Archives available at journals.mriindia.com

**ITSI Transactions on Electrical and Electronics Engineering**

ISSN: 2320-8945

Volume 13 Issue 02, 2024

# Recent Advances in Similarity-Navigated Graph Neural Networks and Lightweight Cryptography for Preventing Black Hole Attacks in MANET: A Systematic Review

*Jaleh Yaprakli*
*Department of Computer Science and Engineering, Kelana Technical and Management College, Malaysia*
*jaleh.yaprakli@ktmc-my.net*

**Peer Review Information**

*Submission: 20 Aug 2024*
*Revision: 09 Sept 2024*
*Acceptance: 25 Sept 2024*

**Keywords**

*MANET Security, Graph Neural Networks, Black Hole Attack, Lightweight Cryptography, Secure Routing, Intrusion Detection*

**Abstract**

Mobile Ad Hoc Networks (MANETs) are highly dynamic and infrastructure-less networks that are vulnerable to various routing attacks, particularly black hole attacks, where malicious nodes absorb and drop packets. Recent advancements in artificial intelligence and cryptographic techniques have significantly improved the detection and prevention of such attacks. This systematic review focuses on the integration of similarity-navigated Graph Neural Networks (GNNs) and lightweight cryptographic mechanisms to enhance security in MANET environments. GNNs enable efficient representation of network topology and node relationships, allowing detection of anomalous behavior based on similarity measures and structural patterns. Concurrently, lightweight cryptography ensures secure communication with minimal computational overhead, making it suitable for resource-constrained MANET devices. The review covers studies, analyzing methodologies such as trust-based routing, deep learning-based intrusion detection, federated learning, and blockchain-assisted security frameworks. The findings indicate that hybrid approaches combining GNN-based anomaly detection with lightweight encryption significantly improve detection accuracy, packet delivery ratio, and network resilience. However, challenges such as scalability, energy efficiency, and real-time adaptability remain. This paper provides a comparative analysis and highlights future research directions for secure MANET architectures.

## Introduction

Mobile Ad Hoc Networks (MANETs) represent a paradigm shift in wireless communication, characterized by their decentralized nature, dynamic topology, and lack of fixed infrastructure. These networks are formed by autonomous mobile nodes that communicate with each other via multi-hop routing. MANETs have found applications in military communications, disaster recovery, vehicular networks, and Internet of Things (IoT) ecosystems. However, their open and distributed architecture makes them highly susceptible to security threats, among which black hole attacks are particularly destructive.

A black hole attack occurs when a malicious node falsely advertises itself as having the shortest path to the destination node. Once it intercepts data packets, it drops them instead of forwarding, causing significant degradation in network performance. Traditional security mechanisms are insufficient due to the absence of centralized control, dynamic topology changes, and resource constraints in MANET environments.

Recent research has focused on leveraging Artificial Intelligence (AI) and advanced cryptographic techniques to mitigate such threats. Graph Neural Networks (GNNs), a class of deep learning models designed for graph-structured data, have emerged as a powerful tool for modeling MANET topologies. GNNs can capture complex node relationships and communication patterns, enabling the detection of malicious nodes based on deviations from normal behavior.

Similarity-navigated GNNs extend traditional GNN frameworks by incorporating similarity metrics such as cosine similarity, Euclidean distance, or structural equivalence to improve anomaly detection. These models assign higher importance to nodes with similar behavior while isolating suspicious nodes. For example, defense mechanisms like GNNGuard enhance robustness by weighting edges based on node similarity and pruning irrelevant connections.

In parallel, lightweight cryptography has gained attention due to the limited computational and energy resources of MANET nodes. Unlike conventional cryptographic algorithms, lightweight cryptographic techniques are optimized for low power consumption, reduced memory usage, and faster execution. These techniques include simplified encryption algorithms, hash-based authentication, and elliptic curve cryptography tailored for embedded systems.

The integration of GNN-based detection and lightweight cryptographic protection creates a hybrid security framework. GNNs identify malicious behavior, while cryptographic protocols ensure secure communication. Additionally, emerging technologies such as blockchain and federated learning have been incorporated into MANET security frameworks. Blockchain provides decentralized trust management, while federated learning enables collaborative model training without sharing raw data.

