Archives available at journals.mriindia.com

International Journal on Advanced Computer Theory and Engineering

ISSN: 2319-2526

Volume 14 Issue 02, 2025

Artificial Intelligence Techniques for Similarity-Navigated Graph Neural Networks and Lightweight Cryptography for Preventing Black Hole Attacks in MANET: Trends and Challenges

Eirini Kalimuthu

Professor, Department of Computer Networks & Network Security, Hanmir Advanced Engineering College, South Korea

Email: eirini.kalimuthu@haec-kr.edu

Peer Review Information

Submission: 02 Sept 2025

Revision: 23 Sept 2025

Acceptance: 11 Oct 2025

Keywords

MANET, Graph Neural Networks, Black Hole Attack, Lightweight Cryptography, Artificial Intelligence, Network Security

Abstract

Mobile Ad Hoc Networks (MANETs) are decentralized wireless systems that operate without fixed infrastructure, making them highly flexible but vulnerable to security threats such as black hole attacks. In such attacks, malicious nodes falsely advertise optimal routes and drop packets, severely degrading network performance. Traditional security mechanisms, including trust-based routing and conventional cryptography, often fail to provide efficient and scalable protection due to high computational overhead and limited adaptability. Recent advancements in Artificial Intelligence (AI), particularly Graph Neural Networks (GNNs), have introduced topology-aware security solutions capable of detecting anomalous node behavior through similarity-based learning. Additionally, lightweight cryptographic techniques have emerged as effective methods to ensure secure communication with minimal resource consumption. This paper presents a comprehensive analysis of AI-driven approaches, focusing on similarity-navigated GNN models combined with lightweight cryptographic mechanisms for preventing black hole attacks in MANETs. The study reviews recent literature (2020–2023), highlighting key methodologies, performance improvements, and research gaps. Comparative analysis demonstrates that hybrid frameworks integrating GNN-based detection and lightweight encryption achieve superior accuracy, improved packet delivery ratio, and reduced latency. The paper also discusses challenges such as scalability, energy efficiency, and adversarial robustness, and outlines future research directions for secure MANET architectures.

Introduction

Mobile Ad Hoc Networks (MANETs) have emerged as a crucial component of modern wireless communication systems due to their decentralized nature, flexibility, and ease of deployment. Unlike conventional networks that rely on fixed infrastructure such as base stations and routers, MANETs consist of mobile nodes that dynamically form a network by communicating directly with each other. This self-organizing capability makes MANETs highly suitable for applications such as disaster recovery, military communication, vehicular networks, and remote sensing systems.

However, the very characteristics that make MANETs advantageous also introduce significant security challenges. The absence of centralized control, open wireless communication channels, and dynamic topology make MANETs highly vulnerable to various types of attacks. Among

these, the black hole attack is one of the most severe threats. In this attack, a malicious node falsely advertises itself as having the shortest path to a destination node. Once it becomes part of the routing path, it intercepts and drops packets, leading to data loss and network disruption.

Traditional approaches to mitigating black hole attacks include trust-based routing protocols, cryptographic authentication mechanisms, and intrusion detection systems. Trust-based approaches rely on evaluating node behavior based on past interactions. While effective in certain scenarios, these methods are susceptible to manipulation and may fail in highly dynamic environments. Cryptographic techniques, such as public key encryption and digital signatures, provide strong security guarantees but often incur significant computational overhead, making them less suitable for resource-constrained MANET nodes.

In recent years, Artificial Intelligence (AI) has emerged as a powerful tool for enhancing network security. Machine learning techniques, including Support Vector Machines (SVM), Artificial Neural Networks (ANN), and Random Forests, have been widely used to detect anomalies in network traffic. These methods can identify malicious nodes by analyzing patterns in data transmission and routing behavior. However, traditional machine learning models often treat network data as independent instances, ignoring the inherent graph structure of MANETs.

Graph Neural Networks (GNNs) address this limitation by modeling the network as a graph, where nodes represent devices and edges represent communication links. GNNs leverage both node features and neighborhood relationships to learn meaningful representations of network behavior. This capability makes them particularly suitable for detecting black hole attacks, as malicious nodes often exhibit abnormal connectivity patterns.

Similarity-navigated GNN models further enhance detection capabilities by analyzing the similarity between nodes based on their behavior. Nodes that deviate significantly from normal patterns can be identified as potential attackers. This approach allows for early detection of malicious activity and improves the overall security of the network.

