest emerged as the best.

The remainder of this paper is organized as follows: Section II describes the proposed methodology, including data preprocessing, feature selection, class balancing, model training, and integration of explainable AI techniques with blockchain-based logging. Section III presents the experimental setup and results, detailing dataset description, model evaluation, and performance comparison. Section IV concludes the paper and outlines directions for future research.

II. Methodology

The proposed UAV Intrusion Detection System (UAV-IDS) follows a modular, sequential workflow to ensure robust detection of replay and denial-of-service (DoS) attacks while

maintaining transparency through explainable AI techniques. The process begins with **data acquisition** from UAV telemetry streams, network taps, and capture files. The dataset—such as the Cyber-Physical Dataset for UAVs & WS-DS—is imported into Google Colaboratory for pre-processing.

Fig. 2 presents the overall workflow of the proposed UAV-IDS, showing the sequential process from dataset acquisition and preprocessing to explainable detection and blockchain logging.

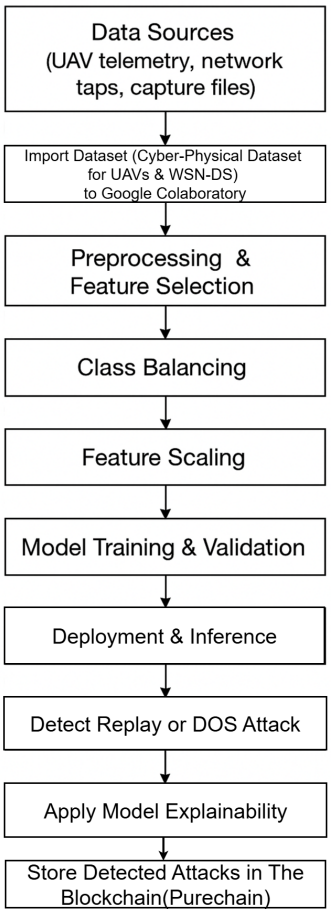

Fig. 2: Workflow of the proposed UAV Intrusion Detection System (UAV-IDS), illustrating the end-to-end process from dataset acquisition, pre-processing to attack detection and secure blockchain-based result storage.

A. Workflow Overview

1) Preprocessing & Feature Selection: Irrelevant identifiers (e.g., MAC addresses, port numbers) are dropped to prevent overfitting. Missing values are handled via imputation or removal. A Pearson correlation matrix is computed, and highly correlated features ($\tau_{\text{corr}} > 95$(threshold)) are pruned to reduce redundancy.
2) Class Balancing: The cleaned dataset is split into training and testing sets using an 80/20 ratio with a fixed random seed (RS). To address imbalance between benign and attack classes, the Synthetic Minority Oversampling Technique (SMOTE) is applied to the training set only.
3) Feature Scaling: A `StandardScaler` is fitted on the balanced training set and applied to both training and testing sets to normalize feature distributions.
4) Model Training & Validation: A tuned Decision Tree Classifier with parameters Θ_{DT} is trained on the scaled dataset. Predictions are made on the test set, and performance is evaluated using accuracy, precision, recall, F1-score, and confusion matrix metrics.
5) Deployment & Inference: The trained pipeline is deployed to an edge gateway or ground station for real-time attack detection. Detected threats are stored securely in the blockchain (Purechain) for forensic integrity.
6) Explainability Module: SHapley Additive exPlanations (SHAP) are used for global and local feature importance visualization, while Locally Interpretable Model-Agnostic Explanations (LIME) can provide lightweight instance-specific explanations.
7) Blockchain Storage of Detected attacks: Detected replay or DoS attack records are immutably stored in the Purechain blockchain, ensuring tamper-proof logging, traceability, and verifiable forensic evidence.

B. Algorithmic Implementation

The complete process is formalized in Algorithm 1, which details the operational sequence from data ingestion to blockchain storage:

DATASET DESCRIPTION

Two benchmark datasets were utilized for validation: the Cyber-Physical UAV Dataset [10], encompassing benign, replay, and DoS attack traffic representative of UAV network environments; and the Wireless Sensor Network Dataset from Kaggle (WSN-DS), including various network attacks such as Flooding, TDMA, Grayhole, and Blackhole. Both datasets underwent extensive preprocessing including removal of redundant identifiers, handling missing values, correlation-based feature pruning, class balancing with SMOTE, and feature standardization, ensuring robust and generalizable model training for UAV-specific and broader network intrusion scenarios.

