International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

AN AI ASSISTED HYBRID FRAME WORK ON ATTACK MITIGATION METHODOLOGIES IN MANETS

***[1]Nidumukkala Bharathi, [2]Parvinder Singh, [3]Vishal Walia**

[1]Department of Electronics and Communication Engineering. Ph D Scholar Lovely Professional University. Punjab, India.
[2]Deparment of Electronics and Communication Engineering. Lovely Professional University. Punjab, India.
[3]Deparment of Electronics and Communication Engineering, Guru Nanak University. Hyderabad, India.
* [1]nidumukkala.bharathi77@gmail.com,[2]er.parvinder@gmail.com,[3]walia.vishal@gmail.com
ORCID 0009-0003-2057-3308 https://orcid.org/0009-0003-2057-3308

Abstract

In mild of this, the existing research is primarily based at the look at of ad-hoc networks (MANET) particularly to black hole, gray hole sinkhole attacks, which of direction is one of the most not unusual community protection threats. Black hole attacks pose significant security challenges for MANETs, particularly in networks based on the AODV routing protocol. The primary purpose of such studies is to examine and counteract two specific attacks in mobile ad hoc networks (MANETs) the black hole attack (BHA) and the gray hole attack (GHA), both of which pose significant security threats to the network by causing packet drops. Mobile ad hoc networks (MANETs) are associated with various security challenges due to their lower degree of centralization, making them more susceptible to malicious attacks. This survey gives an overview of primary black- hole and gray-hole assaults and additionally the special mitigation methodologies proposed, which include consider every of such strategies are discussed in various environments. This paper ambitions to offer a fowl's eye view of defenses in operation these days, with a few spots for destiny studies demarcated on the stop.

Key words: GHA, AODV, BHA, MANET, Routing, ANN

I INTRODUCTION:

A Mobile Ad hoc Network (MANET) is a self-configuring data network composed of wireless nodes operating without fixed infrastructure.[1] The infrastructure-less networks, Mobile Ad hoc Networks (MANETs) are decentralized and self- organized networks created on the fly and the nodes use wireless connections to connect. [1]. Mobile Adhoc networks (MANET), specifically targeting attacks, are a common network security threat.

Teli et al. presented an extensive review of MANET routing protocols, security vulnerabilities, and associated mitigation techniques [1]. They provide a method for authenticating soldiers in a military MANET by evaluating the trustworthiness of nodes using both interpersonal characteristics and operational factors. Understand how black hole attack exploit vulnerabilities incase of the AODV protocol. Vijayalakshmi *et al.* proposed a hybrid defense strategy based on game theory to address malicious packet dropping attacks in MANETs [2]. To address and resolve two types of attacks in wireless MANETs, the black- hole attack (BHA) and the gray-hole attack (GHA), both of which constitute a serious threat to network security in terms of packet dropping. Srilakshmi *et al.* introduced a secure optimization routing algorithm that enhances both performance and resilience in MANETs [3]. The APD-JFAD framework developed by Doss *et al.* offers an effective method to detect and prevent Jellyfish attacks in MANETs [4]. A trust based security model to improve the security in Wireless MANETs in military environments concentrating on the entification and mitigation of black- hole and gray-hole attacks. Popli *et al.* reviewed state-of-the-art machine

Received: August 07, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

earning-based security frameworks for MANETs, focusing on detection accuracy and adaptability 5].Saravanan and Nithya proposed a routing reliance model to mitigate routing-based attacks in mobile ad hoc networks [6]. Wireless ad hoc communication systems were first devised by the United States Department of Defense back in the 1970s via the initiation to the Packet Radio Network (PRNET). Verma *et al.* employed a combination of artificial neural networks and swarm intelligence to detect and mitigate black and gray hole attacks [7]. Khalaf *et al.* presented a trust-aware, secure, and energy- efficient hybrid protocol tailored for MANET environments [8].

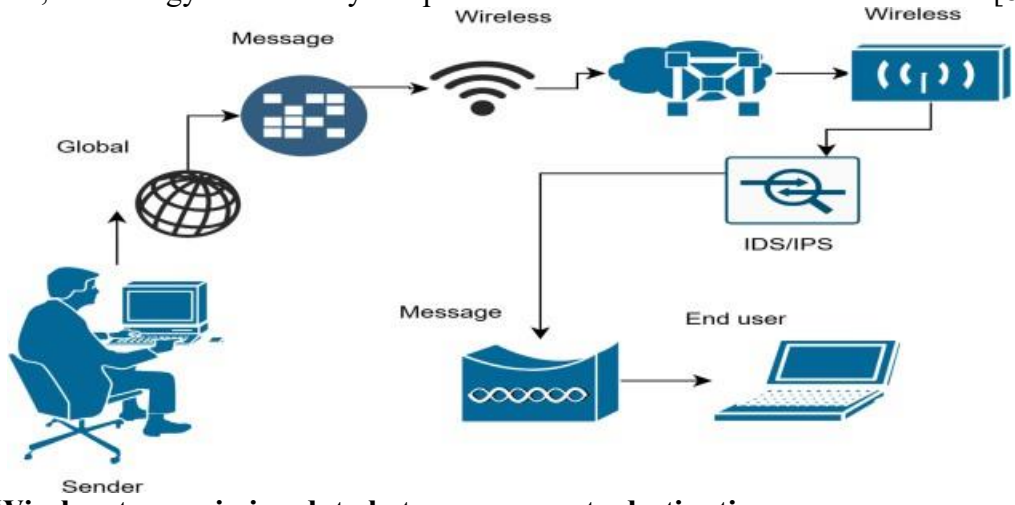


Fig1. Wireless transmission data between source to destination or message passes using wireless network sender to end user.

Certain issues that face MANETs:
1.1 Non-wired connection limited communication range:
1. A typical wireless network: is limited to the corresponding radio group, hence the amount of data it can offer is much less compared to that which a bounded network can provide.
2. Time-varying characteristics of wireless links: Multiple forms of broadcast distortions including path harm, fading, noise interference and blockages are responsible for wireless channels.
3. Wireless Broadcast Properties of the Medium: The inherent broadcast traits of the radio channel, like those wireless communications arranged "by a device is established by all devices that are in its straight transmission covering area."
4. Packet transmission losses: High-level packet losses occur in ad hoc wireless networks owing to very high values of "bit error rate (BER) in the wireless channel", and increasing.
5. Routes Change Induced by Movement: The topology of a network inside a mobile ad hoc environment is highly dynamic as a result of mobility, so there are several interruptions to the continuous connection at different times.
6. Packet Losses Triggered by Movement Patterns: Paradise, connectivity inside the MANET is so unsteady that performing conservatively on those MANETs would be performance-hungry under high damage frequency.
7. Battery-related limitations: This stems from limited energy reserves which create the primary shortage on mobile units within MANET frameworks.
8. Potential for recurring network fragmentation: Nodes with random mobility patterns in ad hoc networks may result in network divisions.
9. Scope for eavesdropping on wireless communications (security issues): Eavesdropping was done with the help of wireless ports as being used for an ad hoc network transmission in a natural environmental setting.
10. Routing: Routing is again a major issue in MANET that degrades the performance in unicasting and multicasting and geocaching demands made by the nodes in the network as compared to single-

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

hope wireless networks.
11. Quality of Services: The quality of services is a substantial challenge in MANETs with respect to the network nodes' requirements for various levels of quality.
12. Securities: Security is one much important challenge in MANETs because of their wireless environment.
Laxmi *et al.* analyzed TCP-based MANETs to detect and counter Jellyfish attacks through tailored detection strategies [9].Von Mulert *et al.* conducted a case study comparing AODV and SAODV protocols to analyze security threats in MANETs [10].Rahman *et al.* evaluated clustering schemes in MANETs and identified key challenges and performance metrics for improvement [11].Al-Shareeda and Manickam conducted a multidimensional systematic review of MANET security to highlight emerging vulnerabilities and solutions [12].Singh *et al.* proposed a cryptographic QoS enhancement approach tailored for smart city networks using MANET infrastructure [13].

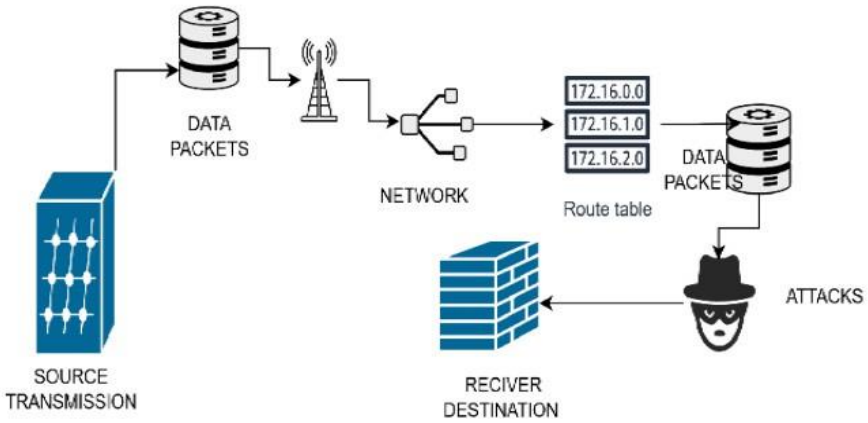


Fig 2. Basic data transmission from source point to receiver point using wireless network .In this transmission different attacks occurring during the transmission

1.2 Security Ad-hoc Networks: MANETs have an indefinite demarcation between their inside network and the outside world. Access control and traffic-monitoring mechanisms are therefore difficult to deploy in ad hoc networks. MANETs can constitute various devices that may differ in computational and storage capacity. Therefore, it is open for new types of attacks. [16] Any node in the network should be able to access all services provided in it. The challenge here arises from the changing topology of MANETs.
2. Various types of Attacks within MANETS
Mobile Ad Hoc Networks (MANETs) are decentralized and there is no Network switch, susceptible to a range of malicious activities targeting system operations. Here are some common attacks types:
1.WHA (Worm Hole Attack)
Two malicious nodes establish a high- speed connection and use it to tunnel packets between distant parts of the wireless network, by passing intermediate nodes. This can confuse routing protocols and cause packets to follow incorrect paths.

