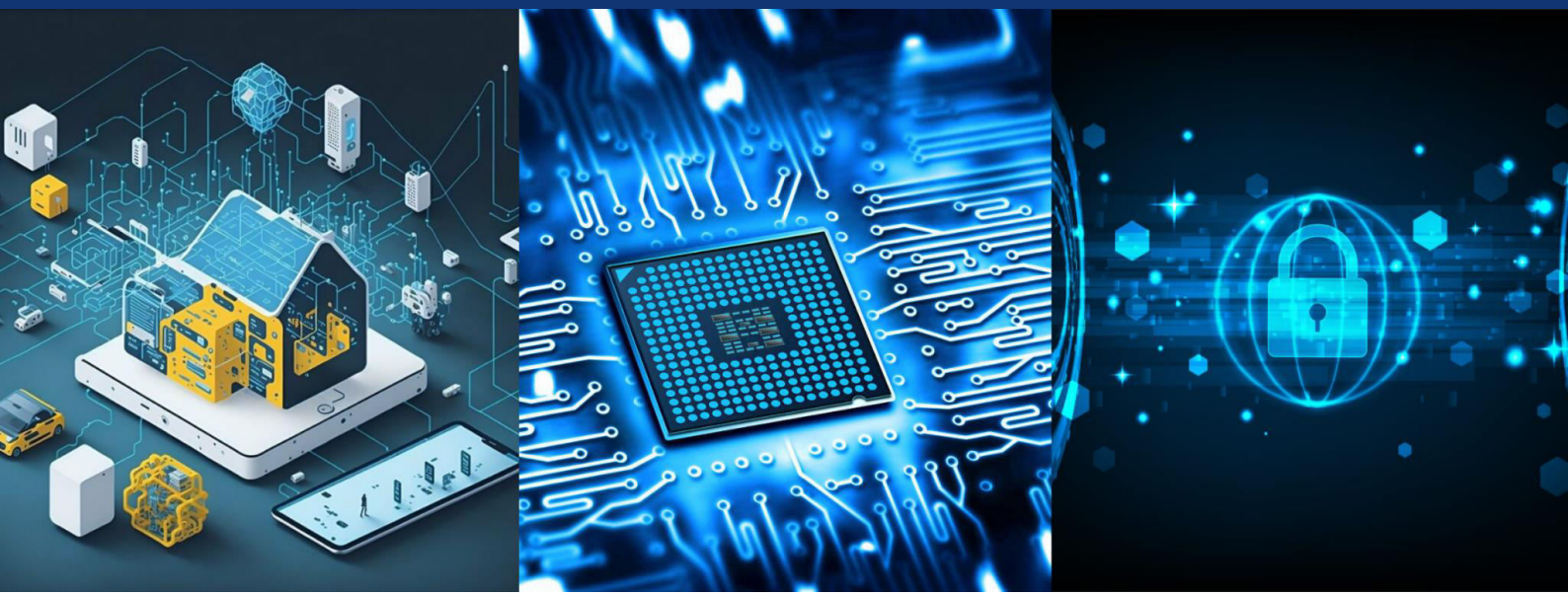
IJIRCCE

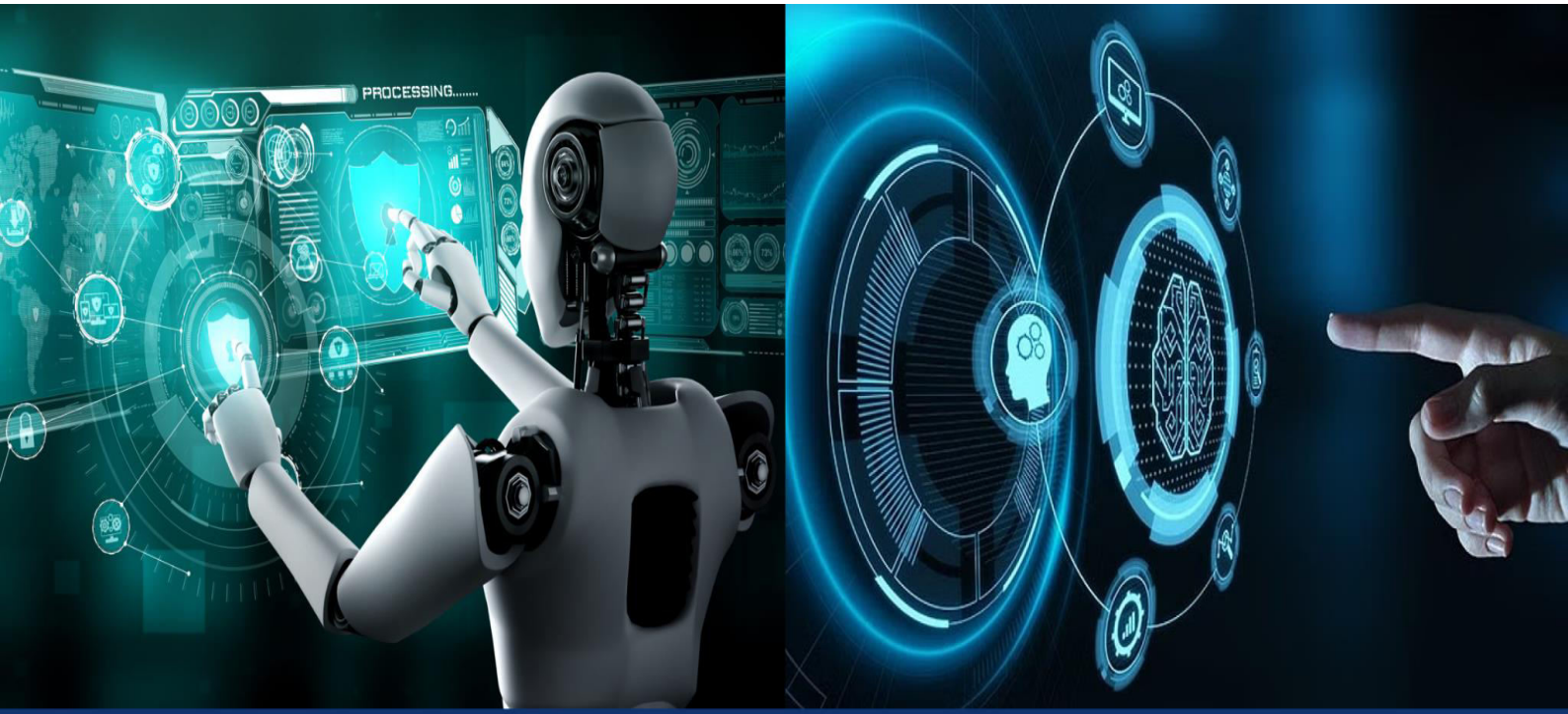
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 13, Issue 4, April 2025

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI:10.15680/IJIRCCE.2025.1304236

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Intrusion Detection and Recovery System for Drone Signals: A Review

Sagar R, Chiranth Gowda C, Ajith D Huggi, Chiranth B R, Kiran Kumar A

School of CSE, REVA University, Bengaluru, India

ABSTRACT: "Unmanned Aerial Vehicles (UAVs) are widely used in various industries; therefore, they are prone to cyber and physical intrusions. In this study, we propose an extensive LSTM-based Intrusion Detection and Recovery System for UAV networks. We classified six classes of operations, that is, different attacks and normal activities, using the WSN-DS dataset. The model provides very high accuracy and utilizes SHAP (SHapley Additive ex Planations) to enable explainable insight into feature importance for transparency in decision-making. An interactive dashboard using Gradio incorporates real-time prediction, recovery animations, defense suggestions, and geo-visualization using folium maps. This framework not only identifies intrusions with good performance but also provides effective guidance for recovery and prevention approaches. The proposed framework proves the viability of combining deep learning with explainability for safe UAV operations."

