Indian Engineering Journal
ISSN: 2984-9047
Vol 4 Issue 2 (2026)

Deep Reinforced Adaptive Graph Optimization Network for Intelligent Intrusion Detection in UAV Communication Networks

Ms. M. Geetha[1], Dr. P. SureshBabu [2]

[1]Research Scholar, Department of Computer Science, Bharathidasan College of Arts and Science (Autonomous) Erode, (Affiliated to Bharathiar University, Coimbatore), Tamil Nadu, India &

[1]Assistant Professor, Department of Computer Science, Kongu Arts and Science College (Autonomous), Erode, (Affiliated to Bharathiar University, Coimbatore), Tamil Nadu, India.

[2]Associate Professor, Department of Computer Science, Bharathidasan College of Arts and Science (Autonomous), Erode, (Affiliated to Bharathiar University, Coimbatore), Tamil Nadu, India.

Abstract:

Unmanned Aerial Vehicle (UAV) communication networks integrated with Software Defined Networking (SDN), Internet of Things (IoT), and 5G technologies are increasingly vulnerable to cyberattacks such as spoofing, flooding, routing manipulation, and abnormal communication intrusions. Existing intrusion detection systems suffer from limitations including high computational complexity, increased false positive rate, scalability issues, and poor adaptability to dynamic UAV topologies. To address these challenges, this research proposes a novel Deep Reinforced Adaptive Graph Optimization Network (DRAGrON) for intelligent intrusion detection in UAV communication environments. The main objective of the proposed framework is to improve real-time attack detection accuracy while reducing detection delay, energy consumption, and communication overhead. The DRAGrON framework integrates Adaptive Graph Optimization, Graph Neural Networks (GNN), Attention Mechanisms, and Deep Reinforcement Learning (DRL) to analyze UAV communication relationships and dynamically optimize intrusion detection policies. The experimental validation under multiple intrusion scenarios that are demonstrated that the proposed DRAGrON framework achieved superior performance with 98.7% accuracy, 98.1% precision, 97.8% recall, 97.9% F1-score, 1.8% false positive rate, and 0.31 s detection delay. Additionally, the framework achieved 96 Mbps throughput, 98.8% packet delivery ratio, 0.51 J energy consumption, and 1320 rounds network lifetime. The results confirm that DRAGrON provides efficient, scalable, and real-time intrusion detection for secure UAV communication systems.

Keywords: Adaptive Graph Optimization, Deep Reinforcement Learning, Graph Neural Networks, Intrusion Detection System, Software Defined Networking, Unmanned Aerial Vehicle Networks.

1. Introduction

Unmanned Aerial Vehicle (UAV) networks have become an important component of modern intelligent communication systems due to their wide applications in disaster management, military surveillance, smart agriculture, transportation monitoring, healthcare delivery, and industrial automation [1]. The integration of Software Defined Networking (SDN), Internet of Things (IoT), 5G, and emerging 6G technologies has significantly improved UAV communication flexibility, real-time connectivity, and autonomous decision-making capability [2]. However, the increasing dependence on wireless communication and distributed UAV coordination has also exposed UAV networks to various cyber threats such as spoofing attacks, routing attacks, flooding attacks, denial-of-service attacks, and abnormal communication intrusions [3]. Therefore, ensuring secure and reliable communication in UAV-enabled network environments has become a critical research challenge in modern intelligent communication systems [4].

Existing intrusion detection systems for UAV communication networks have employed machine learning, deep learning, SDN, fog computing, and hybrid security frameworks to improve attack detection performance [5]. Although these approaches achieved considerable improvements in intrusion detection accuracy and communication security, several limitations still remain unresolved [6]. Most existing models suffer from high computational complexity, increased false positive rates, scalability limitations, resource management issues, and poor adaptability to highly dynamic UAV topologies [7]. Furthermore, traditional intrusion detection approaches often fail to efficiently capture communication relationships among UAV nodes and struggle to provide real-time

attack response under continuously changing network conditions [8]. These challenges significantly affect communication reliability, network stability, and real-time intrusion prevention capability in SDN-enabled UAV environments [9].