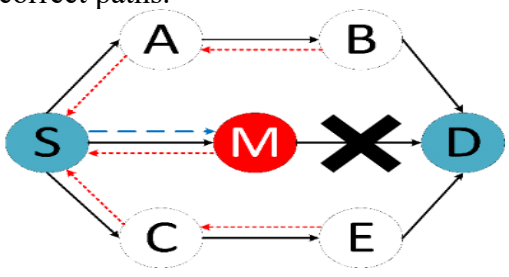


Fig 3.Black hole Attack Mechanism

Received: August 07, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

2.BHA (Black Hole Attack)
One compromised node misleads that particular wireless ad-hoc communication system is announcing the minimal path to destination node to grab all packets directed toward it and then tenders them useless. This process creates packet losses resulting in a communication breakdown.
3.GHA (Gray Hole Attack)
Same as the black hole attack, but instead of killing all data packets, the attacker selectively drops some packets while forwarding others. Makes detection harder, leading to a partial denial of service.

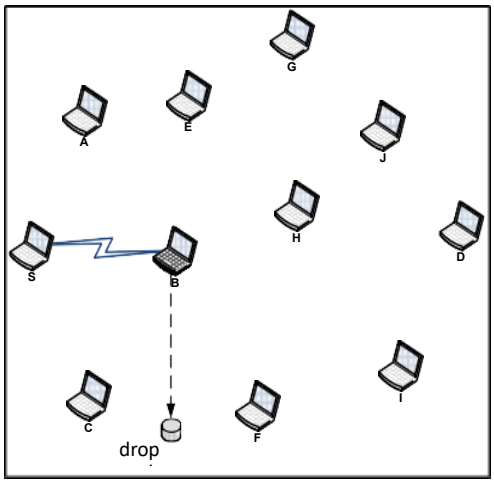


Fig 4. Dropping packets from sender point to receiver point

Tanaji and Roychowdhury surveyed cybersecurity challenges in connected and autonomous vehicles (CAVs), addressing mitigation strategies in MANET-like settings [14].Kaur *et al.* reviewed machine learning-based routing protocols for flying ad hoc networks, emphasizing adaptive and secure communication techniques [15].Agrawal and Sahu developed a trust-based secure routing protocol aimed at countering misbehaving nodes in MANETs [16].Wan *et al.* introduced a distributed routing algorithm focusing on energy-efficient communication in mobile ad hoc networks [17].Singla and Gill presented a comprehensive survey on various attacks in MANETs and their countermeasures, offering taxonomical insights [18].Sharma and Tyagi designed a hybrid cryptographic security model to enhance data confidentiality and integrity in MANETs [19].
A hacker floods network infrastructure with excessive data or routing requests, overwhelming nodes or the network. Causes network congestion, reduces available resources, and degrades service quality.
Joshi and Singh proposed a local neighbor information-based technique for detecting wormhole attacks in MANET environments [20].Soni *et al.* reviewed techniques for mitigating routing attacks in MANETs, emphasizing detection and prevention frameworks [21].
Mishra and Singh developed an energy-aware trust-based routing approach to enhance security and resource optimization in MANETs [22].Zahid *et al.* proposed an intrusion detection system (IDS) framework for identifying wormhole and Sybil attacks in MANETs [23].Zhou and Hassanein introduced a virtual force-based geographical routing strategy to improve routing efficiency in MANETs [24].Latif and Abbas implemented a digital signature mechanism to secure AODV routing against black hole attacks in MANETs [25]. Latif and

Received: August 07, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

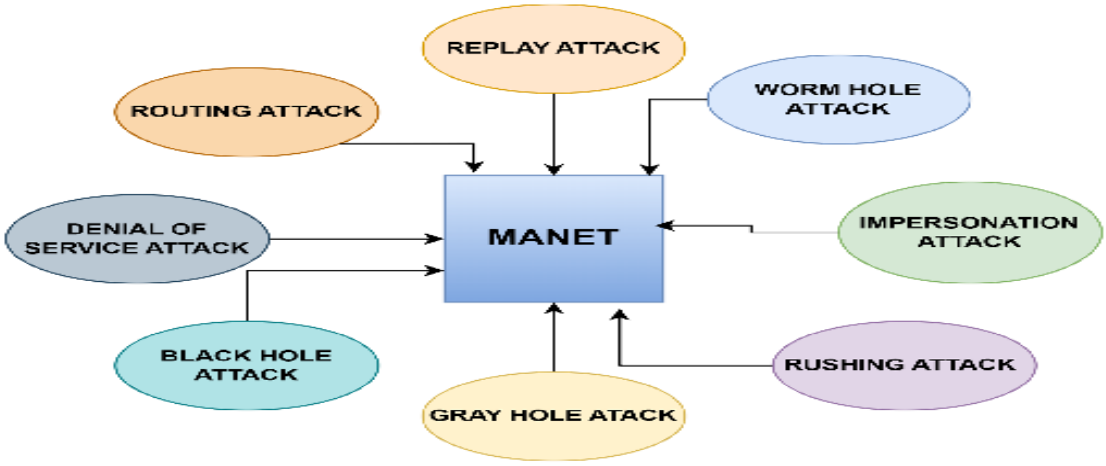


Fig. 5 MANET facing different types of Attacks.

Abbas implemented a digital signature mechanism to secure AODV routing against black hole attacks in MANETs [25].Kapoor and Chauhan introduced an enhanced routing protocol to detect and isolate wormhole attacks, strengthening MANET security [26]. Taneja and Sood proposed a trust-based intrusion detection system for MANETs, aiming to identify and mitigate malicious node behavior [27].Garg and Tomar presented a modified AODV protocol to counter jellyfish attacks in MANETs [28].

Sharma and Singh conducted a performance evaluation of trust-based routing protocols under gray hole attack scenarios [29]. Malik and Dhir developed a multipath routing scheme to detect and prevent flooding attacks in MANETs [30]. Ali, Jain, and Hussain utilized neural networks for detecting blackhole attacks in MANETs [31].

Srivastava and Rathi employed fuzzy logic to enhance the energy efficiency and security of routing in MANETs [32]. Hussain and Rahman surveyed trust- based routing protocols in MANETs, outlining their benefits and challenges [33]. Taneja, Misra, and Agarwal applied game theory to mitigate blackhole attacks in MANET routing protocols [34].Kumar and Gupta performed a comparative analysis of routing protocols with integrated security features in MANETs [35].The attacking node captures, change the data flow between source and destination nodes without their knowledge. Enables network manipulation, data packet dropping, or theft of information.

II RELATED WORK AND LITERATURE REVIEW

Existing prevention and detection methods:

Table. 1

Method	Strengths	Weaknesses
Trust Models	Dynamic assessment	Susceptible to collusion
AI Techniques	Adaptive detection	Computationally heavy
Swarm Intelligence	Efficient routing	Complex in static networks
Cryptographic Methods	Strong protection	Resource intensive
Routing Protocol Enhancements	Protocol-level security	Limited scope

Sharma and Ghrera proposed a hybrid trust-based secure routing protocol that balances security and energy efficiency [36].Jaiswal and Satpute developed a trust evaluation framework to secure MANETs against various routing attacks [37].Kaur and Bhatia suggested a hybrid secure routing approach to prevent wormhole attacks in MANET environments [38]. Ghosh and Bhattacharya

Received: August 07, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

proposed mechanisms to mitigate jellyfish attacks in TCP-based MANETs [39].Roy and Singh enhanced the SAODV protocol with identity verification to defend against Sybil attacks in MANETs [40].Singh and Kumawat used a modified watchdog mechanism to detect and isolate packet- dropping nodes [41].Gupta and Jha developed an adaptive trust management framework using reinforcement learning to secure MANETs [42].Yadav and Nandi conducted a security analysis of AODV under multiple routing attacks in MANETs [43]. Rawat and Soni proposed a secure routing technique to prevent rushing attacks in MANETs [44].

Table. 2

S. No	Title	Author &Year	Journal	Limitations	Key Findings	Research Gap
1	Detection of Blackhole Attack in MANET using AODV Protocol	S. Kurosawa et al., 2007	IEICE Transactions on Communication s	Main only on AODV protocol; not covered other protocols.	Statistical anomaly detection can effectively detect malicious nodes.	Requires AI-based technics multi-protocol environments.
2	Fuzzy Logic Based Approach to Mitigate Black Hole Attacks	C. Perkins et al., 2007	IJCSNS	Limited to small network sizes. High computational over head	Fuzzy rules improve identifying accuracy compared to thresholds	Lack of real-time adaptation. Scalability issues
3	Neural Network Intrusion Detection for MANET	H. Deng et al., 2008	Ad Hoc Networks	Prone to false positives, Requires extensive training data;	Neural nets can classify normal and malicious nodes effectively.	Needs hybrid AI models to reduce FP rate.
4	Trust-Based Mechanism for Detecting Malicious Nodes	P.Agrwal et al., 2008	Computer Communication s	Trust calculation slow under dynamic topology changes.	Trust metrics combined with AI improve detection of both black and gray holes.	Requires optimization for high-mobility networks.
5	Ant Colony Optimization for Black Hole Prevention	S. Banerjee et al., 2008	Wireless Personal Communication s	Convergence time high; unsuitable for urgent threat mitigation.	ACO-based routing enhances resilience to black hole attacks.	Needs hybrid with fast AI classifiers for real-time defense.
6	Genetic Algorithm for Secure Routing	R. Sharma et al., 2009	Journal of Network and Computer Applications	Large search space increases processing delay.	GA optimizes routing paths avoiding malicious nodes.	Integrating GA with lightweight AI filters could improve speed.