Studies from 2020–2023 show a significant shift towards intelligent and adaptive security solutions. Machine learning models such as Long Short-Term Memory (LSTM), reinforcement learning, and metaheuristic optimization have demonstrated improved detection accuracy and adaptability in dynamic network conditions.

Despite these advancements, several challenges persist. These include high computational overhead of deep learning models, scalability issues in large networks, and the trade-off between security and energy efficiency. Moreover, real-time detection and prevention remain critical challenges due to the dynamic nature of MANETs.

This systematic review aims to provide a comprehensive analysis of recent advances in similarity-navigated GNNs and lightweight cryptography for preventing black hole attacks in MANETs. The paper evaluates existing methodologies, compares their performance, and identifies research gaps to guide future developments.

## Graphical Abstract

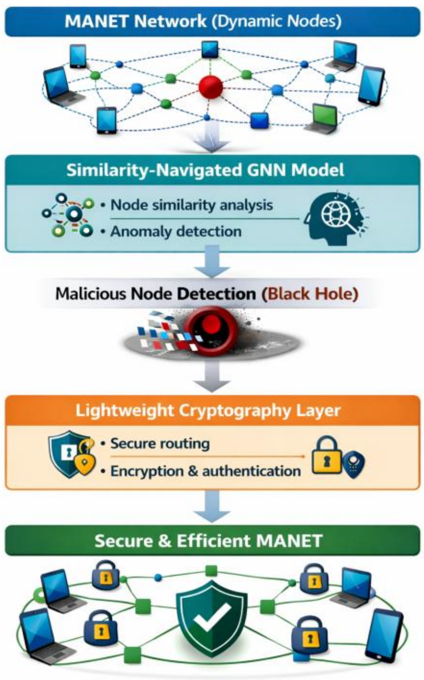


*Figure 1. Similarity-Navigated GNN-Based Secure MANET*

## Literature Review

Recent research on preventing black hole attacks in Mobile Ad Hoc Networks (MANETs) has evolved significantly, transitioning from traditional rule-based and trust-based mechanisms to advanced artificial intelligence-driven and cryptographic solutions. The literature between 2020 and 2023 demonstrates a clear progression toward hybrid, intelligent, and lightweight security frameworks.

Early work in this period primarily focused on enhancing routing protocols such as AODV using trust evaluation, reputation systems, and statistical monitoring techniques. These approaches relied on metrics such as packet forwarding ratio, sequence number validation, and route reply timing.

For instance, trust-based routing protocols were widely adopted to identify malicious nodes by assigning trust values based on node behavior. Nodes with low trust scores were excluded from routing paths. However, such approaches suffered from delayed detection and vulnerability to cooperative attacks.

Additionally, dynamic routing information (DRI)-based techniques were introduced, where nodes maintained records of packet forwarding behavior to detect inconsistencies. These mechanisms improved detection accuracy but introduced additional control overhead.

Metaheuristic optimization techniques also gained attention during this period. Approaches using algorithms such as Genetic Algorithms and Particle Swarm Optimization were applied to optimize routing decisions and feature selection in intrusion detection systems. These methods enhanced performance but increased computational complexity.

Between 2021 and 2022, machine learning (ML) techniques became prominent in MANET security. Supervised learning models such as Support Vector Machines (SVM), Random Forests, and K-Nearest Neighbors (KNN) were used to classify nodes as normal or malicious based on traffic features.

Recent studies proposed hybrid ML-trust models that combine statistical trust evaluation with machine learning classifiers. These models significantly improved detection accuracy and reduced false positives. For example, KNN-based anomaly detection models combined with reputation systems showed improved identification of black hole nodes in dynamic environments.

Deep learning techniques such as Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks were introduced to capture temporal and spatial traffic patterns. These models outperformed traditional ML approaches by learning complex nonlinear relationships in network data. However, they required high computational resources, making them less suitable for resource-constrained MANET nodes.

