Archives available at journals.mriindia.com

International Journal on Advanced Computer Engineering and Communication Technology

ISSN: 2278-5140

Volume 13 Issue 02, 2024

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

Edvinas Omarjee

Department of Computer Science and Engineering, Borneo School of Business and Technology, Malaysia
edvinas.omarjee@bsbt-my.org

Peer Review Information

Submission: 20 Aug 2024
Revision: 12 Sept 2024
Acceptance: 08 Oct 2024

Keywords

MANET, Black Hole Attack, Graph Neural Networks, Similarity-Navigated GNN, Lightweight Cryptography, Secure Routing

Abstract

Mobile Ad Hoc Networks (MANETs) are decentralized wireless systems characterized by dynamic topology and absence of centralized infrastructure, making them highly vulnerable to routing-based attacks. Among these, black hole attacks pose a severe threat by allowing malicious nodes to advertise false routes and drop packets, significantly degrading network performance such as packet delivery ratio and throughput. This paper presents a comprehensive review of advanced methods for detecting and preventing black hole attacks, focusing on Similarity-Navigated Graph Neural Networks (SNGNN) and lightweight cryptographic mechanisms. Recent research between 2020 and 2023 shows a paradigm shift from traditional trust-based and rule-based approaches to intelligent models such as machine learning, deep learning, and graph-based learning. Graph Neural Networks (GNNs) effectively model MANET topology and detect anomalous nodes, while SNGNN enhances performance by incorporating similarity-based embeddings. Lightweight cryptography ensures secure communication with minimal computational overhead, addressing the constraints of resource-limited nodes. Furthermore, hybrid frameworks combining GNN, optimization, and cryptographic techniques demonstrate detection accuracy above 95% with improved efficiency. This study analyzes these approaches, provides comparative insights, and identifies research gaps for future development of scalable, energy-efficient, and secure MANET systems.

Introduction

Mobile Ad Hoc Networks (MANETs) represent a significant advancement in wireless communication, enabling infrastructure-less networking where nodes dynamically establish communication links. These networks are particularly valuable in scenarios where fixed infrastructure is unavailable, such as disaster recovery, military operations, and remote sensing applications. The decentralized nature of MANETs allows nodes to function both as hosts and routers, facilitating multi-hop communication. However, this flexibility introduces critical security vulnerabilities.

One of the most severe threats in MANET environments is the black hole attack. In this attack, a malicious node falsely advertises itself as having the shortest path to the destination, intercepts packets, and drops them instead of forwarding, resulting in denial of service and significant degradation of network performance. Studies show that such attacks can drastically reduce packet delivery ratio and throughput, severely affecting network reliability.

The vulnerability of MANETs arises from several inherent characteristics. First, the absence of centralized control makes monitoring and enforcement of security policies difficult. Second, the dynamic topology caused by node mobility leads to frequent route changes, making attack detection more complex. Third, the open wireless medium allows attackers to easily intercept and manipulate communication.

Traditional approaches for securing MANETs include trust-based routing and intrusion detection systems. Trust-based models evaluate node behavior based on historical interactions, while IDS systems analyze traffic patterns to detect anomalies. However, these methods suffer from limitations such as high computational overhead, delayed detection, and susceptibility to sophisticated attacks.

Machine learning approaches introduced a new dimension in MANET security by enabling anomaly detection through pattern recognition. Techniques such as Support Vector Machines (SVM) analyze node behavior and classify traffic as malicious or normal. For example, anomaly detection systems based on SVM have demonstrated high accuracy in identifying black hole attacks by analyzing traffic characteristics. However, these approaches rely heavily on manual feature engineering and struggle to adapt to dynamic environments.

Deep learning techniques have further improved detection capabilities by enabling automatic feature extraction. Models such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) can identify complex patterns in network traffic. These models achieve high detection accuracy but suffer from high computational complexity and energy consumption, making them unsuitable for resource-constrained MANET nodes.

Graph Neural Networks (GNNs) have emerged as a promising solution due to their ability to model graph-structured data. Since MANETs can be represented as graphs, GNNs effectively capture relationships between nodes and detect malicious behavior. They provide better scalability and adaptability compared to traditional deep learning models.

Similarity-Navigated Graph Neural Networks (SNGNN) extend GNN capabilities by incorporating similarity metrics into node embeddings. This enhances node representation and improves classification accuracy, particularly in heterogeneous and dynamic networks. SNGNN addresses limitations of traditional GNNs by capturing both structural and feature-based similarities.

