THE JOURNAL OF APPLIED ENGINEERING AND TECHNOLOGIES
2026 Vol. 1, No. 3, ISSN (O): 3154-7877

Adaptive Threat Recognition in UAV Swarm Communication Using Collaborative Pattern Learning

Jean Moreau[1], Antoine Laurent[1*]
[1]Department of Computer Science, Institut Polytechnique de Paris, 91120 Palaiseau, France
Corresponding Author*: Antoine Laurent E-mail: antoine.laurent@placeholder.edu

ARTICLE INFO

Keywords
UAV swarm security
network anomaly detection
explainable AI
SHAP
ensemble learning
wireless communication security
intrusion detection

Published:
01 September 2026

ABSTRACT

UAV swarm networks depend on reliable communication among multiple aerial nodes, ground stations, and mission-control systems. However, the high mobility and dynamic topology of UAV swarms make them vulnerable to abnormal traffic caused by jamming, spoofing, flooding, route manipulation, and compromised nodes. This study proposes a SHAP-based ensemble anomaly detection framework for secure communication in UAV swarm networks. The framework combines CatBoost, Random Forest, and AdaBoost classifiers through an adaptive voting strategy to improve robustness under unstable wireless communication conditions. SHAP values are used to identify the most important traffic and topology features behind each anomaly classification. A UAV swarm communication dataset is generated using 60 UAV nodes and 6 ground-control nodes under simulated surveillance and delivery missions, producing 1.58 million labeled traffic records. The dataset includes normal communication, flooding attacks, GPS spoofing-related traffic changes, route disruption, and malicious command injection. After feature extraction, 43 features are retained, including packet loss ratio, route change frequency, control message interval, flow duration, retransmission count, signal-related delay variation, and source-destination traffic imbalance. The proposed model achieves 97.47% accuracy, 96.63% macro-F1, and 98.09% AUC across five traffic classes. Compared with standalone CatBoost and SVM models, the proposed ensemble improves macro-F1 by 1.94% and 5.21%, respectively. SHAP interpretation shows that route change frequency, abnormal control message intervals, retransmission spikes, and sudden traffic concentration are the most important indicators of compromised UAV communication. The results demonstrate that explainable ensemble learning can provide transparent and effective anomaly detection for UAV swarm network security.

1. Introduction

UAV swarm networks have become an important communication paradigm in surveillance, delivery, emergency response, disaster monitoring, border patrol, and smart-city services. Unlike single-UAV systems, UAV swarms depend on frequent coordination among multiple UAV nodes, ground-control stations, and mission-control systems. These communication links support task allocation, route adjustment, status reporting, formation control, and real-time mission feedback (Ramos et al., 2025; Yin et al., 2026). However, the high mobility of UAV nodes, open wireless channels, limited onboard resources, and rapidly changing network topology also expose swarm

Citation: Moreau, J., & Laurent, A. (2026). Adaptive threat recognition in UAV swarm communication using collaborative pattern learning. *The Journal of Applied Engineering and Technologies*, 1(3), 53-60.

https://doi.org/10.64744/tjaet.2026.285.

networks to serious cybersecurity risks. Jamming, GPS spoofing, flooding, route disruption, replay attacks, and malicious command injection may interrupt mission execution, mislead navigation decisions, or cause loss of control over swarm behavior (Meheretu et al., 2025; Yang, 2026). In addition, policy-driven vulnerability risk quantification in large-scale data-security infrastructures provides useful reference for risk-aware security assessment in UAV swarm environments, especially when communication, control, and mission data are distributed across edge, cloud, and command platforms (Shao, 2026).