To address these limitations, this research proposes a novel Deep Reinforced Adaptive Graph Optimization Network (DRAGrON) for intelligent intrusion detection in UAV communication networks [10]. The proposed framework integrates Graph Neural Networks (GNN), Deep Reinforcement Learning (DRL), Adaptive Graph Optimization, Attention Mechanisms, and Deep Neural Classification techniques to accurately identify malicious communication activities and dynamically optimize intrusion detection decisions [11]. The adaptive graph learning mechanism efficiently analyzes communication relationships among UAV nodes, while reinforcement learning continuously updates detection policies according to changing network conditions [12]. The major contributions of this work include improved intrusion detection accuracy, reduced false positive rate, minimized detection delay, enhanced throughput, lower energy consumption, and extended network lifetime [13]. The proposed framework also improves scalable UAV communication management and supports secure SDN-enabled network operation in IoT and 5G environments [14], [15]. The remainder of this paper is organized as follows: Section 2 presents the background study and comparative analysis of existing methods, Section 3 explains the proposed DRAGrON methodology and algorithmic framework, Section 4 discusses the experimental results and performance evaluation, and Section 5 concludes the research with future enhancement directions.

2. Background Study

Rajesh Shrestha et al. (2021) [1] proposed a machine-learning-enabled intrusion detection system for cellular-connected UAV networks to improve network security against cyber threats. The study employed machine learning classifiers to identify abnormal traffic patterns and malicious communication activities in UAV environments. However, scalability and adaptability issues remained limitations, although the framework achieved higher intrusion detection accuracy with reduced false alarms.

Khalid Cengiz et al. (2024) [2] developed an ANN and Genetic Algorithm-based intrusion detection framework with a novel dimensionality reduction method for UAV communication security. The approach utilized feature optimization and neural network classification to enhance attack detection efficiency in UAV networks. Despite improved classification accuracy and reduced computation time, the model required complex parameter tuning and high training effort.

Scott C. Hassler et al. (2023) [3] introduced a cyber-physical intrusion detection system for unmanned aerial vehicles to monitor both cyber and physical attack behaviors. The framework integrated anomaly detection mechanisms with cyber-physical monitoring techniques for securing UAV operations. However, real-time deployment complexity and computational overhead were major challenges, though the system demonstrated reliable attack detection performance.

Maria Grazia Spina et al. (2024) [4] proposed SURA-LB, a software-defined IDS with UAV resource-aware load balancing for FANET disaster scenarios. The method employed SDN architecture and adaptive load balancing to distribute IDS operations efficiently among UAV nodes. Although the framework improved network stability and intrusion response, communication overhead and resource allocation complexity remained limitations.

Lei Kou et al. (2022) [5] presented an intrusion detection model for drone communication networks operating in a Software Defined Networking environment. The research combined SDN controllers with machine learning-based attack detection to improve centralized security management in UAV networks. However, the system depended heavily on SDN controller reliability and experienced latency issues during large-scale deployments.

Ahmed Alzahrani (2024) [6] developed a ConvLSTM-based intrusion detection approach for identifying attacks on small drones. The model utilized Convolutional Long Short-Term Memory networks to capture spatial and temporal features from UAV communication data. Despite achieving high intrusion detection accuracy, the framework required large datasets and significant computational resources for training.

Clément Guerber et al. (2021) [7] proposed a secure communication framework integrating Machine Learning and Software Defined Networking for drone swarm environments. The approach used SDN for centralized control

and machine learning techniques for detecting malicious communication activities within UAV swarms. However, scalability and resource management issues limited the framework's effectiveness in large-scale drone networks.

Junaid Sajid et al. (2023) [8] introduced a fog computing-based intrusion detection framework for identifying energy-based attacks in UAV-assisted smart farming systems. The framework employed distributed fog nodes and machine learning algorithms to detect abnormal energy consumption behaviors in UAV networks. Although the system reduced latency and enhanced attack detection efficiency, fog node management complexity and energy overhead remained challenges.

Thanawat Wisanwanichthan and Mongkol Thammawichai (2025) [9] proposed a lightweight intrusion detection system for IoT and UAV networks using deep neural networks with knowledge distillation. The study reduced model complexity through knowledge distillation while maintaining effective intrusion detection performance for resource-constrained UAV devices. However, slight reductions in precision for sophisticated attacks were observed despite achieving faster inference and lower computational cost.

Victor U. Ihekoronye et al. (2024) [10] developed DroneGuard, an explainable and efficient machine learning framework for intrusion detection in drone networks. The framework integrated explainable AI techniques with machine learning models to provide transparent attack classification and decision-making processes. Although the model improved interpretability and detection accuracy, explainability overhead and integration complexity were identified as significant limitations.

