Frontiers in Computer Science and Artificial Intelligence
ISSN: 2978-8048
DOI: 10.32996/fcsai
Journal Homepage: www.al-kindipublisher.com/index.php/fcsai

FCSAI
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

A Sequence-Connection Oriented Scheme for Detecting Gray/Black Hole Attacks in Mobile Ad-Hoc Networks

Baban Mahmood
Baban Mahmood, Information Technology department, Unviersity of Kirkuk, Kirkuk, Iraq
Corresponding Author: Baban Mahmood, **E-mail**: Baban.mahmoodjaf@gmail.com

| ABSTRACT

Security of routing protocols for Mobile Ad Hoc Networks (MANETs) have been studied extensively. Malicious nodes habitually intervene the process of route establishment and make it complicated to build a reasonable route. In the literature, various mechanisms presented which claim to build secure routes are prone to gray and black hole attacks. In this paper, a novel method is proposed that efficiently detects gray hole attack in addition to detecting black hole attacks. The proposed technique uses two modes, connection oriented and connection-less oriented mode depending on a sequence number sent in the route request packets. A deep and extensive analysis is performed to prove the efficiency of the proposed method as well as show how it prevents malicious nodes from deteriorating the packet forwarding process. The analysis encompasses both presenting the attacks on routing protocols and proofs of how this suggested protocol detects and prevents these attacks. According to the theoretical analysis, the proposed method is expected to maintain great ratio of packet delivery even under gray/black hole attack conditions. This expectation is based on the rigorous prevention of the attacks which leads to build more successful routes.

| KEYWORDS

MANETs; Gray Hole Attack; Blackhole Attack; Security of Routing in MANETs; DoS;

| ARTICLE INFORMATION

ACCEPTED: 01 May 2026 **PUBLISHED:** 29 June 2026 **DOI:** 10.32996/fcsai.2026.5.9.6

1. Introduction

A Mobile Ad hoc Network (MANET) is composed of a number of nodes which are able to operate both as host and router. It is a wireless, decentralized that is formed dynamically by multiple mobile nodes as a self-configured network without using any infrastructure or centralized administration. This means no centralized administration is utilized (e.g. Access Points or Base Stations) [1], [2]. The nodes, besides, cooperatively forward packets on behalf of each other through the communication links [3]– [5]. Different scenarios, wherein building infrastructure is not feasible or somewhat impossible, require applying MANET. Some of these uncontrolled areas include rescue operations in case of disaster, military urgent cases, animal habitats, etc. [6]– [9]. In addition to that, there are various applications which can be supported by using MANETs, examples include vehicular networks, sensors, cyber physical systems, and Internet of Things (IoT) [10]

The functions of routing are categorized into two primary phases: route establishment and packet forwarding. The former is tasked with identifying a route between the source and destination nodes, while the latter is responsible for transmitting data along the route that was built during route establishment. In secure routing protocols, participating nodes are capable of exchanging both data and control information even when malicious entities exist who try to deteriorate the routing protocol's functionality [11].

The primary features of MANET, such as its ever-changing topology, open communication medium, and the decentralized operation of its nodes, make it highly susceptible to threats. Additionally, routing plays a crucial role in the security of the network, this is due to the fact that malignant nodes might falsely assert that they possess legitimate paths to target nodes. A black hole attack is a potential threat to routing, which can significantly disrupt the data forwarding process [12], [13].

The two primary kinds of attacks are active and passive [14]. In passive attacks, malicious nodes do not interfere with routing operation; however, in active attacks, these malignant nodes obstruct the normal functioning of network operations and perpetrate violations. Such disruptions and violations can happen at various layers, including route establishment and/or packet forwarding stages. [7], [15]

An adversary might compromise the functionality of the network by presenting a route that appears to have less nodes than the one offered by a legitimate node [4], [16]. This form of attack is executed by altering certain routing metrics. Another attack category is Impersonation in which malignant nodes adopt the identities of other nodes to launch attacks [17], [18].

Various security mechanisms have been developed to counteract malicious nodes [19]:

- Preventive Mechanism It functions as a defensive strategy by implementing encryption and authentication protocols. These protocols employ both symmetric and asymmetric cryptographic techniques.
  searcher introduces a network-level DNS Sinkholing algorithm that can block access to a domain that is either server ads, web trackers, or websites that may contain malicious content.