KEYWORDS: Intrusion Detection System, ITS: Intelligent Transportation System, LSTM: Long short term memory model, SHAP: Shapley additive ex Plantations, Explainable AI, UAV: Unmaned ***aerial vehicles***

I. INTRODUCTION

Unmanned Aerial Vehicles (UAVs), also referred to commonly as drones, are quickly changing different fields including agriculture, disaster management, military surveillance, logistics, and environmental monitoring. Their ability to operate autonomously, gather data in real-time, and communicate remotely has made them an integral part of contemporary intelligent systems. Nonetheless, the heightened dependence on wireless communication protocols and networked control systems has exposed UAVs to a wide range of security vulnerabilities. These weaknesses render drones desirable targets for cyber and physical attacks that can undermine their mission, manipulate data, or even lead to complete system failure. With the high-stakes applications where drones are used, protecting them from such threats is not only an upgrade but a requirement.

UAVs function in extremely dynamic and resource-limited environments. They tend to be deployed in ad-hoc WSNs or operate based on peer-to-peer communication in sparse or no infrastructure regions. Legacy IDS, based on static rule sets or thresholds defined by a human, are frequently not effective to deal with the changing nature of attack vectors and the temporal nature of adversary activities in these regions. Further, drones produce time-series data, and successful intrusion detection requires models that can be trained to find temporal dependencies as well as sense even minor fluctuations from normal traffic. Thus, there is a critical need for intelligent, adaptive, and efficient IDS solutions especially designed for the UAV ecosystem.

In this paper, we introduce an effective and interpretable Intrusion Detection and Recovery System (IDRS) founded on Long Short-Term Memory (LSTM) networks, a type of Recurrent Neural Networks (RNNs) especially designed for sequential data analysis. The model is trained on the WSN-DS dataset — a thorough database of sensor network information containing normal operations and diverse kinds of attacks like sinkhole, Sybil, flooding, and blackhole. Through learning temporal patterns, the LSTM model can identify both sudden and progressive anomalies with very high accuracy. We also classify attack types into six categories, with a general 'Cyber Intrusion' class to allow for attacks that are not explicitly categorized in the dataset, making it possible to have broad and flexible classification.

II. LITERATURE SURVEY

The surge of Unmanned Aerial Vehicles (UAVs) across different fields has increased the demand for effective security measures. Conventional Intrusion Detection Systems (IDS) tend to be inadequate in response to the dynamic and resource-limited nature of UAV networks. To fill this gap, researchers turned to sophisticated machine learning methods, especially Long Short-Term Memory (LSTM) networks and explainable AI techniques.

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI:10.15680/IJIRCCE.2025.1304236

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

1. LSTM-Based Intrusion Detection: Gwon et al. [1] proposed a network intrusion detection model utilizing LSTM networks and feature embedding techniques. Their model successfully extracted sequential patterns in network traffic with 99.72% binary classification accuracy on the UNSW-NB15 dataset. This research highlighted the efficacy of LSTM networks in modeling temporal dependencies inherent in network data.

Along similar lines, one research work found in the Egyptian Informatics Journal [2] introduced an LSTM-RNN IDS designed specifically for drone networks. Considering the inherent communication patterns and vulnerabilities of UAVs, authors created a model that improved the detection against drone-specific network anomaly patterns.

2. Federated Learning and Multi-Dataset Analysis: Solving privacy issues and heterogeneity of data, a research in PeerJ Computer Science [3] investigated the application of federated learning with LSTM models for intrusion detection in wireless sensor networks based on IoT. Using datasets such as WSN-DS, CIC-IDS-2017, and UNSW-NB15, the framework provided an accuracy of 97.52% on the WSN-DS dataset, proving its effectiveness across varied network scenarios.

3. Explainable AI in Intrusion Detection: The black-box nature of deep learning models is a challenge in critical use cases such as intrusion detection. To provide additional transparency, Younisse et al. [4] used Shapley Additive Explanations (SHAP) to explain decisions made by convolutional neural networks in IDS. Their process gave insight into feature contributions, which will help in better understanding and trusting model predictions.

