Ingénierie des Systèmes d'Information
Vol. 29, No. 6, December, 2024, pp. 2533-2548

Journal homepage: http://iieta.org/journals/isi

Comprehensive Taxonomy of Schemes for Detecting and Mitigating Blackhole Attacks in Mobile Ad-Hoc Networks: A Study on Tactics, Classifications, and Future Directions

Saad M. Hassan[1,2*], Mohd Murtadha B. Mohamad[1], Farkhana B. Muchtar[1]

[1] Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru 81310, Skudai, Malaysia
[2] Computer Science Department, Faculty of Basic Education, AL-Mustansiriya University, Baghdad 10011, Iraq

Corresponding Author Email: murtadha@utm.my

https://doi.org/10.18280/isi.290638

Received: 4 December 2023
Revised: 13 August 2024
Accepted: 28 September 2024
Available online: 25 December 2024

Keywords:
Mobile Ad-hoc Networks (MANETs), packet drop attacks, blackhole, infrastructure-free functioning, conventional routing protocols, cybersecurity

ABSTRACT

This study addresses the vulnerability of several Mobile Ad-hoc Networks (MANET) to packet drop attacks, such as Gray hole, Blackhole, and co-operative Blackhole attacks. MANET's intrinsic features, including infrastructure-free functioning, mobility, and susceptibility to conventional routing protocols, necessitate a robust approach to network communication and security. Our research focuses on the Blackhole cyberattack and its variants, aiming to identify and mitigate their impacts. The study categorizes tactics into fourteen distinct categories, revealing the hybridization of specific strategies. We elucidate the key functions of these tactics, demonstrating how they identify or mitigate operations during ongoing communications. The study provides insights into the benefits of tactics and classifications, showcasing their practical performance on the ground. Our future direction aims to address the identified shortcomings, working toward a more efficient, effective, legitimate, and precise framework for mitigating and preventing various versions of Blackhole attacks in ad hoc networks. The significance of this research lies in enhancing the security of MANETs and advancing strategies for combatting evolving cyber threats.

1. INTRODUCTION

Mobile Ad-hoc Networks (MANETs) are self-organizing networks that do not require a fixed infrastructure for communication. These networks are widely used in various applications, including military operations, disaster management, and emergency response systems. However, the lack of a centralized infrastructure makes MANETs vulnerable to various security threats, including black hole attacks [1]. A black hole attack is a type of Denial of Service (DoS) attack in which a malicious node falsely advertises itself as having the shortest path to the destination node and then drops all the packets it receives. This type of attack can severely affect the performance of the network, leading to a high packet loss rate, increased End-to-End Delay (E to E), and reduced throughput. To address this issue, various detection and mitigation strategies have been proposed in the literature [2-4]. In this paper, we review and compare existing research papers on detecting, preventing, or mitigating black hole and similar attacks in MANETs based on the type of attacks addressed in the article. We examine the quantity of related articles in those papers and the availability of taxonomy or categorization of systems. Our comparison shows that trust-based techniques are a promising approach for preventing black hole attacks in MANETs. However, we also highlight the need for better weight balance among past and present trust levels in these techniques [5]. In addition, we discuss two specific techniques proposed in the literature for combating black hole attacks in MANETs. The first technique is an expanded Ad hoc on-demand multipath distance vector (AOMDV) approach, which spreads sections of the complete message across various channels and encrypts them with a homomorphic encryption method. The simulation results show that the suggested system has a greater throughput and Packet Delivery Ratio (PDR), both of which are desirable characteristics for emergency operations in MANETs. The second technique is the Integrated Cross Interior (ICI) architecture for Intrusion Detection Systems (IDS), which is presented for node routing and protection against black hole attacks. The experimental findings show that ICIs for IDS-based security strategy efficiently lower the reaction time and the cost of mobile routing, and application response time [6-9]. Ensuring secure routing procedures and maintaining a high (PDR) are paramount challenges in the development of Mobile Ad Hoc Networks (MANET). Routing involves the interaction of network entities, encompassing how nodes within the network construct and manage routes in routing tables [10]. These pathways can be established on-demand, pre-established, or a combination of both. Significantly, MANET security is a key focus due to the potential threats posed by external intruders and nodes that can disrupt communication [10, 11].

Various attacks pose risks to MANET, and security mechanisms are imperative [10, 11]. Attacks can manifest in passive or active forms, with passive attacks capturing data without affecting communications, and active attacks disrupting route discovery, leading to the loss of data packets, DoS, message flooding, or poisoning route tables Mitigation of black hole attacks using firefly and artificial neural network

[12-14]. Among these attacks, packet data dropping attacks, including co-operative Blackhole [15], Gray hole [16], and others, are prevalent and highly hazardous. In these scenarios, a node positions itself as an intermediary with the shortest and most recent path to a specific target [17, 18]. However, during data transmission, it deliberately drops packets according to a predetermined or random pattern established after network establishment [14, 19-21]. Each of these packets drop attacks significantly impacts network efficiency and effectiveness.

A comprehensive examination of various Blackhole attack variations reveals gaps in the existing literature, prompting the development of a comprehensive taxonomy encompassing both abatement and detection mechanisms. This study scrutinizes sixteen distinct types of mitigation mechanisms and conducts a thorough summary and evaluation of forty-seven research papers. The assessment is based on multiple criteria, including E to E delay, throughput, (PDR), as well as characteristics, detection type, and associated limitations. This exhaustive review aims to contribute to a more nuanced understanding of the current state of literature on Blackhole attack mitigation and detection mechanisms. Numerous scholars have delved into this issue, developing various techniques and methods for detecting and preventing Blackhole attacks and their variations. The research community has made substantial progress in addressing these challenges to enhance the security and resilience of MANETs. This paper provides a comprehensive review of existing research on black hole attacks in MANETs and identifies trust-based techniques as a promising approach for preventing these attacks. The findings of this study can be useful for future researchers in this field.

Based on the comprehensive study presented in the document, we can synthesize the key contributions into three main points:

(1) Comprehensive Taxonomy and Analysis of Attack Types: The study provides a detailed categorization of fourteen distinct types of attacks in MANETs, revealing the increasing sophistication and hybridization of attack strategies. This taxonomy offers a crucial framework for understanding the evolving threat landscape in MANETs. The research thoroughly analyzes various vulnerability management processes, with a particular focus on the K-neighbour assessment approach, demonstrating the effectiveness of these strategies in identifying suspicious nodes involved in cooperative attacks.

(2) Extensive Performance Evaluation and Experimental Design Overview: The research conducts an extensive evaluation of well-known works from past decades, establishing key performance criteria such as E to-E Delay, Throughput, and (PDR). These metrics provide valuable benchmarks for assessing the effectiveness of security measures in MANETs. Additionally, the study offers a comprehensive overview of experimental designs and simulator usage across various methods, highlighting trends in the field and providing insights into best practices for MANET security research.

(3) Identification of Research Gaps and Future Directions: The article identifies several critical gaps in current research, including the need for better balance in trust-based techniques, improved propagation of protection mechanisms, and the development of lightweight detection methods suitable for resource-constrained environments. Based on these findings, the study outlines recommendations for future research, emphasizing the need for more efficient, effective, and precise frameworks for mitigating various versions of Blackhole attacks in ad hoc networks. This contribution provides a roadmap for future researchers and practitioners in the field of MANET security.

The remaining of the survey is organized as follows. Section 2 provides an overview of Blackhole attacks and their variants, including detailed discussions on conventional Blackhole attacks, Gray Hole attacks, and Co-operative Blackhole attacks. Section 3 analyzes the impact of Blackhole attacks on MANET performance, highlighting key performance metrics affected by these attacks. In Section 4, we present a critical discussion of existing review papers in the field, identifying trends and gaps in current literature. Section 5 offers a comprehensive review and taxonomy of Blackhole attack detection and mitigation schemes. Section 6 explores the concept of Node Trust in MANETs and its role in enhancing network security. Section 7 delves into various Black-Hole Mitigation Strategies, providing a detailed analysis of their effectiveness. Section 8 examines the Experimental Designs and Simulator Usage in MANET security research, offering insights into methodological approaches. Section 9 identifies Research Gaps and provides Recommendations for Future Research, paving the way for further advancements in the field. Finally, Section 10 concludes the survey, summarizing key findings and reiterating the importance of ongoing research in MANET security.

2. OVERVIEW BLACKHOLE ATTACK AND TYPES

A Blackhole attack, the predominant form of packet drop attack, can have severe consequences if not effectively addressed. This attack may manifest in various forms, including cooperative Blackhole, Gray hole, and conventional Blackhole. Due to its sophisticated design, which can deceive security systems, identifying alterations beyond the expected format becomes significantly challenging. Figure 1 illustrates a Blackhole assault along with its different versions.

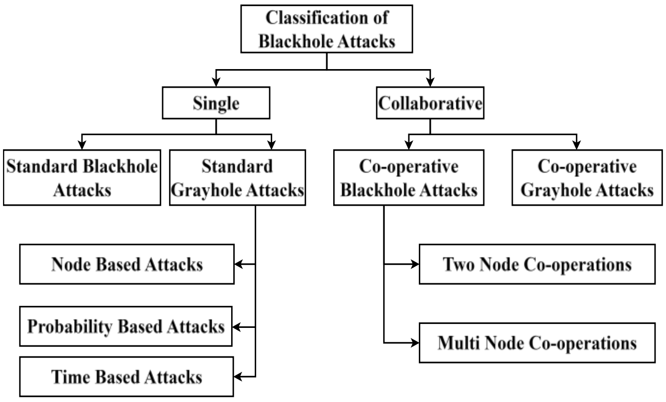
Classification of Blackhole Attacks
Single
Collaborative
Standard Blackhole Attacks
Standard Grayhole Attacks
Co-operative Blackhole Attacks
Co-operative Grayhole Attacks
Node Based Attacks
Probability Based Attacks
Time Based Attacks
Two Node Co-operations
Multi Node Co-operations

Figure 1. Taxonomy of variants of Blackhole attack

The Blackhole invasion represents a highly detrimental packet drop attack, wherein an attacker node responds to an RREQ (Route REQuest) packet by generating a counterfeit RREP (Route REPly) packet. This counterfeit packet contains misleading information, including a reduced number of hops and a destination node number, creating the illusion for the origin node that the RREP packet from the attacking node is legitimate. Consequently, the origin node erroneously believes that the attacking node possesses the most efficient route to the specified destination, despite the attacking node having no actual route to that destination [20-23]. When a data packet is transmitted through the Blackhole node, the packet is dropped and not forwarded, leading to potential data loss [24, 25].

