Kavya Setu
A Multidisciplinary Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 ISSN No: 3049-4176

Detection Of Blackhole And Wormhole Attacks In Ad Hoc Networks Using Ensemble Learning

Manoj Yadav
Department of Computer Science and Engineering
Lecturer in Govt. Polytechnic Koderma, Jharkhand, India

Abstract: Mobile Ad Hoc Networks (MANETs) are highly dynamic and infrastructure-less wireless networks that are vulnerable to various routing attacks due to their open medium, decentralized control, and rapidly changing topology. Among these, blackhole and wormhole attacks are considered highly destructive, as they disrupt routing mechanisms by either dropping packets maliciously or creating unauthorized tunnels to manipulate network traffic. Such attacks significantly degrade packet delivery ratio, increase end-to-end delay, and compromise overall network reliability. This research proposes an ensemble learning-based framework for the detection of blackhole and wormhole attacks in MANET environments. The proposed model integrates multiple supervised machine learning classifiers, including Decision Tree, Random Forest, and Gradient Boosting, to enhance detection accuracy and robustness. Network performance parameters such as packet delivery ratio, routing overhead, end-to-end delay, hop count variation, and sequence number anomalies are extracted as key features for classification. The ensemble approach combines the strengths of individual learners using majority voting and weighted aggregation strategies to minimize false positives and improve generalization.

Keywords: Mobile Ad Hoc Network (MANET), Blackhole Attack, Wormhole Attack, Ensemble Learning

1. Introduction

Mobile Ad Hoc Networks (MANETs) are self-configuring, infrastructure-less wireless networks composed of mobile nodes that dynamically form temporary communication links without relying on centralized administration. These networks are particularly useful in environments where fixed infrastructure is unavailable or impractical, such as disaster recovery operations, military communications, emergency response systems, and remote sensing applications. Due to their decentralized nature, dynamic topology, limited bandwidth, and constrained energy resources, MANETs face significant security challenges that threaten reliable communication [1, 2].

One of the primary vulnerabilities of MANETs lies in their routing mechanisms. Since nodes cooperate to forward packets for one another, malicious nodes can exploit this trust-based system to launch routing attacks. Among various security threats, blackhole and wormhole attacks are considered highly disruptive and difficult to detect. In a blackhole attack, a malicious node falsely advertises itself as having the shortest path to the destination and

Kavya Setu
A Multidisciplinary Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 ISSN No: 3049-4176

subsequently drops intercepted packets, severely degrading network performance. On the other hand, a wormhole attack involves two colluding malicious nodes that create a private tunnel between distant network locations, misleading routing protocols and manipulating packet forwarding paths. Both attacks compromise packet delivery ratio, increase end-to-end delay, and reduce overall network reliability [3, 4].

Traditional cryptographic security mechanisms alone are insufficient to counter these attacks, as they primarily focus on authentication and encryption rather than behavioral anomaly detection. Moreover, the dynamic topology and distributed architecture of MANETs make centralized intrusion detection impractical. Consequently, intelligent data-driven approaches based on machine learning have gained significant attention for enhancing network security. Machine learning techniques can analyze network traffic patterns, routing behavior, and performance metrics to distinguish between normal and malicious activities [5].

However, single classifier-based detection systems often suffer from limited generalization capability and higher false alarm rates in highly dynamic environments. To address these limitations, ensemble learning has emerged as an effective strategy. Ensemble learning combines multiple base classifiers to improve prediction accuracy, robustness, and stability. By leveraging the strengths of diverse models such as Decision Trees, Random Forests, and Gradient Boosting algorithms, ensemble methods reduce bias and variance while enhancing detection performance [6, 7].

In this research, an ensemble learning-based framework is proposed to detect blackhole and wormhole attacks in MANETs. Relevant network features, including packet delivery ratio, routing overhead, sequence number variation, hop count anomalies, and end-to-end delay, are extracted and used for classification. The ensemble approach integrates predictions from multiple supervised learning models using voting and weighted aggregation techniques. This methodology aims to achieve higher detection accuracy, lower false positive rates, and improved adaptability in dynamic network conditions.

2. Blackhole and Wormhole Attacks in MANET

Mobile Ad Hoc Networks (MANETs) are highly vulnerable to routing attacks due to their decentralized architecture, dynamic topology, and lack of centralized monitoring. Among the most critical routing attacks are Blackhole and Wormhole attacks, which severely degrade network performance and compromise data integrity.