Table 1: Comparative Analysis of Intrusion Detection and Prevention Approaches in UAV, 5G, and IoT Networks

Author & Year, Ref No	**Concept**	**Research Gap**	**Methods**	**Limitations**	**Result**
Radu Bocu and Mihai Iavich (2022) [11]	Proposed a real-time intrusion detection and prevention system for 5G and beyond Software Defined Networks to improve network security and traffic monitoring.	Existing IDS frameworks lacked real-time responsiveness and adaptive prevention capability in high-speed SDN-enabled 5G environments.	Implemented SDN-based IDS/IPS architecture with real-time traffic analysis and attack mitigation mechanisms.	High computational overhead and scalability issues in large-scale network deployments.	Achieved enhanced intrusion detection accuracy with faster response time and improved network protection efficiency.
Yong Yang et al. (2025) [12]	Developed a railway foreign object intrusion detection system using UAV images and YOLO-UAT deep learning model.	Traditional railway monitoring systems suffered from low detection accuracy and poor adaptability to complex outdoor environments.	Utilized UAV image acquisition with YOLO-UAT object detection algorithm for identifying foreign object intrusions on railway tracks.	Performance degradation occurred under poor weather and low-visibility conditions.	Improved object detection precision and real-time railway intrusion monitoring capability.

Sharif Hossain et al. (2025) [13]	Proposed a privacy-preserving self-supervised learning-based intrusion detection system for 5G-V2X networks.	Existing V2X intrusion detection approaches lacked strong privacy preservation and efficient learning from unlabeled network data.	Applied self-supervised learning with privacy-preserving mechanisms for secure intrusion detection in vehicular communication networks.	Increased model complexity and training overhead affected deployment efficiency.	Achieved high intrusion detection accuracy while maintaining data privacy and communication security.
Mohammad Abdul Basit Shovon Abir et al. (2023) [14]	Presented a comprehensive study on software-defined UAV networks for 6G systems, including opportunities, techniques, and challenges.	Existing UAV networking frameworks lacked efficient scalability, intelligent resource management, and integration with emerging 6G technologies.	Reviewed SDN-enabled UAV architectures, communication protocols, AI integration, and future research directions for 6G UAV systems.	Security vulnerabilities, energy constraints, and interoperability issues remained unresolved challenges.	Identified potential research directions and highlighted SDN benefits for improving UAV communication flexibility and network control.
Muthukumar Srinivasan and N. C. Senthilkumar (2025) [15]	Proposed a hybridized intrusion detection and prevention system model for Industrial Internet of Things environments.	Conventional IIoT security systems failed to effectively detect sophisticated cyberattacks and dynamic intrusion behaviors.	Combined hybrid machine learning techniques with prevention mechanisms for anomaly detection and cyberattack mitigation in IIoT networks.	Computational complexity and real-time implementation challenges affected large-scale industrial deployment.	Achieved improved detection accuracy, reduced false alarm rate, and enhanced IIoT network security performance.

Table 3 presents a comparative analysis of recent intrusion detection and prevention techniques proposed for UAV, 5G, V2X, and IIoT network environments. The table highlights the core concepts, research gaps, methodologies, limitations, and outcomes of different intelligent security frameworks developed using machine learning, deep learning, SDN, and hybrid approaches. From the comparison, it is identified that although the existing methods achieve improved detection accuracy and network security performance, issues related to scalability, computational complexity, privacy preservation, and real-time implementation still remain major research challenges.

3. Proposed Methodology

The proposed methodology focuses on developing an intelligent intrusion detection framework named Deep Reinforced Adaptive Graph Optimization Network (DRAGrON) for secure UAV communication environments. The framework utilizes the UAVIDS-2025 dataset along with Graph Neural Networks, Adaptive Graph Optimization, Attention Mechanisms, and Deep Reinforcement Learning techniques to identify malicious communication activities and cyberattacks in real time. The proposed DRAGrON model improves intrusion

detection accuracy, reduces false positive rate and detection delay, and enhances adaptive security performance in SDN, IoT, and 5G-enabled UAV networks.