2.1 Blackhole attack

The mechanism of a Blackhole assault is illustrated in Figure 2. In this depiction, node C serves as the assaulting node, and node A initiates the RREQ packet, commencing a route discovery process to find a path to the target node F. Upon receiving the RREQ data packet, the Blackhole node C fabricates a deceptive RREP data packet, featuring a diminished hop count and a destination node number slightly greater than the sequence numbers found in the fields of the last recorded RREQ data packet sent by the origin. Node A, the source node, is misled into believing that this path, transmitted via node C, is the optimal route after receiving the deceptive RREP data packet.

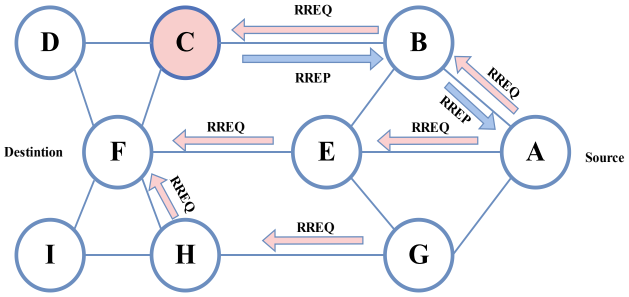

Figure 2. Node C acting as Blackhole by sending fake RREP

However, when node A transmits a data packet to its destination node F, node C intercepts and discards it without forwarding any further. The Blackhole assault significantly diminishes (PDR), and without effective countermeasures, it has the potential to effectively disrupt communication in almost any network. The authentic manifestation of a Blackhole attack, where the malicious attacking node drops all packets, is not common. This form is relatively easy to identify since the absence of packet transmission within a specified timeframe allows for straightforward detection.

2.2 Gray hole attack

Khanna and Sachdeva [19] differentiate Gray-hole attacks from black-hole attacks by highlighting their distinct characteristics. In the route discovery phase, the malicious node initially behaves as a regular (honest) node before transitioning to a malevolent state. These deceptive nodes intercept data packets [26, 27]. The continuously shifting behavior of Gray-hole attacks poses a significant challenge in their detection [26]. Despite starting as a seemingly trustworthy node, the Gray-hole node ultimately reveals its malicious intent by dropping packets. Notably, it selectively drops all UDP packets when forwarding TCP packets, resulting in the discarding of half of all data packets. This deceptive behavior undermines system integrity and proves challenging to identify [21, 28]. The Gray hole cyberattack represents a more nuanced form of attack, wherein the attacker node selectively sends certain packets while dropping others [16, 26]. The sequence of packet loss can vary, typically following one of three patterns:

A) Filtering packets from a single or only a few specific nodes while forwarding packets from the entire network.

B) Using a probabilistic technique to drop packets, rejecting the input stream with a certain probability.

C) Releasing the packet at a specific period while concurrently forwarding it as a seemingly genuine node.

Nodes are chosen either randomly or through an intelligent selection process. Figures 3-7 illustrate the process of establishing a path between the source and the destination during data transmission. Additionally, these figures depict the occurrence of packet dropping when a Gray-hole attack is present in the network.

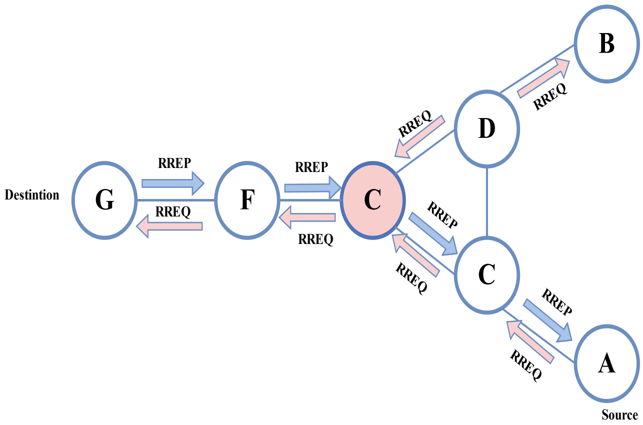

Figure 3. Node E sending a genuine RREP packet (Acting as Gray hole)

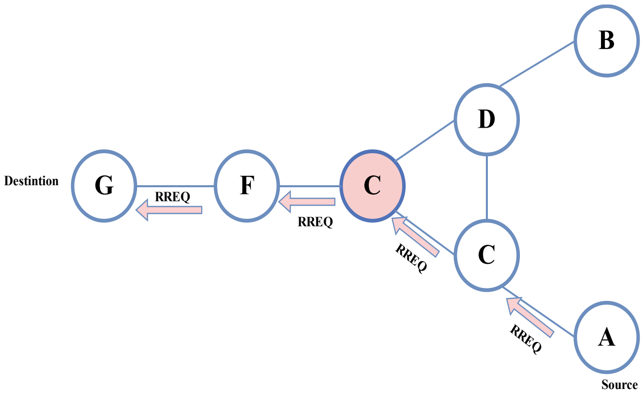

Figure 4. Node E sending a genuine RREP packet (Acting as Gray hole)

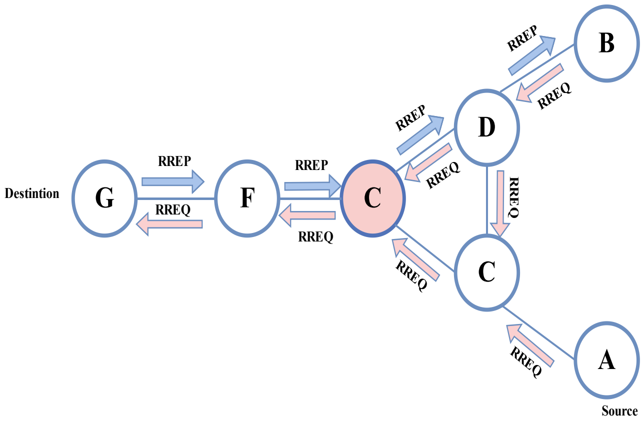

Figure 5. Grayhole node E forwarding incoming packets from node C

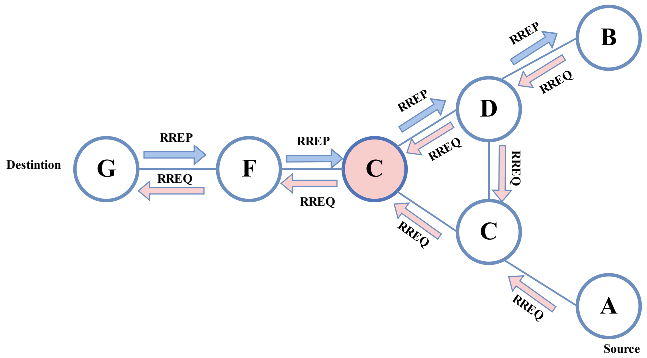

Figure 6. Node E sends a legitimate RREP to source node B for destination node G

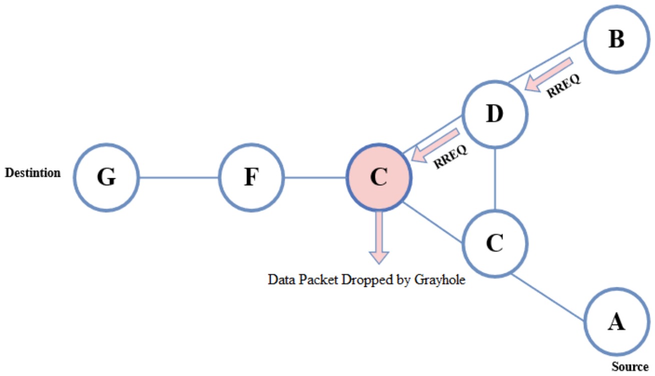

Figure 7. Node E drops all incoming packets from node D

2.3 Co-operative Blackhole attack

One of the variants of Blackhole attacks is the Co-operative Blackhole attack, which is a lethal variant of the Blackhole attack [29]. In this type of attack, two or more hostile nodes collaborate to accomplish the packet drop action [30, 31]. The Co-operative Blackhole attack is more dangerous than the regular Blackhole attack because it is more difficult to detect and mitigate. The malicious nodes can coordinate their actions to drop packets in a way that is not easily distinguishable from normal network behavior. To address this issue, various detection and mitigation strategies have been proposed in the literature. Terai et al. [32] demonstrated a variety of packet-dropping Blackhole and cooperative black hole attacks. The strategies discussed in the study, though, are quite restricted and therefore do not address the entire spectrum of mitigating options. Thanuja and Umamakeswari [33] summarizes Blackhole attacks and a few detection methods such as cryptography-based prevention and IDS-based detection. This paper does not present or discuss the major mitigation techniques. Panda and Pattanayak [29] went through the Blackhole, Gray hole, and cooperative Blackhole attacks, as well as a brief explanation of scheme categorization. Learning-Based strategies are not evaluated, and no categorization as a plan potential is offered. There is a dearth of good categorization of prevention and detection mechanisms in the literature covered in this area, with prominent and crucial mitigation approaches being overlooked. There are no limitations in this research for future study or problems in Blackhole attacks in MANETs provided or explored.

Nodes J and G collaborate as Blackhole nodes in Figure 8, where node J serves as a forwarding node, and node G acts as a sink to discard the data packet.

Initially, when node J receives an RREQ (Route REQuest) packet through node C for the target node I, it responds by transmitting a fraudulent RREP (Route REPly) packet. This fake packet contains an exceptionally large sequence destination number, creating the illusion that it possesses the most recent route to the destination. Subsequently, the source node, node A, sends the data packet along the path that includes these Blackhole nodes. Node J receives the data packet and transfers it to node G, which discards the packet. In this scenario, node J masquerades as a legitimate node, ostensibly forwarding the packet to the next hop, thereby evading detection by the preceding hop.