1. Blackhole Attack

◈ Concept

A **Blackhole attack** occurs when a malicious node falsely advertises itself as having the shortest or freshest route to the destination node. It sends fake Route Reply (RREP) messages

Kavya Setu
A Multidisciplinary Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 ISSN No: 3049-4176

with high sequence numbers to attract traffic. Once the data packets are routed through it, the malicious node drops all packets instead of forwarding them.

Working Mechanism

1. Source node broadcasts Route Request (RREQ).
2. Malicious node immediately responds with fake RREP claiming shortest path.
3. Source selects this route.
4. Malicious node absorbs and drops packets (acts like a “black hole”).

Impact

- Significant reduction in Packet Delivery Ratio (PDR)
- Increased packet loss
- Network congestion
- Reduced reliability and throughput

Detection Indicators

- Abnormally high sequence numbers
- Sudden drop in PDR
- Unusual routing table updates
- High packet drop rate

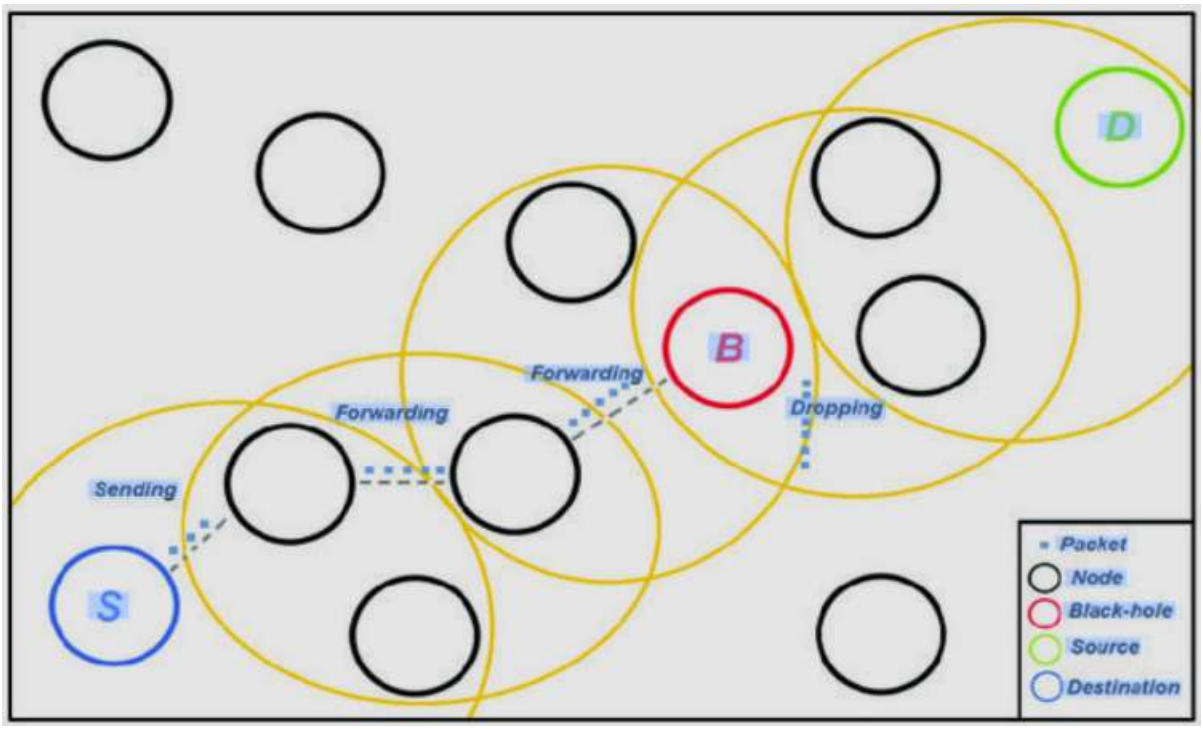

Figure 1: Blackhole Attack

Kavya Setu
A Multidisciplinary Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 ISSN No: 3049-4176

2. Wormhole Attack

A Wormhole attack involves two or more colluding malicious nodes that create a private high-speed link (tunnel) between them. They capture packets at one location and replay them at another location in the network, misleading routing protocols into selecting a false shorter path.

