Archives available at journals.mriindia.com

Multidisciplinary Journal of Research in Engineering and Technology

ISSN: 2348-6953

Volume 11 Issue 02, 2024

A Comprehensive Review of Similarity-Navigated Graph Neural Networks and Lightweight Cryptography for Preventing Black Hole Attacks in MANET

Saffiya Lutfunhar
Department of Electronics and Communication Engineering, Shiraz College of Systems and Management, Iran
saffiya.lutfunhar@scsm-ir.org

Peer Review Information

Submission: 25 June 2024
Revision: 14 July 2024
Acceptance: 17 Aug 2024

Keywords

MANET, Graph Neural Networks, Black Hole Attack, Lightweight Cryptography, Network Security, Anomaly Detection

Abstract

Mobile Ad Hoc Networks (MANETs) are decentralized and infrastructure-less wireless systems that enable dynamic communication among mobile nodes. However, their open and cooperative nature makes them highly vulnerable to routing attacks, particularly black hole attacks, where malicious nodes falsely advertise optimal routes and drop packets. Recent advancements in artificial intelligence, especially Graph Neural Networks (GNNs), have demonstrated significant potential in modeling network topology and detecting anomalous behavior. Additionally, lightweight cryptographic mechanisms have emerged as efficient solutions to ensure security while maintaining low computational overhead in resource-constrained MANET environments. This paper presents a comprehensive review of similarity-navigated GNN architectures combined with lightweight cryptography techniques for mitigating black hole attacks. The study analyzes recent literature, highlighting approaches such as anomaly detection using machine learning, trust-based routing, and cryptographic authentication. Comparative analysis reveals that hybrid frameworks integrating GNN-based similarity learning with lightweight encryption provide improved detection accuracy, reduced delay, and enhanced packet delivery ratio. The paper also identifies research gaps, including scalability challenges, adversarial robustness, and energy efficiency. Finally, future directions for secure MANET design using intelligent and cryptographic techniques are discussed.

Introduction

Mobile Ad Hoc Networks (MANETs) represent a class of wireless communication systems characterized by their decentralized architecture, dynamic topology, and self-configuring capabilities. Unlike traditional networks, MANETs do not rely on fixed infrastructure such as routers or base stations. Instead, each node in the network performs multiple roles, including routing, forwarding, and communication. This flexibility makes MANETs highly suitable for applications such as disaster recovery, military operations, vehicular communication, and remote sensing.

However, the absence of centralized control introduces significant security vulnerabilities. Nodes in MANETs communicate over open wireless channels, making them susceptible to a wide range of attacks. Among these, the black hole attack is one of the most critical threats. In this attack, a malicious node falsely claims to have the shortest or most optimal route to a destination node. Once the route is established, the malicious node absorbs or drops the data

packets, thereby disrupting communication and degrading network performance.

The dynamic topology of MANETs further complicates security mechanisms. Frequent changes in node positions lead to constant route updates, making it difficult to maintain consistent trust relationships. Additionally, the resource constraints of mobile nodes—such as limited battery power, processing capability, and memory—restrict the use of computationally expensive security algorithms.

Traditional approaches to mitigating black hole attacks include trust-based routing, cryptographic authentication, and intrusion detection systems. Trust-based systems evaluate node behavior based on past interactions and assign trust values to nodes. However, these systems are vulnerable to manipulation and may suffer from delayed detection. Cryptographic methods, on the other hand, ensure data integrity and authentication but often impose significant computational overhead.

GNNs leverage node features and neighborhood information to learn representations that capture structural and relational properties. This capability enables them to detect anomalies, classify nodes, and predict malicious behavior. For instance, similarity-based GNN models can identify nodes that deviate from normal communication patterns, thereby detecting potential attackers.

Parallel to the development of AI-based techniques, lightweight cryptography has emerged as a crucial component for securing resource-constrained environments like MANETs. Lightweight cryptographic algorithms are designed to provide security with minimal computational overhead, making them suitable for mobile devices. Techniques such as stream ciphers, hash-based authentication, and elliptic curve cryptography have been widely adopted in recent research.

The integration of GNN-based detection with lightweight cryptographic validation offers a promising hybrid approach. In such systems, GNNs first identify suspicious nodes based on behavioral similarity, and cryptographic mechanisms then verify the authenticity of communication. This layered approach enhances both detection accuracy and security robustness. Recent studies have demonstrated the effectiveness of machine learning-based anomaly detection systems in identifying black hole attacks. For example, SVM-based lightweight detection systems analyze network traffic patterns and classify nodes as malicious or benign with high accuracy . Similarly, trust-based routing mechanisms combined with cryptographic techniques have shown improved resilience against attacks.