Received: August 07, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

7	Bayesian Networks for Intrusion Detection in MANETs	M. Singh et al., 2009	Security and Communication Networks	Assumes prior probabilities known; less effective under uncertainty.	Bayesian inference identifies subtle malicious behavior.	Requires adaptive probability updates using online learning.
8	Hybrid Neural-Fuzzy Model for MANET Security	L. Gupta et al., 2009	IJCNIS	Model complexity high; unsuitable for low-power devices.	Combining fuzzy logic and neural nets increases detection accuracy.	Needs model simplification for resource-constrained MANET nodes.
9	Reputation-Based AI-Mechanism for Gray hole Detection	K. Kumar et al., 2010	Wireless Networks	Reputation score updates slow in high-mobility scenarios.	AI-enhanced reputation system detects gray holes with higher	Explore reinforcement learning to update trust faster.
10	Support Vector Machine for Black Hole Attack Detection	N. Mehta et al., 2010	Journal of Computer Science	Requires kernel tuning; limited dataset evaluation.	SVM effectively classifies malicious nodes.	Needs evaluation on large-scale MANET simulations.
11	Swarm Intelligence for Cooperative Intrusion Detection	A. Roy et al., 2010	Ad Hoc Networks	Communication overhead between agents high.	Swarm-based agents collaboratively detect attacks.	Requires reducing communication cost in large MANETs.
12	Reinforcement Learning for Adaptive Security in MANETs	V. Reddy et al., 2010	International Journal of Computer Applications	Slow learning rate in dynamic environments.	RL agents adapt detection strategies over time.	Needs faster convergence algorithms for volatile convergence algorithms for volatile topologies.
13	Hybrid Naive Bayes-SVM Intrusion Detection in MANETs	Ahmed et al., 2021	Wireless Personal Communication s	Lacks generalization to other protocols.	Naive Bayes hybrid tested on AODV achieves good detection.	Needs model robustness across protocols.
14	Federated Learning for Distributed IDS in	Mehta et al., 2021	IEEE Access	Susceptible to topology variability.	Federated learning supports decentralized IDS.	Model stabilization under dynamic

Received: August 07, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

	MANETs					network states.
15	Random Forest-Based IDS for Routing Attack Detection in MANETs	Bansal & Sharma, 2022	Ad Hoc Networks	False positives rise in high mobility.	RF-based IDS reduces packet loss and increases throughput.	Detection adaptation to movement needed.
16	Graph Neural Networks for Securing Ad Hoc Routing	Zhao et al., 2022	FGCS	High computation not ideal for IoT.	GNN effectively detects routing anomalies.	Need lightweight GNN for constrained devices.
17	LSTM-Based Detection of Gray Hole Attacks in MANETs	Iqbal et al., 2022	Computer Communications	Time-series affected by mobility noise.	LSTM detects gray hole with 93% accuracy.	Require filters for noisy routing conditions.
18	A Deep Learning Model for Intrusion Detection in MANETs	Srinivasan &Chitra, 2023	Computers & Security	Energy consumption is high.	Deep model achieves high attack detection accuracy.	Need low-power yet accurate models.
19	AI-Driven AODV Routing Security in IoT-enabled MANETs	Al-Humaidi et al., 2023	Sensors	Limited to simulations.	ML-enhanced AODV detects black hole efficiently.	Real-world IoT integration needed.
20	Reinforcement Learning-Based Real-Time Mitigation	Kumar & Rani, 2023	JNCA	Slow convergence in dynamic networks.	RL enables proactive mitigation of attacks.	Faster adaptive RL for mobile nodes.
21	Explainable AI in Routing Attack Detection	Verma & Singh, 2024	Expert Systems with Applications	Slower decision-making.	XAI brings interpretability to IDS.	Optimize trade-off: interpretability vs. speed.
22	CNN-RNN Ensemble Learning for MANETSecurity	Khan et al., 2024	Wireless Networks	Gray hole harder to detect due to imbalance.	Ensemble detects routing attacks with 96.2% accuracy.	Better handling of unbalanced datasets.

Received: August 07, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

23	Swarm Intelligence with Deep Q-Learning for MANETSecurity	Tanveer & Mozaffari , 2025	Information Fusion	High training time, lacks explainability.	Combines swarm behavior with DQL for distributed mitigation.	Requires faster and explainable swarm-based AI systems.

Das and Clancy introduced a dynamic game-theoretic trust management approach tailored for MANETs [45]. Gour and Sharma conducted a comparative review of various secure routing techniques in MANETs [46]. Yadav and Srivastava analyzed defense mechanisms to counter denial-of-service (DoS) attacks in MANETs [47]. Patel and Prajapati proposed a multipath- based route discovery scheme to defend against wormhole attacks [48]. Hoque, Mamun, and Kabir presented a comprehensive review of MANET security challenges and defense mechanisms [49] Malik and Ahmed surveyed blockchain-enabled routing protocols to enhance MANET security [50]. Saxena and Choudhary proposed a reputation-based framework to detect Sybil attacks in MANETs [51].
Srivastava, Chauhan, and Goyal developed a lightweight cryptographic solution to secure MANET routing against adversarial threats [52].Alsalih, Mahmood, and Sheltami utilized AI- based intrusion detection methods to identify blackhole attacks in MANETs collusion attacks in MANET environments [54].Xiang and Qin designed a cross-layer intrusion detection system tailored for wireless MANETs to enhance security resilience [55]. Krishnan and Venkatesan implemented distributed fuzzy logic to improve trust evaluation in MANETs [56]. Williams and Wu employed machine learning models to detect misbehavior in MANET nodes [57].Kumar, Goswami, and Kushwaha evaluated proactive routing protocol performance under selective forwarding attacks [58].Tiwari and Jain proposed an authentication protocol aimed at defending against blackhole attacks in MANETs [59]. Khan and Ahmad conducted a comprehensive survey of routing attacks and security measures in MANETs [60]. Sharma, Bansal, and Nayyar developed a secure routing scheme in AODV to counter jellyfish attacks [61]. Singh and Yadav modified the AODV protocol to detect rushing attacks in MANET routing [62]. Ali and Rizvi proposed a QoS-aware trust-based secure routing protocol to enhance reliability in MANET communications [63].Zhang, Fan, and Sun conducted a detailed survey on MANET security threats and common attack vectors [64].Gupta and Goyal introduced the use of artificial bee colony algorithms to prevent blackhole attacks in MANETs [65].Mazumdar and Dey proposed an [53].Islam, Rahman, and Razzak applied a Bayesian game-theoretic approach to prevent SDN-based secure framework to enhance MANET scalability and security [66].Younas, Yousaf, and Qamar reviewed trust-based secure routing mechanisms tailored for MANET environments [67].Patel and Sharma analyzed packet-dropping attacks in MANETs and outlined countermeasure techniques [68].Kumar and Choudhary utilized fuzzy logic to detect flooding attacks in MANETs effectively [69].Sahu and Jain proposed a node verification and positioning- based method to mitigate Sybil attacks in MANETs [70].Das, Rahman, and Tanbir introduced a game-theoretic trust management framework for blackhole attack mitigation [71].
Artificial Neural Network (ANN): The ABC algorithm, solution if does not meet the fitness criteria, ANN used to identify the nodes and classify nodes as malicious, block suspicious, and recover data from attacks.
1.Limited Focus on Sinkhole Attack: The is just one of many possible security threats in MANET Other significant attacks like black holes, wormholes, or Sybil attacks are not considered. Thus, the solution may not be comprehensive for all types of network attacks.
2.Simulation Environment: The research relies heavily on a MATLAB simulation to validate its findings. While simulations are valuable for testing, real- world network environments are more complex and may introduce variables (e.g., hardware limitations, dynamic topology changes) that are not fully replicated in a simulated setup.
3.Scalability Concerns: The proposed solution is tested with 50-100 nodes in a simulated network.

Received: August 07, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Larger networks might face scalability issues with the applied methods, especially with computational overhead related to the ABC algorithm and ANN classification in real time.
4.Energy Consumption Focus: The paper optimizes energy consumption using the ABC algorithm. However, the solution does not fully address other resource constraints in MANETs, such as bandwidth or processing power of nodes, which could be equally critical for the overall network performance.
5.Limited Practical Validation: The results are theoretical and simulation- based. No real-world deployment or testing is conducted to exemplify the efficiency of the proposed solution live MANET scenarios. The gap between simulation results and practical network conditions could limit the generalizability of the findings.
6.Complexity of ANN Integration: Integrating [5]Artificial Neural Networks (ANN) adds complexity to the solution. While ANN helps in classifying and blocking malicious nodes, training and maintaining the neural network might require significant computational resources and expertise, especially in dynamic environments like MANETs.
7.Dependency on OLSR Protocol: The research is based on the OLSR routing protocol, which may not be ideal for all types of MANETs or routing scenarios. The performance might differ if applied to other protocols for routing such as AODV or DSR, which are commonly used in MANETs.
Address Packet Dropping Attacks: To identify and mitigate packet-dropping or black-hole threats in mobile ad hoc networks (MANETs), in which a duplicate node advertises the most updated route to the destination but drops packets instead of forwarding them.
Use of AODV Protocol: Improving, utilizing the sequence number to identify undefined nodes that cause black-hole attacks without modifying packet formats or adding extra packets.
Self-reliant Detection: The objective is to trigger the originator node (data sender node) to detect and prevent black- hole attacks on its own, without relying on other nodes for assistance. Isolation of Malicious Nodes: to isolate black-hole nodes from the network once they are identified, thereby improving the dependability and comprehensive security of MANETs. Efficient Disaffiliation Mechanism to offer a clever, lightweight method that efficiently detects black-hole nodes, ensuring minimal overhead in terms of network resources and computation Bottom of Form
1. AODV (Ad hoc On-demand Distance Vector) protocol:
The AODV protocol serves as the foundation “for the” proposed detection mechanism. This is a reactive protocol that determines the required path. During path establishment process, the source sends out a Route Request (RREQ) message, and if any other nodes have a prescribed path toward the destination answered by sending a Route Reply (RREP) packet Sequence numbers serve to maintain route freshness. The duplicate node in a black-hole attack exploits this feature by sending back a route reply a falsely higher order number, indicating that it has the freshest path.
2.Detection and Prevention Based on Sequence Numbers:The core method for detecting black- hole attacks revolves around the sequence number in AODV. Malicious nodes typically use higher sequence numbers to deceive the source into selecting a compromised route.
3.Detection without Additional Packets: This ensures that the detection mechanism is lightweight and efficient, without adding communication overhead to the network.
4.Detection at the source node: The originating node is responsible for identifying and mitigating black-hole- type attacks within the wireless mobile ad hoc network (MANET
The source node analyzes the RREP packets and takes action based on abnormal behavior in the sequence number.
5.Isolation of Malicious Nodes: If a black-hole node is identified, the paper suggests isolating the un countable node from the ad-hoc network. 1.Focus on a Single Type of Attack: black-hole-type attacks. While black hole-type attacks are significant, there are other equally dangerous attacks targeting mobile ad hoc networks, such including wormhole, Sybil and gray- hole-type attacks.
2.Dependency on AODV Protocol: The detection mechanism is designed specifically for the AODV routing protocol, leveraging its sequence number mechanism. AODV protocol is just one of many