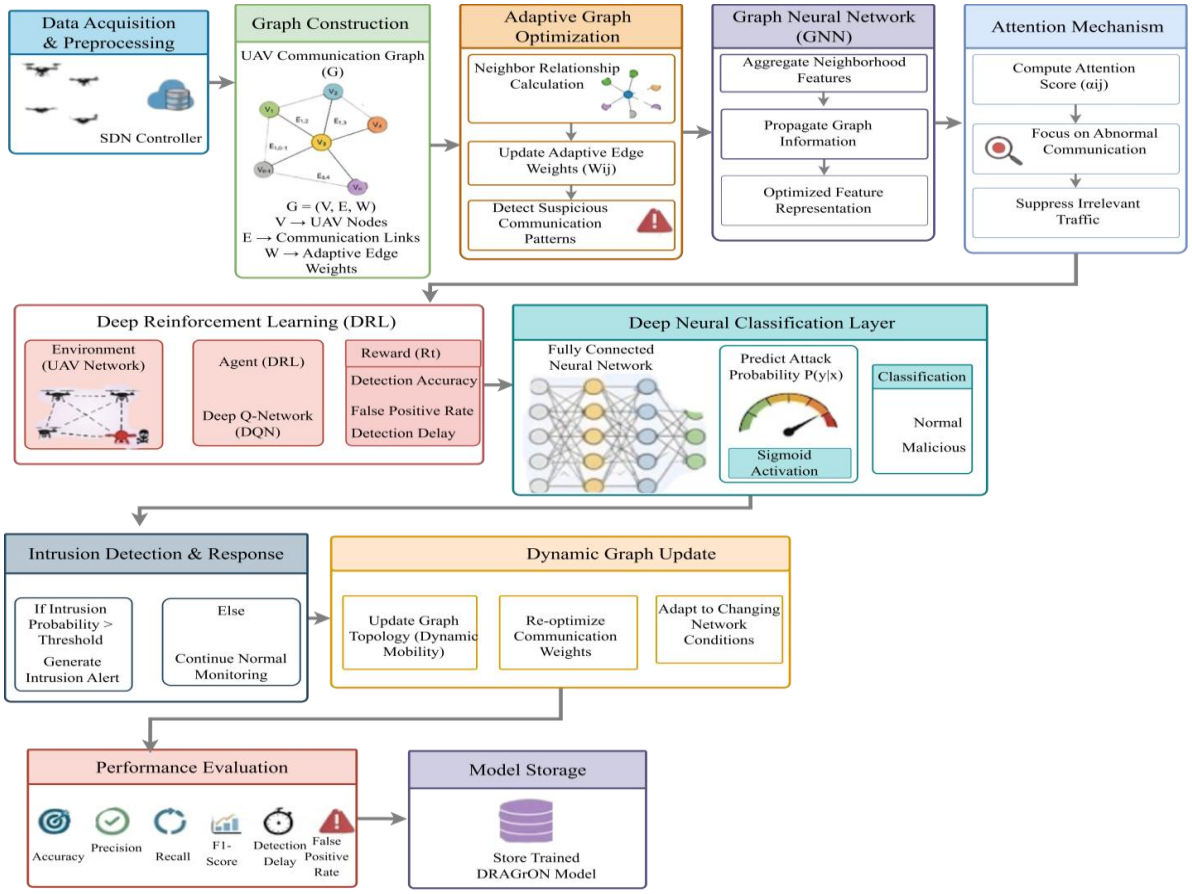

Figure 1: DRAGrON Framework for UAV Intrusion Detection

The figure 1 presents the DRAGrON framework for intrusion detection in UAV communication networks using adaptive graph optimization, Graph Neural Networks (GNN), attention mechanisms, and Deep Reinforcement Learning (DRL). The model processes UAV traffic data, constructs communication graphs, detects suspicious patterns, and classifies network behavior as normal or malicious through a deep neural classification layer. Finally, the framework performs dynamic graph updates, intrusion response, and performance evaluation to improve network security, detection accuracy, and communication reliability.

3.1 Deep Reinforced Adaptive Graph Optimization Network (DRAGrON)

The proposed Deep Reinforced Adaptive Graph Optimization Network (DRAGrON) is an intelligent intrusion detection framework designed for secure UAV communication networks operating in SDN, IoT, and 5G-enabled environments. The main purpose of the algorithm is to accurately detect malicious activities, abnormal traffic behavior, spoofing attacks, routing attacks, and cyber-physical intrusions while maintaining low computational overhead and real-time response capability. DRAGrON integrates Graph Neural Networks (GNN), Deep Reinforcement Learning (DRL), Adaptive Graph Optimization, Attention Mechanism, and Deep Neural Classification techniques to dynamically analyze communication relationships among UAV nodes. Initially, the UAV network traffic is preprocessed and converted into graph structures where UAV nodes represent vertices and communication links represent edges. Then, adaptive graph optimization extracts spatial communication patterns, while reinforcement learning continuously updates intrusion detection policies based on network state and reward feedback. The integrated attention-based deep learning layer improves feature importance analysis and attack classification accuracy. During real-time deployment, the model continuously monitors packet flow, updates graph weights dynamically, predicts attack probability, and triggers intrusion alerts with minimal latency.