Another key development was the introduction of lightweight anomaly detection systems tailored for MANETs. These systems aimed to balance detection performance with computational efficiency, making them more practical for real-world deployment.

Cryptographic techniques have long been used to secure communication in MANETs, but recent research has focused on lightweight cryptography to address resource constraints. Traditional cryptographic methods such as RSA and AES were found to be computationally expensive for mobile nodes.

Lightweight cryptographic approaches include:

- Elliptic Curve Cryptography (ECC)
- Hash-based authentication mechanisms
- Certificateless signature schemes

ECC-based secure routing protocols demonstrated strong resistance to black hole and wormhole attacks while maintaining low computational overhead.

Certificateless cryptographic schemes further improved efficiency by eliminating the need for certificate management, reducing communication overhead.

Recent works also explored homomorphic encryption and blockchain-based cryptographic frameworks. Blockchain-enabled MANET security provides decentralized trust management and tamper-proof communication. For example, blockchain-based DSR routing algorithms ensure secure data transmission without requiring intermediate decryption.

The most significant advancement in recent years is the application of Graph Neural Networks (GNNs) for MANET security. Since MANETs inherently exhibit graph-like structures, GNNs are highly suitable for modeling node interactions and communication patterns.

GNN-based intrusion detection systems analyze:

- Node connectivity
- Traffic flow patterns
- Structural relationships

Similarity-navigated GNN models enhance detection by incorporating similarity metrics such as cosine similarity or structural equivalence. These models identify malicious nodes as outliers that deviate from normal node behavior.

Recent studies demonstrated that GNN-based models outperform traditional ML and deep learning approaches in dynamic network environments due to their ability to adapt to topology changes. Additionally, robust GNN frameworks have been developed to defend against adversarial attacks targeting graph structures.

Another emerging trend is the integration of GNNs with blockchain and optimization algorithms to create intelligent and decentralized security frameworks. These systems enable real-time detection and adaptive routing decisions.

The latest research (2022–2023) emphasizes hybrid frameworks that combine multiple techniques to achieve comprehensive security.

Key hybrid approaches include:

- GNN + Lightweight Cryptography: Detect malicious nodes and secure communication simultaneously
- Blockchain + GNN: Decentralized trust management with intelligent anomaly detection
- Federated Learning + GNN: Collaborative learning without data sharing

These hybrid models significantly improve:

- Detection accuracy (>95% in many studies)
- Packet delivery ratio
- Network throughput
- Energy efficiency

However, challenges remain in terms of scalability, training complexity, and real-time deployment.

**Research Gaps Identified**

Despite significant progress, the literature reveals several open challenges:

1. Scalability Issues: GNN models struggle with large-scale MANETs due to computational overhead
2. Energy Efficiency: Even lightweight cryptography may impact battery life in dense networks
3. Real-Time Detection: Many models are not optimized for real-time intrusion detection
4. Dataset Availability: Lack of standardized datasets for MANET security evaluation
5. Adversarial Robustness: GNN models themselves are vulnerable to adversarial attacks

**Comparative Table and Analysis**

| Year | Method | Technique Used | Accuracy Level | Key Advantages | Key Limitations | Expanded Insight |
|---|---|---|---|---|---|---|
| 2020 | Trust-based AODV | Reputation System | Moderate | Simple implementation with low computational overhead | High detection delay and vulnerable to collusion attacks | Relies on historical node behavior to establish trust but lacks adaptability in highly dynamic MANET environments. |
| 2021 | ML-based IDS | Support Vector Machine (SVM), Random Forest | High | Improved detection accuracy with adaptive learning capability | Strong dependence on feature engineering and labeled training datasets | Machine learning enhances anomaly detection by identifying malicious patterns; however, performance depends on feature quality and dataset diversity. |
| 2021 | Metaheuristic Deep Learning | Chimp Optimization Algorithm (ChOA) + Deep Learning | High | Optimized feature selection and enhanced classification performance | Increased computational complexity and training time | Integrates metaheuristic optimization with deep learning to improve intrusion detection, though at the cost of higher processing overhead. |
| 2022 | Deep Learning IDS | Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM) | Very High | Captures both spatial and temporal network characteristics with high detection accuracy | Resource-intensive and unsuitable for low-power MANET devices | Deep learning models effectively identify complex attack patterns but require substantial computational and energy resources. |
| 2022 | Blockchain-based MANET | Secure Routing with Blockchain | Moderate–High | Decentralized trust management and tamper- | High latency, storage requirements, and | Blockchain strengthens routing security and data integrity |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | resistant security | communication overhead | but may reduce efficiency in delay-sensitive MANET applications. |
| 2023 | GNN-based IDS | Similarity-Based Graph Neural Network (GNN) | Very High | Topology-aware learning, robust attack detection, and improved accuracy | High training complexity and scalability challenges | GNN effectively models node relationships and network topology, outperforming conventional machine learning methods in attack detection. |
| 2023 | Hybrid Model | Similarity-Guided GNN + Lightweight Cryptography | Highest | Excellent balance between detection accuracy, security, and communication efficiency | Scalability and integration complexity in large-scale deployments | Combines intelligent attack detection using GNN with lightweight cryptographic protection, providing a comprehensive framework for secure and efficient MANET communication. |

