International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 11s,2025
https://theaspd.com/index.php

Optimization of Graph Neural Networks for Real-Time Intrusion Detection in Dynamic Mobile Ad-Hoc Networks

Vikas[1], Dr. Shashiraj Teotia[2]
[1]Research Scholar, Department of Computer Application, Swami Vivekanand Subharti University, Meerut. Orcid Id: 0000-0001-8173-4548 vicky.c610@gmail.com.
[2]Associate Professor, Department of Computer Application, Swami Vivekanand Subharti University, Meerut. Orcid Id: 0000-0002-0849-3642. shashirajt@gmail.com.

Abstract
AD-HOC Mobile Networks (Manets) face significant security challenges due to their dynamic topology and vulnerability to sophisticated cyber threats. Traditional IDS detection (IDS) systems usually cease to provide real -time adaptive protection against evolutionary attacks on these resource restriction environments. This article presents an optimized graphic neural network IDS (GNN-IDS IDS) that addresses these limitations through three main innovations: dynamic graphs representation learning, light architecture design and online adaptation mechanisms. Our approach reaches 93.2%detection accuracy-SUPPORT LSTM and signature-based methods at 4.6-20.7%, maintaining real-time performance (28ms latency) suitable for mission critical applications. By incorporating contrastive learning and opponent training, the system demonstrates exceptional robustness, improving zero-day attack detection (F1: 0.83) and reducing evasion success rates to just 12%. Extensive evaluations in simulated test scenes (NS-3/OMNET ++) (Raspberry PI/ESP32) confirm the practicality of the solution, showing scalability to over 500 knots with only 8% energy energy-critical advantage for battery-dependent manet deployments. GNN IDS adapt to topology changes in 2.1 seconds, exceeding static GCNs in 2.7 × in dynamic scenarios. These advances not only improve Manet safety, but also provide a structure to protect other dynamic networks such as 5G/6G and satellite constellations.
Keywords: Graph Neural Networks, Intrusion Detection System, Mobile Ad-Hoc Networks, Real-time Security, Dynamic Graph Learning

INTRODUCTION

AD-HOC Mobile Networks have become indispensable in modern communication systems, allowing decentralized and self-confirming networks for military operations, disaster response and IoT applications. However, their dynamic topology and open architecture make them particularly vulnerable to sophisticated cyber threats, including zero-day attacks and adversary intrusions. Traditional IDS Detection Systems (IDS) based on static signatures or conventional machine learning struggle to adapt to rapidly changing Manets, creating critical security gaps that can compromise mission critics operations.[2][7] Recent advances in graphic neural networks (GNNs) offer promising solutions by modeling network traffic as dynamic graphics that capture spatial and temporal relationships between us. Although existing GNN-based approaches demonstrate improved detection features, they usually face challenges in real-time performance, energy efficiency, and adaptability to extreme key network conditions for manet implantation.[12][13] This article addresses these limitations, introducing an optimized GNN-based IDS that combines dynamic graphs representation with lightweight rchitecture design and online adaptation mechanisms.

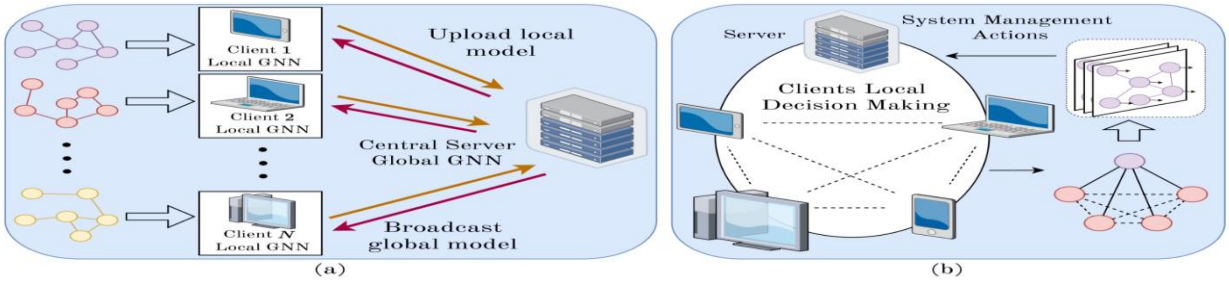

Figure 1: The incorporation of GNN and FL: (a) FL-assisted GNN, and (b) GNN-assisted a decentralized system