- Reactive Mechanism This mechanism is designed to detect misuse and anomalies. In the context of anomaly detection, The typical behavior of participating nodes is determined by gathering pertinent information from the behavior of authentic nodes. Subsequently, anomalous behaviors of nodes are identified through the analysis of the computed statistical tests.

In a network experiencing a Gray Hole attack, packets are initially sent to the target node as if everything is functioning normally during the discovery phase. However, once the network starts to malfunction, these packets are discarded. Initially, gray nodes do not pose a threat because they behave like regular nodes during path discovery. In the context of MANETs, identifying Gray Hole nodes can be challenging, as they fail to provide the correct sequence number during route selection [20].

1.1 Objectives

Protocols, some of them, presented in the literature are prone to gray hole attacks wherein selectively packets are dropped. In this paper, we propose a secure routing protocol using a sequence-connection oriented technique to find and prevent malicious nodes from disrupting the process of normal data forwarding and route discovery. Hence, the main contribution is to design a routing protocol which prevents Gray/Black hole attacks as well as detects attacks on the protocols described in the related work.

1.2 Paper Organization

The rest of the paper is organized as follows: In Section 2, we overview protocols presented in the literature. In Section 3, the proposed protocol design is presented in detail. Section 4 shows the limitations of protocols summarized in Section 2 as well as shows how the proposed protocol detects and prevents these attacks. Section 5 concludes the paper.

2. Related Work

This section presents the recent work related to this proposed idea. Numerous algorithms have been suggested in the past to protect MANET from gray hole attacks. Some of these methods focus on securing routing packets through encryption techniques. While these approaches offer strong resistance to gray hole attacks, they impose a high computational burden on MANET nodes, which is not compatible with MANET's characteristics. Furthermore, majority of these methods are specifically designed to identify and counteract attacks within ad hoc on demand distance vector (AODV) [21] protocol. This section outlines some of the current algorithms aimed at preventing gray/black hole attacks.

Trust management was presented by the authors in [1] as a promising idea that could solve a number of MANET-related issues. Then, in order to detect and isolate flooding assaults and improve network performance during them, a direct trust management strategy was put forth. The suggested technique has some overhead even if it greatly improves MANET speed.

The authors in [3] propose a robust hybrid detection method that significantly enhances the detection and mitigation of black hole and gray hole attacks. Their approach combines cryptographic verification, advanced data mining techniques, and anomaly detection to produce a multi-layered security solution. The suggested hybrid detection approach employs a methodical procedure that starts with anomaly detection to find anomalies, followed by data mining tools to examine and categorize nodes, and cryptographic verification to isolate and authenticate malicious entities. This systematic process ensures complete protection

against black hole and gray hole attacks, enhancing the overall security and reliability of MANETs regardless of the on-demand protocols used.

The authors in [20] described a method for detecting dangerous Black holes and Gray holes using the nodes for intrusion detection in conjunction with the linked dominant set (CDS) methodology. The suggested technique works well for identifying hostile nodes in dense networks, especially those that employ cunning Gray Hole assaults. Neural networks Employed to identify attacks more effectively than traditional approaches, which improve throughput.

In the concept in [22], identifying black hole and gray hole attacks in MANETs is the main goal. A method was put forth to make it easier to identify black hole and gray hole attacks in order to achieve this. By defining the intrusion detection system (IDS) node as the node that sends a query, the technique used a linked dominating set (CDS) methodology to find malicious nodes. To confirm each node in the network, the node sends out a brief status packet with four queries on a regular basis. When legitimate nodes receive status packet, they respond authentically, without fabricated or falsified information, whereas malicious nodes provide deceptive information to evade detection by security mechanisms. Additionally, malicious nodes send false information to disrupt data packet transmission from the source node. The detection of malicious nodes is facilitated by their failure to satisfy the predefined questions in the status packets.

To enhance the DSR routing protocol, Cai and Yi et al. [23] established a Route Confirmation Request (RCONR) and a Route Confirmation Answer (RCONA) method. This approach requires an intermediate node to transmit an RCONR to its following node in addition to the Route Reply (RREP) delivered to the source node. The next-hop node looks for a route to the destination in its cache after getting an RCONR. It provides the source node with an RCONA if a route is available. The correctness of the path can then be confirmed by the source node by comparing the routes shown in the RCONA and the RREP. The source node accepts the path as legitimate if the two routes match. However, because the first node asks its next-hop node to send an RCONA to the source, this approach is vulnerable to cooperative gray hole attacks, which cannot be prevented if two subsequent nodes collude.