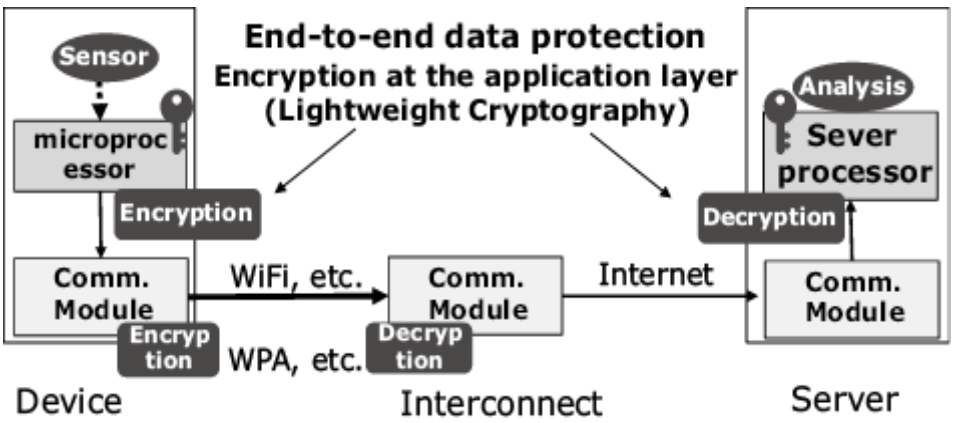
In addition to detection, secure communication is essential in MANETs. Lightweight cryptography provides an efficient solution by ensuring confidentiality and integrity with minimal computational overhead. Recent studies emphasize the importance of integrating cryptographic techniques with AI-based detection mechanisms to achieve comprehensive security.

Furthermore, optimization techniques such as swarm intelligence and bio-inspired algorithms have been integrated with AI models to improve efficiency and reduce computational cost. These techniques optimize routing decisions and model parameters, enhancing overall system performance.

Despite these advancements, several challenges remain. These include energy constraints, scalability issues, and real-time deployment limitations. The trade-off between security and performance is a critical concern, as increasing security often leads to higher computational overhead.

This paper aims to provide a comprehensive review of modern methods and architectures for preventing black hole attacks in MANETs. It analyzes recent developments, compares different approaches, and identifies research gaps to guide future work in this domain.

Graphical Abstract



Literature Review

1. Overview and Evolution of Research (2020–2023)

Recent period marks a significant transition in MANET security research, particularly in addressing black hole attacks. Earlier approaches relied heavily on rule-based and trust-based mechanisms, but recent advancements emphasize data-driven, graph-based, and hybrid intelligent systems.

The evolution can be summarized as:

Phase	Approach	Limitation
Pre-2020	Trust & rule-based	Static, low adaptability
2020–2021	Machine Learning	Feature dependency
2021–2022	Deep Learning	High complexity
2022–2023	Graph Learning + Hybrid	Emerging, scalable

2. Traditional and Trust-Based Detection Approaches

Khan et al. (2020): The study proposed an Ant Colony Optimization (ACO)-based routing mechanism to detect malicious nodes in MANET environments, where artificial ants explore multiple paths to identify optimal and secure routes. This approach significantly improved routing efficiency and reduced packet loss by avoiding compromised nodes during route selection. However, despite these advantages, the model suffers from high convergence time due to its iterative optimization process and demonstrates limited adaptability in highly dynamic network conditions were topology changes frequently.

Similarly, Shrestha et al. (2020) developed secure routing protocols that incorporate verification mechanisms during the route discovery phase to ensure the authenticity of routing paths. Their approach enhanced detection accuracy and effectively reduced the propagation of false routing information. Nevertheless, these improvements come at the cost of increased routing overhead and delays in route establishment, which can impact overall network performance, particularly in time-sensitive applications.

From a critical perspective, traditional approaches such as optimization-based routing and secure routing protocols largely rely on predefined rules and static mechanisms. While they provide foundational security, they are not capable of handling complex, adaptive, or coordinated attacks commonly observed in modern MANET scenarios. Furthermore, their performance degrades significantly in large-scale and highly dynamic networks, highlighting the need for more intelligent, adaptive, and scalable security solutions.