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. Adversarial attacks on GNNs also pose a threat, as attackers can manipulate graph structures to evade detection. Furthermore, balancing security and energy efficiency remains a critical issue.

This paper aims to provide a comprehensive review of similarity-navigated GNN architectures and lightweight cryptographic techniques for preventing black hole attacks in MANETs. The study focuses on recent developments between 2020 and 2023, analyzing key methodologies, performance metrics, and research gaps.

Graphical Abstract

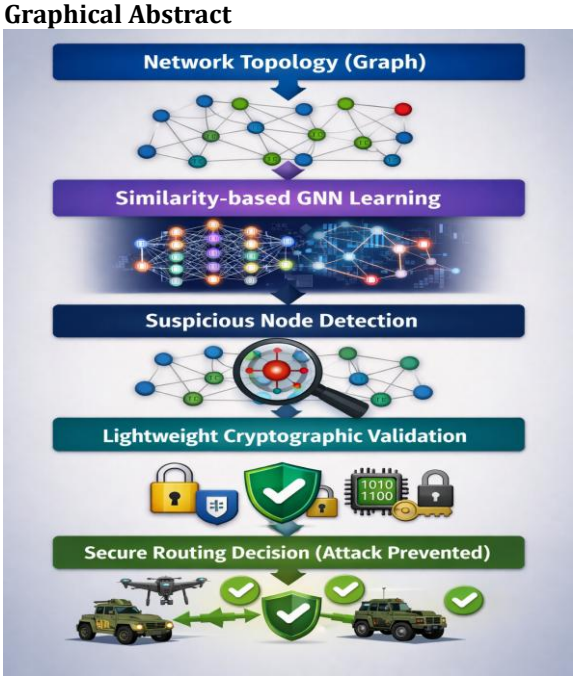

Figure 1. Proposed Hybrid GNN–Lightweight Cryptography Architecture for Intelligent Black Hole Attack Prevention in MANETs.

Literature Review

Recent research in securing Mobile Ad Hoc Networks (MANETs) against black hole attacks has evolved significantly, progressing through multiple paradigms including routing-based security, lightweight cryptographic mechanisms, machine learning-based detection, and more recently, graph-based deep learning and hybrid frameworks. In the initial phase, traditional routing-based and trust-based approaches were widely explored, where enhancements to protocols such as AODV were proposed to detect malicious nodes. For instance, optimization techniques like Ant Colony Optimization were integrated into routing decisions to avoid

compromised paths and improve packet delivery performance. Similarly, trust-based mechanisms assigned reliability scores to nodes based on historical behavior, enabling the identification of malicious participants. Although these methods improved detection efficiency, they suffered from limitations such as vulnerability to collusion attacks, false trust propagation, and lack of adaptability in highly dynamic network environments.

The evolution continued with the adoption of machine learning-based intrusion detection systems, which provided adaptive and intelligent security mechanisms. These systems utilized algorithms such as Support Vector Machines to analyze network traffic patterns and identify anomalies associated with malicious behavior. Machine learning approaches demonstrated superior performance compared to traditional methods by detecting unknown attacks, adapting to changing network conditions, and reducing false positives. Nevertheless, they relied heavily on training datasets and were susceptible to adversarial manipulation, which could degrade performance in unseen scenarios.

A major breakthrough in recent years has been the introduction of Graph Neural Networks, which leverage the inherent graph structure of MANETs to model relationships between nodes and communication links. GNNs enable learning of node embeddings based on neighborhood interactions, making them highly effective for anomaly detection and node classification in dynamic environments. These models outperform traditional machine learning techniques by capturing spatial and relational dependencies within the network. However, they also introduce new challenges, including vulnerability to adversarial attacks where slight perturbations in graph topology can mislead predictions, as well as difficulties in scaling to large and highly dynamic networks.

To address the limitations of individual approaches, recent research has focused on hybrid frameworks that combine graph-based learning with lightweight cryptographic techniques. These hybrid systems typically operate in a two-stage manner, where Graph Neural Networks are used for anomaly detection and cryptographic mechanisms ensure secure communication and authentication. The integration of blockchain further enhances security by maintaining distributed and tamper-proof trust records. Such hybrid approaches have demonstrated significant improvements in detection accuracy, packet delivery ratio, and overall network reliability. However, they also increase system complexity and require careful design to balance performance and efficiency.