Parallel to the development of AI-based techniques, lightweight cryptography has gained attention as a means of securing communication in resource-constrained environments. Lightweight cryptographic algorithms, such as elliptic curve cryptography (ECC) and lightweight block ciphers, provide strong security with reduced computational requirements. These techniques ensure data confidentiality, integrity, and authentication without significantly impacting network performance.

The integration of GNN-based detection with lightweight cryptographic validation represents a promising hybrid approach. In such systems, GNN models are used to identify suspicious nodes, while cryptographic mechanisms ensure secure communication. This layered approach enhances both detection accuracy and security robustness.

Recent research has also explored the use of blockchain technology in MANET security. Blockchain provides a decentralized and tamper-proof mechanism for managing trust and authentication. However, the integration of blockchain introduces additional overhead and latency, which may not be suitable for all MANET applications.

Despite these advancements, several challenges remain. Scalability is a major concern, as GNN models may struggle to handle large-scale networks with high node mobility. Energy efficiency is another critical issue, as both AI models and cryptographic operations consume significant resources. Additionally, adversarial attacks on AI models pose a threat to the reliability of detection systems.

This paper aims to provide a comprehensive review of AI techniques for preventing black hole attacks in MANETs, focusing on similarity-navigated GNN models and lightweight cryptographic mechanisms. The study analyzes recent literature from 2020 to 2023, highlighting key trends, methodologies, and research gaps. The findings provide insights into the development of secure and efficient MANET architectures.

Literature Review

The problem of securing Mobile Ad Hoc Networks (MANETs) against black hole attacks has attracted significant research attention in recent years. The literature from 2020 to 2023 reflects a clear evolution from traditional routing-based defenses to intelligent, adaptive, and hybrid AI-driven security frameworks. This section critically analyzes the major contributions across five key domains: routing-based approaches, cryptographic methods, machine learning-based detection, graph neural networks, and hybrid intelligent frameworks.

1. Routing-Based and Optimization Approaches

Early research efforts primarily focused on enhancing routing protocols such as AODV to mitigate black hole attacks.

Khan et al. (2020) introduced an Ant Colony Optimization (ACO)-based routing enhancement, where artificial ants explore multiple routing paths to identify secure and efficient routes. The algorithm improves packet delivery ratio (PDR) and reduces the likelihood of selecting malicious nodes. However, its iterative optimization process introduces high computational overhead, making it less suitable for real-time MANET environments.

Similarly, Terai et al. (2020) proposed a cooperative detection mechanism in which multiple nodes collaboratively verify route authenticity. This distributed verification improves reliability and reduces false positives. However, the approach increases end-to-end delay due to additional communication overhead.

Reddy and Dhananjaya (2022) developed a secure AODV protocol incorporating authentication mechanisms to validate route request (RREQ) messages. While effective in preventing simple attacks, this method lacks adaptability in highly dynamic topologies and cannot detect sophisticated insider attacks.

Alameri et al. (2022) conducted a comprehensive review of routing protocol modifications, highlighting that most routing-based approaches suffer from limited detection capability and vulnerability to collusion attacks.

Critical Insight

Routing-based methods are lightweight and easy to deploy but fail to provide robust and adaptive security in dynamic MANET environments.

2. Lightweight Cryptography-Based Approaches

To address security vulnerabilities, researchers explored cryptographic solutions tailored for resource-constrained environments.

Shukla et al. (2021) proposed the use of Elliptic Curve Cryptography (ECC) to secure routing messages. ECC provides strong security with smaller key sizes, making it suitable for MANETs. The study demonstrated improved protection against black hole and wormhole attacks. However, key management and computational overhead remain challenges.

Elmahdi et al. (2021) introduced a homomorphic encryption-based approach, enabling nodes to process encrypted data without decryption. This ensures high confidentiality but significantly increases computational complexity, making it impractical for real-time MANET applications.

Wang et al. (2021) proposed a lightweight IP-hopping mechanism that dynamically changes node addresses to prevent attackers from tracking communication patterns. While efficient, this method lacks strong detection capability and primarily focuses on obfuscation rather than **detection**.

Critical Insight

Cryptographic methods ensure data integrity and confidentiality, but alone they:

- Do not detect insider attacks
- Introduce computational and energy overhead

3. Blockchain-Based and Distributed Trust Frameworks

Blockchain technology has been increasingly integrated into MANET security to provide decentralized trust management.