Recent studies have applied machine learning and deep learning methods to UAV intrusion detection. Compared with fixed rule-based methods, data-driven models can better identify abnormal traffic patterns when sufficient labeled data are available (Deng & Yang, 2026; Rathi et al., 2025). They can learn complex relationships among packet transmission, routing behavior, command intervals, retransmission patterns, and source-destination communication changes (Dangore & Sah, 2025; Zhang, 2026). However, UAV swarm intrusion detection still faces several limitations. Many existing datasets are small, closed, or generated under simplified traffic settings (Dolatyabi et al., 2025; G. Gao, R. Gao, C. Lu, et al., 2026). Some experiments involve only a few UAV nodes and limited attack types, which makes it difficult to reflect the communication uncertainty and topology changes of real swarm missions (Alqudsi & Makaraci, 2025; Zhang et al., 2026). As a result, models trained on such datasets may show high accuracy in controlled experiments but may not generalize well to dynamic swarm-level communication scenarios (Bodycomb & Anaissi, 2026; Qi & Qiao, 2026). Another important limitation is the lack of interpretability. Many UAV security models mainly report accuracy, precision, recall, or F1-score, but provide limited explanation of why a traffic flow is classified as abnormal (Khanpour et al., 2025; Su & Wu, 2026). This is problematic in real UAV missions because operators need more than a binary alarm. They need to know whether an anomaly is related to route changes, abnormal command intervals, retransmission spikes, packet loss, delay variation, source-destination traffic concentration, or sudden changes in control messages (Ieropoulos et al., 2026; Li & Liu, 2026). Without interpretable evidence, it is difficult to verify alarms, distinguish cyberattacks from unstable wireless conditions, and make timely operational decisions (Almheiri et al., 2025; Xu et al., 2026). Therefore, UAV swarm anomaly detection requires not only high detection performance, but also feature-level explanation that can support mission-aware security analysis (Huang, 2026; Mohamed et al., 2026).

To address these issues, this study proposes a SHAP-based ensemble anomaly detection framework for secure communication in UAV swarm networks. The framework integrates CatBoost, Random Forest, and AdaBoost through an adaptive voting strategy to improve detection stability under changing wireless conditions and diverse attack patterns. A UAV swarm communication dataset is constructed with 60 UAV nodes and 6 ground-control nodes under simulated surveillance and delivery missions. The dataset contains 1.58 million labeled traffic records, including normal communication, flooding attacks, GPS spoofing-related traffic changes, route disruption, and malicious command injection. After feature extraction, 43 traffic and topology features are retained, including packet loss ratio, route change frequency, control message interval, flow duration, retransmission count, delay variation, and source-destination traffic imbalance. SHAP is further used to explain the contribution of each feature to anomaly classification. The purpose of this study is to develop a practical and explainable security framework for UAV swarm communication. By combining ensemble learning, adaptive voting, and SHAP-based feature interpretation, the proposed method aims to improve anomaly detection accuracy while identifying the main causes

of abnormal swarm communication. This design is meaningful for UAV mission security because it helps operators understand whether an alert is caused by communication instability, routing disorder, abnormal command behavior, or malicious traffic manipulation. Therefore, the proposed framework supports both accurate attack detection and interpretable risk analysis, making it more suitable for deployment in UAV swarm networks with dynamic topology, wireless uncertainty, and mission-critical communication requirements.

2. Materials and Methods

2.1 Sample and Study Scenario Description

The study used a simulated UAV swarm communication network for surveillance and delivery tasks. The network included 60 UAV nodes and 6 ground-control nodes. Each UAV worked as a mobile sensing unit and a relay node. The UAVs exchanged routing packets, control commands, telemetry data, and task-status messages through wireless links. The simulation included changes in flight distance, node speed, link quality, and task stage. These settings were used to reflect the unstable communication conditions of UAV swarm networks. A total of 1.58 million labeled traffic records were collected from normal and abnormal communication states. Each record described short-term communication behavior between source and destination nodes, including packet transmission, routing updates, delay, retransmission, and control-message changes.

2.2 Experimental Design and Control Settings

The experiment contained one normal communication group and four attack groups. The normal group represented regular UAV swarm communication during surveillance and delivery tasks. It was used as the control group. The attack groups included flooding attacks, GPS spoofing-related traffic changes, route disruption, and malicious command injection. These attack types were selected because they can directly affect swarm coordination, routing stability, and mission control. Each group was tested under different node densities, movement patterns, and traffic loads. This setting reduced the effect of a single flight condition on the results. Standalone CatBoost, Random Forest, AdaBoost, and SVM models were used as comparison models. This design allowed the proposed ensemble model to be compared with both tree-based models and a traditional machine learning model.