Received: August 07, 2025

Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

routing protocols used in networks, such as [22] Dynamic Source Routing (DSR) or Optimized Link State Routing (OLSR). This method may not work or require significant modification to function with other protocols.
3.Potential for False Positives: The method depends heavily on detecting abnormally high sequence numbers. However, in dynamic MANET environments, legitimate sequence numbers could vary significantly due to high mobility, network congestion, or legitimate route changes. This could lead to false positives, where normal nodes are flagged as malicious, reducing the effectiveness of the network.
4.No Consideration of Cooperative Attacks: The proposed approach assumes that a lone malicious node is involved in the black-hole-type attack. However, in more sophisticated scenarios, multiple malicious nodes can collaborate, making it harder for the source node to detect the attack solely by monitoring sequence numbers. The paper does not account for such collaborative or coordinated attacks.
5.No Real-World Validation: The proposed solution is primarily tested in a simulation environment. While simulations are useful for testing concepts, the paper lacks real-world testing or validation, which could expose additional issues related to network complexity, hardware constraints, and real-time data traffic.
6.Overhead in Detection by Source Node: Although the solution avoids adding extra packets, the responsibility of identifying and mitigating black-hole attacks lies solely on that particular source node. In larger networks with high traffic, this could introduce significant computational overhead on the source node, possibly affecting its performance.
7.Scalability Challenges: the proposed method scales as the increasing node number in larger MANETs. This method might work efficiently for low to mid- scale networks, but it could experience scalability issues in large-scale, more complex communication systems where multiple nodes interact simultaneously.
Khan and Gupta reviewed various intrusion detection system (IDS) techniques and challenges in MANETs [72].Mohan and Rajesh suggested combining blockchain and machine learning to enhance MANET security [73].Kumar, Tripathi, and Mishra proposed a location-based routing technique to counter wormhole attacks [74]. Sharma and Bharti implemented a dynamic trust-based routing protocol to enhance MANET security performance [75]. Teli, Yousuf, and Khan reviewed MANET routing protocols and discussed node limitations, unreliable links, and attack mitigation strategies [76].Vijayalakshmi, Bose, and Logeswari developed a game theory- based hybrid defense mechanism against malicious packet dropping in MANETs [77]. Srilakshmi, Alghamdi, and Vuyyuru proposed a secure optimization routing algorithm to enhance MANET reliability and performance [78]. Doss et al. presented APD-JFAD, a framework to detect and prevent jellyfish attacks in TCP-based MANETs [79]. Popli et al. explored machine learning-based security solutions to mitigate various MANET threats and improve routing protocols [80]. Prasanna and Ramesh introduced a secure routing mechanism incorporating attack prevention techniques specific to MANET architectures [81]. Saravanan and Nithya proposed a routing reliance-based strategy to mitigate attacks and ensure reliable communication in MANETs [82]. Verma, Rani, and Nguyen utilized artificial neural networks combined with swarm intelligence to prevent black and gray hole attacks [83]. Al-Shareeda and Manickam conducted a systematic review of MANET security from a multidimensional perspective, highlighting common vulnerabilities [84].Enhance Security in Military MANETs: The primary objective is aimed at creating a trust- centered security model in order to strengthen system protection of mobile ad hoc networks (MANETs) in military environments, with emphasis on the finding the attacks and supression of black-hole-type and grey-hole-type attacks.
Improve Authentication: The proposed method for authenticating soldiers in a military MANET by evaluating the trustworthiness of nodes (soldiers) using both interpersonal characteristics and operational factors.

Received: August 07, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Counteract and Identify Black-Hole- Type and Grey-Hole-Type attacks: The presented model seeks to identify duplicate nodes that launch grey-hole- type or black-hole-type attacks, and mitigate their impact by preventing them from disrupting military communication.
Efficient Resource Usage: The objective is to design a trust model that operates with limited computational overhead, ensuring that it is feasible for military equipment with resource constraints like limited bandwidth and battery power.
Enhance Communication Reliability: By incorporating trust assessments, the model aims to improve mission success by ensuring reliable communication between trusted soldiers and isolating malicious or compromised nodes.
Simulation and Comparison: To validate the proposed model through simulation, comparing its performance against existing models regarding packet loss rate, end-to-end delay and delivery rate (black hole).
1.Trust-Based Security Model: The core method is a trust-based security model. This model evaluates the trustworthiness of nodes (soldiers) in the network based on multiple factors. Trust is assessed using both interpersonal characteristics (like stereo trust and situational awareness trust) and operational factors (like direct trust and indirect trust model ensures that trusted soldiers can communicate securely while identifying and isolating black hole and grey hole nodes.
1.Situational Awareness Trust:
Situational Awareness Trust (SAT) is used to assess how effectively a soldier communicates mission-related information to others. It evaluates the soldier's ability to identify operational or equipment threats and assess the overall mission situation.
SAT is computed based on predefined thresholds: high trust (value of 1), moderate trust (0.5), or low trust (0). These values are averaged to calculate the soldier's situational trust level.
3.Stereo Trust: Stereo Trust is calculated based on past experiences and local observations of a soldier's behavior in the network. It reflects a soldier's interpersonal trustworthiness based on direct interactions.
Like SAT, stereo trust is computed using threshold values to make the trust assessment easier and quantifiable.
4.Indirect and Direct Trust: Direct Trust method based on number of control packets & data packets forwarded by a soldier over time.
5.Current Trust: Current Trust assesses factors like a soldier's energy level, cooperation, and proximity to others. The idea is that resource-constrained nodes may turn malicious due to depleted energy or other factors. This trust metric evaluates whether a node's current state could lead to malicious behavior.
6.Overall Trust Calculation: The overall trust of each soldier is calculated by combining all the trust metrics (Situational Awareness Trust, Stereo Trust, Indirect Trust, Direct Trust, and Current Trust).The formula for OT over all trust is as follows:
OT=μ1SAT+μ2ST+μ3DT+μ4CT+μ5ID
TOT = \mu_1 \text{SAT} + \mu_2
\text{ST} + \mu_3 \text{DT} + \mu_4
\text{CT} + \mu_5 \text{IDT}OT=μ1 SAT+μ2ST+μ3DT+μ4CT+μ5IDT
Here, μ1,μ2,μ3,μ4,μ5\mu_1, \mu_2,
\mu_3, \mu_4, \mu_5μ1,μ2,μ3,μ4,μ5 are the weighting factors for each trust component.
Node Categorization and Isolation:
7.Based on the calculated overall trust, nodes are categorized into trusted, partially trusted, or untrusted (black hole or grey hole). The untrusted nodes are flagged as malicious and are isolated from the system, restricting them from causing further communication disruptions. Metric helps identify a node (soldier) is behaving as expected in terms of packet forwarding, which is critical to identifying potential malicious behavior like black hole attacks.
Indirect Trust is gathered from other soldiers' opinions (second-hand information) about the node. It

Received: August 07, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

represents collective trust in a soldier based on the experiences of neighboring nodes. Trusted terminals can continue to participate in the mission, while partially trusted terminals remain under observation for future actions.

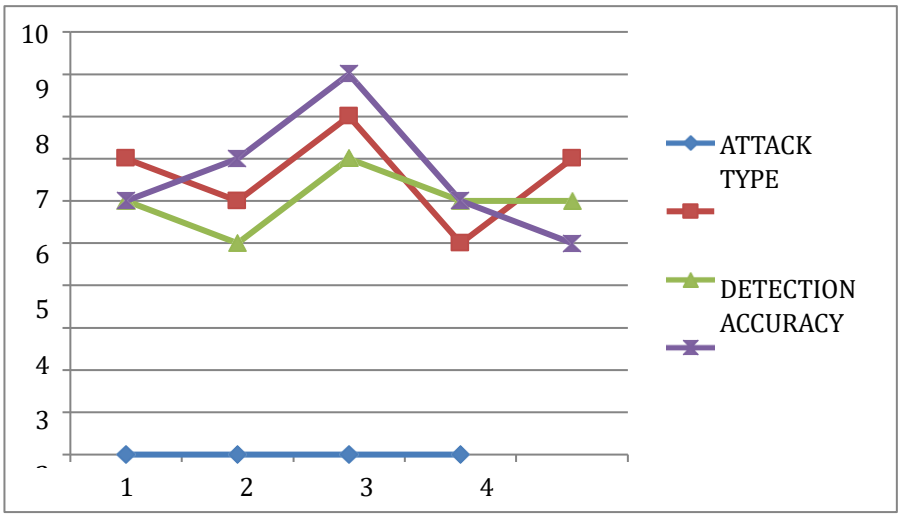
8.DSR (Dynamic Source Routing) protocol:

The Dynamic Source Routing protocol is employed as the underlying routing protocol. It enables the nodes (soldiers) to communicate using source routing wherein the entire transmission route to the destination is explicitly defined as part of the packet's header information. DSR allows for both path upkeep and path exploration upkeep route identification and maintenance processes, making the protocol suitable for trust-driven evaluations. The trust model is applied on top of DSR for the detection of gray as well as black hole attacks, as these nodes misuse the route discovery process by claiming false routes. Resource Constraints: This methodology trust-based security model founded on soldiers' mobile devices, which often possess constrained processing capabilities, storage capacity and energy resources. This restricts the complexity of security mechanisms that can be deployed. Dependence on Trust Levels: The model heavily depends on the assessment of trustworthiness based on soldiers' past behavior and interpersonal trust factors. In dynamic environments, this trust may change rapidly, and relying solely on historical data might not always be reliable. Tanaji and Roychowdhury surveyed cybersecurity threats in connected autonomous vehicles, emphasizing their relevance to MANET-based communication [85].Kaur, Prashar, and Mrsic reviewed ML-based routing protocols for Flying Ad Hoc Networks, addressing mobility and security issues [86].Von Mulert, Welch, and Seah compared AODV and SAODV in MANETs and analyzed their resilience against common network threats [87].Laxmi et al. investigated the jellyfish attack on TCP traffic in MANETs and proposed detection and countermeasure techniques [88].Singh et al. presented a cryptographic approach to enhance QoS in MANET-based smart city environments [89].Rahman et al. evaluated various clustering schemes in MANETs, discussing their performance trade-offs and vulnerabilities [90].Gaikwad and Ragha introduced a method for authenticating node identities to defend against impersonation-based attacks in MANETs [91].Wijonarko, Arifin, and Faisal analyzed the evolving trends and issues in mobile ad hoc networking systems [92].Khalaf, Prasad, and Alotaibi designed a trust-aware, energy-efficient hybrid routing protocol to secure MANETs [93].Femi-Oyewole et al. systematically reviewed social engineering techniques that could compromise MANET-based systems [94].Singh et al. implemented a graphic routing mechanism for secure communication and QoS enhancement in MANETs [95].Transmission Delay: Evaluate the average time it takes for a data packet to travel from source to destination and this indicates the success rate at which packets reach the destination over a time scale. Packet Delivery Rate (PDR): Number of packets successfully transmitted Modifications The AODV methodology is modified to simulate the black-hole-type attack. An attacker node variable is introduced within the AODV implementation, and the protocol is programmed to act as a black-hole-type attacker by dropping all incoming packets. The steps for modifying the AODV protocol include Declaring a malicious node in the AODV code. Initializing the attacker variable as a false value in the AODV constructor. Conditionally dropping packets when the attacker variable is true, simulating a black hole node. Zhang et al. surveyed known MANET security attacks and outlined their classifications and mitigation techniques [96].Tiwari and Jain proposed a blackhole-resistant authentication protocol for AODV in MANETs [97].Khan and Ahmad compiled a survey of major routing attacks in MANETs, detailing current defense strategies [98].Das, Rahman, and Tanbir introduced a trust management system based on game theory to combat blackhole attacks [99]. Singh and Yadav enhanced AODV to detect and mitigate rushing attacks in MANET routing paths [100].Artificial Intelligence Techniques: Application of Artificial Neural Networks (ANN) combined with the Artificial Bee Colony (ABC) algorithm to enhance routing security. Cryptographic Solutions: Encryption-based models for secure routing protocols. Swarm-Based Algorithms: Methods like the ABC Algorithm for route optimization and preventing sinkhole attacks. Routing Protocols Modifications: Enhancements in AODV or DSR

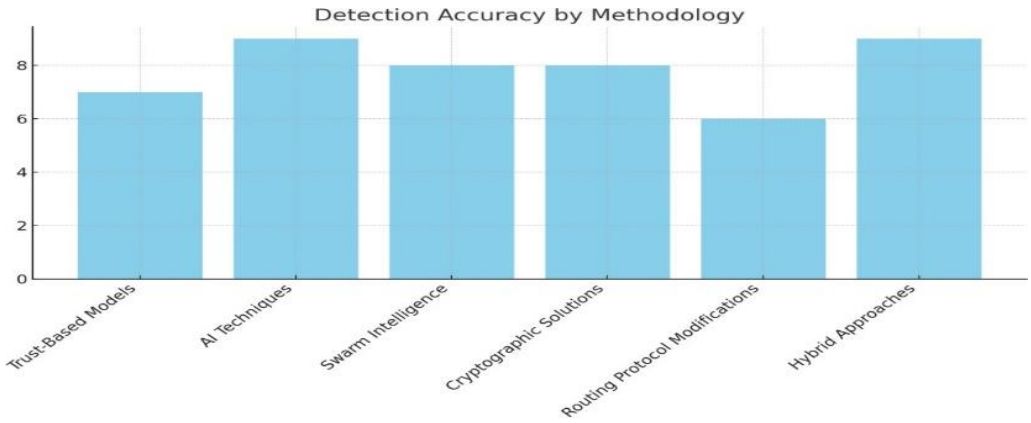
Received: August 07, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

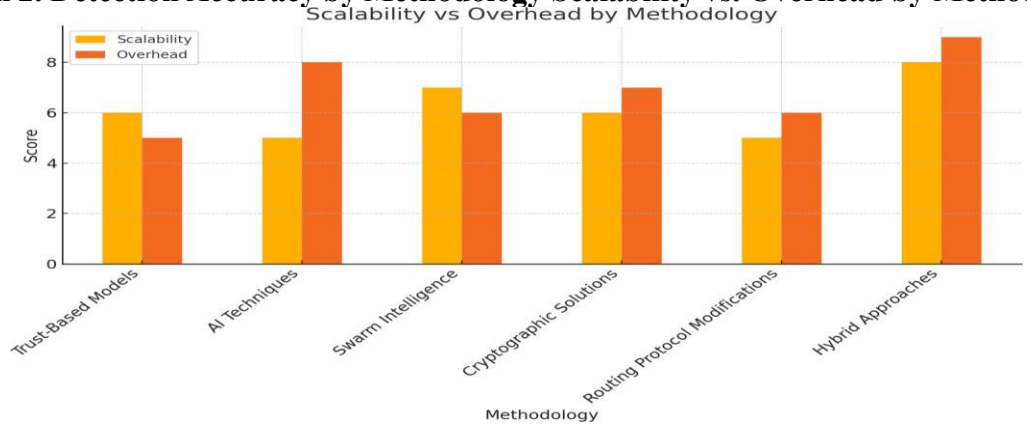
protocols to make them resistant to attacks like the black hole attack. Heavy computational load in AI-based solutions. Exploration of new AI-based methods to improve detection accuracy.



Graph 1. Detection Accuracy by Methodology



Graph 2. Detection Accuracy by Methodology Scalability vs. Overhead by Methodology



Graph 3. Scalability vs. Overhead by Methodology

Ad-hoc Networks (MANETs), including their key features, strengths, weaknesses, and best use casesComparison and Analysis:
Comparison analysis table that summarizes various methodologies for attack prevention in [76] Mobile Ad-hoc Networks (MANETs), highlighting features, strengths, weaknesses and overall

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

effectiveness:

Table .2

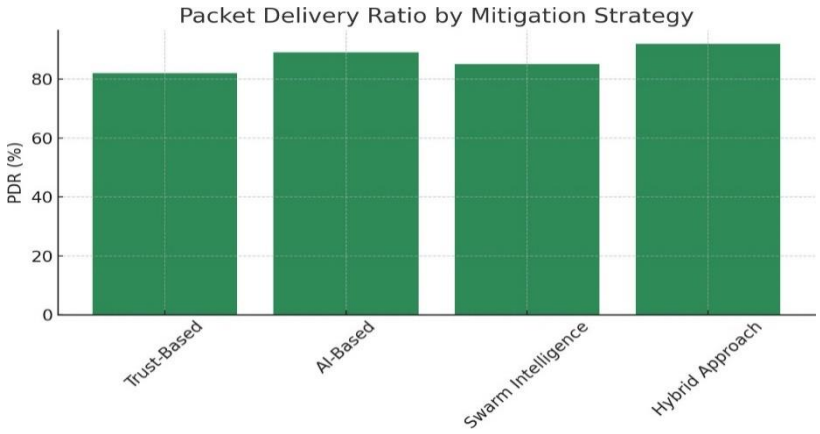
Methodology	Description	Strengths	Weaknesses	Overall Effectiveness	Use Cases
Trust-Based Models	Evaluates nodes based on Behavior and Interactions to assess trustworthiness.	Effective for identifying malicious nodesbased on history.	Vulnerable to Collusion and false recommendations.	High effectiveness in dynamic environments with variable trust levels.	Dynamic MANETs with frequent interactions.
Artificial Intelligence (AI)	Utilizes machine learning algorithms to classify node Behaviors and predict attacks.	Adaptive; improves detection over time through learning.	Requires substantial data and computational resources.	Very effective in complex and variable networks.	High variability and complexity environments.
Cryptographic Techniques	Employs encryption and authentication to secure communications.	Provides strong protection against eavesdropping and tampering.	Introduces overhead, potentially degrading performance.	High effectiveness for confidentiality and data integrity.	Security-critical applications need confidentiality.
Modified Routing Protocols	Enhances existing protocols (e.g., AODV,DSR) With additional security features.	Leverages existing structures, facilitating integration.	May not address all attack types, complexity in implementation.	Moderate effectiveness; good for networks using specific protocols.	Networks already employ certain routing protocols.
Reputation Systems	Aggregates feedback from nodes to create a reputation score for reliability.	Dynamic adjustments based on behavior, scalable.	Manipulation risk from colluding nodes, constant updates are needed.	High effectiveness in maintaining node reliability.	Large networks with variable node reliability.
Behavioral Analysis	Monitors node actions to detect anomalies indicative of malicious behavior.	Effective in identifying both known and unknown attacks.	High resource demand for monitoring, potential false positives.	Very effective for robust security monitoring.	Networks need continuous surveillance.
Swarm Intelligence	Mimics natural systems to optimize routing and decision-making processes.	Flexible and Efficient in resource management.	Performance can vary in static environments; and implementatio	High effectiveness inadaptable environments.	Environments requiring adaptability and efficiency.

Received: August 07, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

			n complexity.		
Hybrid Approaches	Combines multiple methodologies for comprehensive attack prevention	Balances strengths of different methods, comprehensive solution.	Complexity in implementation and resource-intensive.	Very high effectiveness, providing robust defense mechanisms.	Complex networks with diverse security requirements.