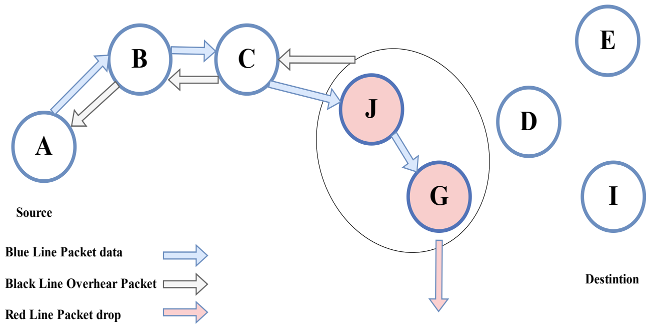

Figure 8. Nodes J and G collaborate to launch a cooperative blackhole attack

3. THE IMPACT OF THE BLACK HOLE ATTACK ON PERFORMANCE MANET

One of the key aspects of this study is the impact of Blackhole attacks on the performance of MANETs. As stated in Table 1, and Figure 9 the impact of the Blackhole attack on the constituent parameters of the MANETs network can lead to a deterioration in network performance in general. The study also shows that the Blackhole attack can affect various performance parameters, including routing problems, (PDR) and throughput, E to E delay, and energy consumption. It is important to note that the impact of the Blackhole attack on MANET performance parameters persists, and there is no 100% solution to this threat. Therefore, it is crucial to continue researching and developing effective detection and mitigation strategies to minimize the impact of Blackhole attacks on the performance of MANETs.

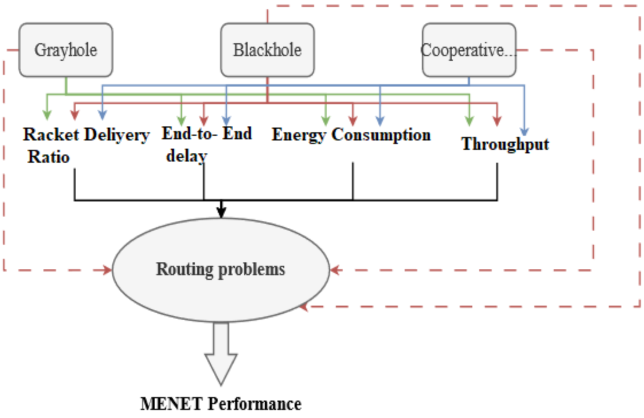

Figure 9. Blackhole attack effects on MANET performance parameter

Table 1. Black hole attack on MANET performance parameters

Attack	Parameter	References
Blackhole effect on	Routing problems	[20, 23, 24, 30, 33-39]
	(PDR) and Throughput	[20, 24, 33, 37-40]
	Eto-E delay	[24, 37, 39]
	Energy Consumption	[36, 39, 41-44]

Table 2. Comparison of existing articles on Blackhole attacks

Authors	Attacks Covered	Count of Mechanisms	Classification	Research Gaps	Limitations
[16]	Blackhole attack, Blackhole, Cooperative, Gray hole attack	91	Yes	No	Learning-based schemes are not considered, and no classification is provided as a scheme future.
[27]	Blackhole	12	Yes	No	There is no classification provided; just standard Blackhole attacks are covered.
[45]	Blackhole, cooperative black hole attack.	14	Yes	No	In the search categorization, the efficiency of the techniques was not mentioned with MANETs, no trust-based scheme in discussed.

4. DISCUSSION OF EXISTING REVIEW PAPERS

This section discusses the existing review papers on detecting, preventing, or mitigating Blackhole and similar attacks in MANETs. The authors compared the preceding publications based on the type of attacks addressed in the article as described in Table 2, the quantity of related articles examined, and the availability of taxonomy or categorization of systems. The paper discussed the merits, drawbacks, and suitability of various detection and mitigation strategies. Another paper reviewed was by Mwangi et al. [45], which presented a survey of Blackhole attacks in MANETs and demonstrated a variety of packet-dropping Blackhole and cooperative Blackhole attacks. One of the papers reviewed was by Gurung and Chauhan [27], which provided a survey of Blackhole attack mitigation techniques in MANETs. The authors also reviewed a paper by Khanna and Sachdeva [16] which provided a survey on Blackhole attacks in MANETs and discussed the impact of these attacks on network performance. The paper also briefly explained scheme categorization and presented a few detection methods such as cryptography-based prevention and IDS-based detection. Overall, the authors found that there is a dearth of good categorization of prevention and detection mechanisms in the literature covered in this area, with prominent and crucial mitigation approaches being overlooked [3]. The authors suggest that future research should focus on developing better categorization and evaluation of these strategies to improve their effectiveness in preventing and mitigating Blackhole attacks in MANETs.

5. REVIEW AND TAXONOMY

While thoroughly examining multiple review publications, we identified various mechanisms for the recognition, prevention, and mitigation of Blackhole threats and their variations in MANET, as illustrated in Figure 10.

In the study by Juneja [31], a session-based suspicious node assessment approach is introduced to identify and prevent cooperative Blackhole attacks. The K-neighbour assessment method is employed to detect suspicious nodes engaging in cooperative attack activities, with assessments randomly conducted over distinct periods during communication.

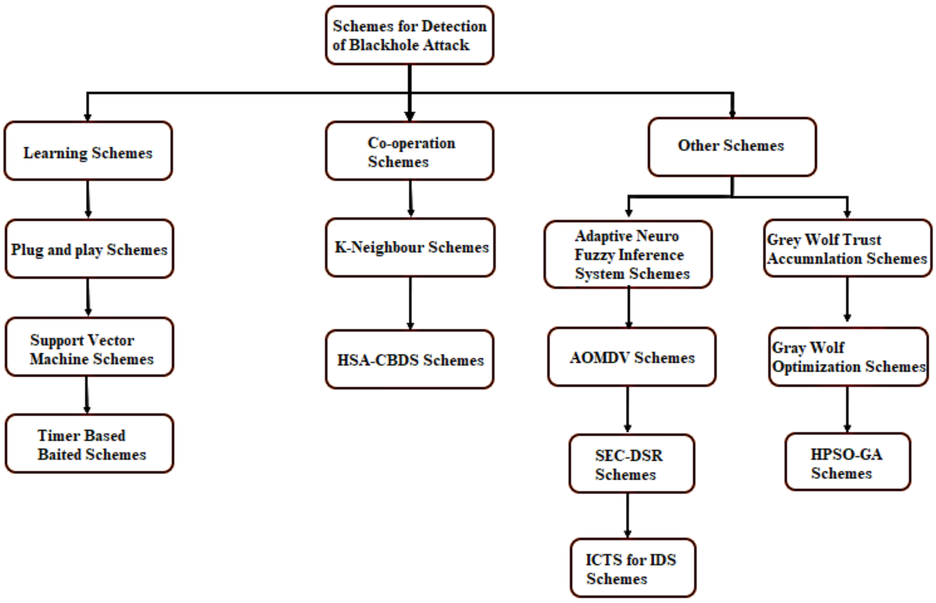
Schemes for Detection of Blackhole Attack
Learning Schemes
Co-operation Schemes
Other Schemes
Plug and play Schemes
K-Neighbour Schemes
Adaptive Neuro Fuzzy Inference System Schemes
Grey Wolf Trust Accumnlation Schemes
Support Vector Machine Schemes
HSA-CBDS Schemes
AOMDV Schemes
Gray Wolf Optimization Schemes
Timer Based Baited Schemes
SEC-DSR Schemes
HPSO-GA Schemes
ICTS for IDS Schemes

Figure 10. The taxonomy of detection and mitigation schemes for blackhole attacks in MANETs [16]

The impact of Blackhole attacks on MANET performance parameters is investigated based on the number of attackers. The current AODV protocol, as per the findings, experiences a reduction in (PDR) by up to 31.45% for static networks, 21.33% for dynamic networks, and 18.96% for highly dynamic networks in the presence of Blackhole attacks. In contrast, the suggested multiple and randomized session-based K-Neighbour assessment approach yields higher PDR values of 81.37%, 73.9%, and 73.21% for static, dynamic, and highly dynamic networks, respectively.

Another approach, presented by Farahani [24], proposes a novel detection method utilizing the K-nearest neighbour (KNN) algorithm for grouping and fuzzy inference for cluster head selection. This approach shows enhanced performance in various network metrics, including (PDR) and throughput.

In wireless mesh network architecture, Vatambeti [40] introduces the Grey Wolf Trust Accumulation (GWTA) Schema to combat Blackhole (BH) and grey hole (GH) attacks. The suggested GWTA aims to discover trustworthy nodes for transmitting information, thereby decreasing the packet loss rate by 98.8% and increasing the throughput ratio by 88bps.

Addressing the broader spectrum of threats, Feng et al. [46] present a plug-and-play system for identifying DoS, privacy threats, and Blackhole threats. The system utilizes a capturing device for packet gathering and a deep learning identification model for attack identification, showing efficient performance with various deep learning models.

In the study by Gautam and Tokekar [47], a Support Vector Machine (SVM) Particle Swarm-based detection approach is proposed for optimising against DDoS and Blackhole attacks in mobile ad hoc networks. However, challenges in detection precision rate indicate the need for additional characteristics for identifying attack traffic.

Moudni et al. [23] suggest a novel approach for detecting Blackhole attacks in MANETs, utilizing Particle Swarm Optimization (PSO) and Adaptive Neuro Fuzzy Inference System (ANFIS). The technique demonstrates strong detection performance and a minimal false alarm rate.

Harmony Search Algorithm (HSA) is recommended by Fahad et al. [48] to reduce latency issues created by the Cooperative Bait Detection Scheme (CBDS) for identifying Blackhole attacks. The suggested technique shows improvements in E-to-E delay, latency, routing overhead, throughput, and PDR.

Vatambeti et al. [49] introduce Gray Wolf Optimization (GWO) in wireless ad hoc network design, combining trust setup data aggregation with Gray Wolf trust accumulation. GWO's behavior identifies Blackhole and grey hole attacks and enhances packet delivery, making the proposed method valuable for MANET packet transmission and routing layer security.

In the study by Yasin and Abu Zant [50], an intelligent Blackhole identification and seclusion approach are proposed, incorporating timers and baiting methods to enhance detection performance. The approach shows promise in maintaining E to E delay, (PDR), and throughput, nearing the native AODV sans Blackholes.

The expanded Ad hoc on-demand multipath distance vector (AOMDV) approach in the study by Elmahdi et al. [35] ensures trustworthy and secure data transmission in hostile nodes in MANETs. The simulation results demonstrate superior throughput and (PDR), making the suggested system suitable for emergency operations in MANETs.

Tyagi and Dembla [51] present a technique to protect routing protocols from Blackhole threats while improving network connection. The proposed approach demonstrates a higher throughput, lower packet drop rate, and reduced collision in a vehicle-to-vehicle (V2V) context.

Using the HPSO-GA technique, Thanuja and Umamakeswari [33] investigate detecting Blackhole attacks in MANETs by employing data routing information (DRI) from surrounding nodes. The HPSO-GA routing mechanism improves throughput ratio and reduces routing overhead and E to E delay.