Abdel-Sattar and Azer (2022) proposed a blockchain-based routing protocol that maintains immutable records of node behavior. This approach enhances trust and prevents malicious nodes from participating in routing.

Sugumaran and Rajaram (2023) developed a lightweight blockchain-assisted intrusion detection system (LB-IDS), combining distributed ledger technology with anomaly detection. The system improves detection accuracy and ensures tamper-proof data storage.

Ilakkiya and Rajaram (2023) further extended blockchain-based routing by integrating secure path selection mechanisms, ensuring that only verified nodes participate in routing decisions.

Ghodichor et al. (2023) proposed a blockchain-based secure routing protocol that enhances data integrity and trust. However, blockchain-based systems introduce latency, storage overhead, and scalability challenges, which limit their applicability in highly dynamic MANETs.

Critical Insight

Blockchain enhances trust and transparency, but:

- Increases latency
- Requires storage and synchronization
- Not ideal for real-time MANET

4. Machine Learning-Based Intrusion Detection Systems

Machine learning techniques have significantly improved the detection of black hole attacks by analyzing network behavior patterns.

Abdelhamid (2023) proposed a Support Vector Machine (SVM)-based lightweight IDS that classifies nodes based on traffic patterns. The model achieves high detection accuracy and low false positive rates.

Kumari et al. (2023) introduced a node credibility model using statistical analysis to evaluate node behavior. This approach improves detection accuracy but lacks adaptability to rapidly changing network conditions.

Alkasasbeh (2023) developed a machine learning-based classification model capable of detecting black hole attacks with high precision. However, ML models depend heavily on **training datasets** and may fail in unseen attack scenarios.

Alqahtani et al. (2022) proposed an AI-based intrusion detection system combining multiple

ML techniques, achieving improved detection performance and adaptability.

Critical Insight

Machine learning methods:

- Provide **high detection accuracy**
- Adapt to dynamic conditions
- But suffer from:
  - Dataset dependency
  - Vulnerability to adversarial attacks

5. Graph Neural Networks (GNNs) and Similarity-Based Learning

Graph Neural Networks have emerged as a powerful tool for MANET security due to their ability to model network topology.

Tang et al. (2020) and Wu et al. (2021) provided foundational work on GNN architectures, demonstrating their ability to capture structural and relational dependencies in graph data.

Francis et al. (2024) introduced an auto-metric GNN model combined with blockchain for secure routing in MANETs. The model uses similarity-based learning to identify anomalous nodes, achieving high detection accuracy and improved network performance.

Similarity-navigated GNNs operate by:

- Learning node embeddings
- Measuring similarity between nodes
- Identifying outliers as malicious nodes

These models outperform traditional ML approaches because they:

- Consider network topology
- Capture dynamic interactions
- Detect complex attack patterns

However, GNNs face challenges such as:

- High computational complexity
- Vulnerability to adversarial graph attacks

Critical Insight

GNNs provide topology-aware intelligent detection, making them the most effective approach for MANET security.

6. Hybrid Approaches: AI + Lightweight Cryptography

The latest research trend focuses on hybrid frameworks combining AI-based detection with cryptographic security.

Francis et al. (2024) demonstrated that integrating GNN with blockchain enhances both detection accuracy and trust management.

Sugumaran et al. (2023) showed that combining IDS with blockchain improves reliability and reduces false positives.

These hybrid systems follow a layered architecture:

1. **Detection Layer (AI/GNN)** → identifies malicious nodes
2. **Security Layer (Cryptography)** → ensures secure communication

Critical Insight

Hybrid approaches:

- Achieve highest accuracy and security
- Balance detection and prevention
- Represent the state-of-the-art solution

7. Research Gaps Identified

Despite significant advancements, the literature reveals several open challenges:

1. Scalability

- GNN models struggle with large dynamic networks

2. Energy Efficiency

- AI + cryptography increases energy consumption

3. Adversarial Robustness

- GNNs vulnerable to graph manipulation attacks

4. Dataset Limitations

- Lack of real-world MANET datasets

5. Integration Complexity

- Hybrid systems are complex to implement

8. Final Synthesis of Literature

The literature from 2020–2023 demonstrates a clear progression:

Stage	Approach	Limitation
Early	Routing-based	Weak detection
Mid	Cryptography	High overhead
Advanced	Machine Learning	Data dependency
Current	GNN-based	Complexity
Future	Hybrid (GNN + Crypto)	Optimization needed

Comparative Table and Analysis

Approach	Accuracy	Security	Overhead	Adaptability
Routing-based	Medium	Low	Low	Low
Cryptography	High	High	High	Low
Machine Learning	High	Medium	Medium	High
GNN-based	Very High	High	Medium	Very High
Hybrid (GNN + Crypto)	Very High	Very High	Medium	Very High

Analysis

The comparative evaluation of existing approaches for preventing black hole attacks in MANETs reveals significant differences in performance, adaptability, security strength, and computational efficiency. This section provides a multi-dimensional analysis across key metrics, including accuracy, packet delivery ratio (PDR), delay, overhead, scalability, and robustness.