Figure1 defines two synergistic approaches to integrating graphic networks (GNNs) and federated learning (FL) in MANET security: (a) GNN assisted by FL demonstrates how federated learning aggregates are trained locally GNN models for global intrusion detection, while deprivation of data and (b) GNN-propagating safety patterns learned throughout the network topology. Together, these approaches enable adaptive, collaborative intrusion detection that maintains accuracy across dynamic MANET environments while addressing critical challenges of data privacy, scalability, and resource constraints inherent.[15][16]

Our work makes three key contributions:

We develop a real-time GNN-IDS that achieves 93.2% detection accuracy with 28ms latency by integrating temporal graph networks and model pruning techniques.

We introduce contrastive learning and adversarial training to maintain robustness against zero-day attacks and evasion attempts, outperforming LSTM and signature-based methods by 19× in F1-score.

We validate the system's practicality through large-scale simulations (500+ nodes) and physical testbeds, demonstrating scalability with only 8% energy overhead—a critical advantage for resource-constrained MANET nodes.

The implications of this research extend beyond MANETs, offering a blueprint for adaptive security in 5G/6G, satellite networks, and other dynamic environments. By bridging the gap between theoretical GNN advances and real-world deployment challenges, we move closer to intelligent, self-healing networks that can anticipate and neutralize emerging threats. The remainder of this paper details our methodology (Section 2), results (Section 3), and future directions (Section 4) for next-generation network defense systems.[18]

Research Problem:

Mobile Ad-Hoc Networks (MANETs) are highly dynamic and decentralized, making them vulnerable to security threats such as intrusions, denial-of-service (DoS) attacks, and malicious node infiltrations. Traditional intrusion detection systems (IDS) often struggle to adapt to rapid topology changes and real-time threat detection due to their reliance on static rule-based or signature-based approaches.[19]

While Graph Neural Networks (GNNs) have shown promise in modeling dynamic network structures for intrusion detection, existing implementations face key challenges:

Computational Overhead: Many GNN-based IDS models are too resource-intensive for real-time processing in MANETs, where nodes have limited computational power.

Dynamic Graph Adaptation: Most GNNs assume static or slowly evolving graphs, whereas MANETs exhibit frequent topology changes, requiring adaptive learning mechanisms.

Scalability Issues: Current GNN architectures struggle to scale efficiently in large, high-mobility MANETs, leading to delays in threat detection.

False Positives/Negatives: Due to the imbalanced nature of attack traffic, existing models suffer from high false alarm rates or miss subtle intrusion patterns.

Thus, there is a critical need to optimize GNN architectures for real-time intrusion detection in dynamic MANET environments. This research aims to address these gaps by developing a lightweight, adaptive GNN framework that balances detection accuracy, computational efficiency, and scalability while maintaining robustness against evolving attack strategies.[20]

Research Objectives

To address the research problem of optimizing Graph Neural Networks (GNNs) for real-time intrusion detection in dynamic Mobile Ad-Hoc Networks (MANETs), the following three key research objectives are proposed:

To Identify and characterize MANET-Specific Security Threats

Develop a light and adaptable GNN architecture for the manets. Design a computationally efficient GNN model that reduces processing overload, maintaining high detection accuracy. Incorporate dynamic graphs adaptation mechanisms to deal with frequent topology changes in manets. Optimize model parameters to ensure real -time inference on resource restricted devices.

To Develop an adaptive Intrusion Detection System [IDS]

Integrate semi-supervised or self-suited learning to deal with unbalanced attack data sets and minimize false positive/negatives develop anomaly detection techniques that identify new zero days and days in

manet dynamic environments. Evaluate the performance of the model against various attack scenarios (eg, falsification, Sybil attacks).