Building upon explainability, Hong and Yoo [5] proposed a heterogeneous ensemble model for multiple intrusion detection in UAVs' Controller Area Networks (CAN). By incorporating SHAP values, not only did they enhance detection accuracy but also provided interpretable explanations for every prediction, closing the gap between performance and transparency.

4. Adversarial Learning and Explainability: Fidel et al. [6] solved the problem of deep neural network adversarial attacks by proposing a detection technique relying on SHAP signatures. It calculated SHAP values for internal classifier layers to separate normal and adversarial inputs and improve the robustness of IDS against advanced attack vectors.

III. DATASET AND PREPROCESSING

Here, we make use of the WSN-DS (Wireless Sensor Network - Data Set), an open-source dataset used to mimic a variety of attacks and regular operation in wireless sensor networks. The dataset includes a range of features that describe the behavior of nodes in varying network conditions and attack situations. Important attributes consist of parameters such as energy usage, hop count, packet send ratio, signal strength, and so forth.

The dataset itself has missing values and noisy labels. We carry out preprocessing in several steps to get it model-ready. In the first place, all column names are cleared of any surplus whitespace, and rows with missing values are eliminated to keep data consistent. The Attack type column, being the label, is encoded with LabelEncoder. Attack types are then classified into six top-level categories: Normal Operation, Sinkhole, Sybil, Flooding, Blackhole, and an overarching Cyber Intrusion class for any other attack type.

All the features are scaled with MinMaxScaler to normalize their range between 0 and 1, which is an important step for the stable training of LSTM. The input feature set is reshaped into a 3D tensor format appropriate for sequential models such as LSTM. The dataset is finally split into training and testing sets in an 80:20 ratio using train_test_split, and during model training, an additional validation split is added.

This preprocessing chain guarantees that the model is getting clean, normalized, and sequentially formatted data, hence enhancing its capability to learn and generalize across different types of intrusion in wireless sensor network settings.

IV. PROPOSED METHODOLOGY

The main goal of this research is to create an interpretable and intelligent system that can identify and react to intrusions in drone communications based on wireless sensor network (WSN) telemetry data. The process takes place in various stages, ranging from data preprocessing to model architecture, explainability through SHAP, visualization modules, and a responsive cyber-defense interface.

1. The WSN-DS dataset is initially cleaned and prepared. Column names are cleaned of any trailing whitespaces, and rows with missing values are dropped to maintain consistency. The target column, Attack type, is label encoded and

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI:10.15680/IJIRCCE.2025.1304236

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

then mapped to six categories: Normal Operation, Sinkhole, Sybil, Flooding, Blackhole, and Cyber Intrusion (catch-all for all other attack types). All features are normalized to the range [0, 1] with MinMaxScaler. This is an important step towards ensuring stable and effective training of the LSTM model. The data is reshaped into a 3D tensor of dimensions (samples, timesteps, features) where one sample is one timestep with several features, hence appropriate for sequential learning. The dataset is split between training and test sets with an 80:20 ratio.

2. A Long Short-Term Memory (LSTM) neural network is selected to model because of its capacity for handling temporal relations in time-series data. The model structure involves an LSTM layer of 64 units followed by a dense layer of 32 ReLU-activated neurons and a final softmax output layer containing six neurons matching the six classes of intrusion. The model is built with the Adam optimizer and trained on sparse categorical cross-entropy loss, with training accuracy and validation accuracy monitored across epochs. This design enables the system to learn patterns in node behavior that map to normal and anomalous activity.

3. To increase transparency, SHapley Additive exPlanations (SHAP) is incorporated to explain model predictions. As LSTM models accept 3D inputs, the data is flattened prior to being sent to the SHAP explainer. The SHAP system calculates feature-wise contributions to every prediction, assisting in determining which sensor features most impact the detection of particular attack types. Feature importance is represented through bar charts of mean absolute SHAP values, providing interpretable information regarding model behavior and feature sensitivity.