In the study by Kumar et al. [52], a lightweight solution approach called SEC-DSR is proposed for identifying and isolating Blackhole nodes in MANETs. This approach, evaluating only control packets for network routing, demonstrates a higher (PDR) and lower E to E latency in the proximity of intruders.

Vinayagam et al. [53] introduces the Integrated Cross Interior (ICI) architecture for Intrusion Detection Systems (IDS) for the identification of Blackhole attacks in MANETs. This IDS-based security strategy proves effective.

The studies in Table 3 presented encompass a broad spectrum of topics within the context of mobile and vehicular ad-hoc networks (MANETs and VANETs). Zhou et al. [54] focused on blockchain-based privacy protection, introducing the Efficient Blockchain-Based Conditional Privacy-Preserving Authentication (EBCPPA) protocol for VANETs. This innovative scheme addresses key revocation issues and inefficiencies associated with on-chain operations, providing a comprehensive solution for secure authentication in VANETs.

In the realm of location privacy within the Internet of Vehicles (IoV), Babaghayou et al. [55] proposed the OVR scheme. Leveraging the silent period feature, this safety-aware location privacy-preserving scheme enhances privacy by allowing overseer vehicles to ensure safety while others enter silence mode. This study showcases the importance of addressing location privacy concerns in the IoV paradigm.

Addressing intrusion detection mechanisms in MANETs, Sultan et al. [56] proposed a technique based on deep learning artificial neural networks (ANNs). This approach aims to predict and isolate DoS attacks, showcasing the potential of advanced machine learning techniques in bolstering the overall security of mobile ad-hoc networks.

Sankar et al. [57] introduced the Safe Routing Approach (SRA) to enhance security in MANETs. By employing behavior analysis to track and monitor attackers during the route discovery process, the SRA provides a mechanism to identify and eliminate attacks, contributing to the robustness of MANET security.

In the context of software-defined cyber-physical systems (CPSs), Cai et al. [58] presented the Adaptive DDoS Attack Mitigation (ADAM) scheme. Addressing the pressing issue of DDoS attacks, the study focuses on detecting and mitigating such attacks in CPSs, showcasing the adaptability required in contemporary cyber-physical environments.

Ahmed et al. [59] explored blockchain-assisted trust management in VANETs. Their proposed framework combines privacy-preserving authentication and context-aware trust management, both enhanced by blockchain technology, underscoring its crucial role in improving privacy and trust in vehicular networks.

Liang and Liu [60] have contributed to the security of VANETs by conducting a thorough analysis of an efficient certificateless aggregate signature scheme. Their study focuses on conditional privacy preservation, adding a layer of understanding to the security aspects of these schemes in vehicular networks.

Yao et al. [61] shifted the focus to cache pollution attack detection in VANETs using ensemble learning in information-centric networking (ICN). This approach provides a valuable contribution to securing ICN-based VANETs by detecting and mitigating cache pollution attacks, which can significantly impact network performance.

Zhang et al. [62] explored adaptive coding and modulation-aided mobile relaying for millimeter-wave flying ad-hoc networks. The study aims to improve E to E throughput by leveraging adaptive coding and modulation in flying ad-hoc networks, showcasing the importance of adapting to the unique characteristics of these networks.

Lastly, Liang and Liu [60] and Hammad et al. [63] presented a security framework for network-based manufacturing systems in an Industry 4.0 context. By utilizing NTRUEncrypt cryptography and the AODV routing protocol, the proposed framework addresses security concerns, emphasizing the need for robust security solutions in advanced manufacturing systems.

These studies contribute to the understanding and advancement of security, privacy, and efficiency in the dynamic environments of mobile and vehicular ad-hoc networks. The diverse range of approaches reflects the multidimensional challenges inherent in these evolving technologies. In this comprehensive exploration of security and privacy solutions within the realm of mobile and vehicular ad-hoc networks (MANETs and VANETs), a detailed comparative overview is presented in the table titled "Comparative Overview of Security and Privacy Solutions in MANETs and VANETs." Table 3 encapsulates a diverse range of studies, each contributing unique insights and innovations to address the dynamic challenges inherent in these network environments. The following paragraphs provide a nuanced discussion of each study, elucidating their respective contributions and highlighting key advancements in the field.

Table 3. Comparative overview of security and privacy solutions in MANETs and VANETs

Authors	Problem Statement	Research Gap	Advantages	Disadvantages	Parameters
[36]	Developing a safe routing approach for MANETs	Limited focus on behavior analysis in existing methods	Enhanced security through behavior analysis	May have limitations in constant updating of attack methods	Behavior Analysis, Routing, Security Monitoring
[54]	Efficient Blockchain-based CPPA scheme for VANETs	Lack of key revocation support; Inefficiency due to on-chain operations	Improved privacy and security; Mitigates key revocation issues	On-chain operations may impact efficiency	PDR, Throughput, Latency, Security Level
[55]	Enhancing location privacy in IoV with road congestion-estimation	Limited attention to past and present trust levels in trust-based methods	Improved location privacy; Utilizes silent period feature	May lack weight balance in trust levels	Location Privacy, Safety, Silent Periods
[56]	Designing an intrusion detection predictive technique for MANETs	Lack of deep learning-based intrusion detection in MANETs	Improved security through deep learning ANNs	Simulation-based evaluation may have limitations	Intrusion Detection, Deep Learning, Security Level
[58]	Addressing DDoS attacks in software-defined CPS	Lack of adaptive DDoS mitigation schemes in CPS	Adaptive DDoS mitigation for improved security	Complexity may impact practicality	DDoS Mitigation, Adaptability, Security Improvement
[59]	Introducing a novel blockchain-assisted trust management framework	Limited context-aware trust management in existing schemes	Enhanced privacy and trust management	Complexity may impact practicality	Blockchain, Privacy, Trust Management, Security
[60]	Security analysis of certificateless aggregate signature schemes	Limited analysis of security in existing schemes	Enhanced security analysis	Limited insights into security issues	Security Analysis, Privacy Preservation
[61]	Introducing a cache pollution attack detection scheme	Limited ensemble learning-based detection in ICN-based VANETs	Improved cache pollution attack detection	May have limitations in dynamic network conditions	Cache Pollution Detection, Ensemble Learning
[62]	Developing an adaptive coding and modulation aided mobile relaying scheme	Limited focus on adaptive schemes for millimeter-wave networks	Improved end-to-end throughput	Complexity may impact practicality	Adaptive Coding, Modulation, Relaying, Throughput
[63]	Proposing a security framework for personalized customization in manufacturing systems	Limited attention to security in personalized customization factories	Enhanced security in Industry 4.0 context	May require further improvements in throughput and (PDR)	Security Framework, Manufacturing Systems, Personalized Customization, Industry 4.0

6. NODE TRUST IN MANETS

Sharma et al. [64] developed an innovative trust system for MANETs that is compatible with DSR, AODV, and opportunistic routing protocols. Their approach leverages reinforcement learning and an incentive mechanism to measure the reliability of each node based on historical data. The trust model is designed to learn optimal strategies based on experiences, making it highly adaptable to changing network conditions. A key feature of this system is its dynamic nature, with trust levels being continuously updated during the packet routing process. This ensures that the network can quickly respond to changes in node behavior. The model also considers energy efficiency, which is crucial for the longevity of MANET operations. However, continuous trust calculations may introduce computational overhead, potentially impacting network performance in resource-constrained environments. Despite this limitation, the system's ability to combine reinforcement learning with trust management represents a significant advancement in MANET security and routing efficiency.

Srilakshmi et al. [65] proposed an optimization cluster-based routing protocol for MANETs that utilizes a Fuzzy Clustering Algorithm for enhanced security and efficiency. The core of their approach lies in the cluster head (CH) selection process, which depends on the maximum trust values derived from a combination of indirect, direct, and recent trust assessments. This multi-faceted trust evaluation helps ensure that the most reliable nodes are chosen as cluster heads, improving overall network security. The protocol demonstrates impressive energy efficiency, achieving a minimum energy usage of 0.10 mJ, compared to 0.12 mJ in networks without attack protection. This energy optimization is crucial for extending the operational life of MANET devices. However, the study has some limitations. It was primarily tested against selective packet-dropping attacks, leaving its effectiveness against other types of network threats uncertain. Despite these limitations, the protocol's energy efficiency and sophisticated trust mechanism make it a noteworthy contribution to MANET routing research.

Veeraiah and Krishna [42] introduced a hybrid routing protocol for MANETs that combines fuzzy clustering with a novel Cat Slap Single-player Algorithm (C-SSA). This innovative approach utilizes direct, indirect, and recent trust values to create a comprehensive trust model. The protocol stands out for its dynamic nature and its ability to be trained and updated online, allowing it to adapt to changing network conditions in real time. Energy efficiency is a key focus of this protocol, with tests showing energy consumption as low as 0.11 mJ, making it suitable for resource-constrained MANET environments. Despite this limitation, the protocol's combination of energy efficiency, dynamic trust evaluation, and novel optimization techniques represents a significant advancement in secure MANET routing, potentially offering improved performance in various mobile ad hoc network scenarios.

Karthik and Krishnan [66] developed a novel approach to MANET security and routing using a k-means algorithm combined with Bayesian inference for trust estimation. Their method incorporates both direct and indirect observations to create a dynamic trust model. The use of k-means clustering helps in grouping nodes with similar trust characteristics, while Bayesian inference allows for probabilistic trust updates based on new observations. The dynamic nature of the trust model allows for continuous updates of trust values, enhancing the network's ability to detect and isolate malicious nodes quickly. However, the computational complexity of the k-means algorithm could pose challenges in resource-constrained environments, potentially limiting its applicability in some MANET scenarios. Despite this limitation, the protocol's ability to balance security, routing efficiency, and energy conservation makes it a valuable contribution to MANET research, particularly for applications were robust security and energy efficiency is paramount.

Ilakkiya and Rajaram [67] proposed an innovative DAG-Blockchain protocol with Multi-Factor PUF (Physically Unclonable Function) authentication for MANET-IoT environments. Their approach incorporates a Secure Trust-based Dijkstra's Method for routing, enhancing both security and efficiency. A key feature of this protocol is its use of a Bi-Directional Gated Recurrent Unit (GRU) for trust estimation, making it a trainable and dynamic system that can adapt to changing network conditions. The protocol also demonstrates improved network lifetime, addressing the critical issue of energy efficiency in MANETs. However, the researchers note potential scalability challenges in very large networks, which could limit its application in extensive IoT deployments. Despite this limitation, the combination of advanced machine learning techniques, blockchain security, and energy-aware design makes this protocol a significant advancement in secure routing for MANET-IoT environments, offering a robust solution for scenarios requiring high security and reliability.