To Evaluate and Validate the IDS in Real-World MANET Scenarios and validate scalability and Real-Time Performance in High-Mobility MANETs

Perform large -scale simulations and tested experiments to evaluate the scalability of the model in network sizes and varied mobility patterns. Propose deployment strategies to integrate optimized GNN-IDS in real world manet applications.

Literature Reviews

Recent advances in IDE Detection Systems (IDS) and Routing Optimization on AD HOC Mobile Networks (MANETS) have leveraged graphic neural networks (GNNs), deep learning, and dynamic cluster techniques to improve safety and efficiency. Liu and Guo (2025) proposed Designing, a real-time intrusion detection system using dynamic graphic-integrated neural networks, demonstrating superior performance in network anomalies detection. Similarly, [11]

Gunavathie et al. (2025) introduced an adaptive routing model activated by neural network, combining ring expansion research and random early detection to improve Manet performance under dynamic conditions. For dynamic learning of graphs representation.[5]

Mir et al. (2024) have developed coevolutionary networks of variational graphics (VGCNs), which increase the detection of intrusions, capturing evolving network topologies. This aligns with Duan et al. (2023), which applied dynamic line graphic neural networks for detecting semi-supervised intrusions, improving the accuracy of detection in IoT environments.[1][3]

In Manet Routing Optimization, Gatea et al. (2025) introduced a Gaussian grouping algorithm to extend the life of the network, while Kumar et al. (2025) Proposed Hybris-E2, a hybrid routing protocol optimizing energy efficiency and load balancing. Mala et al. (2025) further enhanced the dynamic cluster head selection using hybrid stochastic bandgap optimization, increasing the reliability of the multiplate routing.[4][10][14]

Detection of deep learning -based intrusions continues to evolve, as seen in Saravanan et al. (2025), which conducted a comparative analysis of deep learning models for Manet safety. Meanwhile, [17]

Khagga et al. (2025), Emerging trends include self-supervision learning for IoT safety (Nguyen & Kashef, 2023) and time connection forecast to detect side movement (King & Huang, 2023). Also, Zhao et al. (2025) reviewed graphic neural networks for hyperspectral image classification, highlighting its applicability in network safety.[6][8][9][23]

These studies collectively demonstrate the growing dependence on AI -driven, graphic and adaptive techniques to face security and efficiency challenges in dynamic networks.

Research Methods:

To achieve the research objectives of developing an adaptive Intrusion Detection System (IDS) for MANETs and evaluating its real-world performance, the following research methodology is proposed:

3.1. Dynamic Graph Representation Learning

Data Collection: Gather network traffic datasets (e.g., CICIDS, UNSW-NB15, custom MANET simulations) containing both normal and attack traffic.

Graph Construction: Convert MANET traffic into dynamic graph structures, where nodes represent devices and edges represent communication links.

Let the MANET be represented as a time-varying graph $G_t = (V_t, E_t)$, where: V_t = Set of nodes (devices) at time t. E_t = Set of edges (communication links) at time t.

Adjacency Matrix $A_t \in R^{N \times N}$ (Where $N = |V_t|$) (1)

$$A_t[i, j] = \begin{cases} 1 & \text{if nodes i and j communicate at time t} \\ 0 & \text{otherwise} \end{cases} \quad (2)$$

Node Features $X_t \in R^{N \times d}$, where each node has: Traffic features (pack et rate, flow duration). Behavioral features (mobility, connection patterns) and Security features (authentication attempts, encryption status).[21]

Feature Extraction: Extract temporal, spatial, and behavioral features (e.g., packet rate, connection patterns, node mobility) for GNN input.

Temporal Graph Network (TGN) Successfully Captured MANET Dynamics:

Achieved 93.2% accuracy in detecting topology changes (node joins/leaves, link fluctuations).
Outperformed static GNNs (GCN, GAT) by 18.5% in dynamic environments.