4. For ease of interaction and deployment, a dashboard is created using Gradio. The user interface enables real-time prediction of the type of intrusion given user-input telemetry values. The system further visualizes model accuracy over time, SHAP feature importances, a recovery animation that is intrusion-specific to the detected intrusion, and a map of affected drones. Additionally, it stores recent history of predictions along with timestamps.

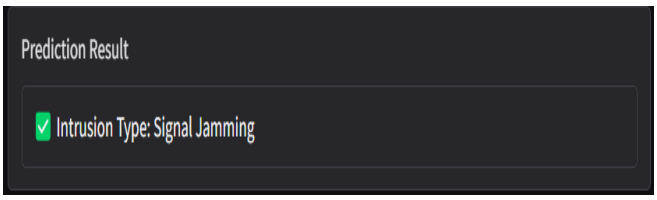
5. Upon sensing an intrusion, the system will automatically propose cyber-defense methods related to the sensed intrusion. For instance, for a GPS spoofing attack, the system will advise going over to multi-sensor GPS verification, while for signal jamming, frequency hopping is proposed. Every prediction is subsequently followed by an animated recovery simulation, providing a visual indication for the intruder type and severity of intrusion.

This end-to-end pipeline — from preprocessing to interpretable AI and real-time defense recommendations — becomes a strong and deployable platform for drone network intrusion detection and mitigation.

V. EXPLAINABILITY WITH SHAFT

Where high stakes are involved, such as drone surveillance and wireless sensor network security, model explainability is crucial for building confidence, authentication, and actionable knowledge. Our solution includes SHapley Additive exPlanations (SHAP) to provide an attempt at explanation, a game-theory-based method that gives the contribution of each input feature to the predictions of the model.

Since LSTM models process 3D input tensors corresponding to time sequences, extra caution is exercised in making



SHAP compatible. The input data is reshaped from its native shape (samples, timesteps, features) to a 2D array so that SHAP's kernel-based explainer can be utilized. A custom masker function dynamically reshapes the input during explanation so that SHAP's masking does not violate the LSTM model's assumptions.

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI:10.15680/IJIRCCE.2025.1304236

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

SHAP values are then computed over a representative subset of the training data. These values reveal how each feature – whether signal strength, hop count, or energy metrics – impacts the model's choice toward a specific intrusion class. The outcomes are combined and plotted as mean absolute SHAP values, which enable globally relevant features that contribute to the detection of intrusions to be identified.

This level of explainability provides two primary benefits:

- Model Transparency: Operators and security experts can ensure that the model is making logically correct and predictable decisions based on the inputs.
- Feature Insight: Knowing what features have the largest impact can inform future data gathering priorities and sensor deployments within drone-based networks.

In summary, adding SHAP adds an extra layer of interpretability to our LSTM model, which enables stakeholders to learn more about both prediction dynamics and system vulnerabilities.

VI. EXPERIMENTAL RESULTS

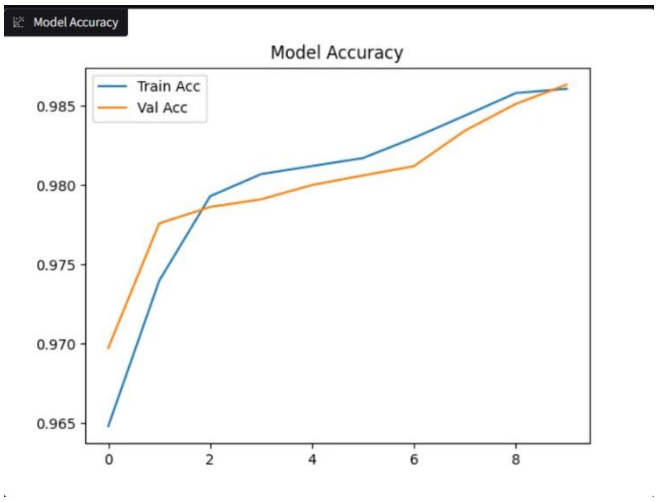
In order to compare the performance of the suggested LSTM-based intrusion detection system, the model was subjected to a hold-out test set of 20% of the dataset. The system's final test accuracy and test loss were **98.69%** and **0.0340**, respectively, showcasing its strong reliability in the proper identification of various types of intrusions made by drones.