Table 4. Overview of trust and routing methods in MANETs

Authors	Method	Key Features	Advantages	Limitations
[64]	Trust system for MANETs using reinforcement learning and incentive mechanism	Compatible with DSR, AODV, and opportunistic routing protocols, dynamic trust updates, energy efficiency	Adaptable to changing network conditions, enhances routing efficiency, considers energy efficiency	Computational overhead from continuous trust calculations
[65]	Optimization cluster-based routing protocol using Fuzzy Clustering Algorithm	CH selection based on trust values from indirect, direct, and recent assessments, energy efficiency	Improved network security, enhanced energy efficiency (0.10 mJ)	Tested mainly against selective packet-dropping attacks
[42]	Hybrid routing protocol combining fuzzy clustering with Cat Slap Single-player Algorithm (C-SSA)	Dynamic trust model with online updates, energy efficiency focus	Adapts to changing network conditions in real-time, low energy consumption (0.11 mJ)	Computational complexity could be a challenge in resource-constrained environments
[66]	MANET security and routing using k-means algorithm and Bayesian inference	Dynamic trust model with continuous updates, probabilistic trust updates, k-means clustering for grouping nodes	Enhances network security and energy conservation	Computational complexity of k-means algorithm may limit applicability
[67]	DAG-Blockchain protocol with Multi-Factor PUF authentication for MANET-IoT environments	Secure Trust-based Dijkstra's Method, Bi-Directional GRU for trust estimation	Enhances security and efficiency, improved network lifetime	Potential scalability challenges in very large networks
[68]	IWT-MRD and AOMDV protocols with Neighbour Node-based Trust Calculation (NN-TC) Model	Combines multiple trust metrics, RSSI-based stability assessment, fuzzy logic for route preservation	Dynamic and adaptable to changing network conditions, improved route stability	Uncertainty in mobile networks handling could impact stability
[69]	TUE-OLSR protocol using cloud model and fuzzy Petri net for trust management	Trust reasoning based on node performance metrics, dynamic trust model	Enhanced accuracy in trust assessments, improved network reliability	Potential drawback in handling uncertainty and the complexity of fuzzy Petri net

Table 5. Summary of strategies for detecting and mitigating attacks in MANETs

Strategy	Description	Merits	Drawbacks	Suitability
Cryptography-based scheme [70]	Utilizes cryptographic technologies (e.g., symmetric key cryptography, digital signatures) for encryption, verification, and integrity.	Provides protection against external threats.	High computation and communication overhead; not effective against internal attackers.	Suitable for static networks, challenging in dynamic environments due to key distribution difficulties.
Overhearing-based scheme [71]	Nodes monitor the transmissions of their neighbors to detect abnormal behavior (e.g., packet dropping).	Can detect single and multiple black-hole nodes.	High false positive rate, increased energy consumption due to constant monitoring.	Effective in moderate to extreme mobility scenarios with good (PDR) and throughput.
Sequence Number Threshold scheme [70]	Sets a dynamic threshold for sequence numbers in routing packets; nodes with sequence numbers above the threshold are flagged as malicious.	Simple and efficient in both static and dynamic scenarios.	Vulnerable to smart attackers who can craft sequence numbers to avoid detection.	Effective in both static and dynamic environments, especially with dynamic thresholds.
Acknowledgment-based scheme [72, 73]	Utilizes acknowledgment packets (e.g., TWOACK, 2ACK) to confirm packet delivery and identify malicious nodes.	Improves detection of routing misbehavior and increases packet delivery rate.	High routing overhead due to the extra control packets, energy consumption increases in dynamic environments.	Better suited for static or low mobility scenarios due to high routing overhead in dynamic scenarios.
Clustering-based scheme [74]	Divides the network into clusters with elected cluster heads responsible for detecting malicious activities within the cluster.	Good against single, multiple, and collusive black-hole attacks.	High computational overhead in dynamic environments; risk of malicious nodes becoming cluster heads.	Effective in static or low mobility environments; overhead increases in high mobility scenarios.
Cross-layer Collaboration scheme [75]	Involves cooperation between multiple network layers (e.g., session and network layers) to detect and prevent attacks.	Ensures high detection accuracy and low false alarms.	Increases routing overhead, delays, and energy consumption due to inter-layer communication.	Suitable for static networks; challenging in highly dynamic scenarios due to layer dependencies.
Cross-checking-based scheme [76]	Nodes cross-check routing information with previous or next-hop nodes to verify the integrity of routing paths.	Effective against cooperative black-hole attacks.	High routing overhead and delay due to extra control packets; increases energy consumption.	More effective in static or low mobility environments; suffers in dynamic environments due to frequent disconnections.
IDS-based scheme [70]	Deploys Intrusion Detection System (IDS) nodes that monitor network traffic and detect malicious activities.	Detects single and multiple black-hole attacks; low routing overhead.	Detection efficiency depends on proper placement of IDS nodes; random placement may lead to missed detections.	Effective in both static and dynamic environments; requires careful deployment of IDS nodes.
Trust-based scheme [74]	Computes trust values for each node based on its behavior and exchanges trust packets periodically.	Detects single and multiple black-hole nodes effectively.	High routing overhead and energy consumption due to monitoring and trust value computation.	Suitable for static networks; suffers from high delay and overhead in dynamic environments.
Hybrid scheme (Trust-aware FuzzyClus-Fuzzy NB [42]	Combines trust and clustering methods to detect and mitigate attacks.	Detects single and multiple black-hole nodes with minimum delay and energy consumption.	High overhead in highly mobile environments due to clustering maintenance.	More effective in less dynamic environments; overhead increases in highly mobile scenarios.
Cross-layer-based scheme [75]	Ensures communication between multiple network layers to detect malicious activities.	High detection accuracy and ensures secure communication.	Complex due to inter-layer dependencies; increases routing overhead.	More suitable for static networks with low node mobility.
SAODV (Secure AODV [77]	Implements security mechanisms (e.g., random numbers, extended control packets) in AODV protocol to ensure secure routing.	Effective against black-hole attacks; ensures route authenticity.	High delay and routing overhead due to additional control packets and verification processes.	Suitable for scenarios requiring high security, but overhead limits applicability in highly dynamic networks.
Cooperative Bait Detection Scheme [78]	Uses bait addresses to lure malicious nodes into revealing themselves and then prevents their participation in routing.	Effective in detecting collaborative attacks; proactive detection mechanism reduces resource wastage.	Can mistakenly identify adjacent nodes as malicious; requires more time to detect and trace malicious nodes.	Suitable for scenarios with suspected collaborative attacks; requires cautious bait address selection.
Explore-based Active Detection (EBAD) [79]	Uses fictitious route request packets to detect malicious nodes by analyzing fake route reply packets.	Reduces energy consumption and detection latency.	Not effective against gray-hole attacks that participate genuinely in route discovery.	Suitable for environments with low to moderate mobility; less effective in highly dynamic environments.

Alyoubi [68] developed the IWT-MRD and AOMDV protocols, incorporating a Neighbour Node-based Trust Calculation (NN-TC) Model for enhanced security and efficiency in MANETs. Their approach combines multiple trust metrics, RSSI-based stability assessment, and fuzzy logic for route preservation, creating a comprehensive system for secure and reliable routing. The trust model is dynamic and trainable, allowing it to adapt to changing network conditions and evolving threat landscapes.

The use of fuzzy logic in route preservation helps in handling the uncertainty inherent in mobile networks, potentially leading to more stable connections. Despite this potential limitation, the protocol's comprehensive approach to trust calculation, route stability, and energy efficiency represents a significant advancement in MANET routing technology, offering improved security and performance for a wide range of mobile ad-hoc network applications.

Wang et al. [69] developed the TUE-OLSR protocol, which incorporates a cloud model and fuzzy Petri net for trust management in MANETs. This innovative approach uses trust reasoning based on node performance metrics to enhance the security and reliability of the network. The integration of the cloud model allows for handling uncertainty in trust evaluations, while the fuzzy Petri net provides a formal framework for trust reasoning. This combination enables a more nuanced and accurate assessment of node trustworthiness compared to traditional binary trust models. The protocol is dynamic, allowing it to adapt to changing network conditions and evolving threat landscapes. Despite this potential drawback, the sophisticated trust reasoning mechanism of TUE-OLSR represents a significant advancement in MANET security, offering improved accuracy in identifying trustworthy nodes and potentially enhancing overall network reliability and performance. We provide a summary of the different trust and routing methods for MANETs in Table 4.

7. BLACK-HOLE MITIGATION STRATEGIES

Wei et al. [2] presents a comprehensive analysis of 14 distinct strategies for mitigating black-hole attacks in MANETs. These strategies are systematically categorized into various approaches, including cryptography-based, overhearing-based, and sequence number threshold-based schemes, among others. Each methodology is specifically designed to address the unique vulnerabilities inherent in MANETs, where nodes are often presumed to be trustworthy. The cryptography-based approaches primarily focus on securing communications through encryption mechanisms, while overhearing-based schemes rely on the continuous monitoring of neighboring node behavior to detect anomalies. For instance, one overhearing-based scheme integrates watchdog and path-rater techniques to identify misbehaving nodes. In contrast, sequence number threshold-based approaches employ dynamic threshold adjustments to detect malicious nodes that manipulate routing information.

Alternative strategies, such as acknowledgment-based and trust-based schemes, utilize diverse methodologies to verify data transmission integrity and node reliability, respectively. Despite the demonstrated efficacy of these techniques, the paper also elucidates their limitations, including increased routing overhead, false positive detections, and elevated energy consumption.

The authors conclude that while each strategy possesses distinct merits, there is no universally applicable solution. The suitability of each approach is contingent upon specific network conditions and the nature of the attacks being mitigated. The paper emphasizes the critical importance of considering these factors in the design of more robust protocols for MANETs.

Table 5 provides a comprehensive overview of these 14 strategies employed in MANETs for the detection and mitigation of various attack types, including black-hole and gray-hole attacks. Each strategy is systematically evaluated based on its core mechanism, advantages, disadvantages, and suitability for different network environments. This analysis highlights the intricate trade-offs between detection accuracy, operational overhead, and network conditions.