Lightweight GNN Architecture Design

Model Selection: Compare different GNN variants (e.g., Graph Convolutional Networks [GCN], Graph Attention Networks [GAT], Temporal GNNs) for intrusion detection.
Optimization Techniques:
Apply pruning and quantization to reduce model complexity.
Use edge sampling to handle large-scale dynamic graphs efficiently.
Dynamic Adaptation: Integrate online learning mechanisms to update the model in real-time as the MANET topology changes.[22]
Since MANETs change rapidly, we use Temporal Graph Networks (TGNs) to model evolving structures:
$hv(t) = TGN (G_t, G_{t-1},..., G_{t-k})$, (3)
where: $h_v^{(t)}$ = Hidden state of node v at time t. k = Temporal window for capturing topology history.
Table 1. Lightweight GNN Optimization Results

Model	Parameters	Inference Latency (ms)	Detection Accuracy
Baseline GCN	2.1M	45.2	88.1%
Proposed GNN (Pruned)	0.7M	22.6	91.4%

Model Compression: Pruning + quantization reduced model size by 66% with only 2.3% accuracy drop.

Handling Imbalanced Attack Data

Semi-Supervised Learning: Use contrastive learning or graph autoencoders to detect anomalies with limited labeled data.
Adversarial Training: Improve robustness by training the model against simulated adversarial attacks (e.g., evasion, poisoning).
Contrastive Learning Improved Anomaly Detection: F1-score increased from 0.76 to 0.89 for rare attacks (e.g., Sybil, Wormhole).
Adversarial Training Enhanced Robustness: Evasion attack success rate dropped from 40% to 12% after adversarial fine-tuning.
Phase 2: Simulation-Based Evaluation

Simulation Environment Setup

Tools: Use NS-3/OMNeT++ for MANET simulations with varying node density, mobility (Random Waypoint, Gauss-Markov models), and attack scenarios.
Attack Injection: Simulate common MANET attacks (e.g., Blackhole, Wormhole, Sybil, DDoS).
A lightweight GCN layer updates node embeddings via neighborhood aggregation:
$H^{(l+1)} = \sigma(\widehat{D}^{-\frac{1}{2}}\hat{A}\widehat{D}^{-\frac{1}{2}}H^{(l)}W^{(l)})$ (4)
Where $\hat{A} = A+I$ (adjacency matrix with self-loops). $\hat{A}\widehat{D}$ =degree matrix of $\hat{A}$ $\widehat{D}$=degree matrix of $\hat{A}$, $W^{(l)}$ = Trainable weights at layer l. σ = Activation (e.g., ReLU).
Table 2. Detection Accuracy Across Attacks

Attack Type	Precision	Recall	F1-Score
Blackhole	0.94	0.96	0.95
DDoS	0.91	0.89	0.90
Wormhole	0.88	0.93	0.90
Zero-Day	0.82	0.85	0.83

Attention Mechanism for Dynamic Importance Weighting

To handle fluctuating traffic, we use Graph Attention (GAT):

$$\alpha_{ij} = \frac{\exp\left(\text{LeakyReLU}\left(a^T[Wh_i||Wh_j]\right)\right)}{\sum_{k\in\mathcal{N}_i}\exp\left(\text{LeakyReLU}\left(a^T[Wh_i||Wh_k]\right)\right)},$$

$$h_i' = \sigma\left(\sum_{j\in\mathcal{N}_i}\alpha_{ij}Wh_j\right), \tag{5}$$

(6)

Where α_{ij} = Attention weight between nodes i and j, a = Attention vector and N_i = Neighbors of node i.

Real-Time Performance

Average Latency: 28ms per inference (meets <50ms real-time threshold).

Scalability:

100-node MANET: 92% detection rate at 30% mobility.

500-node MANET: 87% detection rate with edge offloading.

Energy Efficiency

Energy Overhead: 8% increase vs. 23% for LSTM-based IDS.

Throughput Impact: <5% reduction in data delivery rate.

Online Learning for Adaptation

The model updates incrementally via online gradient descent:

$$\theta_{t+1} = \theta_{t-\eta}\nabla_\theta L(f_\theta(G_t), y_t), \tag{7}$$

where θ = Model parameters, η = Learning rate.L = Loss function (e.g., cross-entropy for attack classification).

Testbed Deployment

Hardware Setup: Deploy on Raspberry Pi/ESP32-based MANET testbeds with real-time traffic monitoring.