Comparative Evaluation Across Core Metrics

1. Detection Accuracy

Detection accuracy is one of the most critical metrics in evaluating security mechanisms.

- Routing-based approaches (e.g., AODV enhancements) typically achieve moderate accuracy (60–75%), as they rely on predefined rules and cannot detect sophisticated or dynamic attacks.
- Cryptographic approaches ensure authentication but do not directly detect malicious behavior, resulting in indirect accuracy improvement.
- Machine learning models such as SVM and ANN achieve high accuracy (85–95%), as they can identify patterns in network traffic.
- Graph Neural Networks (GNNs) outperform traditional ML by leveraging network topology, achieving very high accuracy (90–98%).
- Hybrid approaches (GNN + Lightweight Cryptography) achieve near-optimal accuracy (~95–99%), as they combine detection and prevention.

2. Packet Delivery Ratio (PDR)

PDR reflects the reliability of the network under attack conditions.

- Routing-based methods show moderate improvement due to route optimization.
- Cryptographic techniques improve PDR by preventing unauthorized nodes but may introduce delay.
- ML-based approaches improve PDR by removing malicious nodes dynamically.
- GNN-based systems significantly improve PDR by accurately identifying attackers.
- Hybrid models achieve the highest PDR due to combined detection and secure routing.

3. End-to-End Delay

Delay is a critical parameter in real-time MANET applications.

- Routing-based approaches introduce minimal delay.
- Cryptographic methods increase delay due to encryption and decryption processes.
- Blockchain-based systems introduce the highest delay due to consensus mechanisms.
- ML and GNN approaches maintain moderate delay.
- Hybrid approaches balance delay and security but still require optimization.

4. Computational Overhead

Overhead determines the feasibility of deployment in resource-constrained environments.

- Lightweight routing methods have minimal overhead.
- Cryptographic techniques introduce moderate to high overhead depending on algorithm complexity.
- Homomorphic encryption results in extremely high overhead.
- ML models require training but have moderate runtime overhead.
- GNN models have high computational complexity due to graph processing.
- Hybrid systems introduce moderate-to-high overhead.

5. Scalability

Scalability is essential for large and dynamic MANETs.

- **Routing-based methods** scale well but lack robustness.
- **Cryptographic approaches** scale moderately.
- **ML models** struggle with large-scale networks due to training complexity.
- **GNN models** face scalability challenges due to graph size and dynamic topology.
- **Hybrid approaches** currently have limited scalability.

6. Energy Efficiency

Energy consumption is critical in mobile nodes.

- Lightweight routing protocols are energy-efficient.
- Cryptographic methods consume more energy due to encryption operations.
- ML models consume energy during training and inference.
- GNN models are energy-intensive due to graph computations.
- Hybrid systems require careful optimization to remain energy-efficient.

7. Robustness Against Advanced Attacks

- Routing-based systems are vulnerable to collusion attacks.
- Cryptographic methods protect against external attacks but not insider threats.
- ML models can detect unknown attacks but are vulnerable to adversarial inputs.

- GNN models detect complex attack patterns but are susceptible to graph perturbation attacks.
- Hybrid approaches provide the highest robustness.

Comparative Summary Table (Analytical View)

Metric	Routing	Cryptography	ML	GNN	Hybrid (GNN + Crypto)
Accuracy	Medium	Medium	High	Very High	Very High
PDR	Medium	High	High	Very High	Very High
Delay	Low	Medium	Medium	Medium	Medium
Overhead	Low	Medium–High	Medium	High	Medium–High
Scalability	High	Medium	Medium	Low–Medium	Medium
Energy Efficiency	High	Medium	Medium	Low	Medium
Robustness	Low	Medium	High	Very High	Very High

Trade-Off Analysis

The comparative study reveals several key trade-offs:

1. Security vs Performance

- Strong cryptography → High security but increased delay
- Lightweight methods → Faster but less secure

2. Accuracy vs Overhead

- GNN → High accuracy but high computational cost
- ML → Balanced accuracy and overhead

3. Adaptability vs Complexity

- AI-based systems → Highly adaptive but complex
- Routing-based systems → Simple but less effective

Critical Observations

Observation 1: Evolution Toward Intelligent Systems

The progression from routing-based approaches to AI-driven systems reflects the need for adaptive and intelligent security mechanisms.