A technique for Secure Detection, Prevention, and Elimination of Gray Hole (SDPEGH) attacks was suggested by Radha and Rao [24]. They looked at the NS2 tool's simulation of destination-sequenced distance-vector routing (DSDV). The metrics that were used were throughput, energy expenditure, and packet delivery ratio. The malicious nodes are identified, avoided, and eliminated by the suggested SDPEGH technology. After then, it provides the new source routing table's shortest path. In order for the packet to be sent to the node same as the subsequent hop, the source still selects the malicious node. The gray hole attack was successfully identified and stopped using this technique.

3. Background and Attacks in MANET

Due to its characteristics—such as limited resources, inadequate physical protection, dynamic typology, and a lack of infrastructure—MANETs are vulnerable to security breaches. Due to its wireless nature, MANET security vulnerabilities are more serious [25]. Since every MANET communication layer has unique weaknesses, attacks can also be categorized based on the layer in which they occur [26]. This Section provides the background needed to get acquainted with reactive routing protocols like AODV and different related attacks on the routing process.

3.1 Ad Hoc On-Demand Distance Vector (AODV)

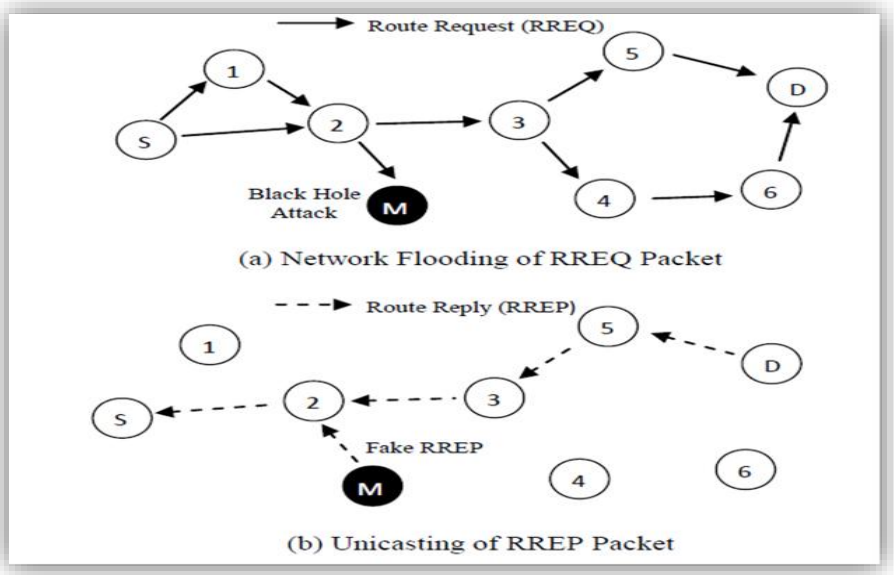
A reactive routing protocol called AODV [21] determines the path between a source and a destination when it is required. A table of routes to known nodes is kept up to date by every node in the network. Route discovery and route maintenance are the two stages that AODV uses to manage this process. The process of finding a legitimate path between a source and destination pair is known as route discovery. [27]. The AODV routing discovery operates as explained below:

1) A source node first looks through its routing table before sending data to a destination node. Data transmission continues if a valid route is discovered; if not, the source node sends out an RREQ packet. The source IP, destination IP, source sequence number, destination sequence number, and broadcast ID number are all included in this packet.
2) A node examines its own cached routing table upon receiving an RREQ packet. It transmits an RREP packet to the source if it has a legitimate path to the destination. Destination IP, destination sequence number, hop count, lifetime, and source IP are all included in the RREP. If the node does not have a valid route to the destination, it spreads out the RREQ packet.
3) The node of origin, source, starts transferring data packets once it has received a RREP packet.

When nodes leave the network or move out of range, the related routes become invalid. In such cases, route maintenance is used to establish new routes and refresh the available routing tables as presented below:

1) To inform the node of origin, source, that the route is not anymore viable, an RRER is sent by the upstream node. The source IP, destination sequence number, and unreachable destination IP are all included in an RRER packet.
2) The path is marked as invalid by every intermediary node.
3) The source initiates a fresh route discovery procedure upon receiving an RERR packet.