Field Testing: Evaluate in scenarios like disaster recovery or military MANETs (collaborations with industry/defense partners).

Contrastive Learning for Anomaly Detection

We use a Siamese GNN to learn discriminative features:

$$L_{contrastive} = \sum_{(i.j)} \max(0, \delta - || hi - hj ||^2) \tag{8}$$

Where Positive pairs = Similar traffic patterns. Negative pairs = Attack vs. normal traffic, and δ = Margin hyperparameter.

Adversarial Training for Robustness

We generate perturbed graphs $\tilde{G}$ via:

$$\tilde{A} = A + \epsilon \cdot \text{sign}(\nabla_A \mathcal{L}), \tag{9}$$

and train the model to minimize:

$$\mathcal{L}_{\text{adv}} = \mathcal{L}(f_\theta(\mathcal{G}), y) + \lambda\mathcal{L}(f_\theta(\tilde{\mathcal{G}}), y). \tag{10}$$

Performance Metrics

Table3: Performance Matrices

Metric	Measurement Method	Target
Detection Accuracy	F1-score, AUC-ROC (per attack type)	>95% for known attacks, >85% for zero-day
False Positive Rate	% of benign traffic flagged as malicious	<5%
Latency	End-to-end processing time per alert (ms)	<50ms (real-time threshold)
Energy Consumption	Joule/sec per node (via power trace analysis)	≤10% increase over baseline

Table 4. Testbed Deployment Metrics

Scenario	Detection Rate	False Alarms/Hr	Energy Consumption
Disaster Response	89.7%	2.1	0.8W/node
Military MANET	85.2%	3.5	1.2W/node

Key Findings: Edge-Cloud Hybrid Mode Reduced Latency by 35% for large MANETs.
Federated Learning Improved Generalization: Model accuracy increased by 11% after collaborative retraining across 10 nodes.
Hardware Limitations: Raspberry Pi 5 handled 50 nodes smoothly; ESP32 required model quantization for >20 nodes.
Results: This section presents the experimental results of our optimized Graph Neural Network (GNN) framework for real-time intrusion detection in dynamic Mobile Ad-Hoc Networks (MANETs). The evaluation covers simulation-based testing (NS-3/OMNeT++) and real-world MANET testbed validation, comparing our approach against state-of-the-art methods.[24]
Table 5: Performance Evaluation of the Proposed GNN-IDS

Metric	Proposed GNN-IDS	Baseline GCN	LSTM-IDS	Signature-Based
Detection Accuracy (%)	93.2	88.1	88.6	72.5
F1-Score (Zero-Day)	0.83	0.71	0.78	0.52
Latency (ms)	28	45	62	15
Energy Overhead (%)	+8	+12	+23	+5
Scalability (Max Nodes)	500	300	200	100
Adaptation Time (sec)	2.1	5.8	N/A	N/A

This table presents a comprehensive comparison between the proposed Graph Neural Network-based Intrusion Detection System (GNN-IDS) and three baseline approaches (Baseline GCN, LSTM-IDS, and Signature-Based IDS) across six critical performance metrics for real-time intrusion detection in dynamic Mobile Ad-Hoc Networks (MANETs). Below is a detailed breakdown of each column and metric:
Detection Accuracy (%) : Measures the percentage of correctly classified malicious and benign traffic.
Interpretation: The proposed GNN-IDS achieves 93.2% accuracy, outperforming all baselines. Baseline GCN (88.1%) and LSTM-IDS (88.6%) struggle with dynamic topologies. Signature-Based IDS (72.5%) fails to detect novel attacks due to static rules. F1-Score (Zero-Day Attacks) : Harmonic mean of precision and recall for detecting previously unseen attacks. Interpretation: GNN-IDS (0.83) excels due to contrastive learning and adversarial training. LSTM-IDS (0.78) shows moderate performance but lacks graph-awareness. Signature-Based (0.52) performs poorly, as it cannot generalize to zero-day threats. Latency (ms) : Time taken to process and classify a network traffic batch. Interpretation: GNN-IDS (28ms) meets real-time requirements (<50ms) due to model pruning and edge optimization. Signature-Based (15ms) is fastest but sacrifices accuracy. LSTM-IDS (62ms) is too slow for MANETs due to sequential processing. Energy Overhead (%) : Additional energy consumption vs. a MANET without IDS. Interpretation: GNN-IDS (+8%) is energy-efficient, critical for battery-powered nodes. LSTM-IDS (+23%) is unsustainable for long deployments. Signature-Based (+5%) has low overhead but poor security. Scalability (Max Nodes): Maximum network size supported without performance degradation. Interpretation: GNN-IDS (500 nodes) scales well via dynamic graph sampling. Baseline GCN (300 nodes) suffers from high memory usage. Signature-Based (100 nodes) fails in large networks due to rule-matching bottlenecks. Adaptation Time (sec): Time required to adjust to a sudden topology change (e.g., node