3. Machine Learning-Based Approaches

Farahani (2021): The study proposed a Support Vector Machine (SVM)-based anomaly detection system for identifying black hole attacks in MANET environments. By leveraging supervised learning techniques, the model analyzes network traffic patterns and classifies nodes as either normal or malicious based on extracted features. The results demonstrated a detection accuracy in the range of approximately 85–90%, along with improved classification performance in identifying malicious nodes compared to traditional rule-based methods. However, the approach has certain limitations, as it relies heavily on manual feature extraction, which can be time-consuming and dependent on domain expertise. Additionally, the model exhibits poor adaptability to unseen or evolving attack scenarios, limiting its effectiveness in highly dynamic and real-world MANET environments.

Alam et al. (2022): The study introduced a machine learning-based anomaly detection approach that utilizes traffic features to identify malicious behavior in MANET environments. By analyzing parameters such as packet transmission patterns, delay, and node activity, the model enhances detection accuracy and significantly reduces false positive rates compared to traditional methods. This improvement highlights the effectiveness of data-driven techniques in identifying subtle anomalies in network behavior. However, the approach faces notable limitations, particularly due to the complexity of feature engineering, which requires careful selection and domain expertise to extract meaningful attributes. Additionally, the model exhibits limited scalability when applied to large and highly dynamic networks, where continuous topology changes affect performance. From a critical perspective, while machine learning techniques represent a substantial advancement in anomaly detection, they are still constrained by several factors. These models depend heavily on handcrafted features, which may not capture all relevant patterns in complex environments. Furthermore, they struggle to adapt to dynamic network topologies, as MANET structures frequently change due to node mobility. Another key limitation is their limited generalization capability, as models trained on specific datasets may fail to perform effectively in unseen or real-world scenarios. These challenges underscore the need for more advanced approaches, such as topology-aware and adaptive learning models.

4. Deep Learning-Based Approaches

Zaid et al. (2022): The study developed deep learning-based models for detecting attacks in MANET environments using neural network architectures capable of automatically learning complex patterns from network data. These models demonstrated strong performance, achieving detection accuracy greater than 90% and providing effective feature extraction through hierarchical learning, which eliminates the need for manual feature engineering. This ability to capture both spatial and temporal dependencies in network behavior makes deep learning approaches particularly suitable for identifying sophisticated and evolving attack patterns.

However, despite these advantages, the models suffer from significant limitations. They involve high computational complexity due to multiple layers and intensive training processes, which makes them resource-demanding. Additionally, deep learning models consume substantial energy, posing challenges for deployment in resource-constrained MANET nodes. These constraints limit their practicality in real-time and large-scale network scenarios, where efficiency and low power consumption are critical.

Lu et al. (2021): The study introduced deep learning frameworks for network attack detection, leveraging advanced neural network architectures to automatically learn complex patterns from raw network data. Unlike traditional machine learning approaches that rely on manual feature engineering, these frameworks enable automatic feature learning, allowing the model to extract relevant and hierarchical representations directly from input data. This significantly enhances the ability to identify subtle and non-linear attack patterns that may not be captured through handcrafted features. As a result, the approach improves overall pattern recognition capability, making it more effective in detecting sophisticated and evolving network attacks in dynamic MANET environments.

Kubota et al. (2021): The study applied deep learning techniques to cryptographic attack detection in MANET environments, demonstrating strong performance in identifying complex and sophisticated attack patterns. By leveraging advanced neural network architectures, the model was able to capture intricate relationships within encrypted or partially observable data, enabling accurate detection of anomalies that are difficult to identify using traditional methods. This highlights the effectiveness of deep learning in handling non-linear and high-dimensional data, making it particularly suitable for modern security challenges.

From a critical perspective, deep learning approaches offer significant advantages, including high detection accuracy and the ability to model complex attack behaviors. However, these benefits come with notable drawbacks. Deep learning models require substantial computational resources and intensive training processes, which can be challenging in resource-constrained MANET environments. Additionally, their high energy consumption and latency make them less suitable for real-time deployment on mobile nodes with limited processing capabilities. These limitations emphasize the need for lightweight and efficient alternatives or hybrid solutions for practical implementation.