This comprehensive review not only synthesizes the current state of research in MANET security but also provides a foundation for future investigations. By delineating the strengths and weaknesses of each approach, the study offers valuable insights for researchers and practitioners seeking to develop more effective and context-appropriate security solutions for MANETs.

8. EXPERIMENTAL DESIGNS AND SIMULATOR USAGE

Table 6 presents a comprehensive synthesis of experimental methodologies and simulator utilization across various studies in MANETs. A clear pattern emerges from this analysis, with NS-2 serving as the predominant simulation platform, being used in four out of the seven documented studies. This widespread adoption of NS-2 suggests its established role as a standard tool for MANET simulations.

The experimental designs show consistent parameters across studies, particularly in their simulation environments. Network areas typically range from 670m × 670m to 1000m × 1000m, with most studies opting for larger areas around 800m × 800m or 1000m × 1000m. Node populations vary significantly across studies, ranging from 30 to 150 nodes, allowing for evaluation across different network densities.

A notable consistency across studies is the packet size, with multiple studies using 512 bytes as their standard packet size. Maximum node speeds vary between studies, with most setting maximum velocities between 5-20 m/s, though one study [80] explored higher speeds up to 90 m/s. Simulation durations also show variation, ranging from 120 seconds to 900 seconds, enabling analysis of network behavior over different time scales.

The experimental parameters reflect diverse approaches to testing network performance. Some studies, such as Common Neighbor Listening [74] and DCM vs AODV [75], explicitly incorporate malicious nodes in their experimental design, while others focus on different aspects of network performance. Network configurations vary from simple setups with basic parameters to more complex scenarios involving specific attack models and defense mechanisms.

One interesting observation is the variation in transmission ranges and bandwidth specifications. Where specified, transmission ranges typically fall around 250m, and bandwidth is often set at 2Mbps, suggesting these as common baseline parameters for MANET simulations.

Table 6. Summary of Experimental Designs and Simulator Usage

Method	Simulator	Experimental Design Parameters
Custom Protocol [70]	ns-2 (v2.27)	- Area: 1000m × 1000m
		- Nodes: 30
		- Range: 250m
		- Speed: 5 m/s
		- Protocol: AODV
		- Bandwidth: 2Mbps
		- Duration: 600s
		- Pause time: 10s
TWOACK and S-TWOACK [72]	Not specified	- Area: 670m × 670m
		- Nodes: 40 mobile nodes
		- Range: 250m
		- Speed: max 20 m/s
		- Packet size: 512 bytes
		- Duration: 900s
		- Traffic: 10-30 CBR pairs
Common Neighbor Listening [74]	NS2	- Area: 1000m × 1000m
		- Nodes: 50 (5 malicious)
		- Speed: max 20m/s
		- Data rate: 1 packet/s
		- Packet size: 512 bytes
		- Duration: 600s
		- Bandwidth: 2Mbps
		- MAC: IEEE 802.11
DCM vs AODV [75]	NS2	- Area: 1000m×500m
		- Nodes: 50 or 100 mobile nodes
		- Speed: 0-10 m/s
		- Radio coverage: 150m diameter
		- Packet size: 512 bytes
		- Transmission rate: 0.33s
		- Queue size: 50 packets
		- Total packets: 2500
		- Pause time: 200s
D-CBDS [78]	NS2	- Area: 800m × 800m
		- Nodes: 150 randomly deployed
		- Random attacker selection
SAODV vs AODV [80]	Not specified	- Area: 800m × 800m
		- Nodes: 60
		- Time: 120s
		- Speed: 10-90 m/s
		- Payload: 512 bytes
		- Load: 100 items

The experimental designs revealed in Table 6 serve as a valuable resource for researchers, offering insights into best practices for experimental methodology and facilitating direct comparisons between diverse blackhole attack mitigation strategies in MANETs. This comprehensive overview not only synthesizes the current state of research but also provides a foundation for future investigations in MANET security.

9. RESEARCH GAPS AND RECOMMENDATIONS FOR FUTURE RESEARCH

A comprehensive analysis of extant research literature has illuminated several critical gaps in current studies. Future investigative efforts should address these lacunae to develop a more efficient, effective, legitimate, and precise framework for mitigating and preventing various iterations of Blackhole attacks in Ad hoc networks. The identified research gaps include:

Trust-based methodologies, while gaining prominence due to their preventive nature, often lack equilibrium in considering historical and contemporary trust levels. Many extant studies rely solely on (PDR) for trust estimation [23, 40]. The propagation of diverse data types and the efficacy of protection mechanisms frequently prove insufficient, enabling malicious nodes to inflict substantial damage prior to their complete isolation [51]. As mitigation and detection systems increase in complexity, future research must prioritize the development of lightweight methodologies that are both pragmatic and accurate in real-world scenarios, considering the inherent power and bandwidth limitations of Ad hoc networks [23, 51, 54]. Additionally, cooperation across three or more nodes remains inadequately addressed or minimized in the majority of current and previous studies.

Based on this comprehensive literature review and the identified research gaps, we propose the following directions for future research in MANET security, with a particular focus on Blackhole attack detection and mitigation:

1. Adaptive Trust Models:
- Current Issue: Existing trust-based techniques often lack balanced consideration of historical and current trust levels.
- Future Direction: Develop dynamic trust models that adjust the weighting of historical and current trust data based on network conditions and attack patterns.
- Proposed Approach: Integrate machine learning algorithms, such as reinforcement learning, to optimize trust calculation parameters in real-time, ensuring more accurate and context-aware trust assessment.
2. Lightweight Security Solutions:
- Current Issue: Complex mitigation/detection systems are often impractical due to MANET power and bandwidth constraints.
- Future Direction: Design energy-efficient security protocols that maintain effectiveness while minimizing resource consumption.
- Proposed Approach: Explore edge and fog computing paradigms to offload intensive computations, and develop optimized cryptographic algorithms for resource-constrained devices.
3. Collaborative Defense Mechanisms:
- Current Issue: Cooperation across multiple nodes is inadequately addressed in current studies.
- Future Direction: Develop robust collaborative defense mechanisms leveraging the distributed nature of MANETs to enhance security.
- Proposed Approach: Investigate blockchain-based solutions for secure, decentralized node collaboration, enabling trustless consensus on network security states and collective threat mitigation decision-making.
4. Cross-Layer Security Frameworks:
- Current Issue: Most existing solutions focus on security at specific network layers, leaving intersectional vulnerabilities.
- Future Direction: Design comprehensive cross-layer security frameworks providing holistic protection against multi-vector attacks.
- Proposed Approach: Develop an integrated security architecture coordinating defense mechanisms across physical, MAC, network, and application layers, utilizing machine learning for cross-layer anomaly detection.
5. Proactive Threat Intelligence:
- Current Issue: Current systems are largely reactive, allowing significant damage before attack detection.
- Future Direction: Implement proactive threat intelligence systems capable of predicting and preventing attacks before occurrence.
- Proposed Approach: Utilize predictive analytics and AI-driven threat modeling to forecast potential attack vectors based on network behavior patterns and global threat intelligence feeds.
6. Quantum-Resistant Security Protocols:
- Current Issue: Emerging quantum computing technologies threaten to compromise many current cryptographic systems.
- Future Direction: Develop quantum-resistant security protocols to future-proof MANET security.
- Proposed Approach: Investigate and implement post-quantum cryptographic algorithms, such as lattice-based or hash-based schemes, adapted for MANET resource constraints.
7. Bio-Inspired Security Mechanisms:
- Current Issue: Traditional security approaches often struggle with the dynamic and decentralized nature of MANETs.
- Future Direction: Explore bio-inspired algorithms and mechanisms for more adaptive and resilient security solutions.
- Proposed Approach: Investigate the application of concepts from swarm intelligence, artificial immune systems, and evolutionary algorithms to develop self-organizing and self-healing security mechanisms for MANETs.
8. Context-Aware Security:
- Current Issue: Current security solutions often apply uniform policies regardless of network context or environment.
- Future Direction: Develop context-aware security frameworks that adapt strategies based on the network's current state, application requirements, and environmental factors.
- Proposed Approach: Implement machine learning models to analyze various contextual factors (e.g., node mobility patterns, traffic types, physical environment) for dynamic adjustment of security policies and mechanisms.

10. CONCLUSION

This exhaustive investigation has rigorously analyzed the susceptibility of MANETs to diverse packet drop attacks, with a particular emphasis on Gray hole, Blackhole, and Co-operative Blackhole threats. A notable contribution of this research is the development of a taxonomy encompassing fourteen distinct attack categories, underscoring the increasing complexity and hybridization of malicious strategies. This classification framework serves as a crucial tool for comprehending the dynamic threat environment in MANETs, thereby informing both contemporary and prospective security protocols.

In evaluating the efficacy of detection and mitigation approaches, the research yields promising outcomes through the examination of various vulnerability management methodologies, notably the K-neighbour assessment technique. This approach has exhibited considerable effectiveness in identifying nodes suspected of participating in collaborative attacks, indicating substantial potential for bolstering MANET security in practical applications. Moreover, the study assesses critical performance indicators, including (E to E), Throughput, and (PDR), which function as essential metrics for evaluating the robustness of security measures within MANETs.

The pragmatic implications of this research are multifaceted, extending to diverse domains where secure and dependable communication is essential. For instance, enhanced security protocols derived from this study can be implemented in military communications, ensuring secure and reliable information exchange in combat scenarios. Furthermore, more resilient MANETs can enhance disaster response mechanisms by facilitating improved coordination and information dissemination during crises. The security strategies explored also possess the potential for adaptation to Internet of Things (IoT) environments, safeguarding the proliferating network of interconnected devices that frequently form ad hoc networks.

In summation, this research establishes a robust foundation for future investigations and practical applications in MANET security. By offering crucial insights into countering blackhole attacks and their variations, it contributes significantly to the advancement of more secure and reliable MANETs. The findings have broad-reaching implications, not only advancing technological progress but also potentially influencing economic and societal domains by reinforcing the security and resilience of MANET-based systems across various sectors.

ACKNOWLEDGMENT

Appreciation to Universiti Teknologi Malaysia, researchers and those involved in preparing this paper, "Pembangunan Sistem Pemantauan Dan Peramalan Penyelenggaraan Seni Bina Warisan Berasaskan IoT" (Grant No.: Q.J130000.5028.10G12).

REFERENCES

[1] Dusia, A., Sethi, A.S. (2021). Software-defined architecture for infrastructure-less mobile Ad Hoc networks. In 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), Bordeaux, France, pp. 742-747.

