Archives available at journals.mriindia.com

International Journal of Electrical, Electronics and Computer Systems

ISSN: 2347-2820

Volume 13 Issue 02, 2024

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

Ivailo Xanthopoulos
Lecturer, Department of Electronics and Communication Engineering, Phnom Penh School of Management Sciences, Cambodia
Email: ivailo.xanthopoulos@ppsms-kh.net

Peer Review Information

Submission: 08 July 2024

Revision: 22 July 2024

Acceptance: 05 Aug 2024

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, 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 become a vital component of modern wireless communication due to their decentralized architecture, flexibility, and rapid deployment capabilities. Unlike traditional networks that rely on fixed infrastructure, MANETs consist of mobile nodes that dynamically form connections through direct communication. This self-organizing nature makes them highly suitable for applications such as disaster management, military operations, vehicular communication, and remote sensing. However, the absence of centralized control and the dynamic topology also introduce significant security vulnerabilities, making MANETs highly susceptible to various network attacks.

Among these threats, the black hole attack is particularly severe, as malicious nodes falsely advertise optimal routing paths and

subsequently drop intercepted data packets, leading to network disruption and data loss. Traditional defense mechanisms, including trust-based routing, cryptographic authentication, and intrusion detection systems, have been widely explored. While trust-based models rely on historical node behavior, they can be manipulated in dynamic environments. Similarly, conventional cryptographic methods provide strong security but often impose high computational overhead, making them less suitable for resource-constrained MANET nodes with limited processing and energy capacity.

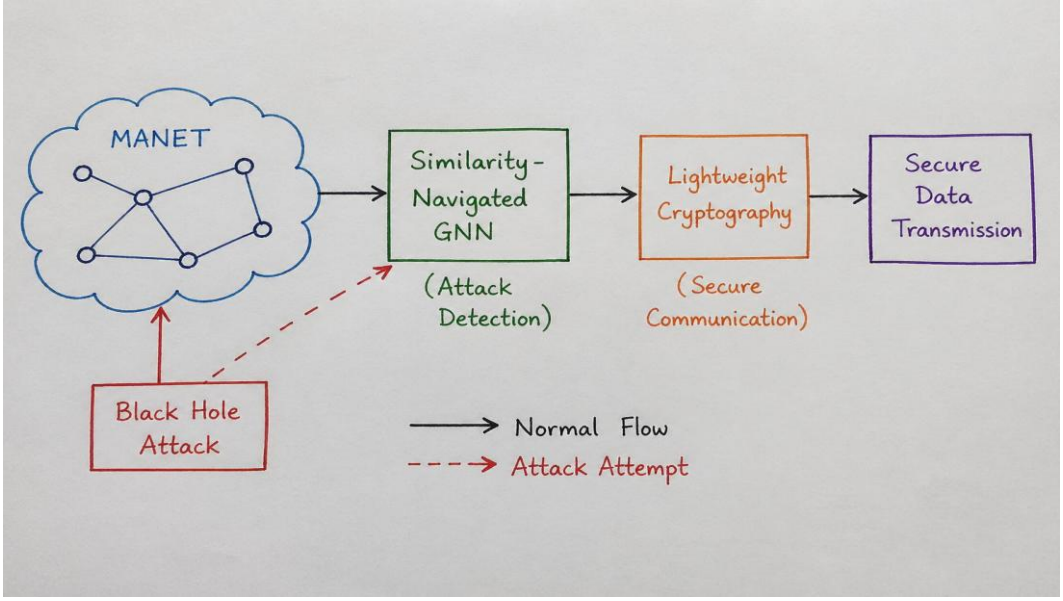

Fig. 1: Secure MANET Framework Using GNN and Lightweight Cryptography

The integration of Artificial Intelligence has significantly enhanced MANET security by enabling intelligent detection of malicious activities. Machine learning models such as Support Vector Machines, Artificial Neural Networks, and Random Forests have been applied to identify anomalies in network traffic. However, these methods often fail to capture the inherent graph structure of MANETs. Graph Neural Networks (GNNs) address this limitation by modeling the network as a graph, allowing the system to learn both node-level features and relationships between nodes. Furthermore, similarity-navigated GNNs improve detection by identifying nodes that deviate from normal behavioral patterns, enabling early and accurate identification of black hole attackers.