III. EXPERIMENTAL SETUP AND RESULT

Experiments were conducted using five machine learning classifiers, Decision Tree, Random Forest, Logistic Regression, Gaussian Naïve Bayes, and K-Nearest Neighbors—on a cloud-based platform. The Decision Tree achieved 99.40% accuracy on the UAV dataset with near-perfect F1 scores for replay and DoS attacks. Random Forest demonstrated superior performance on the WSN-DS dataset with F1 scores above 0.99 for most attack types. Explainability tools SHAP and

Algorithm 1: UAV Intrusion Detection System (IDS) with Explainable AI (SHAP & LIME)

Input: D_{raw} (dataset: Cyber-Physical UAV Dataset and WSN-DS), τ_{corr} (correlation threshold), Col_{drop} (columns to drop), RS (random seed), Θ_{DT} (Decision Tree hyperparameters) **Output:** metrics (evaluation results), $\text{SHAP}_{\text{values}}$, LIME_{exp}
$D_{\text{clean}} \leftarrow \text{DropColumns}(D_{\text{raw}}, \text{Col}_{\text{drop}})$ $D_{\text{clean}} \leftarrow \text{HandleMissing}(D_{\text{clean}}, \text{method} = \text{"impute/drop"})$
$\text{Corr}_M \leftarrow \text{ComputeCorrelation}(D_{\text{clean}}[\text{Features}])$
$\text{Features}_{\text{sel}} \leftarrow \text{PruneCorrelated}(\text{Corr}_M, \tau_{\text{corr}})$
$X, y \leftarrow \text{SplitFeaturesLabels}(D_{\text{clean}}, \text{Features}_{\text{sel}}, \text{"class"})$
$X_{\text{train}}, X_{\text{test}}, y_{\text{train}}, y_{\text{test}} \leftarrow \text{TrainTestSplit}(X, y, \text{ratio} = 0.8, rs = RS)$
$X^{\text{res}}_{\text{train}}, y^{\text{res}}_{\text{train}} \leftarrow \text{SMOTE\_Resample}(X_{\text{train}}, y_{\text{train}}, \text{"auto"})$
$\text{scaler} \leftarrow \text{FitScaler}(X^{\text{res}}_{\text{train}})$
$X^{s}_{\text{train}} \leftarrow \text{Transform}(\text{scaler}, X^{\text{res}}_{\text{train}})$
$X^{s}_{\text{test}} \leftarrow \text{Transform}(\text{scaler}, X_{\text{test}})$
$\text{model} \leftarrow \text{TrainModel}(\text{DecisionTree}, X^{s}_{\text{train}}, y^{\text{res}}_{\text{train}}, \Theta_{\text{DT}})$
$y_{\text{pred}} \leftarrow \text{Predict}(\text{model}, X^{s}_{\text{test}})$ $\text{metrics} \leftarrow \text{Evaluate}(y_{\text{test}}, y_{\text{pred}}, \{\text{"Acc"}, \text{"Prec"}, \text{"Rec"}, \text{"F1"}, \text{"CM"}\})$
$\text{SHAP}_{\text{values}} \leftarrow \text{ComputeSHAP}(\text{model}, X^{s}_{\text{train}})$
$\text{LIME}_{\text{exp}} \leftarrow \text{ComputeLIME}(\text{model}, X^{s}_{\text{test}}, i_{\text{sel}})$ **Return** $\{\text{metrics}, \text{SHAP}_{\text{values}}, \text{LIME}_{\text{exp}}\}$ **Save** $\{\text{model}, \text{scaler}, \text{Features}_{\text{sel}}, RS, \text{Col}_{\text{drop}}, \Theta_{\text{DT}}\}$
Store Detected Threats in the blockchain

LIME provided critical insights into feature importance and individual predictions, while blockchain integration enabled tamper-proof logging of detected intrusions, enhancing forensic reliability.

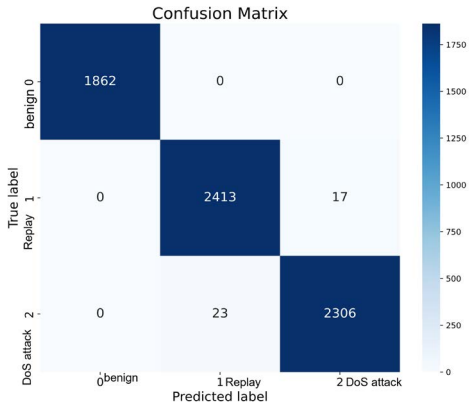

Fig. 3: This confusion matrix shows high classification accuracy of 99.1% and an overall F1-score of 0.991, with minimal misclassifications mainly between Replay and DoS attack classes for Cyber-Physical UAV Dataset .