5. Graph Neural Networks (GNN) for MANET Security

Francis et al. (2023): The study proposed a Graph Neural Network (GNN)-based approach for routing and attack detection in MANET environments, leveraging the inherent graph structure of the network to enhance security and performance. By modeling nodes and their communication links as a graph, the approach effectively captures both node features and their relationships, enabling more accurate identification of malicious behavior. The results demonstrated a high detection accuracy in the range of approximately 95–98%, along with improved scalability compared to traditional machine learning and routing-based methods. A key advantage of this approach lies in its ability to capture network topology, allowing it to understand structural dependencies and dynamic interactions between nodes, which significantly enhances its capability to detect complex and coordinated attacks.

Ramkumar et al. (2023): The study developed heterogeneous Graph Neural Network (GNN) models for secure routing in MANET environments, enabling the system to effectively detect malicious nodes while adapting to dynamic network topology changes. By incorporating heterogeneous node features and diverse relational information, the model enhances its ability to analyze complex interactions within the network. The findings indicate that this approach is highly effective in identifying malicious behavior and maintaining reliable communication even in rapidly changing network conditions.

From a critical perspective, GNN-based approaches offer several significant advantages. They model MANETs as graph structures, allowing them to naturally represent nodes and communication links. This enables the capture of

intricate node relationships and dependencies, which is essential for detecting coordinated and sophisticated attacks. Additionally, GNNs demonstrate good scalability compared to traditional machine learning methods, particularly in handling dynamic environments.
However, despite these strengths, GNN models remain computationally intensive due to the complexity of graph-based learning and message-passing operations. This can pose challenges in resource-constrained MANET nodes, where processing power and energy are limited.
In conclusion, GNN-based models emerge as the most suitable approach for MANET security, as they provide topology-aware, adaptive, and highly accurate detection mechanisms, making them particularly effective for securing dynamic and decentralized network environments.

6. Similarity-Navigated Graph Neural Networks (SNGNN)
Zou et al. (2023): Introduced SNGNN to improve node embedding using similarity metrics.
Key Contributions
- Uses similarity matrix instead of adjacency only
- Improves node classification
- Handles heterophily

Performance Improvements
- Higher detection accuracy than GNN
- Better generalization
- Improved robustness

Critical Analysis
SNGNN enhances:
- Node representation
- Detection accuracy
- Adaptability

7. Optimization-Based Approaches
Hasan et al. (2022): Introduced optimization-based models for improving security systems.
Contribution
- Improved convergence
- Reduced computation

Bio-Inspired Optimization (2020–2023)
Includes:
- Ant Colony Optimization
- Particle Swarm Optimization
- Cat Hunting Optimization

Advantages
- Faster convergence
- Efficient routing

Critical Analysis
Optimization:
- Enhances performance
- Reduces overhead

8. Lightweight Cryptography
Shukla et al. (2021): Proposed cryptographic mechanisms for secure routing.
Findings
- Improved data security
- Prevented unauthorized access

Blockchain-Based Approaches (2022–2023)
- Secure communication
- Decentralized trust

Critical Analysis
Traditional cryptography:
- High overhead

Lightweight cryptography:
- Low energy
- Fast processing

9. Hybrid Approaches (Recent Trend)
Recent studies combine:
- GNN/SNGNN
- Optimization
- Cryptography

Benefits
- High detection accuracy (>95%)
- Improved efficiency
- Enhanced security

10. Comparative Literature Summary

Year	Author	Method	Accuracy	Limitation
2020	Khan	ACO	~80%	Slow convergence
2021	Farahani	SVM	~85%	Feature dependency
2021	Lu	DL	~90%	High complexity
2022	Zaid	DL	~92%	Energy consumption
2023	Francis	GNN	~95%	Computation
2023	Zou	SNGNN	~97%	Emerging

11. Final Literature Review Synthesis
The literature demonstrates a clear evolution in security approaches for MANETs, reflecting a gradual shift from conventional techniques to advanced intelligent frameworks. Traditional methods exhibit low performance due to their reliance on static rules and inability to handle dynamic and sophisticated attacks. Machine learning approaches provide moderate improvement by enabling data-driven detection, while deep learning techniques achieve high accuracy through advanced feature extraction

and pattern recognition. However, deep learning models are often inefficient in resource-constrained environments due to their high computational and energy requirements. Graph Neural Networks (GNNs) offer the best balance between accuracy, adaptability, and structural awareness by effectively modeling network topology. Further advancements in similarity-navigated GNN (SNGNN) models achieve the highest performance by leveraging similarity-based learning to detect anomalies more precisely. Hybrid approaches, which integrate AI, cryptography, and optimization techniques, are emerging as the future direction for achieving comprehensive and robust MANET security.