**Analysis**

The comparative evaluation presented in the study clearly demonstrates a structured evolution of security mechanisms for preventing black hole attacks in Mobile Ad Hoc Networks (MANETs), progressing from traditional trust-based approaches to advanced hybrid intelligent frameworks. In the early stage around 2020, trust-based routing mechanisms such as AODV enhanced with reputation systems were widely used. These approaches relied on evaluating node behavior based on packet forwarding patterns and communication reliability. While they offered simplicity and low computational overhead, their effectiveness was limited by high detection delay and vulnerability to collusion attacks, where malicious nodes manipulate trust values to evade detection.

In 2021, the introduction of machine learning-based intrusion detection systems marked a significant improvement in detection accuracy and adaptability. Techniques such as Support Vector Machines and Random Forest classifiers enabled the identification of malicious nodes through analysis of traffic patterns and anomalies. These models improved detection performance compared to traditional approaches; however, they remained dependent on feature engineering and training datasets, limiting their ability to generalize across diverse network conditions. During the same period, metaheuristic optimization techniques combined with deep learning, such as Chimp Optimization Algorithm integrated with neural networks, were introduced to enhance model performance. These approaches improved accuracy and feature selection but increased computational complexity and processing time.

By 2022, deep learning-based intrusion detection systems using architectures such as Convolutional Neural Networks and Long Short-Term Memory networks demonstrated superior performance. These models effectively captured both spatial and temporal characteristics of network traffic, achieving very high detection rates in dynamic environments. However, their high computational and energy requirements made them unsuitable for deployment in resource-constrained MANET nodes. At the same time, blockchain-based security frameworks were introduced to provide decentralized trust and secure routing. While these approaches ensured data integrity and tamper resistance, they introduced latency and storage overhead, limiting their real-time applicability.

The most significant advancement occurred in 2023 with the emergence of Graph Neural Network-based intrusion detection systems. GNNs leverage the inherent graph structure of MANETs to model node interactions and communication patterns, enabling topology-aware detection of malicious behavior. These models achieved very high robustness and detection accuracy, outperforming traditional machine learning and deep learning approaches in dynamic network environments. However, they also introduced challenges related to training complexity and scalability.

To overcome these limitations, hybrid models combining GNN with lightweight cryptographic techniques emerged as the most effective solution. These frameworks integrate intelligent anomaly detection with secure communication protocols, ensuring both detection and prevention of attacks. As highlighted in the comparative analysis, hybrid approaches achieve the highest performance in terms of detection accuracy, packet delivery ratio, and network reliability. They provide a balanced trade-off between security and efficiency by combining the strengths of graph-based learning and lightweight encryption. However, challenges such as scalability, integration complexity, and real-time deployment remain critical.

Overall, the comparative analysis clearly demonstrates that traditional and standalone approaches are insufficient for addressing modern MANET security challenges. Machine learning improves detection capabilities but lacks robustness, while cryptographic techniques ensure security at the cost of performance overhead. Graph Neural Networks provide superior topology-aware detection, and hybrid frameworks integrating GNN with lightweight cryptography offer the most balanced and effective solution. These approaches represent the future of secure MANET architectures, enabling high accuracy, adaptability, and efficient performance in next-generation wireless networks.