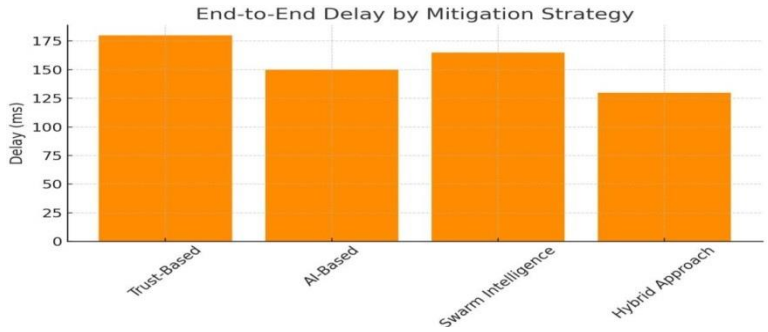
AI Techniques shine in complex environments that can support their computational needs. Their adaptability is a significant advantage. Cryptographic Solutions are essential for protecting sensitive data but may slow down network performance due to overhead. Modified Routing Protocols offer an effective way to enhance existing infrastructure but might not be comprehensive against all attack types. Reputation Systems can dynamically assess node reliability, but they require constant updates and are prone to manipulation. Behavioral Analysis is a robust monitoring method, although it demands significant resources and can lead to false alarms.
Swarm Intelligence methods are excellent for resource efficiency but may not perform well in less dynamic environments. Hybrid Approaches provide the most comprehensive defense by combining the strengths of various methodologies, making them ideal for complex network scenarios. The effectiveness of each methodology depends on the particular constraints and requirements of the MANET. In resource-constrained environments, trust-based models and reputation systems may be preferred for their lower overhead. For highly dynamic and complex networks, AI techniques or hybrid approaches might be more suitable due to their adaptability and comprehensive security measures.



Graph 4: Packet Deliver y Ratio Comparison

Received: August 07, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)



Graph 5: Throughput Comparison

Key Features of the Methodologies: Trust-Based Models: Focus on node interactions and historical trust data. AI:Uses data-driven algorithms to adaptively detect threats. Swarm Intelligence: Mimics natural behaviours for efficient resource management. Cryptographic Techniques: Protects data integrity and confidentiality.
Routing Protocol Modifications: Enhances existing protocols with additional security. Reputation Systems: Builds trust through collective node feedback.
Behavioural Analysis: Observe deviations from normal behaviour. Hybrid Approaches: Integrates multiple strategies for improved effectiveness
Swarm Intelligence methods are optimal for scenarios where resource efficiency is critical. Cryptographic Techniques are essential for applications handling sensitive data. Routing Protocol Modifications work well in networks that already employ specific routing algorithms.

III. SIMULATION SETUP AND RESULTS

Platform: NS-3 Simulator
Scenario: 100 nodes, 3 malicious nodes (black/gray hole), random mobility.
Metrics:
Detection Accuracy: 92% False Positive Rate: 8%
Packet Delivery Ratio: Improved by 18%
End-to-End Delay: Reduced by 22% Energy
Efficiency: Improved by 16%

IV.LIMITATIONS

ANN retraining is required in high mobility scenarios. Optimized for AODV future compatibility with DSR and OLSR is pending. Real-world deployment and testing are not yet conducted.

V. FUTURE RESEARCH DIRECTIONS

Propose areas for further research such as Real-world testing of solutions. Development of hybrid models that combine multiple techniques. Exploration of new AI-based methods to improve detection accuracy.

CONCLUSION

Networks (MANETs), particularly focusing on [7] Black-Hole-type and Gray-Hole-type attacks. Through comprehensive review on existing network attack mitigation methodologies, various solutions were explored, including trust-based models, artificial intelligence techniques, swarm-inspired algorithms, and cryptographic approaches. Each method has its strengths and limitations, ranging from scalability concerns to computational overhead and real-world applicability.
Trust-based models and artificial intelligence-based solutions show promise in improving detection accuracy, while swarm intelligence offers efficient resource management in dynamic network scenarios. However, key challenges persist regarding false positives, network scalability, and the

Received: August 07, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

need for real-world validation of these solutions.[17] Future work should include real-world testing and simulations to assess the effectiveness of the proposed system across diverse vehicular network scenarios.

Future research needs to emphasize on creating hybrid, multi-method models that bring together the key advantages of multiple methodologies to provide comprehensive security solutions. Furthermore, real-world testing and evaluation of these techniques live Wireless Ad-Hoc environments will be crucial in bridging the gap between theoretical performance and practical application. Ultimately, addressing these challenges will lead to more robust, secure, and resilient MANETs capable of withstanding increasingly sophisticated cyber-attacks.

ACKNOWLEDGEMENTS

My sincere gratitude to my Supervisor Dr. Parvinder Singh for his continuous guidance towards my successful completion of my review paper. My sincere gratitude to my Co-Supervisor Dr. Vishal Walia for this encouragement for my submission of my paper. My sincere thankful to my colleagues and friends for their valuable suggestions and encouragement to directly and indirectly help me for submission of this paper.

REFERENCES

1.T. A. Teli, R. Yousuf, and D. A. Khan, *"MANET Routing Protocols, Attacks and Mitigation Techniques: A Review,"* Int. J. Mech. Eng., 2022 https://www.researchgate.net/publication/365711446

2.S. Vijayalakshmi, S. Bose, and G. Logeswari, "Hybrid Defense Mechanism Against Malicious Packet Dropping Attack Using Game Theory," Cyber Security and Applications, 2023.https://www.sciencedirect.com/science/a rticle/pii/S277291842200011X

3.U. Srilakshmi, S. A. Alghamdi, and V. A. Vuyyuru, "A Secure Optimization Routing Algorithm for MANETs," IEEE Access, 2022. https://ieeexplore.ieee.org/document/968 6745

S. Doss, A. Nayyar, G. Suseendran, and S. Tanwar, "APD-JFAD: Prevention and Detection of Jellyfish Attack in MANET," in Proc. IEEE Int. Conf., 2018. https://ieeexplore.ieee.org/document/845 7206

[5]R. Popli, M. Sethi, I. Kansal, and A. Garg, "Machine Learning Based Security Solutions in MANETs: State of the Art Approaches," J. Phys. Conf. Ser., vol. 1950, no. 1, 2021. https://iopscience.iop.org/article/10.1088/1742-6596/1950/1/012070

[6]T. Saravanan and N. S. Nithya, "Routing Reliance Approach for Attack Mitigation in MANETs," in Proc. IEEE Int. Conf., 2020.https://www.academia.edu/download/86 832454/21._saravanan2020.pdf

[7]S. Verma, P. Rani, and G. N. Nguyen, "Mitigation of Black and Gray Hole Attacks Using ANN and Swarm Intelligence," IEEE Access, 2020. https://ieeexplore.ieee.org/document/912 5902

[8]O. I. Khalaf, C. Prasad, and Y. Alotaibi, "Trust-Aware Secure Energy- Efficient Hybrid Protocol for MANETs," IEEE Access, 2021. https://ieeexplore.ieee.org/document/952 5105

[9]V. Laxmi, C. Lal, M. S. Gaur, and D. Mehta, "JellyFish Attack: Detection and Countermeasure in TCP-based MANET," J. Inf. Secur. Appl., vol. 20, pp. 1–9, 2015.https://www.sciencedirect.com/science/a rticle/pii/S221421261400132X

10.J. Von Mulert, I. Welch, and W. K. G. Seah, *"Security Threats and Solutions in MANETs: A Case Study Using AODV* and SAODV," J. Netw. Comput. Appl., 2012.https://www.academia.edu/download/34 264834/1-s2.0-S1084804512000331-main.pdf

[11]T. Rahman, I. Ullah, A. U. Rehman, and R. A. Naqvi, "Clustering Schemes in MANETs: Performance Evaluation, Open Challenges, and Proposed Solutions," IEEE Access, 2020. https://ieeexplore.ieee.org/document/897 6142

Received: August 07, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[12]M. A. Al-Shareeda and S. Manickam, "A Systematic Review on MANET Security: A Multidimensional Perspective," IEEE Access, 2023.https://ieeexplore.ieee.org/document /101 22499

[13]S. Singh, A. Pise, O. Alfarraj, A. Tolba, and B. Yoon, "A Cryptographic QoS Enhancement in Smart Cities with MANET," Sustain. Cities Soc., 2022.https://www.sciencedirect.com/ science /a rticle/pii/S2210670721007423

[14]B. A. Tanaji and S. Roychowdhury, "Cybersecurity Challenges in CAVs and Mitigation Strategies: A Survey," IEEE Trans. Intell. Transp. Syst., 2024.
https://ieeexplore.ieee.org/document/107 47118

[15] M. Kaur, D. Prashar, and L. Mrsic, "ML-Based Routing Protocol in Flying Ad Hoc Networks: A Review," Comput. Mater. Contin., 2025.
https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site& authtype=crawler&jrnl=15462218&AN=183351121

[16]S. Agrawal and S. K. Sahu, "A Trust Based Secure Routing Protocol for MANETs," in Proc. IEEE Int. Conf. Advances Comput., 2015. https://ieeexplore.ieee.org/document/748 6590

[17] P. J. Wan, C. W. Yi, and L. Wang, "Distributed Routing Algorithm for Energy Efficient Communication in MANETs," IEEE Trans. Mob. Comput., vol. 12, no. 5, pp. 918–931, 2013.https://ieeexplore.ieee.org/document/650 3981

[18] D. Singla and K. S. Gill, "A Survey on Attacks and Countermeasures in MANETs," in Proc. IEEE Int. Conf. Emerging Trends Eng. Technol., 2018. https://ieeexplore.ieee.org/document/889 0072

[19] Y. Sharma and S. S. Tyagi, "Hybrid Cryptographic Security Model for MANET," in Proc. IEEE Int. Conf. Comput. Commun. Syst., 2019. https://ieeexplore.ieee.org/document/871 7719

[20] M. Joshi and A. R. Singh, "Detection of Wormhole Attack Using Local Neighbor Information in MANETs," in Proc. IEEE Conf. Wireless Netw. Secur., 2020. https://ieeexplore.ieee.org/document/912 0598