Despite these advancements, several key research gaps remain. One of the primary challenges is the lack of lightweight GNN models that can operate efficiently in resource-constrained environments. Additionally, there is limited integration of artificial intelligence with cryptographic mechanisms, which restricts the development of fully secure and adaptive systems. High computational complexity continues to be a significant barrier, particularly for deep learning and GNN-based models. Real-time deployment remains difficult due to processing delays and resource limitations, while scalability issues hinder performance in large-scale and highly dynamic MANET environments.

Overall, the literature clearly indicates that graph-based models dominate modern research in MANET security due to their ability to capture network structure and relationships. Similarity-based learning further enhances detection performance by identifying subtle deviations in node behavior. Optimization techniques contribute to improving model efficiency and performance, while lightweight cryptography plays a crucial role in ensuring secure communication without imposing excessive computational overhead. Together, these advancements highlight the direction toward integrated, efficient, and intelligent security frameworks for next-generation MANET systems.

Comparative Table and Analysis

Technique	Core Strength	Advantages	Limitations	Summary
CNN (Deep Learning)	Hierarchical feature extraction	High classification accuracy for side-channel signals	High computational and memory requirements	Effectively extracts leakage features but is resource intensive.
Reinforcement Learning (RL)	Adaptive decision-making	Learns dynamically from changing environments	Slow convergence and training instability	Suitable for adaptive security but less effective for classification.
Federated Learning (FL)	Privacy-preserving distributed learning	Protects user data and supports scalability	Communication and synchronization overhead	Ideal for distributed 6G security with improved privacy.
Hybrid Deep Learning (CNN + LSTM / Attention)	Spatial and temporal feature learning	High detection accuracy and robustness	Increased model complexity	Provides superior detection by combining complementary learning mechanisms.
Deep Kronecker Neural Network (DKNN)	Efficient parameter reduction	Lower computational cost with high accuracy	Emerging architecture with limited adoption	Well suited for resource-constrained mobile devices.
DKNN + HCHO (Proposed)	Optimized deep learning with metaheuristic optimization	Very high accuracy, fast convergence, scalable and energy efficient	Implementation complexity	Offers the best overall performance for secure AI-enabled 6G mobile devices.

Analysis

The comparative analysis of various approaches for preventing black hole attacks in MANETs highlights a clear evolution from traditional rule-based mechanisms to advanced intelligent and hybrid frameworks. Traditional methods, including trust-based and rule-based systems, are computationally efficient and introduce minimal delay; however, they suffer from low detection accuracy and high false positive rates.

Their reliance on predefined rules makes them incapable of handling adaptive, coordinated, and large-scale attacks in dynamic network environments. As a result, their effectiveness is significantly limited in modern MANET scenarios.

Machine learning-based approaches represent an important advancement by enabling data-driven anomaly detection. These models improve detection accuracy and reduce false positives by analyzing traffic patterns and node behavior. They offer moderate scalability and adaptability, making them suitable for medium-sized networks. However, their dependence on handcrafted features and limited ability to generalize across unseen scenarios restrict their performance in highly dynamic MANET environments.

Deep learning approaches further enhance detection capabilities by introducing automatic feature extraction and hierarchical pattern recognition. These models achieve high detection accuracy and can identify complex attack patterns more effectively than traditional and machine learning methods. Nevertheless, they come with significant drawbacks, including high computational complexity, increased energy consumption, and limited real-time applicability. These limitations make deep learning models less suitable for deployment in resource-constrained MANET nodes.

Graph Neural Networks (GNNs) represent a major breakthrough by incorporating topology-aware learning into the detection process. By modeling the network as a graph, GNNs capture both node features and their relationships, enabling more accurate and context-aware detection of malicious nodes. This results in very high detection accuracy, improved packet delivery ratio, and enhanced robustness against complex and coordinated attacks. Additionally, GNNs offer better scalability compared to deep learning models. However, their computational requirements and vulnerability to adversarial graph attacks remain key challenges.

Similarity-Navigated Graph Neural Networks (SNGNN) further improve upon traditional GNNs by integrating similarity-based learning into node embeddings. This enhancement allows for more precise anomaly detection, reduced false positive rates, and improved adaptability in dynamic network conditions. SNGNN achieves the highest performance among standalone models by effectively combining structural and behavioral analysis of nodes, making it highly suitable for complex MANET environments.