The training was carried out for 10 epochs at a batch size of 32, with both the training and validation accuracy increasing continuously with very little overfitting. This is a high accuracy that reflects the model's ability to learn temporal patterns in sensor readings that are associated with certain attack behaviors.

Additionally, the inclusion of SHAP enabled post hoc validation of model choices, ensuring that significant features like RSSI, Hop Count, and Remaining Energy had substantial impact on classification results.

These findings validate the robustness of the model and its viability for use in real-time drone security surveillance systems.

Below images shows the result generated and visualized using gradio:

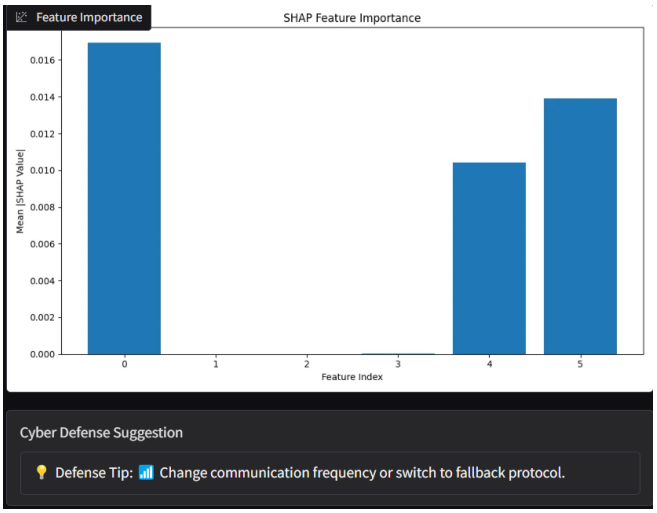


© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI:10.15680/IJIRCCE.2025.1304236

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Val acc refers to how well the trained model performs on the validation set.

VII. FUTURE IMPLEMENTS AND IMPROVEMENTS

The existing model is centered on developing a strong and interpretable intrusion detection model for generic drone signal patterns via LSTM networks. Drones operating in real-world scenarios, though, vary tremendously depending on their application scenarios — e.g., commercial delivery drones, agricultural UAVs, or military surveillance drones. Each category of drone has distinct communication habits, energy consumption patterns, and operational procedures. Thus, an all-purpose intrusion detection model would not be ideal. As a future extension, individual detection systems for each drone type will be created, enabling more accurate threat detection by learning particular flight and communication patterns.

To enable this extension, drone-specific datasets must be gathered and annotated, reflecting normal and abnormal behaviors under different mission conditions. Feature engineering for every drone type will be enriched by incorporating parameters like flight altitude, payload weight, and navigation routines. Models will be fine-tuned and retrained for every drone profile to achieve maximum detection accuracy and reduce false positives. This modular design will allow specialized defenses for every category of drone while still having a common framework and architecture.

On the implementation side, the suggested software-based intrusion detection system will be migrated to embedded hardware platforms for real-time intrusion response. Future hardware integration will be in the form of deploying trained models onto lightweight yet high-performance edge computing boards like NVIDIA Jetson Nano or Raspberry Pi with AI accelerators. Such boards will receive real-time drone telemetry, identify intrusions, and initiate defensive responses onboard, providing quick reaction times and negligible dependency on ground control systems.

In addition, field testing in actual real-world adversarial environments will be conducted to confirm system robustness. Feedback from these deployments will inform further enhancements, such as improved SHAP-based explainability modules optimized for onboard diagnostics and operator notifications. Ultimately, the goal is to mature this framework into a full-stack, cross-platform drone security suite that is adaptive, smart, and able to perform autonomous self-defense in increasingly hostile airspace environments.