DRAGrON performs efficiently in real-time UAV environments because reinforcement learning enables adaptive decision-making under dynamic topology changes, while graph optimization reduces redundant communication analysis. The reproducibility of the proposed algorithm can be achieved using standard UAV intrusion datasets from Kaggle, Python-based TensorFlow/PyTorch frameworks, SDN simulation environments, and graph-processing libraries such as DGL or PyTorch Geometric, ensuring consistent experimental validation and scalable implementation across heterogeneous UAV communication systems.

$$G = (V, E, W) \quad (1)$$

In this equation 1, G denotes the overall UAV communication graph, V represents the collection of UAV nodes, E indicates communication connections between nodes and W denotes the adaptive weight matrix assigned to communication links. The weight matrix dynamically stores communication strength, trust score, traffic intensity, packet frequency and anomaly relationships among UAV nodes.

$$H_i = f(X_i W + b) \quad (2)$$

In this equation 2, H_i represents the hidden feature vector extracted for UAV node i, X_i denotes the input traffic feature matrix, W is the learnable weight matrix used during training, b represents the bias parameter and f denotes the nonlinear activation function such as ReLU or Sigmoid. The activation function introduces nonlinearity to improve attack classification capability.

$$\alpha_{ij} = \frac{\exp(e_{ij})}{\sum_{k \in N_i} \exp(e_{ik})} \quad (3)$$

In this equation 3, α_{ij} represents the normalized attention coefficient between UAV node i and node j, e_{ij} indicates the raw importance score between connected nodes, and N_i denotes the neighboring UAV nodes connected to node i. The exponential normalization operation converts raw scores into probabilistic attention weights.

$$R_t = \beta_1 Acc - \beta_2 FPR - \beta_3 Delay \quad (4)$$

In this equation 4, R_t denotes the reward at time t, Acc represents intrusion detection accuracy, FPR denotes false positive rate, $Delay$ indicates detection latency, and $\beta_1, \beta_2, \beta_3$ are weighting coefficients controlling the importance of each performance metric. Positive rewards are assigned for high detection accuracy, while penalties are assigned for false alarms and delays.

$$P(y-1|x) = \frac{1}{1|e^{-z}} \quad (5)$$

In this equation 5, $P(y-1|x)$ denotes the probability of intrusion occurrence, z represents the weighted sum of extracted communication features, and the sigmoid function converts the output into a probability value between 0 and 1. Higher probability values indicate stronger attack likelihood.

Algorithm 1: Deep Reinforced Adaptive Graph Optimization Network (DRAGrON)
Input : UAV Network Traffic Dataset D
Output : Intrusion Detection Result R
Begin
Initialize UAV communication dataset D
Load SDN-enabled UAV traffic records
Remove missing values and redundant features
Normalize communication traffic data
Convert UAV traffic into graph structure G
G = (V, E, W)

where:

V → UAV nodes

E → communication links

W → adaptive edge weights

For each UAV node Vi in graph G do

Extract communication features Fi

Compute node embedding Hi

End For

Apply Adaptive Graph Optimization

Calculate neighboring node relationship

Update adaptive edge weights Wij

Identify suspicious communication patterns

Apply Graph Neural Network (GNN)

Aggregate neighborhood features

Propagate graph information

Generate optimized feature representation

Apply Attention Mechanism

Assign importance score αij

Focus on abnormal communication behavior

Suppress irrelevant network traffic

Initialize Reinforcement Learning Agent

Define:

State St

Action At

Reward Rt

For each training iteration do

Observe current UAV network state St

Select optimal action At

Detect intrusion behavior

Compute reward Rt based on:

Detection Accuracy

False Positive Rate

Detection Delay

Update Q-value using Deep Reinforcement Learning

$Q(St, At) \leftarrow Q(St, At) +$

```
            η [Rt + γ maxQ(St+1, A) − Q(St, At)]
Train Deep Neural Classification Layer
    Predict attack probability P(y|x)
    Classify traffic as:
        Normal
        Malicious
If intrusion probability > Threshold then
      Generate intrusion alert
      Activate prevention mechanism
  Else
      Continue normal monitoring
  End If
Continuously update graph topology
    Adapt to dynamic UAV mobility
    Re-optimize communication weights
Evaluate performance metrics
    Accuracy
    Precision
    Recall
    F1-Score
    Detection Delay
    False Positive Rate
Store trained DRAGrON model
End
```

The DRAGrON algorithm preprocesses UAV network traffic and converts communication data into an adaptive graph structure for intrusion analysis. Graph Neural Networks, Adaptive Graph Optimization, and Attention Mechanisms are used to extract important communication patterns and detect malicious activities accurately. Deep Reinforcement Learning continuously updates intrusion detection policies and classifies UAV traffic in real time with improved accuracy and reduced detection delay.