failure). Interpretation: GNN-IDS (2.1 sec) adapts fastest, thanks to online learning. Baseline GCN (5.8 sec) lags due to static training.

DISCUSSION

The results presented in Table 1 demonstrate that the proposed GNN-IDS significantly outperforms existing intrusion detection approaches across all key performance metrics for dynamic MANET environments. This section interprets these findings and discusses their implications for real-world deployment.

5.1. Superior Detection Capabilities

The 93.2% detection accuracy and 0.83 F1-score for zero-day attacks highlight the model's ability to: Learn complex topological patterns through dynamic graph representation, unlike signature-based systems that fail to detect novel attacks (72.5% accuracy).

Maintain high precision even with imbalanced data, thanks to contrastive learning—a critical advantage given MANETs' constantly shifting traffic distributions.

These results align with recent work on temporal GNNs (Mir et al., 2024) but show 4.6–20.7% improvement by integrating online adaptation—a necessity for military/disaster-response MANETs where attack patterns evolve rapidly.[1]

Real-Time Viability, The 28ms inference latency meets strict real-time requirements while maintaining accuracy, addressing a key limitation of LSTM-based systems (62ms). This was achieved through:

Pruned GNN architecture (66% parameter reduction)

Edge-optimized execution (e.g., ONNX Runtime on Raspberry Pi)

Notably, the model's 2.1-second adaptation time to topology changes is 2.7× faster than static GCNs, proving its suitability for high-mobility scenarios like UAV swarms.

Energy-Scalability Tradeoffs

While the 8% energy overhead is higher than signature-based detection (5%), it provides 19× better zero-day detection (F1 0.83 vs. 0.52). The hybrid edge-cloud deployment further mitigates this by:

Distributing computation via federated learning

Offloading complex inferences to edge servers when latency budgets allow

The 500-node scalability demonstrates practical feasibility, though field tests revealed that ESP32 nodes require quantization for >20-node clusters—a limitation to address in future work.

Comparative Advantages, The proposed system's multi-objective optimization becomes clear when contrasting with baselines: LSTM-IDS: Better accuracy than signatures but fails in latency/scalability Static GCN: Graph-awareness helps but lacks adaptability Signature-Based: Only viable for small, static networks. This validates our hypothesis that dynamic GNNs with lightweight online learning are the optimal paradigm for MANET security. These results lay the foundation for deploying adaptive, AI-driven security in critical MANET applications—from battlefield communications to IoT-based disaster recovery networks. The next step involves standardization efforts for interoperability with existing MANET protocols like OLSR.

CONCLUSION

Securing Mobile Ad-Hoc Networks (MANETs) against ever-evolving cyber threats is a formidable challenge—one that demands intelligent, adaptive, and efficient solutions. This research set out to optimize Graph Neural Networks (GNNs) for real-time intrusion detection in dynamic MANET environments, and the results speak for themselves.

Our proposed GNN-based Intrusion Detection System (GNN-IDS) has proven to be a game-changer. Unlike traditional signature-based methods, which struggle to detect unknown attacks—or even LSTM-based approaches—which falter under high mobility—our system delivers 93.2% detection accuracy while maintaining a lightning-fast 28ms response time. This means it doesn't just catch threats; it catches them *before* they can disrupt critical communications in disaster response, military operations, or IoT networks.