Fig. 1. Black hole attack [4].



3.2 Denial of Service Attacks (DoS)

Any incident that reduces or stops a network's ability to carry out its intended function is considered a denial-ofservice attack. By restricting authorized users from accessing resources, the goal is to reduce network capacity and deprive nodes' communication of the resources of the network resources by discarding data packets [28].

3.3 Black Hole Attacks

Route request (RREQ) signals from neighboring nodes are purposefully answered by a malicious node in a black hole attack, a form of denial of service (DoS) attack. The attacker pretends to have a valid shortest path to the intended location. Consequently, all data packets directed towards the target are absorbed and discarded. Identifying black hole nodes with a higher sequence number is particularly challenging, especially when the network's sequence number closely resembles that of the attacker. [12], [29], [30]. The behavior of a black hole attack is depicted in Figure 1, where the source node S must create a route to the destination D to transmit packets of data to it. The AODV [21] routing protocol, which is covered later in IV-A, bombards the whole network with an RREQ control packet in order to find a route to node D. Both benign and black hole nodes receive the request during regular AODV operation.

Nevertheless, a replay with a high sequence number is received by the source node because the black hole node (B) responds with false information. Additionally, the source receives back route reply (RREP) packets from the destination and other nodes (such as 2 and 4) that have valid routes to the destination. These packets contain the destination's real sequence numbers, which are typically less than the sequence number supplied by the black hole node. In order to create a path to the destination node D, the source node S selects the route reply that the black hole node (B) sent. The black hole node stops all packets from being sent to the destination node after controlling the routing process [4].

3.4 Gray Hole Attacks

A well known type of DoS attack is a gray hole assault. In this kind of attack, the adversarial node successfully constructs the path to the target, but not every data packet is sent via the gray hole node.

A black hole attack is not the same as a gray hole attack. A malicious node selectively drops packets in a gray hole assault/attack [31]. A malignant node uses the route discovery process to pose as a trustworthy node before starting to discard packets. First and foremost, a gray hole may decide to forward all packets to certain nodes while rejecting those that are scheduled for or coming from particular nodes. In addition, a gray hole may exhibit wicked behavior for a while before functioning normally like other nodes. Furthermore, a gray hole node has the ability to temporarily stop receiving packets from specified nodes before returning to regular operation. Because of this uncertainty, it is somewhat difficult to identify these kinds of attacks [32].

Because Dynamic Source Routing (DSR) lacks a security mechanism, gray hole attacks that employ DSR in MANET selectively delete data packets. Therefore, by just not adhering to DSR rules appropriately, hostile nodes can execute a gray hole attack.

Furthermore, the malicious nodes have the ability to drop any UDP transmission. Additionally, the attacker can employ a statistical technique, such dropping only 50% of the packets, which can seriously destabilize the network.

4. Proposed Protocol Design

Our protocol securely establishes a route between a source and a destination node as well as detects black/gray hole attacks/assaults on routing protocols of MANETs. Any on demand routing protocol like AODV that creates routes before data transmission process can use this approach. In this study, we demonstrate the workflow of our suggested protocol using the AODV ideas. The aforementioned points are explained in the ensuing subsections.

4.1 Basic Route Discovery

In on-demand routing protocols, a route to the destination is established when a source node, denoted as S, requires the transmission of data packets to a destination, referred to as D. Specifically, within the Ad hoc On-Demand Distance Vector (AODV) protocol, A node sends out a route request to all of its nearby nodes when it needs to establish a path to a destination. If an intermediate node has a new route to the destination, it responds to the source node; if not, it broadcasts the route request to all of its neighbors. Until a path to the target is discovered, this procedure keeps going.