2.3 Measurement Methods and Quality Control

Traffic data were collected from UAV-to-UAV and UAV-to-ground communication links. The measured variables included packet loss ratio, route change frequency, control message interval, flow duration, retransmission count, signal-related delay variation, source-destination traffic imbalance, node degree, routing table update frequency, and abnormal command frequency. Raw traffic logs were checked before feature extraction. Duplicate records, incomplete packet traces, and records with invalid timestamps were removed. Time windows with missing communication states were excluded. Numerical features were checked against the simulation range to remove invalid values. Class labels were assigned according to the known communication state of each scenario. To reduce label noise, each attack period was matched with its traffic window. Boundary records between normal and attack states were checked separately. After quality control, 43 traffic and topology features were kept for model training and testing.

2.4 Data Processing and Model Formulas

The dataset was divided into training, validation, and testing sets by stratified sampling. This method kept the class distribution similar across the three sets. Numerical features were scaled

when required by the comparison model. Tree-based models used the original feature values. Let x_i be the feature vector of the i-th traffic record, and let y_i be its class label. The ensemble prediction was obtained by adaptive weighted voting:

$$\hat{y}_i = \arg\max_c \sum_{m=1}^{M} w_m I(h_m(x_i)=c)$$

where $h_m(x_i)$ is the prediction of the m-th base model, w_m is its weight, c is a traffic class, and$I(\cdot)$ is the indicator function. Model performance was measured by accuracy, macro-F1, and AUC. Macro-F1 was calculated as:

$$\text{Macro-F1} = \frac{1}{K}\sum_{k=1}^{K} \frac{2P_kR_k}{P_k+R_k}$$

where K is the number of classes, P_k is the precision of class k, and R_k is the recall of class k. Macro-F1 was used because it gives the same weight to each class and is suitable for multi-class anomaly detection.

2.5 Model Training and SHAP-Based Interpretation

CatBoost, Random Forest, and AdaBoost were trained as base models. Their outputs were combined by the adaptive voting method. Hyperparameters were selected on the validation set. The final results were reported on the independent testing set. All comparison models used the same data split to keep the evaluation fair. After training, SHAP analysis was used to explain the effect of each feature on the classification result. Global SHAP values were used to rank the main features across all traffic classes. Local SHAP values were used to explain single abnormal records. This step showed whether an anomaly was mainly linked to route changes, abnormal control-message intervals, retransmission spikes, delay variation, or traffic concentration. The SHAP results were used only for explanation and did not change the original labels.

3. Results and Discussion

3.1 Overall Detection Performance

The proposed SHAP-based ensemble model showed good performance in detecting abnormal communication in UAV swarm networks. It achieved 97.47% accuracy, 96.63% macro-F1, and 98.09% AUC across five traffic classes. These results show that the model can distinguish normal communication from flooding attacks, GPS spoofing-related traffic changes, route disruption, and malicious command injection. The macro-F1 score is important because it reflects the model performance on each class rather than only on the largest class. Compared with standalone CatBoost and SVM models, the proposed ensemble improved macro-F1 by 1.94% and 5.21%, respectively. This result suggests that a single classifier may not capture all traffic changes in UAV swarm networks. Similar results have been reported in recent UAV intrusion detection studies, where ensemble models showed better stability under complex airborne network traffic conditions (Islam et al., 2026; Ma, 2026). As shown in Fig. 1, an ensemble framework can combine feature processing and classification in a more stable way for UAV network intrusion detection.

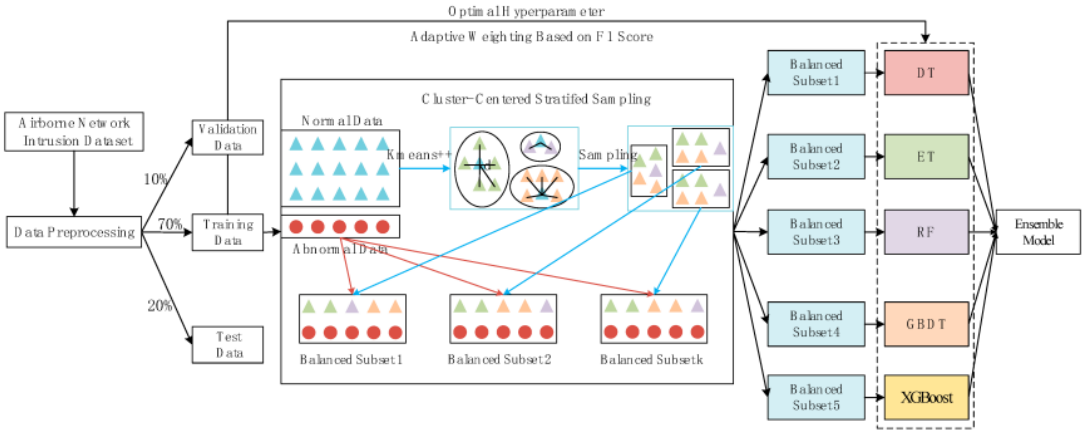

Fig. 1. Comparison of the proposed ensemble model with baseline classifiers for UAV swarm anomaly detection.