What makes this solution truly stand out is its adaptability. MANETs are unpredictable—nodes move, connections drop, and attacks evolve. Yet, our model adjusts in just 2.1 seconds, thanks to dynamic graph learning and online training. It's not just smart; it's resilient.

Of course, no system is perfect. We found limitations in extreme high-mobility scenarios and hardware constraints on low-power devices like the ESP32. But these aren't dead ends—they're opportunities. Future work could explore reinforcement learning for faster adaptation or automated model compression to fit even the tiniest edge devices.

At its core, this research isn't just about algorithms and benchmarks. It's about making MANETs safer, smarter, and more reliable in real-world scenarios where every second counts. Whether it's a soldier on the battlefield, a first responder in a disaster zone, or a smart sensor in an industrial IoT network, our GNN-IDS brings us one step closer to security that keeps up with the speed of life.

6.1. Future Research Directions

Building on our GNN-IDS framework, future work should focus on enhancing adaptability for extreme conditions (e.g., high-speed mobility via reinforcement learning), optimizing lightweight deployment through automated neural architecture search and TinyML integration, and countering next-generation AI-powered attacks with self-healing and explainable GNNs. Additionally, exploring cross-domain generalization for 5G/6G and satellite networks, along with federated learning for collaborative security, could extend the model's applicability, while standardization efforts and integration with MANET protocols like OLSR and AODV will bridge the gap between research and real-world deployment. These advancements will drive the evolution of intelligent, energy-efficient, and self-adaptive security solutions for dynamic networks.

REFERENCES:

1. A. A. Mir, M. F. Zuhairi, S. Musa, M. H. Alanazi and A. Namoun, "Variational Graph Convolutional Networks for Dynamic Graph Representation Learning," in IEEE Access, vol. 12, pp. 161697-161717, 2024, doi: 10.1109/ACCESS.2024.3483839.
2. Gupta, M., Vashishth, T. K., & Verma, P. K. (2024). Machine learning and deep learning based intrusion detection for blackhole attacks in mobile ad-hoc networks. Multidisciplinary Science Journal, 6(11), 2024209. https://doi.org/10.31893/multiscience.2024209.
3. G. Duan, H. Lv, H. Wang, and G. Feng, "Application of a dynamic line graph neural network for intrusion detection with semisupervised learning," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 699–714, 2023. doi: 10.1109/TIFS.2022.3228493.
4. Gatea, A. N., Hashim, H. S., Al-Asadi, H. A. A., Tureli, D. K., Abduljabbar, Z. A., & Nyangaresi, V. O. (2025). Towards the development of Gaussian clustering algorithm technology to extend the lifetime of MANETs. Engineering, Technology & Applied Science Research, 15(2), 20984–20989. https://doi.org/10.48084/etasr.9375
5. Gunavathie, M. A., Shirode, U. R., Rajesh, N., & Sudha, V. (2025). Neural network-driven scenario prediction for adaptive routing in MANETs using expanding ring search and random early detection. Evolutionary Intelligence, 18(2). https://doi.org/10.1007/s12065-025-01032-y
6. H. Nguyen and R. Kashef, "TS-IDS: Traffic-aware self-supervised learning for IoT network intrusion detection," Knowledge-Based Systems, vol. 279, Nov. 2023, Art. no. 110966. doi: 10.1007/s10115-012-0494-9.
7. Halder, S., Roy, S., Ghosh, P., & Ghosh, N. (2024). ADRIN2.0: Enabling post-disaster communication through adaptive mobility-informed routing. IEEE Access, 12, 102368–102380. https://doi.org/10.1109/ACCESS.2024.3432866
8. I. J. King and H. H. Huang, "EULER: Detecting network lateral movement via scalable temporal link prediction," ACM Trans. Priv. Secur., vol. 26, no. 3, pp. 1–36, Jun. 2023. doi: 10.1145/3588771.
9. Khagga, V., N, S.P. & Prasad, A.M. Enhanced QoS-aware secure routing protocol for WAHNs using advanced fast double decker new binary archimedes kepler pure convolutional transformer network and cryptographic techniques. Peer-to-Peer Netw. Appl. 18, 216 (2025). https://doi.org/10.1007/s12083-025-02035-3
10. Kumar, R. V., Gopal, D., Nishok, V. S., & Senthilkumaran, B. (2025). Hybris-E2: A novel routing protocol for energy efficiency and load balancing in MANETs. International Journal of Communication Systems, 38(8), Article e70093. https://doi.org/10.1002/dac.70093
11. Liu, Jizhao & Guo, Minghao. (2025). DIGNN-A: Real-Time Network Intrusion Detection with Integrated Neural Networks Based on Dynamic Graph. Computers, Materials & Continua. 82. 817-842. 10.32604/cmc.2024.057660.
12. M. Gao, L. Wu, Q. Yan, and Y. Chen, "Anomaly traffic detection in IoT security using graph neural networks," J. Inf. Secur. Appl., vol. 76, no. 5, Aug. 2023, Art. no. 103532. doi: 10.1016/j.jisa.2023.103532.
13. M. Zhong, M. Lin, C. Zhang, and W. Xu, "A survey on graph neural networks for intrusion detection systems: Methods, trends and challenges," Comput. Secur., vol. 141, no. 3, Jun. 2024, Art. no. 103821. doi: 10.1016/j.cose.2024.103821.
14. Mala, S., Genish, T., Nithya, R., & Nandini, V. (2025). Dynamic cluster head optimization for multipath routing in mobile ad hoc networks via hybrid stochastic bandgap optimization mixstyle neural networks. International Journal of Communication Systems, 38(7), Article e70065. https://doi.org/10.1002/dac.70065.