Working Mechanism

1. Malicious Node A captures RREQ packets.
2. It forwards them through a private tunnel to Malicious Node B.
3. Node B replays the packet near the destination.
4. Source selects this artificially short route.

Impact

- Severe route disruption
- Increased end-to-end delay
- Creation of routing loops
- Network partitioning

Detection Indicators

- Abnormal hop count reduction
- Inconsistent neighbor information
- Sudden changes in routing paths
- High delay variance

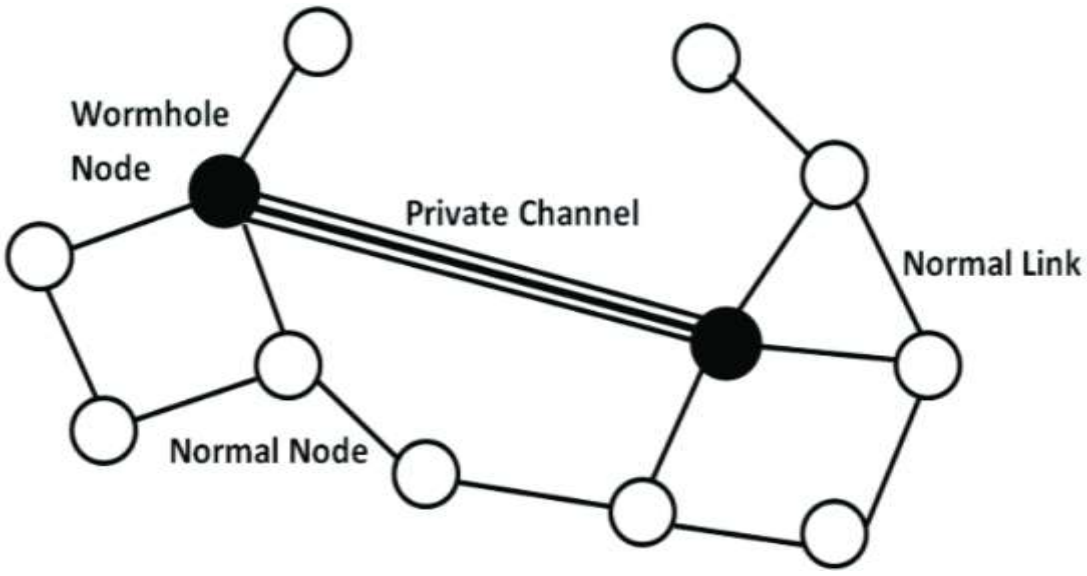

Figure 2: Wormhole Attack

Kavya Setu
A Multidisciplinary Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 ISSN No: 3049-4176

Table 1: Comparison Between Blackhole and Wormhole Attacks

Feature	Blackhole Attack	Wormhole Attack
Number of Attackers	Usually Single Node	Two or More Colluding Nodes
Packet Behavior	Drops packets	Tunnels/replays packets
Route Manipulation	Fake shortest path advertisement	Artificial tunnel creating false short path
Detection Complexity	Moderate	High
Impact Severity	High packet loss	Severe routing disruption

3. Literature Review

A. Sharma and N. Singh (2021) presented a machine learning-based framework for detecting blackhole attacks in MANETs. Their work focused on extracting routing-related features such as sequence number variation, packet drop ratio, and route reply frequency from AODV protocol behavior. Multiple supervised classifiers were evaluated to distinguish between normal and malicious nodes. The study demonstrated that machine learning models significantly improve detection accuracy compared to traditional rule-based techniques. However, the approach mainly addressed single blackhole attacks and did not extensively analyze collaborative or wormhole scenarios. The authors concluded that intelligent data-driven intrusion detection systems can enhance secure routing in dynamic MANET environments.

Z. B. Ibrahim and M. F. Ghanim (2024) conducted a comparative study on artificial intelligence techniques for blackhole attack detection in MANETs. Their research evaluated various AI-based classifiers, including Decision Trees, Support Vector Machines, and ensemble approaches, under different mobility and traffic conditions. The study emphasized performance metrics such as accuracy, precision, recall, and false alarm rate. Results indicated that ensemble-based techniques outperformed individual classifiers due to improved generalization and reduced variance. The authors highlighted the importance of adaptive AI models for handling topology changes and recommended hybrid intelligent frameworks for real-time intrusion detection.