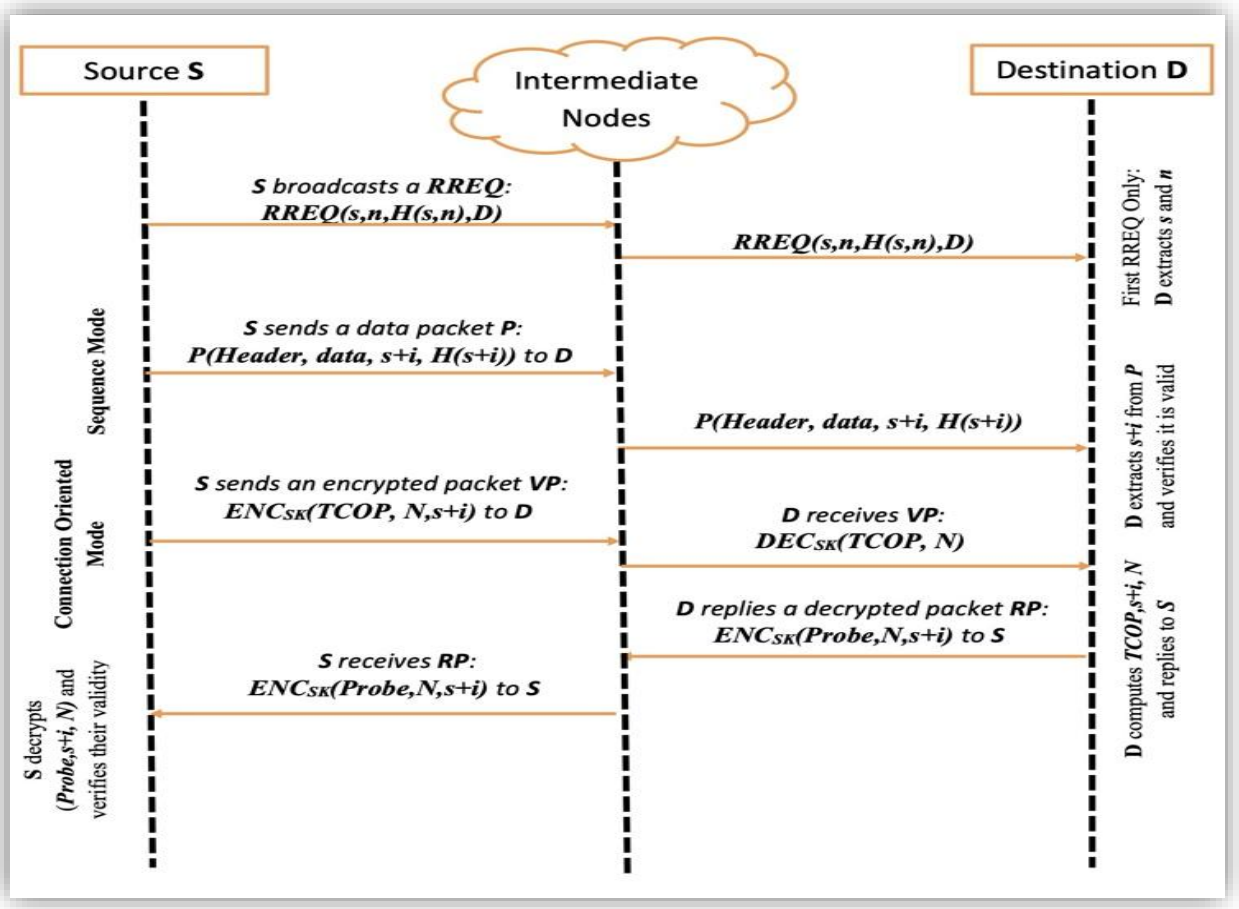
4.2 Gray Hole Detection

We assume both S and D have a shared symmetric key (SK) and there are multiple paths between them. A malicious node may allow a route to be established, but it can drop all or part of the data packets intended to a destination D. To detect such behaviors, we propose an algorithm that operates in the following two modes.