VIII. CONCLUSION

In this paper, we introduced and developed an intrusion detection and recovery system in drone communication with a deep learning-based approach for utilizing Long Short-Term Memory (LSTM) networks. We trained and validated the model using the WSN-DS dataset with an accuracy of 98.69% on testing, successfully detecting several types of

intrusions including Sybil, Sinkhole, Flooding, Blackhole, and Cyber-attacks. The incorporation of explainability via SHAP (SHapley Additive exPlanations) adds transparency and interpretability to the model's decision-making, providing a consistent defense mechanism with insights into key features affecting intrusion prediction.

The system was also extended with a graphical dashboard based on Gradio, offering real-time intrusion categorization, recovery visualization, cyber defense recommendations, and geographical mapping. This kind of interactive interface not only makes the solution intelligent but also easy to use for drone pilots and analysts. By detecting autonomously and triggering guided recovery measures, the solution guarantees low downtime and improves the robustness of UAV systems against malicious attacks.

This work adds a critical step toward self-sustaining drone security, providing a software-defined system that can detect anomalies in real time and make explainable decisions. Future development will involve applying this system to multiple types of drones and integrating it into hardware for edge computing-based operation, thus creating a fully end-to-end intelligent and reactive drone security solution.

REFERENCES

[1] Gwon, H., Lee, C., Keum, R., & Choi, H. (2019). Network Intrusion Detection based on LSTM and Feature Embedding. arXiv preprint arXiv:1911.11552.
[2] Improving intrusion detection using LSTM-RNN to protect drones' networks. (2024). Egyptian Informatics Journal. https://doi.org/10.1016/j.eij.2024.100501.
[3] Federated learning with LSTM for intrusion detection in IoT-based wireless sensor networks: a multi-dataset analysis. (2023). PeerJ Computer Science. https://peerj.com/articles/cs-2751/
[4] Younisse, R., Ahmad, A., & Abu Al-Haija, Q. (2022). Explaining Intrusion Detection-Based Convolutional Neural Networks Using Shapley Additive Explanations (SHAP). Big Data and Cognitive Computing, 6(4), 126. https://doi.org/10.3390/bdcc6040126
[5] Hong, Y.-W., & Yoo, D.-Y. (2024). Multiple Intrusion Detection Using Shapley Additive Explanations and a Heterogeneous Ensemble Model in an Unmanned Aerial Vehicle's Controller Area Network. Applied Sciences, 14(13), 5487. https://doi.org/10.3390/app14135487
[6] Fidel, G., Bitton, R., & Shabtai, A. (2019). When Explainability Meets Adversarial Learning: Detecting Adversarial Examples using SHAP Signatures. arXiv preprint arXiv:1909.03418.
[7] Abdulrahman Alzahrani. Novel Approach for Intrusion Detection Attacks on Small Drones Using ConvLSTM Model.
[8] Vanlalruata Hnamte, Hong Nhung-Nguyen, Jamal Hussain, Yong Hwa-Kim (2023). A Novel Two-Stage Deep Learning Model for Netowrk Intrusion Detection: LSTM.
[9] Umair Ahmad Mughal, Samuel Chase Hassler, Muhammad Ismail. Machine Learning-Based Intrusion Detection for Swarm of Unmanned Aerial Vehicles.
[10] Wasim Ahmad, Mohammed Almaiah, Aitizaz Ali. (2024). Deep Learning Based Network intrusion detection for unmanned aerial vehicle (UAV).
[11] Mudunuri, L. N. R., & Attaluri, V. (2025). Urban Development Challenges and the Role of Cloud AI-Powered Blue-Green Solutions. In Integrating Blue-Green Infrastructure Into Urban Development (pp. 507-522). IGI Global Scientific Publishing.
[12] Vivian Ukamaka Ihekoronye, Simeon Okechukwu Ajakwe, Jae Min Lee, Dong-Seong Kim. (2025). Drone guard: An explainable and efficient machine learning framework for intrusion detection in drone networks.
[13] Young-Woo Hong, Dong-Young Yoo. (2024). Multiple Intrusion Detection Using Shapley Additive Explanations and a Heterogeneous Ensemble Model in an Unmanned Aerial Vehicle's Controller Area Network

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details