3.2 Detection Results across Different Attack Types

The model performed better on flooding attacks and malicious command injection than on route disruption and GPS spoofing-related traffic changes. Flooding attacks usually cause a clear rise in packet frequency, retransmission count, and traffic concentration. Malicious command injection also changes the timing and frequency of control messages. These features are easier to separate from normal communication. In contrast, route disruption and GPS spoofing-related traffic changes are harder to detect because they may look similar to normal route changes caused by UAV movement, link loss, or signal delay. This explains why some boundary samples were misclassified. This finding is consistent with recent studies on UAV intrusion detection, which reported that changing topology and overlapping traffic features can increase false alarms (Mohamed et al., 2026; Wang et al., 2026). Therefore, detection models for UAV swarms should not rely only on packet-level features. Route stability, node interaction, mission phase, and time-window features should also be included.

3.3 Effect of the Ensemble Learning Strategy

The adaptive ensemble strategy improved model stability under changing wireless communication conditions. CatBoost captured nonlinear relations among traffic and topology features. Random Forest reduced the risk of unstable prediction by using multiple decision trees. AdaBoost improved the classification of difficult samples by focusing more on records that were misclassified in earlier rounds. Their combination produced better results than a single classifier. This is important for UAV swarm networks because communication states can change quickly during flight. A model that works well during stable routing may perform poorly when route changes, packet loss, or control-message frequency increase (Zhu et al., 2025). The adaptive voting method reduced this problem by adjusting the contribution of each base model. Compared with deep learning-based IDS models, the proposed model also has a clearer feature structure and is easier to explain. This makes it more suitable for mission-control systems that need both accurate detection and clear warning information (Memon et al., 2026; Xue et al., 2025).

3.4 SHAP Interpretation and Practical Security Meaning

The SHAP results showed that route change frequency, abnormal control message interval, retransmission spikes, signal-related delay variation, and source-destination traffic imbalance were the main signs of abnormal UAV communication. These features are closely related to swarm coordination and route stability. Frequent route changes may indicate route disruption or GPS spoofing-related traffic changes. Abnormal control-message intervals may suggest malicious

command injection. Retransmission spikes and traffic concentration are more related to flooding attacks and link overload. As shown in Fig. 2, SHAP can explain how each feature affects the final anomaly decision. This improves model transparency in security monitoring. It also helps operators understand why an alarm is raised. However, this study still has limitations. The dataset was generated in a simulated UAV swarm environment. Real UAV missions may include stronger interference, hardware limits, mixed attacks, and incomplete traffic records. Future work should test the model with real flight communication data and add online updating to improve long-term use (Al-Mekhlafi et al., 2025; G. Gao, R. Gao, R. Gao, et al., 2026).

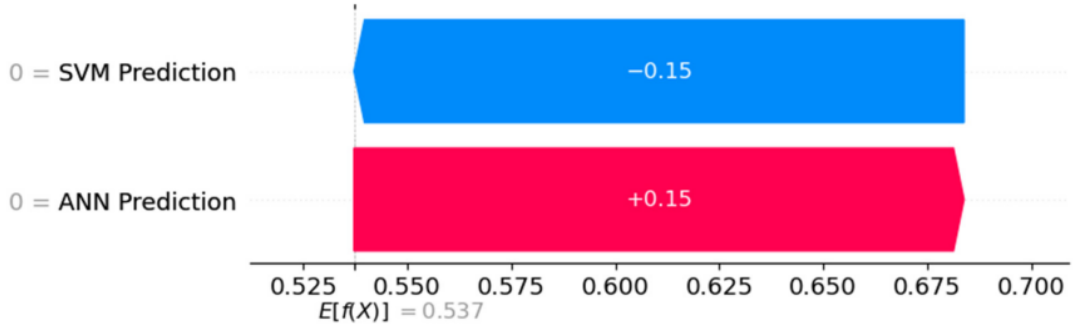

Fig. 2. SHAP results showing the main features linked to abnormal UAV swarm communication.