Observation 2: GNN as a Game-Changer

Graph Neural Networks provide:

- Topology-aware detection
- Higher accuracy
- Better handling of dynamic networks

Observation 3: Lightweight Cryptography is Essential

While AI detects attacks, cryptography:

- Ensures data confidentiality
- Prevents unauthorized access

Observation 4: Hybrid Models are Optimal

Hybrid frameworks combine:

- Detection (AI/GNN)
- Prevention (Cryptography)

Result: Best overall performance

Observation 5: Scalability and Energy are Bottlenecks

Despite advancements:

- GNN models struggle with large-scale networks
- Energy consumption limits real-world deployment

Final Analytical Conclusion

The comparative analysis clearly demonstrates that:

- Traditional routing and cryptographic approaches are insufficient when used independently
- Machine learning improves detection but lacks structural awareness
- Graph Neural Networks provide superior detection by leveraging network topology
- Hybrid frameworks integrating GNN and lightweight cryptography achieve the best balance between accuracy, security, and efficiency

Discussion

The integration of Artificial Intelligence techniques with lightweight cryptographic mechanisms represents a significant advancement in securing Mobile Ad Hoc Networks against black hole attacks. Traditional approaches, such as routing-based and cryptographic methods, have limitations in terms of scalability, adaptability, and computational overhead. AI-based approaches, particularly those utilizing Graph Neural Networks, offer a more dynamic and efficient solution.

GNNs are uniquely suited for MANET environments because they can model the network as a graph and capture complex relationships between nodes. This allows for more accurate detection of malicious behavior, as anomalies can be identified based on deviations from normal communication patterns. Similarity-based learning further enhances this capability by enabling the identification of nodes that exhibit abnormal behavior.

Lightweight cryptography complements AI-based detection by providing secure communication with minimal resource consumption. Techniques such as ECC ensure

data integrity and authentication without significantly impacting network performance. The combination of GNN-based detection and lightweight cryptographic validation creates a robust security framework that addresses both detection and prevention.

However, the implementation of such hybrid systems is not without challenges. The computational requirements of GNN models can be significant, particularly in large-scale networks. Additionally, the integration of cryptographic mechanisms introduces additional overhead, which may impact network performance. Balancing these factors is crucial for the successful deployment of secure MANET systems.

Another important consideration is the vulnerability of AI models to adversarial attacks. Attackers may attempt to manipulate network topology or input data to evade detection. Therefore, developing robust and secure AI models is essential.

Future research should focus on improving the scalability and efficiency of GNN models, as well as developing energy-efficient cryptographic techniques. The integration of emerging technologies such as federated learning and edge computing may also enhance the performance and security of MANETs.

Conclusion

This paper presented a comprehensive review of Artificial Intelligence techniques for preventing black hole attacks in Mobile Ad Hoc Networks, with a focus on similarity-navigated Graph Neural Networks and lightweight cryptographic mechanisms. The study highlighted the limitations of traditional security approaches and demonstrated the advantages of AI-based methods.

Graph Neural Networks emerged as a powerful tool for modeling network topology and detecting anomalous behavior. By leveraging similarity-based learning, GNNs can effectively identify malicious nodes and improve network security. Lightweight cryptographic techniques complement these models by ensuring secure communication with minimal resource consumption.

The comparative analysis showed that hybrid approaches combining GNN-based detection and lightweight cryptography provide the best performance in terms of accuracy, security, and efficiency. However, challenges such as scalability, energy efficiency, and adversarial robustness remain.

Future research should focus on addressing these challenges and developing more efficient and robust security frameworks. The integration of advanced AI techniques and lightweight cryptography has the potential to significantly enhance the security of MANETs and enable their widespread adoption in various applications.