[2] Wei, D., Cao, H., Liu, Z. (2016). Trust-based ad hoc on-demand multipath distance vector routing in MANETs. In 2016 16th international symposium on Communications and Information Technologies (ISCIT), Qingdao, China, pp. 210-215. https://doi.org/10.1109/ISCIT.2016.7751623

[3] Masood, A., Scazzoli, D., Sharma, N., Le Moullec, Y., Ahmad, R., Reggiani, L., Alam, M.M. (2020). Surveying pervasive public safety communication technologies in the context of terrorist attacks. Physical Communication, 41: 101109. https://doi.org/10.1016/j.phycom.2020.101109

[4] Yaseen, Q.M., Aldwairi, M. (2018). An enhanced AODV protocol for avoiding black holes in MANET. Procedia Computer Science, 134: 371-376. https://doi.org/10.1016/j.procs.2018.07.196

[5] Usman, M., Jan, M.A., He, X., Nanda, P. (2020). QASEC: A secured data communication scheme for mobile Ad-hoc networks. Future Generation Computer Systems, 109: 604-610. https://doi.org/10.1016/j.future.2018.05.007

[6] Krishnan, R.S., Julie, E.G., Robinson, Y.H., Kumar, R., Thong, P.H. (2020). Enhanced certificate revocation scheme with justification facility in mobile ad-hoc networks. Computers & Security, 97: 101962. https://doi.org/10.1016/j.cose.2020.101962

[7] Balaji, S., Sasilatha, T. (2019). Detection of denial of service attacks by domination graph application in wireless sensor networks. Cluster Computing, 22(Suppl 6): 15121-15126. https://doi.org/10.1007/s10586-018-2504-5

[8] Gomathy, V., Padhy, N., Samanta, D., Sivaram, M., Jain, V., Amiri, I.S. (2020). Malicious node detection using heterogeneous cluster based secure routing protocol (HCBS) in wireless adhoc sensor networks. Journal of Ambient Intelligence and Humanized Computing, 11(11): 4995-5001. https://doi.org/10.1007/s12652-020-01797-3

[9] Sushma, T. (2021). A review of the cluster based mobile adhoc network intrusion detection system. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(2): 2070-2076.

[10] Cunha, B., Brito, C., Araújo, G., Sousa, R., Soares, A., Silva, F.A. (2021). Smart traffic control in vehicle ad-hoc networks: A systematic literature review. International Journal of Wireless Information Networks, 28(3): 362-384. https://doi.org/10.1007/s10776-021-00517-8

[11] Elwahsh, H., Gamal, M., Salama, A.A., El-Henawy, I.M. (2018). A novel approach for classifying Manets attacks with a neutrosophic intelligent system based on genetic algorithm. Security and Communication Networks, 2018(1): 5828517. https://doi.org/10.1155/2018/5828517

[12] Rani, P., Kavita, Verma, S., Rawat, D.B., Dash, S. (2022). Mitigation of black hole attacks using firefly and artificial neural network. Neural Computing and Applications, 34(18): 15101-15111. https://doi.org/10.1007/s00521-022-06946-7

[13] Srikaanth, P.B., Nagarajan, V. (2021). Fuzzy rough set derived probabilistic variable precision-based mitigation technique for vampire attack in MANETs. Wireless Personal Communications, 121(1): 1085-1101. https://doi.org/10.1007/s11277-021-08673-z

[14] Mohammadi, P., Ghaffari, A. (2019). Defending against flooding attacks in mobile ad-hoc networks based on statistical analysis. Wireless Personal Communications, 106: 365-376. https://doi.org/10.1007/s11277-019-06166-8

[15] Khanna, N., Sachdeva, M. (2018). Critical review of techniques for detection and mitigation of co-operative blackhole attack in MANET. International Journal of Advanced Science and Technology, 110: 1-12. https://doi.org/10.14257/ijast.2018.110.01

[16] Khanna, N., Sachdeva, M. (2019). A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and its variants in MANETs. Computer Science Review, 32: 24-44. https://doi.org/10.1016/j.cosrev.2019.03.001

[17] Gowtham, M.S., Subramaniam, K. (2019). Congestion control and packet recovery for cross layer approach in MANET. Cluster Computing, 22(Suppl 5): 12029-12036. https://doi.org/10.1007/s10586-017-1548-2

[18] Pandey, S., Singh, V. (2020). Blackhole attack detection using machine learning approach on MANET. In 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, pp. 797-802. https://doi.org/10.1109/ICESC48915.2020.9155770

[19] Manaa, M.E., Shamsi, S.D. (2018). Improved manet routing protocols performance using optimization methods, International Journal of Engineering & Technology, 7: 642-648. https://doi.org/10.14419/ijet.v7i4.19.27975

[20] Reddy, B., Dhananjaya, B. (2022). The AODV routing protocol with built-in security to counter blackhole attack in MANET. Materials Today: Proceedings, 50: 1152-1158. https://doi.org/10.1016/j.matpr.2021.08.039

[21] Gupta, P., Bansal, P. (2019). Packet drop analysis with variation in area and number of nodes in MANET. SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology, 11(1): 9-16.

https://doi.org/10.18090/samriddhi.v11i01.2

[22] Alattas, K.A. (2021). A novel method for avoiding congestion in a mobile ad hoc network for maintaining service quality in a network. International Journal of Computer Science & Network Security, 21(9): 132-140. https://doi.org/10.22937/IJCSNS.2021.21.9.18

[23] Moudni, H., Er-rouidi, M., Mouncif, H., El Hadadi, B. (2019). Black hole attack detection using fuzzy based intrusion detection systems in MANET. Procedia Computer Science, 151: 1176-1181. https://doi.org/10.1016/j.procs.2019.04.168

[24] Farahani, G. (2021). Black hole attack detection using K-nearest neighbor algorithm and reputation calculation in mobile ad hoc networks. Security and Communication Networks, 2021(1): 8814141. https://doi.org/10.1155/2021/8814141

[25] Varshney, I., Kumar, G.A. (2019). Study of mobile Ad-hoc network's challenges and characteristics. International Journal of Scientific Research in Science and Technology, 6(4): 2019. https://doi.org/10.32628/IJSRST196447

[26] Breen, W.A., Devi, S.D., Sushmitha, E., Suveetha, V. (2018). Reducing the effectiveness of gray-hole attack in manet. International Journal of Engineering Technology, 7: 305-308. https://doi.org/10.14419/ijet.v7i3.34.19213

[27] Gurung, S., Chauhan, S. (2018). A novel approach for mitigating gray hole attack in MANET. Wireless Networks, 24: 565-579. https://doi.org/10.1007/s11276-016-1353-5

[28] Kshirsagar, V.H., Kanthe, A.M., Simunic, D. (2018). Trust based detection and elimination of packet drop attack in the mobile ad-hoc networks. Wireless Personal Communications, 100: 311-320. https://doi.org/10.1007/s11277-017-5070-x

[29] Panda, N., Pattanayak, B.K. (2018). Defense against co-operative black-hole attack and gray-hole attack in MANET. International Journal of Engineering & Technology, 7(3.4): 84-89.

[30] Bhardwaj, S., Kumar, V. (2020). Secure co-operative neighbour-based approach for detection and prevention of black hole attack in wireless mobile ad-hoc networks. International Journal of Wireless and Mobile Computing, 19(1): 62-72. https://doi.org/10.1504/IJWMC.2020.109268

[31] Juneja, K. (2020). Random-session and K-neighbour based suspected node analysis approach for cooperative blackhole detection in MANET. Wireless Personal Communications, 110(1): 45-68. https://doi.org/10.1007/s11277-019-06711-5

[32] Terai, T., Yoshida, M., Ramonet, A.G., Noguchi, T. (2020). Blackhole attack cooperative prevention method in manets. In 2020 Eighth International Symposium on Computing and Networking Workshops (CANDARW), Naha, Japan, pp. 60-66. https://doi.org/10.1109/CANDARW51189.2020.00024

[33] Thanuja, R., Umamakeswari, A. (2019). Black hole detection using evolutionary algorithm for IDS/IPS in MANETs. Cluster Computing, 22(Suppl 2): 3131-3143. https://doi.org/10.1007/s10586-018-2006-5

[34] Thebiga, M., SujiPramila, R. (2020). A new mathematical and correlation coefficient based approach to recognize and to obstruct the black hole attacks in MANETs using DSR routing. Wireless Personal Communications, 114: 975-993. https://doi.org/10.1007/s11277-020-07403-1

[35] Elmahdi, E., Yoo, S.M., Sharshembiev, K. (2020). Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks. Journal of Information Security and Applications, 51: 102425. https://doi.org/10.1016/j.jisa.2019.102425

[36] Shukla, M., Joshi, B.K., Singh, U. (2021). Mitigate wormhole attack and blackhole attack using elliptic curve cryptography in MANET. Wireless Personal Communications, 121: 503-526. https://doi.org/10.1007/s11277-021-08647-1

[37] Aranganathan, A., Suriyakala, C.D., Vedanarayanan, V. (2021). Discovery and Deterrence of Black hole attack in clustering ad hoc networks based on software agents. In Soft Computing Techniques and Applications: Proceeding of the International Conference on Computing and Communication (IC3 2020), pp. 681-689. https://doi.org/10.1007/978-981-15-7394-1_62

[38] Sivanesh, S., Sarma Dhulipala, V.R. (2022). Analytical termination of malicious nodes (ATOM): an intrusion detection system for detecting black hole attack in mobile ad hoc networks. Wireless Personal Communications, 124: 1511-1524. https://doi.org/10.1007/s11277-021-09418-8

[39] Mekkaoui, K., Teggar, H. (2023). Mitigation of smart black hole attacks using universal sink detection method in graph theory. PREPRINT (Version 1), Research Square. https://doi.org/10.21203/rs.3.rs-2423431/v1

[40] Vatambeti, R. (2020). A novel wolf based trust accumulation approach for preventing the malicious activities in mobile ad hoc network. Wireless Personal Communications, 113(4): 2141-2166. https://doi.org/10.1007/s11277-020-07316-z

[41] Singh, A., Hasan, M. (2018). An improved mechanism to prevent blackhole attack in manet. In Progress in Advanced Computing and Intelligent Engineering: Proceedings of ICACIE 2016, 1: 511-520. https://doi.org/10.1007/978-981-10-6872-0_48