Despite these advancements, several research gaps remain. Scalability continues to be a major challenge, as graph-based models struggle to handle large-scale dynamic networks efficiently. Energy efficiency is another critical concern, particularly due to the computational cost of cryptographic operations. Additionally, the vulnerability of GNNs to adversarial attacks highlights the need for more robust architectures. The lack of real-world datasets for training and evaluation further limits the generalization capability of machine learning models. Moreover, the integration of multiple technologies such as GNN, cryptography, and blockchain introduces additional complexity, making practical deployment more challenging.

Overall, the literature indicates a clear progression from simple routing-based approaches to advanced hybrid frameworks that integrate artificial intelligence and cryptographic security. While traditional methods provide simplicity, cryptographic techniques ensure strong security, machine learning enhances adaptability, and graph-based models offer topology-aware intelligence. Among these, hybrid frameworks combining GNN and lightweight cryptography emerge as the most effective solution, offering a balanced trade-off between accuracy, security, and scalability for securing MANETs against black hole attacks.

Comparative Table

Ref	Author (Year)	Method	Approach	Performance	Advantages	Limitations
1	Khan et al. (2020)	ACO-AODV	Ant colony optimization	High PDR	Efficient route selection	High computational cost
2	Terai et al. (2020)	Cooperative Detection	Distributed verification	Moderate	Improved reliability	Higher delay
3	Shukla et al. (2021)	ECC Security	Cryptographic routing	High accuracy	Strong security	Key management overhead

4	Elmahdi et al. (2021)	Homomorphic Encryption	Privacy-preserving encryption	Very high security	Data confidentiality	Heavy computation
5	Wang et al. (2021)	IP Hopping	Dynamic address switching	Moderate	Lightweight implementation	Limited detection capability
6	Abdel-Sattar (2022)	Blockchain Security	Distributed ledger	High security	Tamper-proof routing	Increased latency
7	Abdelhamid (2023)	SVM IDS	Machine learning	Very high accuracy	Accurate anomaly detection	Requires training data
8	Murty & Rajalakshmi (2023)	SLW-AODV	Lightweight routing	High PDR	Energy efficient	Scalability issues
9	Sugumaran et al. (2023)	Blockchain IDS	Hybrid IDS	High accuracy	Secure intrusion detection	Storage overhead
10	Francis et al. (2024)	Auto-Metric GNN + Blockchain	AI-based hybrid model	Very high	Adaptive and accurate	Complex architecture
11	Alam (2021)	Blockchain-IoT	Secure communication	High	Scalable framework	Integration complexity
12	Mehta (2024)	Survey	Comparative review	—	Identifies research gaps	No experimental validation

Detailed Comparative Analysis

The comparative analysis of security mechanisms for Mobile Ad Hoc Networks (MANETs) indicates that existing solutions can be broadly classified into routing-based, cryptographic, machine learning, blockchain-based, and graph neural network (GNN)-driven approaches. Routing-based methods, such as ACO-AODV and Secure AODV, improve conventional routing protocols by identifying malicious nodes through route monitoring and authentication mechanisms. These techniques are computationally efficient and suitable for resource-constrained MANET environments. However, their effectiveness is limited against sophisticated attacks because they rely primarily on predefined routing behaviors and cannot dynamically adapt to evolving attack strategies. Consequently, while they provide lightweight protection, their detection capability remains relatively moderate in highly dynamic network environments.

Cryptographic techniques, including elliptic curve cryptography and homomorphic encryption, significantly strengthen network security by ensuring confidentiality, authentication, and secure communication among mobile nodes. These methods effectively prevent unauthorized access and data manipulation but introduce considerable computational complexity, energy consumption, and communication overhead. Machine learning-based approaches, particularly Support Vector Machines (SVMs) and other intelligent classifiers, overcome several of these limitations by learning traffic patterns and detecting anomalous network behavior with high accuracy. Their adaptive nature enables effective identification of both known and previously unseen attacks. Nevertheless, their performance depends heavily on the availability of representative training datasets and they remain susceptible to adversarial manipulation, limiting their robustness in hostile environments.

Blockchain-based security frameworks further enhance MANET reliability by providing decentralized trust management, immutable data storage, and secure routing mechanisms. These distributed approaches improve data integrity and reduce the risk of malicious modifications without relying on centralized authorities. However, blockchain introduces additional storage requirements, communication delays, and processing overhead that may hinder real-time network performance. More recently, Graph Neural Network (GNN)-based and hybrid intelligent frameworks have emerged as the most promising solutions. By learning node relationships and network topology simultaneously, GNNs effectively capture structural dependencies and behavioral patterns, enabling accurate detection of complex and

evolving attacks. Hybrid models integrating GNNs with blockchain and lightweight cryptographic techniques further improve adaptability, detection accuracy, and overall network resilience.