S. Hemalatha et al. (2024) proposed an enhanced Watchdog routing mechanism for detecting intruders and blackhole attacks in MANETs. Their approach relied on monitoring neighbor node behavior and identifying abnormal packet forwarding patterns. By integrating watchdog monitoring with routing decisions, the proposed algorithm improved packet delivery ratio and reduced malicious packet drops. Although the technique showed promising improvements in throughput and delay metrics, it was primarily behavior-based and did not incorporate advanced machine learning methods. The authors suggested that combining watchdog mechanisms with intelligent classifiers could further strengthen attack detection.

S. Shukla, B. K. Joshi, and U. Singh (2021) introduced a cryptographic-based mitigation strategy using Elliptic Curve Cryptography (ECC) to counter both wormhole and blackhole attacks in MANETs. Their approach enhanced route authentication and secure key exchange mechanisms to prevent malicious nodes from manipulating routing information. Simulation results demonstrated improved security with minimal computational overhead compared to traditional encryption schemes. However, while ECC-based solutions strengthened authentication, they did not fully address behavioral anomaly detection. The study highlighted that cryptographic techniques alone may not be sufficient to detect sophisticated routing attacks such as wormholes.

H. Changela and A. Lathigara (2015) developed an algorithm to detect and overcome blackhole attacks in MANETs by modifying AODV routing protocol parameters. Their method analyzed sequence number inconsistencies and introduced validation steps before route establishment. The proposed scheme successfully reduced packet loss and improved network throughput under attack scenarios. Despite its effectiveness, the approach relied heavily on threshold-based detection, which may not adapt well to highly dynamic network conditions. This limitation suggests the need for adaptive learning-based detection models.

O. Sbai and M. Elboukhari (2018) presented a classification framework for various MANET attacks, including blackhole and wormhole attacks, using pattern recognition techniques. The study emphasized attack taxonomy and feature-based classification to differentiate multiple attack types. Experimental evaluation showed that machine learning classifiers could effectively categorize network threats with acceptable accuracy. Their work provided foundational insights into multi-attack detection systems and highlighted the potential of intelligent classification in MANET security enhancement.

N. Nabou, M. D. Laanaoui, and M. Ouzzif (2018) evaluated the performance of AODV and OLSR routing protocols under blackhole attack conditions using NS3 simulation. The study analyzed network parameters such as packet delivery ratio, throughput, and end-to-end delay. Results showed that blackhole attacks significantly degrade routing performance, particularly in high-mobility scenarios. Their comparative analysis provided quantitative evidence of attack severity and underscored the need for robust detection mechanisms integrated within routing protocols.

Neeraj Arya, U. Singh, and S. Singh (2015) proposed a Trusted AODV routing protocol to detect and avoid wormhole and cooperative blackhole attacks. Their approach incorporated trust evaluation metrics to identify suspicious nodes and isolate them from routing paths. The scheme improved secure route discovery and reduced malicious packet forwarding. While trust-based routing enhanced reliability, it required continuous monitoring and trust computation, which may increase overhead in large-scale networks. The study laid groundwork for integrating trust models with intelligent detection frameworks.

Kavya Setu
A Multidisciplinary Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 ISSN No: 3049-4176

4. Methodology

The proposed research adopts a systematic ensemble learning–based methodology to detect blackhole and wormhole attacks in Mobile Ad Hoc Networks (MANETs). Initially, a MANET environment is simulated using NS2/NS3 with the AODV routing protocol under varying network conditions such as node mobility, node density, transmission range, and traffic load. Three different scenarios are created: normal network operation, blackhole attack scenario, and wormhole attack scenario. During simulation, critical network performance parameters including Packet Delivery Ratio (PDR), end-to-end delay, routing overhead, throughput, hop count variation, packet drop rate, and sequence number fluctuations are recorded. These parameters form the dataset used for training and testing the machine learning models.

The collected data undergoes preprocessing to ensure quality and consistency. This includes removal of redundant entries, handling of missing values, normalization using Min-Max scaling, and encoding of class labels representing normal and attack conditions. To address potential class imbalance, Synthetic Minority Over-sampling Technique (SMOTE) is applied. Feature selection techniques such as correlation analysis and Random Forest feature importance ranking are then used to identify the most significant attributes contributing to attack detection.