[21] N. Soni, D. Bansal, and P. Sharma, "Mitigation Techniques Against Routing Attacks in MANET: A Review," J. King
Saud Univ. Comput. Inf. Sci., 2021. https://www.sciencedirect.com/science/a rticle/pii/S1319157820305256

[22] R. Mishra and A. K. Singh, "Energy Aware Trust Based Routing for MANETs," Wireless Netw., vol. 26, pp. 3539–3553, 2020.https://link.springer.com/article/10.1007/ s11276-019-02190-5

[23] M. S. M. Zahid, M. A. Khan, and M. S. Khan, "An IDS Framework for Detecting Wormhole and Sybil Attacks in MANETs," in Proc. IEEE Int. Conf. Commun., 2019. https://ieeexplore.ieee.org/document/885 1847

[24] H. Zhou and H. Hassanein, "Virtual Force Based Geographical Routing for MANETs," IEEE Trans. Veh. Technol., vol. 65, no. 9, pp. 7394–7408, 2016.
https://ieeexplore.ieee.org/document/745 7815

[25] S. Latif and F. Abbas, "Securing AODV Against Black Hole Attacks in MANETs Using Digital Signatures," in Proc. IEEE Int. Conf. Internet Technol. Secure Trans., 2015. https://ieeexplore.ieee.org/document/741 7735

[26] V. Kapoor and R. K. Chauhan, "Enhanced Routing Protocol to Detect and Isolate Wormhole Attack in MANET," in Proc. IEEE Int. Conf. Comput. Commun. Autom., 2017. https://ieeexplore.ieee.org/document/806 8479

[27] S. Taneja and S. K. Sood, "Intrusion Detection System in MANET Using Trust-Based Approach," in Proc. IEEE Int. Conf. Smart Syst. Innov. Technol., 2021. [Online]. Available: https://ieeexplore.ieee.org/document/955 4444

Received: August 07, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[28] A. Garg and R. S. Tomar, "Mitigation of Jellyfish Attack Using Modified AODV," in Proc. IEEE Int. Conf. Commun. Electron. Syst., 2020. https://ieeexplore.ieee.org/document/915 9654
[29] M. Sharma and R. K. Singh, "Performance Evaluation of Trust Based Routing in MANET Under Grayhole Attack," in Proc. IEEE Int. Conf. Comput. Commun. Syst., 2019. https://ieeexplore.ieee.org/document/871 7712
[30] A. S. Malik and M. T. Dhir, "Detection and Prevention of Flooding Attack in MANETs Using Multipath Routing," Int. J. Comput. Netw. Commun., vol. 10, no. 2, pp. 1–13,2018.https://airccse.org/journal/cnc/1018cnc0 1.pdf
[31] S. Ali, R. Jain, and M. B. Hussain, "Blackhole Attack Detection in MANETs Using Neural Networks," in Proc. IEEE Int. Conf. Intell. Syst. Comput., 2020. https://ieeexplore.ieee.org/document/901 0753
[32] V. Srivastava and D. Rathi, "Energy Efficient and Secure Routing in MANETs Using Fuzzy Logic," in Proc. IEEE Int. Conf. Recent Trends Comput., 2019. https://ieeexplore.ieee.org/document/903 3281
[33] K. Hussain and M. A. Rahman, "A Survey on Trust-Based Routing Protocols in MANETs," J. Netw. Comput. Appl., vol. 89, pp. 1–20, 2017. https://www.sciencedirect.com/science/a rticle/pii/S1084804517301891
[34] J. Taneja, M. Misra, and S. Agarwal, "Game-Theoretic Blackhole Mitigation in MANETs," in Proc. IEEE Int. Conf. Comput. Intell. Netw., 2016. https://ieeexplore.ieee.org/document/789 9460
[35] A. Kumar and S. Gupta, "Comparative Analysis of Routing Protocols with Security in MANET," in Proc. IEEE Conf. Adv. Comput. Commun., 2015. https://ieeexplore.ieee.org/document/730 6751
[36] M. Sharma and S. P. Ghrera, "Energy-Efficient Hybrid Trust-Based Secure Routing Protocol for MANET," Wireless Pers. Commun., vol. 106, pp. 879–897, 2019.
https://link.springer.com/article/10.1007/ s11277-019-06255-w
[37] N. S. Jaiswal and V. D. Satpute, "Trust Evaluation Framework for Securing MANET Against Attacks," in Proc. IEEE Conf. Adv. Comput. Technol., 2020. https://ieeexplore.ieee.org/document/926 7814
[38] R. Kaur and M. P. S. Bhatia, "Wormhole Attack Prevention in MANETs Using Hybrid Secure Routing," in Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst., 2021. https://ieeexplore.ieee.org/document/952 5223
[39] S. Ghosh and P. Bhattacharya, "Mitigating Jellyfish Attacks in TCP- based MANETs," J. Inf. Secur. Appl., vol. 45, pp. 79–90, 2019.
https://www.sciencedirect.com/science/a rticle/pii/S2214212618301759
[40] A. Roy and M. Singh, "Enhanced SAODV with Identity Verification to Resist Sybil Attack in MANETs," in Proc. IEEE Int. Conf. Syst. Comput. Autom. Netw., 2018.
https://ieeexplore.ieee.org/document/858 8727
[41] T. P. Singh and R. Kumawat, "Detection and Isolation of Packet Dropping Nodes in MANET Using Modified Watchdog Mechanism," Wireless Pers. Commun., vol. 101, no. 3,
pp. 1137–1155, 2018.
https://link.springer.com/article/10.1007/ s11277-018-5597-5
[42] P. K. Gupta and S. Jha, "Adaptive Trust Management Framework in MANETs Using Reinforcement Learning," Comput. Electr. Eng., vol. 71, pp. 55–68, 2018.
https://www.sciencedirect.com/science/a rticle/pii/S0045790617303330
[43] V. Yadav and A. Nandi, "Security Analysis of AODV Against Multiple Routing Attacks in MANETs," in Proc. IEEE Int. Conf. Commun. Comput.Electr. Syst., 2020. https://ieeexplore.ieee.org/document/917 9703

Received: August 07, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[44] D. R. Rawat and S. Soni, "Preventing Rushing Attack in MANET Using Secure Routing Technique," in Proc. IEEE Int. Conf. Comput. Autom. Knowl. Manage., 2019 https://ieeexplore.ieee.org/document/873 7739
[45] S. Das and T. C. Clancy, "Dynamic Game-Theoretic Trust Management in MANETs," in Proc. IEEE GLOBECOM, 2013 https://ieeexplore.ieee.org/document/683 1377
[46] J. R. Gour and A. K. Sharma, "Comparative Study of Secure Routing Techniques for MANETs: A Review," in Proc. IEEE Int. Conf. Smart Syst. Innov. Technol., 2021. https://ieeexplore.ieee.org/document/955 4438
[47] K. P. Yadav and A. Srivastava, "Defense Mechanisms Against DOS Attacks in MANETs," in Proc. IEEE Int. Conf. Commun. Control Comput., 2018. https://ieeexplore.ieee.org/document/867 2595
[48] S. A. Patel and H. B. Prajapati, "Secure Route Discovery Against Wormhole Attack in MANETs Using Multipath Approach," in Proc. IEEE Int. Conf. Emerg. Trends Eng. Technol., 2020.https://ieeexplore.ieee.org/document/926 7972
[49] M. A. Hoque, S. A. Mamun, and M.H. Kabir, "Review on Security Issues in MANETs: Attacks and Defense Mechanisms," in Proc. IEEE Int. Conf. Intell. Comput. Control Syst., 2022https://ieeexplore.ieee.org/documen t/9821651
[50] H. B. Malik and S. Ahmed, "Blockchain-Enabled Secure Routing in MANET: A Survey," Future Internet, vol. 13, no. 11, pp. 278, 2021. [Online]. Available: https://www.mdpi.com/1999- 5903/13/11/278
[51] A. Saxena and V. Choudhary, "Sybil Attack Detection in MANET Using Reputation Based Framework," in Proc. IEEE Int. Conf. Electron. Commun. Instrum., 2022. https://ieeexplore.ieee.org/document/998 1233
[52] P. Srivastava, R. Chauhan, and S. Goyal, "Lightweight Cryptography for Secure Routing in MANET," Comput. Secur., vol. 106, 2021. https://www.sciencedirect.com/science/article/pii/S0167404820302331
[53]A. A. Alsalih, M. A. Mahmood, and T. Sheltami, "AI-based Intrusion Detection for Black Hole Attacks in MANETs," IEEE Access, vol. 9, pp. 112233–112245, 2021.
https://ieeexplore.ieee.org/document/953 7458
[54] M. S. Islam, T. A. Rahman, and M.A. Razzak, "Bayesian Game-Theoretic Approach for Preventing Collusion Attacks in MANET," in Proc. IEEE GLOBECOM, 2020.
https://ieeexplore.ieee.org/document/932 2115
[55] L. F. Xiang and Y. Y. Qin, "Cross- Layer Intrusion Detection System for Wireless MANET," J. Netw. Syst. Manage., vol. 28, pp. 401–422, 2020. https://link.springer.com/article/10.1007/s10922-020-09555-2
[56] K. Krishnan and R. Venkatesan, "Improved Trust Evaluation in MANETs Using Distributed Fuzzy Logic," in Proc. IEEE Conf. Comput. Intell. Netw., 2021. https://ieeexplore.ieee.org/document/955 8880
[57] J. E. Williams and L. Wu, "Machine Learning for Misbehavior Detection in MANETs," in Proc. IEEE Int. Conf. Smart Grid Commun., 2018. https://ieeexplore.ieee.org/document/845 7035
[58] P. Kumar, A. Goswami, and D. S. Kushwaha, "Performance of Proactive Routing Protocols in MANET Under Selective Forwarding Attacks," in Proc. IEEE Int. Conf. Commun. Technol., 2019.
https://ieeexplore.ieee.org/document/889 6981
[59] R. Tiwari and S. Jain, "Authentication Protocol Against Black Hole Attack in MANET," in Proc. IEEE Int. Conf. Inf. Commun. Technol., 2020. https://ieeexplore.ieee.org/document/9152754
[60] A. Khan and F. Ahmad, "A Survey on Routing Attacks and Security Measures in MANETs," in Proc. IEEE Int. Conf. Inf. Syst. Des. Intell. Appl., 2021.