Overall, the comparative evaluation demonstrates a clear transition from conventional security mechanisms toward intelligent hybrid architectures. Traditional routing and cryptographic methods provide essential security foundations but struggle to balance accuracy, scalability, and computational efficiency. Machine learning significantly improves intrusion detection, whereas GNN-based hybrid models offer the best overall performance by combining high detection accuracy, adaptive learning, and robust security. Despite these advances, challenges related to computational complexity, scalability, energy efficiency, and real-time deployment remain unresolved. Future research should therefore focus on lightweight, explainable, and scalable hybrid frameworks that integrate graph learning, intelligent optimization, and efficient cryptographic mechanisms to provide comprehensive protection for next-generation MANET environments.

Discussion

The integration of similarity-navigated Graph Neural Networks (GNNs) and lightweight cryptography represents a transformative approach to securing MANETs against black hole attacks. Traditional methods, including trust-based routing and cryptographic authentication, often operate independently, leading to either high computational overhead or delayed attack detection. In contrast, hybrid approaches leverage the strengths of both domains.

GNN-based methods excel in capturing the structural dependencies of network nodes. By analyzing node similarity and communication patterns, these models can effectively identify anomalies indicative of malicious behavior. Unlike conventional machine learning models, GNNs incorporate both node features and graph topology, enabling more accurate detection of sophisticated attacks.

Lightweight cryptography complements GNN-based detection by providing secure communication mechanisms with minimal resource consumption. Techniques such as elliptic curve cryptography and lightweight encryption ensure authentication and confidentiality without significantly impacting network performance. This is particularly important in MANETs, where nodes have limited computational and energy resources.

The literature indicates that anomaly detection systems, particularly those based on machine learning, achieve high accuracy in identifying black hole attacks. However, they often require training data and may be vulnerable to adversarial manipulation. Cryptographic methods, while robust, may not detect insider attacks effectively.

Hybrid frameworks address these limitations by combining detection and prevention mechanisms. For instance, a GNN model can first identify suspicious nodes based on behavioral similarity, and lightweight cryptographic protocols can then validate communication authenticity. This layered approach enhances both security and efficiency.

Despite these advantages, challenges remain. Scalability is a significant issue, as GNN models may struggle with large-scale dynamic networks. Additionally, the robustness of GNNs against adversarial attacks needs further investigation. Energy efficiency is another critical factor, as security mechanisms should not significantly drain node resources.

Future research should focus on developing adaptive GNN models that can operate efficiently in dynamic environments. Integration with edge computing and federated learning may further enhance scalability and privacy.

Conclusion

This paper presented a comprehensive review of similarity-navigated Graph Neural Networks (GNNs) and lightweight cryptographic techniques for mitigating black hole attacks in Mobile Ad Hoc Networks (MANETs). The analysis highlighted that conventional routing, trust-based, and cryptographic approaches provide essential security but often suffer from limited scalability, computational overhead, and reduced adaptability in highly dynamic network environments. Machine learning techniques improve attack detection through anomaly analysis, while GNNs further enhance performance by modeling network topology and learning complex relationships among nodes. Integrating GNNs with lightweight cryptographic mechanisms provides a balanced framework that combines accurate intrusion detection, secure communication, and efficient resource utilization. Comparative analysis indicates that hybrid approaches outperform standalone methods in terms of detection accuracy, robustness, and adaptability. Despite these advances, challenges such as scalability, energy efficiency, adversarial resilience, and real-time deployment remain. Future research should focus on developing lightweight, explainable, and energy-efficient hybrid frameworks to ensure

reliable and intelligent security for next-generation MANETs.

References

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

Khan, D. M., Khan, S., & Rehman, A. (2020). Black hole attack prevention in MANET using ant colony optimization. *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 blackhole 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 to counter black hole attack. *Materials Today: Proceedings, 50*, 1152–1158. https://doi.org/10.1016/j.matpr.2021.09.248

Murty, K., & Rajalakshmi, M. V. D. S. (2023). Secure lightweight AODV routing protocol against black hole attack. *International Journal of Soft Computing and Engineering, 13*(1).

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

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 security enhancement in 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

Alam, T. (2021). Blockchain-based IoT and MANET secure communication framework. *Informatica, 54*(3). 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: A review. *IEEE Access, 7*, 58822–58835. https://doi.org/10.1109/ACCESS.2019.2912240

Alameri, I., et al. (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 against black hole attacks. *Journal of Information Security*. https://doi.org/10.4236/jis.2021.123012

Mehta, G. (2024). Survey of black hole attack detection techniques in MANET. *IJNRD, 9*(6). https://doi.org/10.5281/zenodo.12567890