4. Conclusion

This study proposed a SHAP-based ensemble method for detecting abnormal communication in UAV swarm networks. The method combined CatBoost, Random Forest, and AdaBoost through adaptive voting and used SHAP to explain the effect of key traffic and topology features. The proposed model achieved 97.47% accuracy, 96.63% macro-F1, and 98.09% AUC across five communication classes. Compared with single classifiers, the ensemble model showed better stability under changing wireless conditions and complex swarm traffic patterns. SHAP results showed that route change frequency, abnormal control message intervals, retransmission spikes, delay variation, and source-destination traffic imbalance were closely linked to compromised UAV communication. These results suggest that explainable ensemble learning can improve detection accuracy and make model decisions easier to understand. The method can support real-time monitoring, early warning, and post-event analysis in surveillance, delivery, and emergency UAV missions. However, this study used simulated traffic data. Real UAV networks may involve stronger signal interference, hardware limits, mixed attacks, and incomplete communication records. Future work should test the method with real flight data and improve online updating for long-term use.

Acknowledgments

We are grateful to all respondents who participated in this study.

References

1. Al-Mekhlafi, Z. G., Altmemi, J. M., Al-Shareeda, M. A., Al-Hchaimi, A. A. J., Homod, R. Z., Mohammed, B. A., ... & Alkhabra, Y. A. (2025). ChebIoD: a Chebyshev polynomial-based lightweight authentication scheme for internet of drones environments. Scientific Reports, 15(1), 32897.
2. Almheiri, S. J., Shah, A. A., Abbas, S., Ahmad, M., & Khan, M. A. (2025). Smart sustainable cyber security: modelling an interpretable and transparent threat detection with explainable

artificial intelligence. Discover Sustainability, 6(1), 442.
3. Alqudsi, Y., & Makaraci, M. (2025). UAV swarms: research, challenges, and future directions. Journal of Engineering and Applied Science, 72(1), 12.
4. Bodycomb, M., & Anaissi, A. (2026). An Adaptive Model Aggregation Framework for Enhanced Swarm Learning. ACM Transactions on Knowledge Discovery from Data.
5. Dangore, M., & Sah, H. R. (2025). Cross-layer trust management to secure wireless communication routing protocol. Peer-to-Peer Networking and Applications, 18(5), 277.
6. Deng, X., & Yang, J. (2026). Design of a Quantitative Futures Trading Model Incorporating Multimodal Feature Fusion and Tail Risk Control. Available at SSRN 6702398.
7. Dolatyabi, P., Regan, J., & Khodayar, M. (2025). Deep learning for traffic scene understanding: A review. IEEE Access, 13, 13187-13237.
8. Gao, G., Gao, R., Gao, R., Zhou, H., & Lu, C. (2026, March). Performance Study of Enterprise SMS Communication Scheduling Mechanisms in Triple-Play Convergence Environments. In 2026 IEEE 8th International Conference on Communications, Information System and Computer Engineering (CISCE) (pp. 82-86). IEEE.
9. Gao, G., Gao, R., Lu, C., Gao, R., & Kuang, Y. (2026, March). Security Governance Methods and Quantitative Evaluation for Enterprise SMS and Verification Code Systems. In 2026 International Conference on Generative Artificial Intelligence and Information Security (GAIIS) (pp. 455-458). IEEE.
10. Huang, R. (2026). ConfSched: Confidence-Threshold Routing for Efficient Edge-Cloud Activity Recognition. World Journal of Engineering and Technology, 14(2), 471-486.
11. Ieropoulos, V., Anthi, E., Spyridopoulos, T., Burnap, P., Carnelli, P., & Khan, A. (2026). Federated detection at the edge: collaborative anomaly detection for resource-limited IoT. IEEE Internet of Things Journal.
12. Islam, M. S., Ahmed, F., Ishtiaq, W., Hossain, M. A., Islam, M. S., & Tarek, M. M. (2026). Advanced explainable ensemble models for multi-class intrusion detection in heterogeneous drone and industrial networks. Journal on Information Security.
13. Khanpour, A., Wang, T., Vahidi-Shams, A., Ectors, W., Nakhaie, F., Taheri, A., & Claudel, C. (2025). UAV-Based Intelligent Traffic Surveillance System: Real-Time Vehicle Detection, Classification, Tracking, and Behavioral Analysis. arXiv preprint arXiv:2509.04624.
14. Li, Y., & Liu, S. (2026, May). A Study on Dynamic Optimization of Alerting Policies and Multi-Agent Decision-Making Mechanisms in Cloud Environments. In 2026 7th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT) (pp. 703-706). IEEE.
15. Ma, Y. (2026). Industrial Financial Risk Prediction Model Based on Graph Neural Network and Knowledge Graph Inference. Journal of Circuits, Systems and Computers, 35(16), 2650103.
16. Meheretu, S. E., Nigussie, E., Gebremeskel, G. B., & Hailesilassie, S. Y. (2025). A Systematic Literature Review on Spoofing and Jamming Approaches in Unmanned Aerial Vehicles Navigation. Journal of Aerospace Technology and Management, 17, e3425.
17. Memon, M., Talpur, S., Narejo, S., & Sanin, C. (2026). Development of non-gps drone mission control for 2 autonomous horizontal navigation. In Computational Intelligence in Surveillance Systems Using Image Processing (pp. 83-95). Elsevier.
18. Mohamed, M., Mohamed, D., & Alosman, K. (2026). Spatio-Temporal Graph Neural Networks for Zero-Day Intrusion Detection in Low-Altitude Autonomous UAV Swarms. Ad Hoc Networks, 104251.
19. Qi, C., & Qiao, X. (2026). Using AI to Monitor AI: Automated Operations Through Log-Driven Intelligence. Available at SSRN 6795840.