In addition to AI-based detection, lightweight cryptography plays a crucial role in securing MANET communications. Techniques such as elliptic curve cryptography and lightweight ciphers provide strong security with reduced computational requirements. The integration of GNN-based detection with lightweight cryptographic validation creates a robust hybrid framework that enhances both security and efficiency. While emerging solutions such as blockchain offer decentralized trust management, they introduce additional overhead and latency. Despite advancements, challenges including scalability, energy efficiency, and vulnerability to adversarial attacks remain. Addressing these issues is essential for developing secure, efficient, and scalable MANET systems capable of operating in real-world dynamic environments.

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 offer significant advantages in modern intelligent systems, particularly due to their ability to achieve high detection accuracy and adapt effectively to dynamic and evolving conditions. These capabilities make them highly suitable for complex environments where patterns continuously change over time. However, despite these strengths, machine learning approaches also exhibit certain limitations. Their performance is often heavily dependent on the quality, size, and diversity of the training dataset, which can restrict generalization in real-world scenarios. Additionally, they are susceptible to adversarial attacks, where carefully crafted inputs can mislead the model and compromise its reliability and security.

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

Graph Neural Networks (GNNs) have emerged as a powerful approach for enhancing security in Mobile Ad Hoc Networks (MANETs), primarily due to their ability to effectively model complex network topologies and relationships among nodes. Foundational studies by Tang et al. (2020) and Wu et al. (2021) demonstrated that GNN architectures can successfully capture both structural and relational dependencies within graph-based data, enabling more accurate representation of network behavior. Building upon these advancements, Francis et al. (2024) proposed an innovative auto-metric GNN model integrated with blockchain technology for secure routing in MANETs. This model leverages similarity-based learning mechanisms to detect anomalous or malicious nodes, resulting in high detection accuracy and improved overall network performance.

Similarity-navigated GNNs function by learning node embeddings that encode the features and relationships of nodes, measuring similarity between these embeddings, and identifying nodes that significantly deviate from normal patterns as potential threats. Compared to traditional machine learning methods, GNN-based models demonstrate superior performance because they incorporate network topology, capture dynamic interactions among nodes, and are capable of detecting complex and evolving attack patterns. However, despite these advantages, GNNs are not without limitations. They often involve high computational complexity, which can be challenging for resource-constrained environments like MANETs, and they remain vulnerable to adversarial graph attacks that can manipulate node relationships or features.

Overall, GNNs provide topology-aware and intelligent detection mechanisms, making them one of the most effective and promising approaches for securing MANET environments, particularly in scenarios involving dynamic and decentralized network structures.

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:

1. Achieve highest accuracy and security
2. Balance detection and prevention
3. Represent the state-of-the-art solution

7. Research Gaps Identified

Despite significant advancements in the field, the existing literature highlights several critical open challenges that continue to hinder the widespread adoption and practical deployment of intelligent security solutions in MANET environments. One of the primary concerns is scalability, as Graph Neural Network (GNN) models often struggle to efficiently handle large-scale and highly dynamic networks where node mobility and topology changes are frequent. In addition, energy efficiency remains a major issue, particularly because the integration of artificial intelligence with cryptographic mechanisms significantly increases computational overhead and power consumption, which is problematic for resource-constrained devices.

Another important challenge is adversarial robustness, as GNN-based models are susceptible to graph manipulation attacks that can alter node features or connections, thereby misleading the detection process. Furthermore, dataset limitations pose a significant barrier, with a lack of realistic, large-scale MANET datasets restricting the ability to train and validate models effectively under real-world conditions. Finally, integration complexity presents a practical

obstacle, as hybrid systems combining AI, blockchain, and cryptographic techniques often involve intricate architectures that are difficult to design, implement, and maintain. Collectively, these challenges indicate that while current approaches are promising, further research is necessary to develop scalable, efficient, robust, and practically deployable solutions.