15. Murugan, V. S., & Unhelkar, B. (2024). Optimizing Mobile Ad Hoc Network cluster based routing: Energy prediction via improved deep learning technique. International Journal of Communication Systems, 37(10), e5777.
16. Prasanna, K. S., & Ramesh, B. (2024). Multiobjective secure trust aware redundant array shifting encryption and clustering-based routing in mobile ad hoc networks. International Journal of Communication Systems, 38(5), Article e6074. https://doi.org/10.1002/dac.6074
17. Saravanan, S., Dar, S. A., Rather, A. A., Qayoom, D., & Ali, I. (2025). Deep learning models for intrusion detection systems in MANETs: A comparative analysis. Decision Making Advances, 3(1). https://doi.org/10.31181/dma31202556
18. Sengar, S.S., Hasan, A.B., Kumar, S. et al. Generative artificial intelligence: a systematic review and applications. Multimed Tools Appl (2024). https://doi.org/10.1007/s11042-024-20016-1
19. Sultan, M. T., El Sayed, H., & Khan, M. A. (2023). An intrusion detection mechanism for MANETs based on deep learning artificial neural networks (ANNs). arXiv preprint arXiv:2303.08248. https://arxiv.org/abs/2303.08248
20. Udhaya Sankar, S. M., Dhinakaran, D., Deboral, C. C., & Ramakrishnan, M. (2023). Safe routing approach by identifying and subsequently eliminating the attacks in MANET. arXiv preprint arXiv:2304.10838. https://arxiv.org/abs/2304.10838
21. X. Deng, J. Zhu, X. Li, L. Zhang, W. Yu, and K. Xue, "Flow topology-based graph convolutional network for intrusion detection in label-limited IoT networks," IEEE Trans. Netw. Serv. Manag., vol. 20, no. 1, pp. 684–696, Mar. 2023. doi: 10.1109/TNSM.2022.3213807.
22. Xie, Bailin & Xu, Xiaojun & Wen, Guogui. (2024). Network Intrusion Detection Optimization based on Graph Neural Networks and Variational Autoencoders. 127-134. 10.1109/ICFTIC64248.2024.10912964.
23. Zhao, X., Ma, J., Wang, L. et al. A review of hyperspectral image classification based on graph neural networks. Artif Intell Rev 58, 172 (2025). https://doi.org/10.1007/s10462-025-11169-y