20. Ramos, G. S., Pinto, M. F., & Haddad, D. B. (2025). Advancing UAV swarm autonomy with ARCog-NET for task allocation, path planning, and formation control. Robotica, 43(7), 2565-2609.
21. Rathi, G., Kamble, S., & Sharma, N. (2025). AI-driven road traffic management: a comprehensive review of outlier detection techniques and challenges: G. Rathi et al. Knowledge and Information Systems, 67(10), 8267-8309.
22. Shao, W. (2026). Policy-Driven Vulnerability Risk Quantification framework for Large-Scale Cloud Infrastructure Data Security. arXiv preprint arXiv:2604.06252.
23. Su, D., & Wu, Y. (2026). Multilevel Growth and Social Network Modeling for Functional Communication Enhancement in Students with Intellectual Disabilities.
24. Wang, Y., Chen, J., Arias, R., Wang, Y., & Yin, X. (2026). Development and Validation of a Patient-Friendly Digital Assessment Platform for Precision Screening of Oral Anti-Obesity Medications (AOMs).
25. Xu, S., Ma, Q., Liu, H., & Yue, L. (2026). Continuous Reorganization and Performance Preservation of Agent Memory Structure Under Distributed Change Environments.
26. Xue, Z., Zi, Y., Qi, N., Gong, M., & Zou, Y. (2025, August). Multi-level service performance forecasting via spatiotemporal graph neural networks. In 2025 5th International Conference on Intelligent Communications and Computing (ICICC) (pp. 202-206). IEEE.
27. Yang, J. (2026). Stage-Coupled Computational Framework for Stratified Accessibility and Equity Analysis in Community-Based Elderly Care Services.
28. Yin, J., Huang, Y., & Rao, H. (2026). A Study on User Behavior Signal-Driven Predictive Models for Digital Platform Consumption Trends. Available at SSRN 6607298.
29. Zhang, Z. (2026). A Study on Return Optimization in E-commerce for Complex Consumer Goods Driven by Installation Information Quality. Available at SSRN 6734720.
30. Zhang, Z., Gao, Y., & Tong, Y. (2026). Semantic-Temporal Graph Learning for Demand Forecasting and Resource Allocation in Public Information Systems. Available at SSRN 6792279.
31. Zhu, W., Yao, Y., & Yang, J. (2025). Optimizing Financial Risk Control for Multinational Projects: A Joint Framework Based on CVaR-Robust Optimization and Panel Quantile Regression.