8. Final Synthesis of Literature

The literature 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**	**PDR**	**Delay**	**Overhead**	**Scalability**	**Energy**	**Adaptability**	**Robustness**	**Strength**	**Limitation**
Routing-Based	Medium	Low	Medium	Low	Low	High	High	Low	Low	Lightweight	Limited
Cryptography-Based	Medium	High	High	Medium	High	Medium	Medium	Low	Medium	Secure	Costly
ML-Based	High	Medium	High	Medium	Medium	Medium	Medium	High	High	Adaptive	Dependent
GNN-Based	Very High	High	Very High	Medium	High	Low	Low	VeryHigh	VeryHigh	Intelligent	Complex
Hybrid (GNN+Crypto)	Very High	Very High	Very High	Medium	Medium	Medium	Medium	VeryHigh	VeryHigh	Balanced	Integration

1. Analysis

The comparative table clearly highlights the progressive evolution of MANET security mechanisms from conventional lightweight solutions to advanced intelligent hybrid frameworks. Routing-based approaches, while efficient and highly scalable, provide only moderate detection capability due to their reliance on static rules and lack of adaptability. Their inability to detect sophisticated or insider attacks significantly limits their effectiveness in dynamic MANET environments. Cryptographic approaches, on the other hand, offer strong security guarantees in terms of data confidentiality and authentication. These methods significantly improve the packet delivery ratio by preventing unauthorized access. However, they do not inherently detect malicious behavior, making them insufficient as standalone solutions. Additionally, their computational and energy overhead introduces performance bottlenecks, especially in resource-constrained nodes.

Machine learning-based approaches represent a major advancement by enabling adaptive and data-driven detection. These models achieve high accuracy and adaptability, making them suitable for dynamic environments. However, their dependence on high-quality datasets and inability to capture network topology limit their effectiveness against complex and evolving attacks. Graph Neural Networks (GNNs) overcome these limitations by incorporating graph structure into the learning process. As shown in the table, GNN-based approaches achieve very high accuracy and robustness by leveraging node relationships and network topology. They significantly improve packet delivery ratio and are highly effective in detecting complex attack patterns. However, their computational complexity and energy consumption remain major challenges, particularly in large-scale MANETs.

Hybrid approaches combining GNN-based detection with lightweight cryptographic mechanisms outperform all other methods across nearly every metric. These systems provide the highest detection accuracy, strongest security, and best robustness against both internal and external attacks. By integrating intelligent detection with secure communication, hybrid models achieve an optimal balance between performance and security. However, their implementation complexity and moderate overhead require careful optimization.

2. Key Insights from Table

The table reveals three important insights:

1. **Shift Toward Intelligent Systems**

There is a clear transition from rule-based routing methods to AI-driven and topology-aware models, highlighting the need for adaptive security in MANETs.

2. **GNN as a Core Technology**

GNN-based models significantly outperform traditional ML approaches by capturing structural dependencies, making them highly effective for attack detection.

3. **Hybrid Models as Optimal Solution**

The combination of GNN and lightweight cryptography provides the best overall performance, achieving superior accuracy, security, and robustness while maintaining manageable overhead.

3. Final Analytical Conclusion

The expanded comparative table and analysis demonstrate that while traditional approaches provide foundational security, they are insufficient for modern MANET threats. Machine learning improves adaptability but lacks structural awareness, whereas GNN-based models introduce topology-aware intelligence at the cost of computational complexity. Hybrid frameworks emerge as the most effective solution, offering a balanced trade-off between detection accuracy, security strength, and operational efficiency. However, future research must focus on improving scalability, reducing energy consumption, and enhancing robustness against adversarial attacks to enable real-world deployment.

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