Experimental evaluation is first demonstrated in Fig. 3 with a confusion matrix achieving 99.1% accuracy and an overall F1-score of 0.991, with only minor misclassifications between Replay and DoS. To enhance interpretability, Fig. 4 and Fig. 5 illustrate Replay and DoS predictions clarified by feature contributions, demonstrating how the model reaches confident decisions. Fig. 7 shows SHAP-based feature importance, where timestamp c dominates across Replay, benign, and DoS classifications.

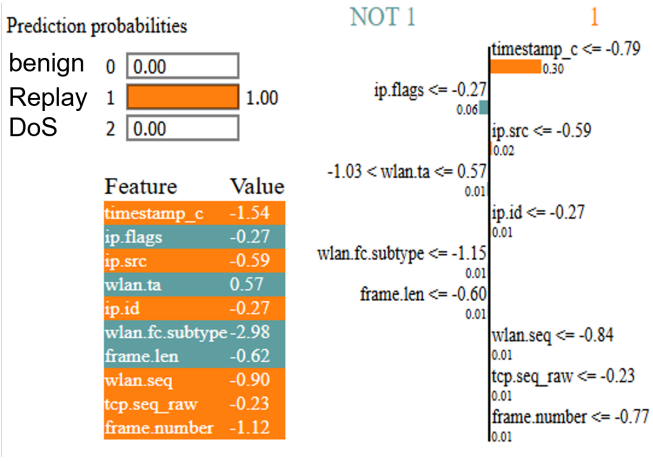

Fig. 4: The model predicts Replay (class 1) with 100% probability, driven mainly by orange features like timestamp_c, ip.src, and wlan.fc.subtype, which outweigh opposing teal features supporting benign for Cyber-Physical UAV Dataset.

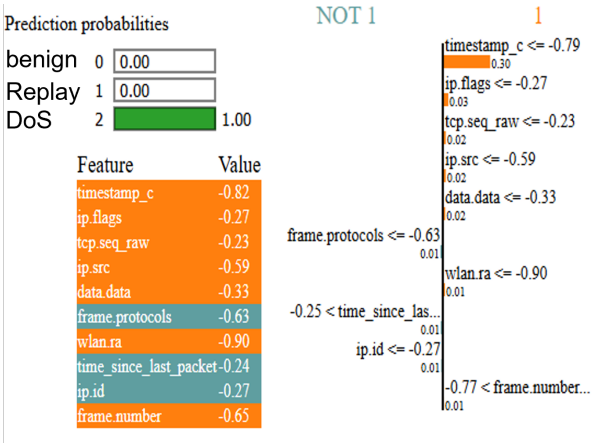

Fig. 5: The LIME plot for Cyber-Physical UAV Dataset shows the model predicted DoS (probability=1.00), with key features like low timestamp_c, ip.src, and wlan.ra (all orange) strongly driving this classification.

For the broader WSN-DS dataset, Fig. 6 provides a confusion matrix confirming strong performance across Normal, Flooding, TDMA, Grayhole, and Blackhole classes, with minimal confusion. Fig. 9 complements this by summarizing global SHAP feature impacts across these classes, emphasizing ADV_S and SCH_S as most influential. Fig. 8 highlights

a case where the model predicts Normal traffic with 100% certainty, reinforcing its reliability in benign recognition.

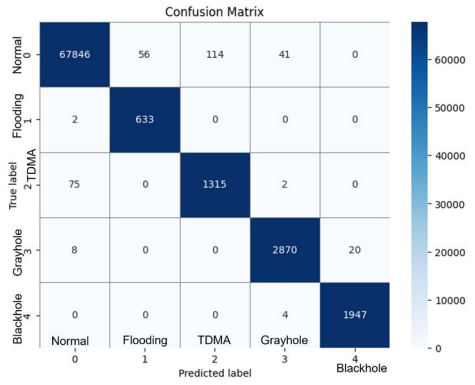

Fig. 6: The confusion matrix for WSN-DS dataset shows high accuracy and strong F1-scores, with most samples correctly classified: 67,846 Normal, 633 Flooding, 1,315 TDMA, 2,870 Grayhole, and 1,947 Blackhole. Misclassifications are minimal, mainly between TDMA–Normal and Grayhole–Blackhole.