[42] Veeraiah, N., Krishna, B.T. (2019). Trust-aware FuzzyClus-Fuzzy NB: Intrusion detection scheme based on fuzzy clustering and Bayesian rule. Wireless Networks, 25: 4021-4035. https://doi.org/10.1007/s11276-018-01933-0

[43] Sefati, S., Abdi, M., Ghaffari, A. (2021). Cluster-based data transmission scheme in wireless sensor networks using black hole and ant colony algorithms. International Journal of Communication Systems, 34(9): e4768. https://doi.org/10.1002/dac.4768

[44] Talukdar, M.I., Hassan, R., Hossen, M.S., Ahmad, K., Qamar, F., Ahmed, A.S. (2021). Performance improvements of AODV by black hole attack detection using IDS and digital signature. Wireless Communications and Mobile Computing, 2021(1): 6693316. https://doi.org/10.1155/2021/6693316

[45] Mwangi, E.G., Muketha, G.M., Ndungu, G.K. (2019). A review of security techniques against black hole attacks in mobile ad hoc networks. In 2019 IST-Africa Week Conference (IST-Africa), Nairobi, Kenya, pp. 1-8. https://doi.org/10.23919/ISTAFRICA.2019.8764862

[46] Feng, F., Liu, X., Yong, B., Zhou, R., Zhou, Q. (2019). Anomaly detection in ad-hoc networks based on deep learning model: A plug and play device. Ad Hoc Networks, 84: 82-89.

https://doi.org/10.1016/j.adhoc.2018.09.014

[47] Gautam, D., Tokekar, V. (2020). A novel approach for detecting DDoS attack in MANET. Materials Today: Proceedings, 29: 674-677. https://doi.org/10.1016/j.matpr.2020.07.332

[48] Fahad, A.M., Ahmed, A.A., Alghushami, A.H., Alani, S. (2019). Detection of black hole attacks in mobile ad hoc networks via hsa-cbds method. In Intelligent Computing & Optimization, pp. 46-55. https://doi.org/10.1007/978-3-030-00979-3_5

[49] Vatambeti, R., Supriya, K.S., Sanshi, S. (2020). Identifying and detecting black hole and gray hole attack in MANET using gray wolf optimization. International Journal of Communication Systems, 33(18): e4610. https://doi.org/10.1002/dac.4610

[50] Yasin, A., Abu Zant, M. (2018). Detecting and isolating Black-Hole attacks in MANET using timer based baited technique. Wireless Communications and Mobile Computing, 2018(1): 9812135. https://doi.org/10.1155/2018/9812135

[51] Tyagi, P., Dembla, D. (2019). A secured routing algorithm against black hole attack for better intelligent transportation system in vehicular ad hoc network. International Journal of Information Technology, 11(4): 743-749. https://doi.org/10.1007/s41870-018-0160-x

[52] Kumar, A., Varadarajan, V., Kumar, A., Dadheech, P., Choudhary, S.S., Kumar, V.A., Veluvolu, K.C. (2021). Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm. Microprocessors and Microsystems, 80: 103352. https://doi.org/10.1016/j.micpro.2020.103352

[53] Vinayagam, J., Balaswamy, C.H., Soundararajan, K. (2019). Certain investigation on MANET security with routing and blackhole attacks detection. Procedia Computer Science, 165: 196-208. https://doi.org/10.1016/j.procs.2020.01.091

[54] Zhou, X., He, D., Khan, M.K., Wu, W., Choo, K.K.R. (2022). An efficient blockchain-based conditional privacy-preserving authentication protocol for vanets. IEEE Transactions on Vehicular Technology, 72(1): 81-92. https://doi.org/10.1109/TVT.2022.3204582

[55] Babaghayou, M., Chaib, N., Lagraa, N., Ferrag, M.A., Maglaras, L. (2023). A safety-aware location privacy-preserving IOV scheme with road congestion-estimation in mobile edge computing. Sensors, 23(1): 531. https://doi.org/10.3390/s23010531

[56] Sultan, M.T., Sayed, H.E., Khan, M.A. (2023). An intrusion detection mechanism for MANETs based on deep learning Artificial Neural Networks (ANNs). arXiv preprint arXiv:2303.08248. https://doi.org/10.48550/arXiv.2303.08248

[57] Sankar, S.M., Dhinakaran, D., Deboral, C.C., Ramakrishnan, M. (2023). Safe routing approach by identifying and subsequently eliminating the attacks in MANET. arXiv preprint arXiv:2304.10838. https://doi.org/10.48550/arXiv.2304.10838

[58] Cai, T., Jia, T., Adepu, S., Li, Y., Yang, Z. (2023). ADAM: An adaptive DDoS attack mitigation scheme in software-defined cyber-physical system. IEEE Transactions on Industrial Informatics, 19(6): 7802-7813. https://doi.org/10.1109/TII.2023.3240586

[59] Ahmed, W., Di, W., Mukathe, D. (2023). Blockchain-assisted privacy-preserving and context-aware trust management framework for secure communications in VANETs. Sensors, 23(12): 5766. https://doi.org/10.3390/s23125766

[60] Liang, Y., Liu, Y. (2022). Analysis and improvement of an efficient certificateless aggregate signature with conditional privacy preservation in VANETs. IEEE Systems Journal, 17(1): 664-672. https://doi.org/10.1109/JSYST.2022.3180221

[61] Yao, L., Zheng, Z., Wang, X., Zeng, Y., Wu, G. (2022). Detection of cache pollution attack based on ensemble learning in ICN-based VANET. IEEE Transactions on Dependable and Secure Computing, 20(4): 3287-3298. https://doi.org/10.1109/TDSC.2022.3196109

[62] Zhang, J., Chen, S., Chai, W.K., Hanzo, L. (2023). Adaptive coding and modulation aided mobile relaying for millimeter-wave flying ad-hoc networks. IEEE Internet of Things Journal, 11(2): 3282-3301. https://doi.org/10.1109/JIOT.2023.3296058

[63] Hammad, M., Jillani, R.M., Ullah, S., Namoun, A., Tufail, A., Kim, K.H., Shah, H. (2023). Security framework for network-based manufacturing systems with personalized customization: An industry 4.0 approach. Sensors, 23(17): 7555. https://doi.org/10.3390/s23177555

[64] Sharma, V., Beniwal, R., Kumar, V. (2024). Multi-level trust-based secure and optimal IoT-WSN routing for environmental monitoring applications. The Journal of Supercomputing, 80: 11338-11381. https://doi.org/10.1007/s11227-023-05875-z

[65] Srilakshmi, U., Alghamdi, S.A., Vuyyuru, V.A., Veeraiah, N., Alotaibi, Y. (2022). A secure optimization routing algorithm for mobile ad hoc networks. IEEE Access, 10: 14260-14269. https://doi.org/10.1109/ACCESS.2022.3144679

[66] Karthik, M.G., Krishnan, M.M. (2021). Hybrid random forest and synthetic minority over sampling technique for detecting internet of things attacks. Journal of Ambient Intelligence and Humanized Computing, 1-11. https://doi.org/10.1007/s12652-021-03082-3

[67] Ilakkiya, N., Rajaram, A. (2024). Blockchain-enabled lightweight intrusion detection system for secure MANETs. Journal of Electrical Engineering & Technology, 19(4): 2667-2681. https://doi.org/10.1007/s42835-023-01749-9

[68] Alyoubi, A.A. (2024). Enhancing data security in mobile ad-hoc network (MANETs) using trust-based approach with RSSI and fuzzy logic. Mobile Networks and Applications, 1-17. https://doi.org/10.1007/s11036-024-02336-6

[69] Wang, X., Zhang, P., Du, Y., Qi, M. (2020). Trust routing protocol based on cloud-based fuzzy petri net and trust entropy for mobile ad hoc network. IEEE Access, 8: 47675-47693. https://doi.org/10.1109/ACCESS.2020.2978143

[70] Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., Nemoto, Y. (2007). Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method. International Journal of Network Security, 5(3): 338-346.

[71] Marti, S., Giuli, T.J., Lai, K., Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, Boston Massachusetts, USA, pp. 255-265. https://doi.org/10.1145/345910.34595

[72] Balakrishnan, K., Deng, J., Varshney, V.K. (2005). TWOACK: preventing selfishness in mobile ad hoc networks. In IEEE Wireless Communications and Networking Conference, New Orleans, LA, USA, pp. 2137-2142. https://doi.org/10.1109/WCNC.2005.1424848

[73] Liu, K., Deng, J., Varshney, P.K., Balakrishnan, K. (2007). An acknowledgment-based approach for the detection of routing misbehavior in MANETs. IEEE Transactions on Mobile Computing, 6(5): 536-550. https://doi.org/10.1109/TMC.2007.1036

[74] Peng, G., Chuanyun, Z. (2006). Routing attacks and solutions in mobile ad hoc networks. In 2006 International Conference on Communication Technology, Guilin, China, pp. 1-4. https://doi.org/10.1109/ICCT.2006.341678

[75] Yu, C.W., Wu, T.K., Cheng, R.H., Chang, S.C. (2007). A distributed and cooperative black hole node detection and elimination mechanism for ad hoc networks. In Emerging Technologies in Knowledge Discovery and Data Mining: PAKDD 2007 International Workshops, pp. 538-549. https://doi.org/10.1007/978-3-540-77018-3_54

[76] Ramaswamy, S., Fu, H., Sreekantaradhya, M., Dixon, J., Nygard, K.E. (2003). Prevention of cooperative black hole attack in wireless ad hoc networks. In International Conference on Wireless Networks, 2003: 570-575.

[77] Deng, H., Li, W., Agrawal, D.P. (2002). Routing security in wireless ad hoc networks. IEEE Communications Magazine, 40(10): 70-75. https://doi.org/10.1109/MCOM.2002.1039859

[78] Khalaf, O.I., Ajesh, F., Hamad, A.A., Nguyen, G.N., Le, D.N. (2020). Efficient dual-cooperative bait detection scheme for collaborative attackers on mobile ad-hoc networks. IEEE Access, 8: 227962-227969. https://doi.org/10.1109/ACCESS.2020.3045004

[79] Pu, C., Lim, S., Chae, J., Jung, B. (2019). Active detection in mitigating routing misbehavior for MANETs. Wireless Networks, 25: 1669-1683. https://doi.org/10.1007/s11276-017-1621-z

[80] Tamilselvan, L., Sankaranarayanan, V. (2008). Prevention of Wormhole Attack in MANET. https://www.iiis.org/cds2008/cd2008sci/sci2008/papers pdf/s129dt.pdf.