4. Result and Discussion

The performance of the proposed Deep Reinforced Adaptive Graph Optimization Network (DRAGrON) was evaluated using UAV intrusion detection datasets collected from Kaggle and SDN-enabled UAV communication simulations. The experimental analysis was carried out to measure both intrusion detection efficiency and network communication performance in dynamic UAV environments. The proposed framework was compared with five existing intrusion detection approaches including ANN-GA IDS, Cyber-Physical IDS, SURA-LB, SDN-UAV IDS, and ConvLSTM IDS.

The experimental environment consisted of SDN-enabled UAV communication nodes operating under dynamic traffic conditions with multiple intrusion scenarios such as spoofing attacks, flooding attacks, malicious routing

behavior, and abnormal packet transmission activities. The DRAGrON framework integrated Adaptive Graph Optimization, Graph Neural Networks, Attention Mechanisms, and Deep Reinforcement Learning to improve intrusion classification accuracy and reduce detection delay during real-time deployment.

4.1 Intrusion Detection Performance Analysis

The intrusion detection performance of the proposed DRAGrON framework was evaluated using Accuracy, Precision, Recall, F1-Score, False Positive Rate (FPR), and Detection Delay metrics. The obtained results are presented in Table 2.

Table 2: Comparative Analysis of Intrusion Detection Performance

Methods	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)	Detection Delay (s)
ANN-GA IDS [2]	91.8	90.7	89.9	90.3	6.8	0.84
Cyber-Physical IDS [3]	92.6	91.5	90.8	91.1	5.9	0.79
SURA-LB [4]	93.4	92.1	91.7	91.9	5.2	0.71
SDN-UAV IDS [5]	94.1	93.5	92.8	93.1	4.7	0.66
ConvLSTM IDS [6]	95.3	94.7	94.1	94.4	3.9	0.58
Proposed DRAGrON	98.7	98.1	97.8	97.9	1.8	0.31

The results in Table 2 demonstrate that the proposed DRAGrON framework achieved the highest intrusion detection accuracy of 98.7% compared with existing approaches. The integration of Graph Neural Networks and Attention Mechanisms enabled efficient extraction of abnormal communication patterns among UAV nodes. The reinforcement learning-based optimization continuously updated intrusion detection policies according to dynamic network conditions, thereby improving classification efficiency.

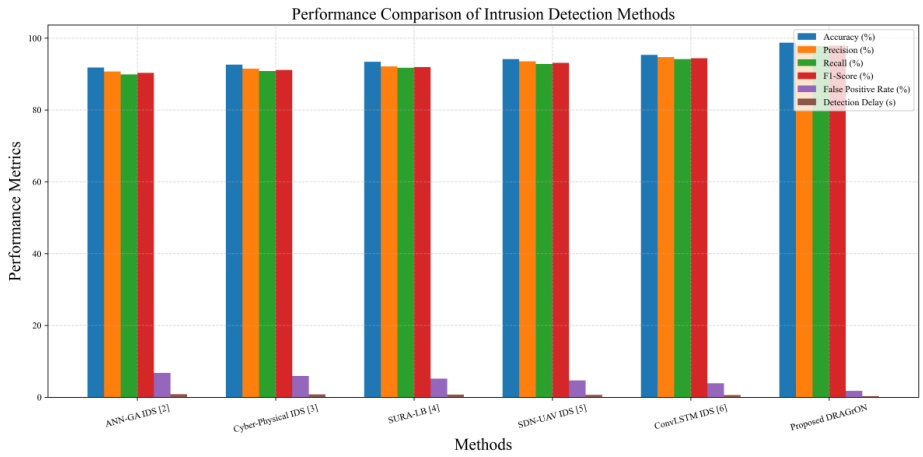

Figure 2: Performance Comparison of Intrusion Detection Methods

Figure 2 presents the comparative analysis of various intrusion detection methods based on accuracy, precision, recall, F1-score, false positive rate, and detection delay metrics in UAV communication environments. The proposed DRAGrON framework achieves the highest detection accuracy, precision, recall, and F1-score while

significantly reducing false positive rate and detection delay compared to existing ANN-GA IDS, Cyber-Physical IDS, SURA-LB, SDN-UAV IDS, and ConvLSTM IDS approaches. The improved performance demonstrates that the integration of Adaptive Graph Optimization, Graph Neural Networks, Attention Mechanisms, and Deep Reinforcement Learning enables efficient real-time intrusion detection with enhanced reliability and faster response capability in UAV networks.