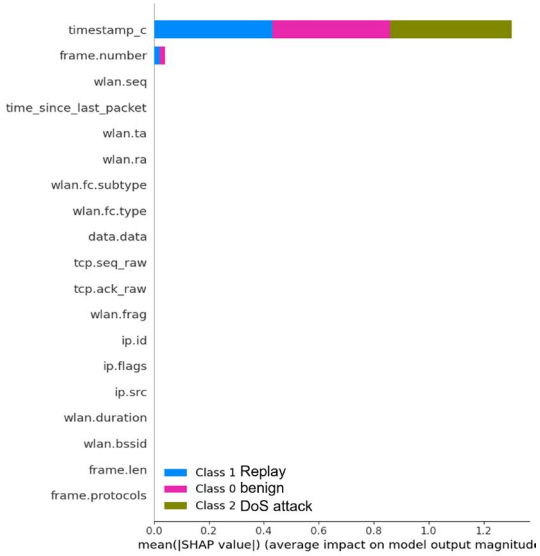

Fig. 7: shows the SHAP-based feature importance per class, highlighting timestamp_c as the most influential feature for Replay, benign, and DoS attack classifications for Cyber-Physical UAV Dataset .

Table III presents a comparative analysis of five machine learning classifiers on the WSN-DS dataset. Results show that Random Forest consistently outperformed other models, achieving the highest precision, recall, and F1-scores across most attack classes, with overall accuracy exceeding 99%. The Decision Tree classifier also demonstrated strong performance but showed reduced effectiveness in minority classes such as TDMA and Grayhole compared to Random Forest. Logistic Regression, Gaussian Naïve Bayes, and K-Nearest

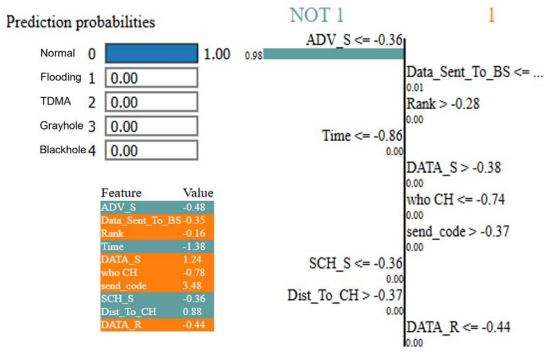

Fig. 8: The model predicts NOT-1 (Normal) on WSN-DS dataset with 100% probability, mainly due to strong opposing evidence from teal-highlighted features (ADV_S, Time, SCH_S, Dist_To_CH).

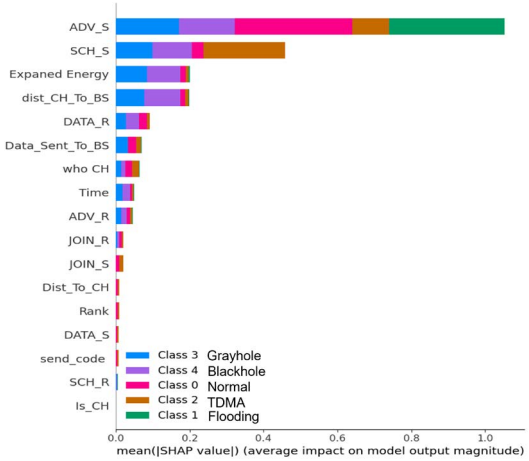

Fig. 9: The SHAP summary plot for WSN-DS dataset shows that ADV_S and SCH_S are the most influential features across all five classes (Normal, Flooding, TDMA, Grayhole, Blackhole).

Neighbors achieved competitive results on certain classes but suffered from either lower overall accuracy or class-specific misclassifications. These findings highlight Random Forest as the most robust and generalizable model for heterogeneous UAV network attack scenarios, while Decision Tree remains a lightweight alternative with competitive performance.

TABLE II: Performance Evaluation with Related Works

Authors	AI model	Replay Attack Accuracy	Dos Attack Accuracy	XAI
[5]	—	—	—	—
[6]	—	$> 95\%$	—	—
[7]	SVD-CNN	$< 100\%$	—	—
[8]	RF	—	99.37	—
[9]	DT	—	99.56%	SHAP
[11]	RF	99.6%	99.5%	—
Ours	DT & RF	99.4%	98.5%	SHAP + LIME