- ***Sequence Mode*** After the route is discovered, data packets are sent. In the first mode, a sequence number is added to data packets. The sequence number starts with s which is incremented by one for each consecutive packet. This allows the destination to predict a packet with a predefined sequence number to arrive at D. The source sends both s and the total number of packets n along with the RREQ to the destination. The source uses one way hash function for these two numbers, H(s,n), and puts them in the RREQ. When D receive the RREQ, it extracts both n and s and it knows that the first data packet has a sequence number of s, the ith packet's sequence number is s + i, and the last sequence number is s + n.
- ***Connection Oriented Mode*** The second mode is temporary connection oriented communications between source and destination nodes. In this mode, the destination sends an acknowledgment to the source on some of the data packets. As an illusion to the malicious node, a random number of packets are selected as the oriented communication:
  - *Verification Packet* Let r be a random number in a predefined range [x,y]; after sending each r data packets, an extra encrypted Verification Packet (VP) is sent to D. VP consists of a temporary connection oriented packet (TCOP) and a Nonce N. TCOP asks the destination to send a reply back to the source node via the reverse path when VP is received by D. When D receives the VP, it decrypts the VP and knows that it needs to reply, hence it encrypts a response packet (RP) and sends it back to the source. Each data packet has a sequence number; the sequence number starts with s which is incremented by one for each consecutive packet.
    Each VP is also assigned a sequence number equal to the sequence number of the last data packet sent by the source node before sending a VP. This technique allows the destination to predict a packet with a predefined sequence number to arrive at D. For example, if the last packet that D has received has a sequence number j, the next expected sequence number is j + 1, but if D receives a sequence number k greater than j + 1, it means that m (i.e., k − (j + 1)) packet(s) have been dropped. This gives a prediction to D that there may be a malicious node in the route. In this case, either there is a gray hole node in the path or a packet normally dropped due to any network related problem(e.g., congestion and/or overflow).
  - *Detection Packet* If m, the number of packets dropped, is less than a predefined threshold th, it is expected to be normal packet dropping. However, if it is greater the th, then D considers it as a gray hole problem and broadcasts an encrypted notification packet to S asking it to switch to a gray hole detection mode.
  - *Gray Hole Detection Mode* The source node S temporarily stops sending regular packets and sends v consecutive VPs to D. If D receives all the packets and replies to all, then S resumes it normal packet forwarding mode. If number of VPs arrived at D is less than a VP threshold vpth, then that path is considered unsecured and a gray hole attack is available. Therefor, the source initiates a diagnoses process to find out which node caused the problem.

After the two modes explained above are implemented successfully, the proposed algorithm detects and prevents gray hole attack from deteriorating the normal flow of data packets. The description of the proposed method is depicted in Figure 2.

Fig. 2. Formal description of the proposed method, route discovery



5. Évaluation and discussion of the attacks found using the suggested approach

This section presents a security analysis, demonstrating the susceptibility of certain related studies to gray/black hole attacks. A detailed examination is provided on how our method effectively discovers and mitigates attacks by adversarial nodes across the protocols identified in the literature. Additionally, the impact of these attacks on routing is thoroughly discussed.

The authors in [22] introduced a technique for the continuous observation of neighboring nodes' behavior to identify malicious actions. Although this watchdog mechanism is effective in some situations, It is vulnerable to collusion attempts and may generate false positives in dynamic network situations.

The authors of [33] created a sophisticated anomaly detection framework that uses machine learning methods for pattern identification in addition to statistical modeling of typical network behavior. Although this approach offers greater flexibility in response to evolving network circumstances, it necessitates meticulous adjustment to minimize false alarms.

The hybrid detection method proposed in [3] operates in a sequential manner, starting with anomaly detection to spot irregularities, followed by data mining techniques to analyze and classify nodes, and concluding with cryptographic verification to authenticate and isolate malicious entities. This step-by-step approach ensures thorough protection against black hole and gray hole attacks, thereby enhancing the overall security and reliability of MANETs.

The verification process described in [23] is not encrypted. Additionally, the node's promiscuous mode allows the black/malicious node to forward the hello packet to the target node and then impersonate it. Consequently, all the forwarded packets are dropped due to the originating node's perception that this path is valid. It is important to note, nevertheless, that our suggested approach does not send the verification packet in plain text. Since the malicious node is unaware that the packet is for verification, it may discard it, signaling that the route cannot be confirmed and so detecting the attack. This stops the black or malicious node from mimicking the destination.

The algorithm in reference [34] causes a significant latency since nodes have to wait till numerous RREPs are formed. As a result of the delay, stale routes may be constructed

In order to solve flooding issues, the approach in [24] ensures that resources are allocated fairly among all contending neighbors. These RREQs are processed only when the number of RREQs from the neighbor in issue is less than the RREQ Accept

Limit, which is a threshold that ensures neighbors consistently use a node's resources. To ascertain if a node is functioning maliciously or not, the method additionally establishes a threshold known as the RREQ Black-List Limit. Consequently, the node is blacklisted and all of its requests are momentarily stopped as the quantity of RREQs exceeds the limit of the RREQ's Black-List.