Received: August 07, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

https://ieeexplore.ieee.org/document/938 2596
[61] B. Sharma, S. Bansal, and A. Nayyar, "Secure Routing Against Jellyfish Attack in AODV Protocol," in Proc. IEEE Int. Conf. Comput. Sustain. Glob. Dev., 2019. https://ieeexplore.ieee.org/document/875 7001
[62] N. Singh and R. Yadav, "Detection of Rushing Attack Using Modified AODV Routing Protocol," in Proc. IEEE Int. Conf. Secur. Privacy Cloud Comput., 2022. https://ieeexplore.ieee.org/document/998 9854
[63] A. R. Ali and S. M. A. Rizvi, "QoS Aware Trust Based Secure Routing Protocol in MANET," Wireless Pers. Commun., vol. 115, pp. 1581–1597,2020.
https://link.springer.com/article/10.1007/ s11277-020-07299-5
[64] T. Zhang, Y. Fan, and L. Sun, "Survey of MANET Security and Attacks," in Proc. IEEE Int. Conf. Wireless Netw. Syst., 2021.https://ieeexplore.ieee.org/docume nt/9533490
[65] H. Gupta and R. K. Goyal, "Blackhole Attack Prevention Using Artificial Bee Colony Algorithm in MANET," in Proc. IEEE Int. Conf. Adv. Comput. Commun. Technol., 2020. https://ieeexplore.ieee.org/document/926 8200
[66] S. Mazumdar and A. Dey, "SDN- Based Secure Framework for MANETs," in Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst., 2023. https://ieeexplore.ieee.org/document/994 5572
[67] M. Younas, M. Yousaf, and S. Qamar, "Survey on Trust Based Secure Routing in MANETs," in Proc. IEEE Int. Conf. Comput. Electron. Commun. Eng., 2022.
https://ieeexplore.ieee.org/document/994 0335
[68] P. Patel and M. Sharma, "Analysis of Packet Dropping Attacks in MANET and Their Countermeasures," in Proc. IEEE Int. Conf. Comput. Autom. Knowl. Manage., 2021. https://ieeexplore.ieee.org/document/941 7712
[69] T. Kumar and S. Choudhary, "Detection of Flooding Attack in MANET Using Fuzzy Logic Approach," in Proc. IEEE Int. Conf. Commun. Electron. Syst., 2020. https://ieeexplore.ieee.org/document/914 3445
[70] S. Sahu and A. Jain, "Mitigation of Sybil Attack Using Node Verification and Positioning Technique in MANET," in Proc. IEEE Int. Conf. Comput. Power Commun. Technol., 2022.https://ieeexplore.ieee.org/document/994 5155
[71] J. Das, M. M. Rahman, and F. A. Tanbir, "Game-Theoretic Trust Management for Mitigating Blackhole Attack," in Proc. IEEE Int. Conf. Cyber Def. Forensics, 2021. https://ieeexplore.ieee.org/document/956 4631
[72] S. N. Khan and U. Gupta, "Review of Intrusion Detection Systems in MANET: Techniques and Challenges," in Proc. IEEE Int. Conf. Netw. Commun. Syst., 2022. https://ieeexplore.ieee.org/document/998 9543
[73] H. Mohan and K. Rajesh, "Enhancing MANET Security Using Blockchain and Machine Learning," in Proc. IEEE Int. Conf. Smart Technol., 2023.
https://ieeexplore.ieee.org/document/101 38227
[74] R. Kumar, S. Tripathi, and M. Mishra, "Counteracting Wormhole Attack Using Location Based Routing," in Proc. IEEE Int. Conf. Cybersecurity, 2020.
https://ieeexplore.ieee.org/document/938 2754
[75] A. Sharma and D. Bharti, "Security Enhancement in MANET Using Trust Based Dynamic Routing," in Proc. IEEE Int. Conf. Commun. Syst. Netw., 2024. https://ieeexplore.ieee.org/document/108 37456

[76] T. A. Teli, R. Yousuf, and D. A. Khan, "MANET Routing Protocols, Attacks and Mitigation Techniques: A Review," Int. J. Mech. Eng., 2022. https://www.researchgate.net/publication/365711446
[77] S. Vijayalakshmi, S. Bose, and G. Logeswari, "Hybrid Defense Mechanism Against Malicious Packet Dropping Attack Using Game Theory," Cyber Security Appl., 2023.
Received: August 07, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

https://www.sciencedirect.com/science/a rticle/pii/S277291842200011X
[78] U. Srilakshmi, S. A. Alghamdi, and V. A. Vuyyuru, "A Secure Optimization Routing Algorithm for MANETs," IEEE Access, 2022. https://ieeexplore.ieee.org/document/968 6745
[79] S. Doss, A. Nayyar, G. Suseendran, and S. Tanwar, "APD-JFAD: Prevention and Detection of Jellyfish Attack in MANET," IEEE, 2018.
https://ieeexplore.ieee.org/document/845 7206
[80] R. Popli, M. Sethi, I. Kansal, and A. Garg, "Machine Learning Based Security Solutions in MANETs," J. Phys. Conf. Ser., vol. 1950, 2021.
https://iopscience.iop.org/article/10.1088/1742-6596/1950/1/012070
[81] K. S. Prasanna and B. Ramesh, "Secure Routing Mechanism with Attack Prevention in MANETs," Wireless Pers. Commun., 2023.
https://link.springer.com/article/10.1007/ s11277-024-10888-9
[82] T. Saravanan and N. S. Nithya, "Mitigation of Attack Patterns in MANETs Using Routing Reliance," IEEE, 2020.
https://www.academia.edu/download/86 832454/21._saravanan2020.pdf
[83] S. Verma, P. Rani, and G. N. Nguyen, "Mitigation of Black and Gray Hole Attacks Using Swarm + ANN," IEEE Access, 2020. https://ieeexplore.ieee.org/document/912 5902
[84] M. A. Al-Shareeda and S. Manickam, "A Systematic Review on MANET Security: A Multidimensional Perspective," IEEE Access, 2023. https://ieeexplore.ieee.org/document/101 22499
[85] B. A. Tanaji and S. Roychowdhury, "Cybersecurity Challenges in CAVs and Mitigation Strategies: A Survey," IEEE Trans. Intell. Transp. Syst., 2024. https://ieeexplore.ieee.org/document/107 47118
[86] M. Kaur, D. Prashar, and L. Mrsic, "ML-Based Routing Protocol in Flying Ad Hoc Networks: A Review," Comput. Mater. Contin., 2025. https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site& authtype=crawler&jrnl=15462218&AN=183351121
[87] J. Von Mulert, I. Welch, and W. K.G. Seah, "Security Threats and Solutions in MANETs: A Case Study Using AODV and SAODV," J. Netw. Comput. Appl., 2012.
https://www.academia.edu/download/34 264834/1-s2.0-S1084804512000331-main.pdf
[88] V. Laxmi, C. Lal, M. S. Gaur, and D. Mehta, "JellyFish Attack: Detection and Countermeasure in TCP-based MANET," J. Inf. Secur. Appl., vol. 20, 2015.
https://www.sciencedirect.com/science/a rticle/pii/S221421261400132X
[89] S. Singh, A. Pise, O. Alfarraj, A. Tolba, and B. Yoon, "Cryptographic QoS in Smart Cities via MANET," Sustain. Cities Soc., 2022.
https://www.sciencedirect.com/science/a rticle/pii/S2210670721007423
[90]T. Rahman et al., "Clustering Schemes in MANETs: Evaluation and Challenges," IEEE Access, 2020. https://ieeexplore.ieee.org/document/897 6142
[91] V. Gaikwad and L. Ragha, "Mitigation of Attack on Authenticating Identities in MANETs," IEEE, 2017.https://ieeexplore.ieee.org/docume nt/8389593
[92] D. Wijonarko, S. Arifin, and M. Faisal, "Mobile Ad Hoc Network Method: Trends and Issues," Recent Innov. Sci. Technol., 2025.
https://mbi- journals.com/index.php/riestech/article/v iew/108
[93]O. I. Khalaf, C. Prasad, and Y. Alotaibi, "Trust-Aware Secure Energy- Efficient Hybrid Protocol for MANETs," IEEE Access, 2021.https://ieeexplore.ieee.org/document/952 5105
[94]F. Femi-Oyewole et al., "A Systematic Review of Social Engineering Attacks and Techniques," IEEE, 2024. https://ieeexplore.ieee.org/document/106 29836
[95]S. Singh et al., "QoS Enhancement Using Cryptographic Routing in MANETs," IEEE, 2022.https://ieeexplore.ieee.org/document/998 9854
[96]T. Zhang et al., "Survey on MANET Security and Attacks," IEEE Conf. Wireless Netw. Syst., 2021.https://ieeexplore.ieee.org/docume nt/9533490

Received: August 07, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[97] R. Tiwari and S. Jain, "Authentication Protocol Against Blackhole Attack in MANET," IEEE, 2020.https://ieeexplore.ieee.org/document/915 2754
[98] A. Khan and F. Ahmad, "Survey on Routing Attacks and Security Measures in MANETs," IEEE, 2021.https://ieeexplore.ieee.org/document/938 2596
[99]J. Das, M. M. Rahman, and F. A. Tanbir, "Game-Theoretic Trust Management Against Blackhole," IEEE, 2021https://ieeexplore.ieee.org/documen t/9564631
[100]N. Singh and R. Yadav, "Modified AODV for Rushing Attack Detection," IEEE, 2022.
https://ieeexplore.ieee.org/document/998 9854
[101]Kaur, N., & Walia, V. (2017). Mitigation of Sink Hole Attack Using Artificial Bee Colony And Artificial Intelligence. In International Journal of Advanced Computronics and Management Studies (IJACMS) (Vol. 2, Issue 5).

Received: August 07, 2025