TABLE III: Performance Comparison of based on WSN-DS Dataset

Model	Class	Precision	Recall	F1-Score	Accuracy
Logistic Regression	0	0.9706	0.9697	0.9701	0.9541
	1	1.0000	1.0000	1.0000	1.0000
	2	0.9820	0.9268	0.9536	0.9910
	3	0.5011	0.5961	0.5444	0.9583
	4	0.6347	1.0000	0.7766	0.9974
GaussianNB	0	0.9686	0.9773	0.9729	0.9543
	1	0.9141	0.9953	0.9529	0.9999
	2	0.9894	0.9202	0.9535	0.9895
	3	0.9715	0.9847	0.9781	0.9611
	4	0.9800	0.9893	0.9846	0.9967
KNeighbors	0	0.9967	0.9803	0.9884	0.9706
	1	0.8829	0.9970	0.9364	0.9999
	2	0.9208	0.9443	0.9324	0.9935
	3	0.9836	0.9905	0.9870	0.9613
	4	0.9898	0.9979	0.9938	0.9973
Random Forest	0	0.9988	0.9969	0.9979	0.9542
	1	0.9188	0.9968	0.9561	0.9939
	2	0.9202	0.9447	0.9323	0.9934
	3	0.9839	0.9903	0.9871	0.9612
	4	0.9898	0.9979	0.9938	0.9973
Decision Tree	0	0.9987	0.9920	0.9953	0.9543
	1	0.9301	0.9843	0.9564	0.9935
	2	0.7416	0.9461	0.8306	0.9756
	3	0.9812	0.9876	0.9844	0.9608
	4	0.9883	0.9928	0.9905	0.9969

Finally, Table II compares the proposed framework against related works in replay and DoS attack detection.

Prior studies often focused on either replay or DoS attacks and, in many cases, lacked explainability. For example, Zhang et al. [6] achieved high replay detection accuracy in generic CPS but did not consider UAV networks, while Ihekoronye et al. [7] demonstrated strong DoS detection but without replay attack coverage or XAI integration. Similarly, Shen and Qin [8] addressed replay and false data injection in power grids, yet without applicability to UAVs. In contrast, our system uniquely achieves high detection accuracy for both replay (99.4%) and DoS (98.5%) attacks, while incorporating SHAP and LIME for interpretability. This dual focus on accuracy and explainability establishes the novelty and practical value of our approach in UAV network security. Unlike prior works that addressed either Replay or DoS and often lacked explainable AI, our approach uniquely covers Replay, DoS, and integrates XAI in the UAV domain for transparent and reliable UAV decision-making in mission-critical environments.

IV. Conclusion and Future Work

This paper proposed a lightweight and explainable intrusion detection system (IDS) tailored for UAV networks, focusing on detecting replay and denial-of-service (DoS) attacks. By combining feature-optimized preprocessing, Decision Tree and Random Forest classifiers, and explainability methods (SHAP and LIME), the system achieved near-perfect accuracy on both UAV-specific and WSN-DS datasets. Unlike prior works that addressed either replay or DoS attacks without transparency, our framework integrates high detection accuracy with interpretability, making it suitable for deployment in resource-constrained UAV environments. Future research will extend this work by validating the IDS on real UAV testbeds, exploring adaptive learning for evolving threats, and integrating cooperative detection across drone swarms for enhanced resilience.

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-2024-00438430, 34%).

References

[1] S. O. Ajakwe and D.-S. Kim, "Time sensitive anti-infoswarm agnostic intelligence for safe uav communication," in *2024 15th International Conference on Information and Communication Technology Convergence (ICTC)*, 2024, pp. 1614–1619.

[2] 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. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1570870522000853

[3] 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.

[4] G. C. Amaizu, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Investigating network intrusion detection datasets using machine learning," in *2020 International Conference on Information and Communication Technology Convergence (ICTC)*, 2020, pp. 1325–1328.

[5] M. A. Al-Shareeda, S. Manickam, S. A. Laghari, and A. Jaisan, "Replay-attack detection and prevention mechanism in industry 4.0 landscape for secure secs/gem communications," *Sustainability*, vol. 14, no. 23, 2022. [Online]. Available: https://www.mdpi.com/2071-1050/14/23/15900

[6] Z. Zhang, M. Li, and L. Xie, "Data-driven replay attack detection for unknown cyber-physical systems," *Information Sciences*, vol. 670, p. 120562, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0020025524004754

[7] Y. Shen and Z. Qin, "Detection, differentiation and localization of replay attack and false data injection attack based on random matrix," *Scientific Reports*, vol. 14, no. 1, p. 2758, 2024.

[8] 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.

[9] 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.

[10] S. Hassler, U. Mughal, and M. Ismail, "Cyber-physical dataset for uavs under normal operations and cyber-attacks," 2023. [Online]. Available: https://dx.doi.org/10.21227/6f22-py65

[11] S. O. Ajakwe, K. L. Olabisi, and D.-S. Kim, "X-cid: Exhaustive ensemble technique for cyber invasion detection in drone transportation network," in *2024 IEEE 5th International Conference on Electro-Computing Technologies for Humanity (NIGERCON)*. IEEE, 2024, pp. 1–5.