A malicious assault causes AODV to drop more packets as the frequency of attacks rises. In comparison to the standard AODV, it is discovered that the suggested AODV protocol has reduced routing overhead but performs worse when additional malicious nodes are added. Due to a lack of capacity, this technique may result in the blocking of valid nodes. It can even handle malicious nodes that cooperate. This study combined several methods to get rid of coordinated attacks. On the other hand, the proposed method detects such malicious nodes and prevents them from deteriorating the network functioning at a lower cost compared to the method in [24].

6. Conclusion

We developed a new and safe technique in this research that detects and blocks gray/black hole attacks on MANETs. The sequence number that is sent with the route request packet is what this suggested protocol relies on. Sequence mode and connection-oriented mode are separated by the sequence number. Because of its generality, the suggested security plan can be used with any on-demand routing protocol. The latest attacks on routing protocols are thoroughly examined and discussed. The results of the detection investigation demonstrated that our suggested approach both detects and prevents these attacks from interfering with the process of data forwarding and route building. As a result, this suggested method stops the majority of hostile nodes' attempts at gray/black hole attacks.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest
ORCID iD https://orcid.org/my-orcid?orcid=0000-0002-3787-265X
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] A. Alzahrani and N. Thomas, "Analysing the performance of a trustbased aodv in the presence of a flooding attack," Applied Sciences, vol. 14, no. 7, p. 2874, 2024.
[2] N. Naveen and J. Nirmaladevi, "Secure bio-inspired optimization with intrusion aware on-demand routing in manets," Scientific Reports, vol. 15, 07 2025.
[3] M. Yazdanypoor, S. Cirillo, and G. Solimando, "Developing a hybrid detection approach to mitigating black hole and gray hole attacks in mobile ad hoc networks," Applied Sciences, vol. 14, no. 17, p. 7982, 2024.
[4] H. Moudni, M. Er-Rouidi, H. Mouncif, and B. El Hadadi, "Fuzzy logic based intrusion detection system against black hole attack in mobile ad hoc networks," International Journal of Communication Networks and Information Security, vol. 10, no. 2, pp. 366–373, 2018.
[5] M. Aamir and M. A. Zaidi, "A buffer management scheme for packet queues in manet," Tsinghua Science and Technology, vol. 18, no. 6, pp. 543–553, 2013.
[6] S. Jain, A. Shastri, and B. K. Chaurasia, "Analysis and feasibility of reactive routing protocols with malicious nodes in manets," in Proceedings of International Conference on Communication Systems and Network Technologies (CSNT), April 2013.
[7] G. Liu, H. Dong, Z. Yan, X. Zhou, and S. Shimizu, "B4sdc: A blockchain system for security data collection in manets," IEEE Transactions on Big Data, pp. 1–1, 2020.
[8] V. N. Talooki, H. Marques, and J. Rodriguez, "Energy efficient dynamic manet on-demand (e2dymo) routing protocol," in Proceedings of International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), June 2013.
[9] H. Shen and L. Zhao, "Alert: An anonymous location-based efficient routing protocol in manets," IEEE Transactions on Mobile Computing, vol. 12, no. 6, pp. 1079–1093, June 2013.
[10] Y. Ju, M. Yang, C. Chakraborty, L. Liu, Q. Pei, M. Xiao, and K. Yu, "Reliability–security tradeoff analysis in mmwave ad hoc–based cps," ACM Trans. Sen. Netw., vol. 20, no. 2, Jan. 2024. [Online]. Available: https://doi.org/10.1145/3582556
[11] M. M. Rashid, M. Isawi, and B. A. Mahmood, "An extensive analysis of the ad hoc network," in Proceedings of the 6th International Conference on Engineering & MIS 2020, 2020, pp. 1–9.
[12] H. Kalkha, H. Satori, and K. Satori, "Preventing black hole attack in wireless sensor network using hmm," Procedia computer science, vol. 148, pp. 552–561, 2019.
[13] B. A. Mahmood, A. A. Majeed, and A. C. Shakir, "An end to end key establishment scheme for detecting black hole attacks in mobile ad hoc networks," Indonesian Journal of Electrical Engineering and Computer Science, vol. 21, no. 2, pp. 1193–1200, 2021.
[14] A. K. Abdelaziz, M. Nafaa, and G. Salim, "Survey of routing attacks and countermeasures in mobile ad hoc networks," in Proceedings of IEEE International Conference on Computer Modelling and Simulation (UKSim), April 2013.