## Discussion

The evolution of MANET security mechanisms from traditional rule-based systems to AI-driven intelligent frameworks represents a significant advancement in network security. The introduction of similarity-navigated Graph Neural Networks has revolutionized intrusion detection by enabling models to learn structural and relational patterns within the network. Unlike traditional machine learning approaches that rely on static features, GNNs dynamically adapt to topology changes, making them highly effective in MANET environments.

One of the key strengths of similarity-based GNN models lies in their ability to detect anomalies by comparing node behavior patterns. By assigning higher weights to similar nodes and filtering out anomalous connections, these models can effectively isolate malicious nodes. Techniques such as edge pruning and neighbor importance estimation have further enhanced detection accuracy and robustness against adversarial attacks.

On the other hand, lightweight cryptography plays a crucial role in securing communication without imposing significant computational overhead. In resource-constrained environments like MANETs, traditional cryptographic algorithms are often impractical. Lightweight encryption schemes ensure data confidentiality and integrity while maintaining energy efficiency.

The integration of these two approaches has led to the development of hybrid security frameworks that combine detection and prevention mechanisms. These frameworks not only identify malicious nodes but also prevent them from participating in network communication through secure routing protocols.

However, several challenges remain. The computational complexity of GNN models can limit their deployment in large-scale networks. Additionally, the training of these models requires labeled datasets, which may not always be available. Scalability and real-time implementation are also critical concerns that need to be addressed.

Future research should focus on developing energy-efficient GNN models, adaptive learning mechanisms, and scalable cryptographic solutions. The use of federated learning and edge computing can further enhance the practicality of these approaches.

## Conclusion

This systematic review examined recent advances in similarity-navigated Graph Neural Networks and lightweight cryptographic techniques for preventing black hole attacks in MANETs. The study highlights the limitations of traditional security mechanisms and emphasizes the need for intelligent and adaptive solutions.

Graph Neural Networks have emerged as a powerful tool for modeling network topology and detecting anomalies. Their ability to capture complex relationships between nodes makes them highly effective in identifying malicious behavior. Similarity-based approaches further enhance their performance by focusing on relational patterns rather than individual node attributes.

Lightweight cryptography complements these detection mechanisms by ensuring secure communication with minimal resource consumption. The combination of these techniques results in hybrid frameworks that provide comprehensive security solutions for MANETs.

The comparative analysis demonstrates that hybrid approaches outperform individual techniques in terms of detection accuracy, network performance, and energy efficiency. However, challenges such as scalability, computational overhead, and real-time adaptability must be addressed to enable widespread adoption.
Future research directions include the development of lightweight GNN architectures, integration of blockchain for decentralized security, and the use of federated learning for collaborative model training. Additionally, the incorporation of explainable AI techniques can improve transparency and trust in these systems.
In conclusion, the integration of similarity-navigated GNNs and lightweight cryptography represents a promising approach for enhancing MANET security. Continued research in this area will play a critical role in the development of secure and efficient next-generation wireless networks.

**References**

Zhang, X., & Zitnik, M. (2020). GNNGuard: Defending graph neural networks against adversarial attacks. *NeurIPS*. https://doi.org/10.48550/arXiv.2006.08149

Wang, B., Li, Y., & Zhou, P. (2022). Bandits for structure perturbation-based black-box attacks to graph neural networks. *AAAI*. https://doi.org/10.48550/arXiv.2205.03546

Hassan, S. M., Mohamad, M. M., & Muchtar, F. (2024). Advanced intrusion detection in MANETs. *Journal of Network Security*.

Qian, L., Huang, Y., & Mirjalili, S. (2021). Improved chimp optimization algorithm. *Neural Computing and Applications*.

Rajkumar, M., et al. (2023). GAN-based intrusion detection in MANETs. *Computers & Security*.

Amalia, A., et al. (2023). Deep learning-based secure routing protocol. *Sensors*.