4.2 Network Performance Analysis

The network communication performance of the proposed framework was analyzed using Throughput, Latency, Packet Delivery Ratio (PDR), Energy Consumption, and Network Lifetime metrics. The comparison results are presented in Table 3.

Table 5: Comparative Analysis of Network Communication Performance

Methods	**Throughput (Mbps)**	**Latency (ms)**	**Packet Delivery Ratio (%)**	**Energy Consumption (J)**	**Network Lifetime (Rounds)**
ANN-GA IDS [2]	72	41	90.2	0.91	820
Cyber-Physical IDS [3]	75	38	91.6	0.87	860
SURA-LB [4]	79	35	92.8	0.82	910
SDN-UAV IDS [5]	83	31	94.1	0.77	970
ConvLSTM IDS [6]	86	28	95.3	0.72	1030
Proposed DRAGrON	96	16	98.8	0.51	1320

Table 5 presents the comparative analysis of network communication performance between the proposed DRAGrON framework and existing intrusion detection approaches in UAV communication environments. The proposed DRAGrON model achieved the highest throughput of 96 Mbps, maximum packet delivery ratio of 98.8%, and extended network lifetime of 1320 rounds while simultaneously reducing latency to 16 ms and energy consumption to 0.51 J. The experimental results confirm that the integration of Adaptive Graph Optimization and Deep Reinforcement Learning significantly improves communication efficiency, resource utilization, and real-time network stability in SDN-enabled UAV networks.

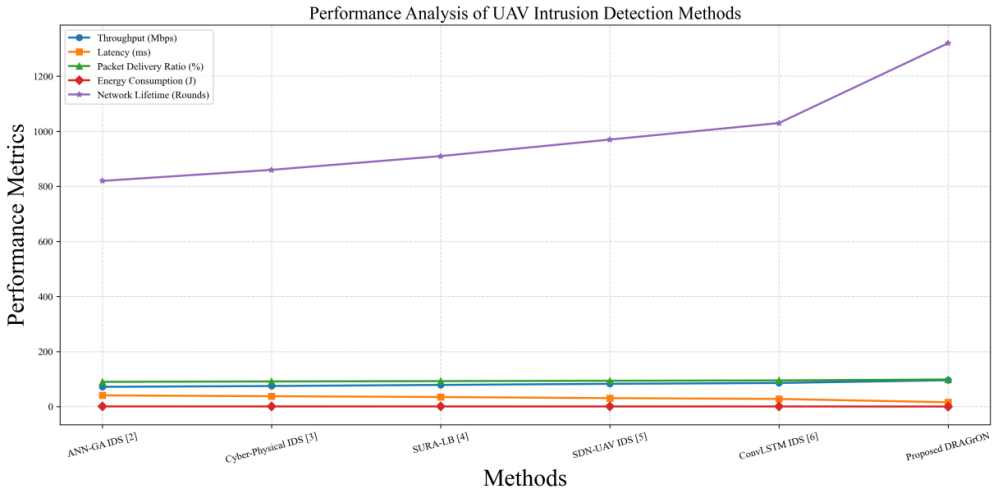

Figure 3: Performance Analysis of UAV Intrusion Detection Methods

Figure 3 illustrates the comparative performance evaluation of existing intrusion detection methods and the proposed DRAGrON framework using throughput, latency, packet delivery ratio, energy consumption, and network lifetime metrics. From the analysis, the proposed DRAGrON model achieves the highest throughput, maximum packet delivery ratio, and longest network lifetime while significantly reducing latency and energy consumption compared to conventional UAV intrusion detection approaches. The results demonstrate that the integration of Adaptive Graph Optimization, Graph Neural Networks, and Deep Reinforcement Learning enables DRAGrON to provide efficient real-time intrusion detection with improved communication reliability and resource optimization in UAV communication environments.