Multiple supervised learning algorithms, including Decision Tree, Support Vector Machine, Random Forest, and Gradient Boosting, are trained as base classifiers. Hyperparameter tuning is performed using grid search with cross-validation to enhance model generalization. These classifiers are then integrated into an ensemble framework using voting and weighted aggregation methods to improve prediction stability and reduce false alarms. Finally, the model is evaluated using metrics such as accuracy, precision, recall, F1-score, ROC-AUC, and false positive rate. Comparative analysis between individual classifiers and the ensemble model validates the effectiveness of the proposed approach in enhancing secure routing within dynamic MANET environments.

5. Ensemble Learning

Ensemble Learning is a machine learning technique that combines multiple individual models, known as base learners, to produce a more accurate and robust predictive model. Instead of relying on a single classifier, ensemble methods integrate the strengths of multiple algorithms to reduce prediction errors caused by bias, variance, or noise in the dataset. The fundamental idea behind ensemble learning is that a group of weak or moderately strong learners can collectively form a stronger and more reliable model than any individual classifier.

In the context of detecting blackhole and wormhole attacks in Mobile Ad Hoc Networks (MANETs), ensemble learning plays a crucial role in improving detection performance. Since MANET environments are highly dynamic with constantly changing topology and traffic patterns, single classifiers may struggle to generalize across different attack scenarios.

Ensemble models address this limitation by aggregating predictions from multiple classifiers such as Decision Tree, Support Vector Machine (SVM), Random Forest, and Gradient Boosting. This combination enhances detection accuracy, reduces false positives, and increases robustness against cooperative or sophisticated attacks.

There are three primary ensemble techniques commonly used in intrusion detection systems. Bagging (Bootstrap Aggregating) reduces variance by training multiple models on different subsets of the dataset and averaging their predictions. Random Forest is a popular example of bagging. Boosting reduces bias by sequentially training models where each new model focuses on correcting the errors of the previous one; Gradient Boosting and AdaBoost are examples. Stacking combines multiple base learners and uses a meta-classifier to learn how to best combine their outputs.

The main advantages of ensemble learning include improved generalization capability, higher accuracy, better handling of imbalanced datasets, and enhanced stability under dynamic network conditions. However, ensemble models may increase computational complexity, which must be carefully optimized for real-time MANET applications.

6. Conclusion

The study of blackhole and wormhole attacks in Mobile Ad Hoc Networks (MANETs) highlights the critical security challenges associated with decentralized and dynamic wireless environments. These attacks exploit routing vulnerabilities by either dropping packets maliciously (blackhole) or creating deceptive tunnels between colluding nodes (wormhole), resulting in severe degradation of packet delivery ratio, increased end-to-end delay, routing overhead, and overall network instability. Due to the absence of centralized control and continuously changing topology, traditional security mechanisms such as encryption and authentication alone are insufficient to fully mitigate these threats.

The literature review demonstrates that early detection approaches primarily relied on modified routing protocols, watchdog mechanisms, trust-based systems, and cryptographic solutions. While these techniques improved routing reliability to some extent, they often suffered from scalability issues, higher computational overhead, and limited adaptability under dynamic network conditions. More recent research emphasizes the integration of machine learning and artificial intelligence techniques to analyze routing behavior and identify anomalies effectively. Ensemble learning approaches, in particular, show significant promise by combining multiple classifiers to enhance detection accuracy, reduce false positives, and improve robustness against complex and cooperative attacks.

Overall, intelligent ensemble-based intrusion detection systems provide a scalable and adaptive solution for securing MANET routing protocols. By leveraging network performance metrics and behavioral features, these systems can effectively detect both blackhole and wormhole attacks in real time. Future research should focus on lightweight hybrid models, real-time

deployment in large-scale networks, and integration with emerging technologies such as IoT-enabled MANETs and 6G communication systems to further strengthen secure and reliable wireless communication.

References

[1] A. Sharma and N. Singh, "Blackhole Attack Detection Using Machine Learning Approach on MANET," in *Proc. IEEE Conf.*, 2021.