[15] R. Skaggs-Schellenberg, N. Wang, and D. Wright, "Performance evaluation and analysis of proactive and reactive manet protocols at varied speeds," in 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Jan 2020, pp. 0981–0985.
[16] Vaithiyanathan, G. S. R., E. E. N., and S. Radha, "A novel method for detection and elimination of modification attack and ttl attack in ntp based routing algorithm," in Proceedings of International Conference on Recent Trends in Information, Telecommunication and Computing (ITC), March 2010.
[17] N. W. Lo, M. C. Chiang, and C. Y. Hsu, "Hash-based anonymous secure routing protocol in mobile ad hoc networks," in Proceedings of Asia Joint Conference on Information Security (AsiaJCIS), May 2015.
[18] I. Woungang, S. K. Dhurandher, M. S. Obaidat, and R. D. Peddi, "A dsr-based routing protocol for mitigating blackhole attacks on mobile ad hoc networks," Security and Communication Networks, vol. 9, no. 5, pp. 420–428, 2016.
[19] P. Joshi, "Security isues in routing protocols in manet at network layer," Procedia Computer Science, vol. 3, pp. 954–960, 2011.
[20] S. Younas, F. Rehman, T. Maqsood, S. Mustafa, A. Akhunzada, and A. Gani, "Collaborative detection of black hole and gray hole attacks for secure data communication in vanets," Applied Sciences, vol. 12, no. 23, p. 12448, 2022.
[21] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in Proceedings of Second IEEE Workshop on Mobile Computing Systems and Applications, WMCSA, Feb 1999.
[22] Z. Ali Zardari, J. He, N. Zhu, K. H. Mohammadani, M. S. Pathan, M. I. Hussain, and M. Q. Memon, "A dual attack detection technique to identify black and gray hole attacks using an intrusion detection system and a connected dominating set in manets," Future Internet, vol. 11, no. 3, 2019. [Online]. Available: https://www.mdpi.com/19995903/11/3/61
[23] J. Cai, P. Yi, J. Chen, Z. Wang, and N. Liu, "An adaptive approach to detecting black and gray hole attacks in ad hoc network," in 2010 24th IEEE international conference on advanced information networking and applications. IEEE, 2010, pp. 775–780.
[24] M. Radha and M. N. Rao, "Gray hole attack detection prevention and elimination using sdpegh in manet," International Journal of Engineering and Advanced Technology (IJEAT), vol. 8, no. 3, 2019.
[25] A.-S. K. Pathan, Security of self-organizing networks: MANET, WSN, WMN, VANET. CRC press, 2016.
[26] K. Pavani and D. Avula, "Performance evaluation of mobile adhoc network under black hole attack," in International Conference on Software Engineering and Mobile Application Modelling and Development (ICSEMA 2012). IET, 2012, pp. 1–6.
[27] S. Misra and S. Goswami, "Network routing: fundamentals, applications, and emerging technologies," 2017.
[28] Z. Ali Zardari, J. He, N. Zhu, K. H. Mohammadani, M. S. Pathan, M. I. Hussain, and M. Q. Memon, "A dual attack detection technique to identify black and gray hole attacks using an intrusion detection system and a connected dominating set in manets," Future Internet, vol. 11, no. 3, p. 61, 2019.
[29] N. Sharma and A. Sharma, "The black-hole node attack in manet," in 2012 second international conference on Advanced Computing & Communication Technologies. IEEE, 2012, pp. 546–550.
[30] B. Mahmood, A. Ibrahim, and D. Manivannan, "Sariadne: A secure source routing protocol to prevent hidden-channel attacks," in Proceedings of 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, 2016, 2016.
[31] M. C. K. Reddy and B. Sripriya, "A study on gray-hole attacks in mobile ad-hoc networks," 2017.
[32] S. Jain and A. Khuteta, "Detecting and overcoming blackhole attack in mobile adhoc network," in 2015 International Conference on Green Computing and Internet of Things (ICGCIoT). IEEE, 2015, pp. 225– 229.
[33] D. Chou and M. Jiang, "A survey on data-driven network intrusion detection," ACM Comput. Surv., vol. 54, no. 9, Oct. 2021. [Online]. Available: https://doi.org/10.1145/3472753
[34] M. Mohanapriya and I. Krishnamurthi, "Modified dsr protocol for detection and removal of selective black hole attack in manet," Computers & Electrical Engineering, vol. 40, no. 2, pp. 530–538, 2014.