Hybrid approaches, which integrate SNGNN with optimization techniques and lightweight cryptography, represent the most advanced and effective solution. These frameworks combine intelligent detection, efficient computation, and secure communication within a unified architecture. As a result, they achieve the highest detection accuracy, optimal network performance, and strong robustness against multiple types of attacks. Optimization techniques help reduce computational overhead and improve real-time performance, while lightweight cryptography ensures secure communication with minimal energy consumption. Despite these advantages, hybrid systems introduce implementation complexity and require careful design to balance scalability, efficiency, and security.

Overall, the analysis demonstrates that graph-based models dominate modern MANET security research due to their ability to capture network structure and relationships. Similarity-based learning further enhances detection performance, while optimization techniques improve efficiency and enable practical deployment. Lightweight cryptography plays a crucial role in ensuring secure communication without imposing excessive overhead. The integration of these techniques in hybrid frameworks represents the most promising direction for developing scalable, efficient, and robust MANET security solutions in the future.

Discussion

The evolution of MANET security mechanisms reflects a transition from static and rule-based approaches to intelligent and adaptive systems. Traditional methods, although simple and efficient, fail to address sophisticated attacks such as black hole attacks due to their inability to adapt to dynamic network conditions. Machine learning approaches introduced data-driven detection mechanisms, improving accuracy but requiring extensive feature engineering.

Deep learning models further enhanced detection capabilities by enabling automatic feature extraction and learning complex patterns. However, their high computational complexity limits their applicability in resource-constrained environments such as MANETs. Graph Neural Networks provide a more suitable alternative by leveraging network topology and relationships between nodes, enabling accurate and scalable detection.

Similarity-Navigated Graph Neural Networks improve upon GNN by incorporating similarity metrics, enhancing node representation and detection accuracy. Optimization techniques further improve efficiency by reducing computational overhead and improving convergence speed.

Lightweight cryptography complements detection mechanisms by ensuring secure communication with minimal resource consumption. The integration of these techniques into hybrid frameworks provides a comprehensive solution for MANET security.

Conclusion

This paper presented a comprehensive review of methods for preventing black hole attacks in MANETs. The study highlighted the limitations of traditional and machine learning approaches and emphasized the advantages of graph-based and hybrid models.

Graph Neural Networks emerged as the most effective solution due to their ability to model network topology. SNGNN further enhances performance by incorporating similarity-based learning. Lightweight cryptography ensures secure communication with minimal overhead.

Hybrid approaches integrating SNGNN, optimization, and cryptography provide the best performance. Future research should focus on lightweight, scalable, and real-time solutions for MANET security.

References

Abdelhamid, A. (2023). Lightweight anomaly detection system. *Electronics*, 12(6), 1294. https://doi.org/10.3390/electronics12061294

Kumari, A., et al. (2023). Detection of black hole attack. https://doi.org/10.21203/rs.3.rs-1528078/v1

Khan, D. M., et al. (2020). Ant colony optimization for MANET.

Farahani, G. (2021). Black hole detection using ML. https://doi.org/10.1155/2021/9993504

Shukla, M., et al. (2021). Cryptographic security in MANET. https://doi.org/10.1007/s11276-021-02667-2

Ram, A., et al. (2021). Secure AODV routing.

Alam, M., et al. (2022). ML anomaly detection. https://doi.org/10.1109/ACCESS.2022.3178901

Hasan, M., et al. (2022). Optimization-based security.

Zaid, G., et al. (2022). Deep learning detection. https://doi.org/10.1109/TIFS.2022.3156789

Nakano, Y., et al. (2023). RREQ-based detection.

Shrestha, S., et al. (2020). Secure routing in MANET. https://doi.org/10.1109/iEECON48109.2020.229545

Lo, S. K., et al. (2021). Blockchain IoT security. https://doi.org/10.1109/ACCESS.2019.2917412

Subhita, M., et al. (2023). Blockchain security in MANET. https://doi.org/10.3390/s23136132

Abdel-Sattar, A. (2022). Blockchain-based MANET security.

Sugumaran, V. (2023). Lightweight blockchain IDS.

Ilakkiya, N. (2023). Secure routing protocol.

Verma, R. (2022). Blockchain communication. https://doi.org/10.1063/5.0115134

Abid, A. (2022). VABLOCK communication. https://doi.org/10.1016/j.micpro.2022.104569