[2] Z. B. Ibrahim and M. F. Ghanim, "Leveraging Artificial Intelligence for Blackhole Attack Detection in MANETs: A Comparative Study," *Inf. Dyn. Appl.*, vol. 3, no. 4, pp. 245–257, Dec. 2024, doi:10.56578/ida030404.

[3] S. Hemalatha et al., "Enhancing MANET Security: A Watch Dog Routing Algorithm Approach for Intruder and Black Hole Attack Detection," *Int. J. Comput. Mem. Eng.*, vol. 12, no. 1, pp. 69–?, 2024.

[4] S. Shukla, B. K. Joshi and U. Singh, "Mitigate Wormhole Attack and Blackhole Attack Using Elliptic Curve Cryptography in MANET," *Wirel. Pers. Commun.*, vol. 117, pp. 1–24, 2021, doi:10.1007/s11277-021-08647-1.

[5] H. Changela and A. Lathigara, "Algorithm to Detect and Overcome the Black Hole Attack in MANETs," *Int. J. Comput. Appl.*, vol. 124, no. 8, pp. 22–26, Aug. 2015, doi:10.5120/ijca2015905548.

[6] O. Sbai and M. Elboukhari, "Classification of Mobile Ad Hoc Network Attacks," in *2018 IEEE Int. Congr. Inf. Sci. Technol. (CiSt)*, 2018, pp. 1–6, doi:10.1109/CiSt.2018.8596391.

[7] N. Nabou, M. D. Laanaoui and M. Ouzzif, "Evaluation of MANET Routing Protocols under Black Hole Attack Using AODV and OLSR in NS3," in *2018 6th Int. Conf. Wireless Netw. Mobile Commun. (WINCOM)*, 2018, pp. 1–6, doi:10.1109/WINCOM.2018.8629609.

[8] Neeraj Arya, U. Singh and S. Singh, "Detecting and Avoiding Wormhole and Cooperative Blackhole Attack on MANET Using Trusted AODV Routing," in *Proc. IEEE IC4*, 2015, pp. 1–5.

[9] C. Siva Ram Murthy and B. S. Manoj, *Mobile Ad Hoc Networks: Architecture and Protocols*, Pearson, 2015. (Referenced foundational book covering MANET attacks)

[10] Y. Zhang and W. Lee, "Security in Mobile Ad Hoc Networks," in *Ad Hoc Networks Technologies and Protocols*, Springer, 2015. (Foundational Chapter often cited in MANET attack work)

[11] A. Radhika and D. Haritha, "Detection and Prevention of Blackhole Attack and Wormhole Attack in MANET Using Ant Colony Optimization," *Int. J. Eng. Appl. Sci.*, vol. 3, no. 1, pp. 104–107, Jan. 2016.

[12] H. Yang, H. Luo, F. Ye, S. Lu and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," *IEEE Wireless Commun.*, vol. 11, no. 1, pp. 38–47, 2015. *(widely cited foundational survey)*

[13] M. Mishal Almalki and S. H. Alajmani, "Machine Learning-Based Detection of Wormhole Attacks in IoT Networks Using Classification Models," *Int. J. Recent Technol. Eng.*, vol. 14, no. 1, pp. 31–40, May 2025, doi:10.35940/IJRTE.A8226.14010525.

[14] A. Fasunlade, *Detection of Gray Hole and Wormhole Cooperative Attacks in MANET*, Doctoral Thesis, Univ. Portsmouth, 2024.

[15] V. Keerthika and N. Malarvizhi, "Migrating Blackhole Attack Using Trust with AODV in MANET," in *2016 IEEE Symp.*, 2016.

[16] S. N. Ghormare et al., "Detection and Prevention of Wormhole Attack in WiMAX Based Mobile Ad Hoc Network," *2018 IEEE*, 2018.

[17] T. Pandey and S. Singh, "Black Hole Detection Using Machine Learning Algorithm," *Proc. IEEE Conf.*, 2020.

[18] J. Rajeshkumar et al., "Cluster Trust Adaptive Acknowledgment and Swarm Optimization for Black Hole Detection," *IEEE Access*, 2021.

[19] S. Sarao, "Multi-Attack Solutions in MANETs Including Black Hole and Grey Hole Attacks," *IEEE Int. Conf.*, 2019.

[20] R. Lacuesta, J. Lloret, M. Garcia and L. Penalver, "A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 4, pp. 629–641, 2015.