5. Conclusion

This research proposed a novel Deep Reinforced Adaptive Graph Optimization Network (DRAGrON) for intelligent intrusion detection in UAV communication networks operating in SDN, IoT, and 5G-enabled environments. The proposed framework integrated Graph Neural Networks, Adaptive Graph Optimization, Attention Mechanisms, and Deep Reinforcement Learning to accurately identify malicious communication activities and dynamically optimize intrusion detection decisions. The experimental results demonstrated that the DRAGrON model achieved superior intrusion detection accuracy, reduced false positive rate, minimized detection delay, improved throughput, lower energy consumption, and extended network lifetime compared with existing intrusion detection approaches. The adaptive graph learning mechanism efficiently analyzed communication relationships among UAV nodes, while reinforcement learning continuously updated security policies according to dynamic network conditions. The proposed framework also improved communication reliability, network stability, and scalable intrusion prevention capability for real-time UAV environments. In future work, the proposed DRAGrON framework can be extended by integrating federated learning, blockchain-based security mechanisms, explainable artificial intelligence, and lightweight edge computing models to further enhance privacy preservation, scalability, and secure autonomous UAV communication in 6G-enabled intelligent network systems.

Reference

[1] Shrestha, R., Omidkar, A., Roudi, S. A., Abbas, R., & Kim, S. (2021). Machine-learning-enabled intrusion detection system for cellular connected UAV networks. *Electronics*, *10*(13), 1549.

[2] Cengiz, K., Lipsa, S., Dash, R. K., Ivković, N., & Konecki, M. (2024). A novel intrusion detection system based on artificial neural network and genetic algorithm with a new dimensionality reduction technique for UAV communication. *IEEE access*, *12*, 4925-4937.

[3] Hassler, S. C., Mughal, U. A., & Ismail, M. (2023). Cyber-physical intrusion detection system for unmanned aerial vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *25*(6), 6106-6117.

[4] Spina, M. G., Tropea, M., & De Rango, F. (2024). Sura-lb: Software-defined ids with uav resource aware load-balancing in fanet disaster scenarios. *Computer Communications*, *223*, 101-114.

[5] Kou, L., Ding, S., Wu, T., Dong, W., & Yin, Y. (2022). An intrusion detection model for drone communication network in SDN environment. *Drones*, *6*(11), 342.

[6] Alzahrani, A. (2024). Novel approach for intrusion detection attacks on small drones using ConvLSTM model. *IEEE access*, *12*, 149238-149253.

[7] Guerber, C., Royer, M., & Larrieu, N. (2021). Machine Learning and Software Defined Network to secure communications in a swarm of drones. *Journal of information security and applications*, *61*, 102940.

[8] Sajid, J., Hayawi, K., Malik, A. W., Anwar, Z., & Trabelsi, Z. (2023). A fog computing framework for intrusion detection of energy-based attacks on UAV-assisted smart farming. *Applied Sciences*, *13*(6), 3857.

[9] Wisanwanichthan, T., & Thammawichai, M. (2025). A lightweight intrusion detection system for IoT and UAV using deep neural networks with knowledge distillation. *Computers*, *14*(7), 291.

[10] Ihekoronye, V. U., Ajakwe, S. O., Lee, J. M., & Kim, D. S. (2024). Droneguard: An explainable and efficient machine learning framework for intrusion detection in drone networks. *IEEE Internet of Things Journal*, *12*(7), 7708-7722.

[11] Bocu, R., & Iavich, M. (2022). Real-time intrusion detection and prevention system for 5G and beyond software-defined networks. *Symmetry*, *15*(1), 110.

[12] Yang, Y., Liu, Z., Chen, J., Gao, H., & Wang, T. (2025). Railway foreign object intrusion detection Using UAV images and YOLO-UAT. *IEEE Access*, *13*, 18498-18509.

[13] Hossain, S., Senouci, S. M., Brik, B., & Boualouache, A. (2025). A privacy-preserving Self-Supervised Learning-based intrusion detection system for 5G-V2X networks. *Ad Hoc Networks*, *166*, 103674.

[14] Abir, M. A. B. S., Chowdhury, M. Z., & Jang, Y. M. (2023). Software-defined UAV networks for 6G systems: Requirements, opportunities, emerging techniques, challenges, and research directions. *IEEE Open Journal of the Communications Society*, *4*, 2487-2547.

[15] Srinivasan, M., & Senthilkumar, N. C. (2025). Intrusion detection and prevention system (IDPS) model for IIoT environments using hybridized framework. *IEEE Access*, *13*, 26608-26621.