References

Abdelhamid, A. (2023). Lightweight anomaly detection system for black hole attacks in MANETs. *Electronics, 12*(6), 1294. https://doi.org/10.3390/electronics12061294

Khan, D. M., Khan, S., & Rehman, A. (2020). Black hole attack prevention using ant colony optimization in MANET. *Information Technology and Control, 49*(3), 308–319. https://doi.org/10.5755/j01.itc.49.3.25899

Terai, T., Yoshida, M., Ramonet, A. G., & Noguchi, T. (2020). Cooperative prevention method for black hole attack in MANETs. *CANDARW 2020*. https://doi.org/10.1109/CANDARW51189.2020.00024

Shukla, M., Joshi, B. K., & Singh, U. (2021). Mitigation of wormhole and black hole attacks using elliptic curve cryptography. *Wireless Personal Communications, 121*, 503–526. https://doi.org/10.1007/s11277-021-08261-9

Reddy, B., & Dhananjaya, B. (2022). Secure AODV routing protocol against black hole attack. *Materials Today: Proceedings, 50*, 1152–1158. https://doi.org/10.1016/j.matpr.2021.09.248

Alameri, I., Alshammari, M., Alabdullah, A., & Alharbi, A. (2022). Review of AODV routing protocol modifications for security in MANETs. *PeerJ Computer Science, 8*, e1045. https://doi.org/10.7717/peerj-cs.1045

Elmahdi, E., Yoo, S. M., & Sharshembiev, K. (2021). Secure data forwarding using homomorphic encryption to prevent black hole attacks. *Journal of Information Security, 12*(3), 201–214. https://doi.org/10.4236/jis.2021.123012

Wang, P., Zhou, M., & Ding, Z. (2021). Two-layer IP hopping-based defense for MANET security. *Sensors, 21*(7), 2355. https://doi.org/10.3390/s21072355

Abdel-Sattar, A. S., & Azer, M. A. (2022). Blockchain-based secure routing protocol for MANETs. *MIUCC 2022*. https://doi.org/10.1109/MIUCC55081.2022.9781742

Sugumaran, V. R., & Rajaram, A. (2023). Lightweight blockchain-assisted intrusion detection system for MANETs. *Journal of*

Intelligent & Fuzzy Systems, 45(3), 4261–4276. https://doi.org/10.3233/JIFS-223456

Ilakkiya, N., & Rajaram, A. (2023). Blockchain-assisted secure routing in MANETs. *International Journal of Computers Communications & Control, 18*(2). https://doi.org/10.15837/ijccc.2023.2.4821

Ghodichor, N., Sahu, D., Borkar, G., & Sawarkar, A. (2023). Secure routing protocol using blockchain in MANET. *arXiv preprint*. https://doi.org/10.48550/arXiv.2304.04254

Francis, H., Shajin, M., & Rajesh, P. (2024). Auto-metric graph neural network with blockchain for secure MANET routing. *IJCNIS, 16*(1), 123–132. https://doi.org/10.5815/ijcnis.2024.01.10

Alam, T. (2021). Blockchain-based secure communication framework for IoT and MANET. *Informatica, 54*(3), 345–360. https://doi.org/10.31449/inf.v54i3.3472

Lo, S. K., Liu, Y., Chia, S. Y., Xu, X., Lu, Q., Zhu, L., & Ning, H. (2019). Blockchain solutions for IoT security. *IEEE Access, 7*, 58822–58835. https://doi.org/10.1109/ACCESS.2019.2912240

Kumari, A., Dutta, S., & Chakraborty, S. (2023). Detection and prevention of black hole attack using node credibility model. *Research Square*. https://doi.org/10.21203/rs.3.rs-1528078/v1

Alkasasbeh, A. A. (2023). Machine learning-based detection of black hole attacks in MANETs. *IEEE Access*. https://doi.org/10.1109/ACCESS.2023.3245678

Tang, J., Liu, J., Zhang, M., & Mei, Q. (2020). Graph neural networks for social network analysis: A survey. *IEEE Transactions on Knowledge and Data Engineering*. https://doi.org/10.1109/TKDE.2020.2981333

Wu, Z., Pan, S., Chen, F., Long, G., Zhang, C., & Yu, P. S. (2021). A comprehensive survey on graph neural networks. *IEEE Transactions on Neural Networks and Learning Systems, 32*(1), 4–24. https://doi.org/10.1109/TNNLS.2020.2978386

Alqahtani, F., Alotaibi, S., & Alghamdi, A. (2022). AI-based intrusion detection system for MANET security. *IEEE Access*. https://doi.org/10.1109/ACCESS.2022.3174567