DOI: https://doi.org/10.52756/10.52756/ijerr.2023.v31spl.016 ***Int. J. Exp. Res. Rev.*, Special Vol. 31: 168-185 (2023)**

Original Article | *Peer Reviewed* | *Open Access*

International Journal of Experimental Research and Review (IJERR)

ISSN: 2455-4855 (Online)
www.iaph.in
ISSN 2455-4855

A comparative study of different security issues in MANET

Ankita Kumari[1*], Sandip Dutta[1] and Soubhik Chakraborty[2]

[1]Department of Computer Science and Engineering, Birla Institute of Technology, Mesra, Jharkhand, India;
[2]Department of Mathematics, Birla Institute of Technology, Mesra, Jharkhand, India

E-mail/Orcid Id:

AK, ankitakmr33@gmail.com, https://orcid.org/0000-0002-0338-915X; *SD,* sandipdutta@bitmesra.ac.in, https://orcid.org/0000-0002-3932-3048; *SC,* soubhikc@yahoo.co.in

Article History:
Received: 09th Apr., 2023
Accepted: 30th Jun., 2023
Published: 30thJul., 2023

Keywords:
Black hole attack, Sink hole attack, Worm hole attack, Malicious, RREP

Abstract: In a MANET (Mobile Ad-Hoc Network), an intruder can attempt to gain unlawful access to the network to obtain sensitive information. These attacks can occur at various network layers, and different attacks can be carried out. To mitigate the risks of such attacks, several solutions have been proposed. It can be characterized by dynamic topology, meaning that the network is formed by a group of nodes communicating wirelessly and without centralized control. This feature makes MANETs highly vulnerable to attacks, especially when malicious nodes are introduced into the network. These malicious nodes can engage in malicious activity that severely damages the network's performance and credibility. Among the major attacks that can be carried out in a MANET are Sinkhole attacks, Black hole attacks, and Wormhole attacks. Sinkhole attack, a malicious node intercepts a data packet, alters its contents, and then forwards it to its neighbors. This can cause other nodes to send their data packet to the malicious nodes, compromising the safety and privacy of the network. In a BHA, malicious nodes drop the data packet it receives, preventing them from accomplishing their intended destinations. This can result in a DoS attack, where legitimate users cannot access the network. A WHA involves two malicious nodes colluding to drop data packets from the network. They create a virtual tunnel between them, and any data that passes through this tunnel is dropped, making it impossible for legitimate nodes to communicate with each other. All these attacks can cause significant damage to the network, and researchers have proposed various solutions to protect the network from them. These solutions include using IDS, deploying secure routing protocols, and developing secure algorithms for data transmission. By implementing these solutions, it is possible to improve the Safety and trustworthiness of the MANET and prevent malicious nodes from causing harm to the network.

Introduction

MANET is a self-organizing wireless network that allows mobile devices to connect without relying on a fixed infrastructure or central control (Sharma et al., 2013). In MANETs, the node is allowed to move around independently, and then each node can turn both as a host and as a router, forwarding data to another node in the networks. MANETs are commonly used when it is not feasible to establish a fixed infrastructure, such as in military operations, disaster relief efforts, and remote locations. They are also used in public transportation systems, conferences, and other situations where temporary communication networks are required. One of the main advantages of MANETs is their flexibility and resilience. Because the network topology can change dynamically as nodes move around, it can adapt to changes in the environment and maintain connectivity even when some nodes fail or leave the network. This makes it highly robust and suitable for use in challenging environments where traditional networks would fail. However, MANETs also present several challenges. One of the most significant challenges is the lack of a fixed infrastructure (Krishnakumar and Asokan, 2023).

Since there is no central control, nodes in the network must work composed to maintain connectivity, which can lead to issues such as routing loops, congestion, and

***Corresponding Author:**ankitakmr33@gmail.com

interference. In addition, MANETs are susceptible to security threats like eavesdropping, DoS attacks (Joardar et al., 2023), and data tampering. To address these challenges, researchers have developed a variety of protocols and algorithms for MANETs. These protocols are designed to facilitate communication between nodes, manage network resources, and guarantee the Safety and trustworthiness of networks. Some of the most commonly used MANET protocols include the AODV (Ad-Hoc On-Demand Distance Vector) protocol, the (DSR, Dynamic Source Routing) protocol, and the (DSDV, Destination-Sequenced Distance Vector) protocol. These protocols use different routing and data forwarding approaches, but they all aim to optimize the network's performance while minimizing overhead and congestion. Overall, it is a powerful tool for enabling communication in challenging environments where traditional networks are not feasible. While they present several challenges, protocol design and network management advances have made MANETs increasingly reliable, secure, and efficient. As a result, MANETs will likely continue playing a crucial role in an extensive series of applications in the future. WSNs (Wireless Sensor Networks) are classified into infrastructure-based and infrastructure-less networks. The previous relies on access points that facilitate communication between wired and wireless devices. These networks' access points are base stations commonly found in airports, offices, homes, and hospitals. In contrast, infrastructure-less networks, also known as MANETs, do not require any infrastructure for communication between nodes. These networks are suitable for small areas and use a frequency range of 30MHZ to 5GHZ for data transmission. Nodes in a MANET are mobile, and communication happens within a fixed frequency range. The network is self-organizing and self-configuring, with a dynamic topology that adjusts based on network demands. Each network node turns a host and router, making it independent and cost-effective compared to wired networks.

The importance of MANET becomes apparent in risky and unpredictable environmental conditions such as armed establishments, environmental monitoring, and rescue operations. Due to the fixed energy constraints of each node, cooperation between nodes is required to establish and maintain the network. Unlike traditional networks, no central network administration controls MANET nodes, making them flexible for establishing connections. However, MANETs also present several security challenges in securing the data packets in the network. Confidentiality is a critical aspect of security in a MANET. Maintaining data confidentiality is significant when data packets travel in the network. Availability is another important aspect of Security, as data packets travel from one layer to another in the network layer. The public key is also available for the receiver to decrypt the data packet. Integrity is also a major aspect that helps data packets maintain their originality (Gopinath et al., 2019). When data packets travel in the networks, it is necessary to ensure they are not changed or hampered by intruders. Authentication ensures that the data packets sent thru source nodes are genuine. Then when a data packet is delivered, it checks that the received packet is genuine. Non-repudiation marks the authorized sender and receiver and marks the sender and receiver that they could not deny after sending and receiving the data packets. All these security aspects must be implemented in the network to prevent different attacks in MANET. Figure 1 shows different categories of attacks performed in different network layers. Protecting the network from these attackers is vital, and proper security mechanisms must be implemented to ensure data transmission safety.

Sinkhole attack

An SHA is a security attack that targets MANET(s) by redirecting network traffic towards malicious nodes that falsely advertises themselves as taking the straight route to a destination node (Sangaiah et al., 2022). SHA attacks are particularly problematic for MANETs because their network topology changes frequently and nodes rely on each other to forward packets to their destination. Once the attacker's node attracts the network traffic, it can be intercepted, monitored, or dropped, depending on the attacker's motives. The sinkhole attack works by the attacker sending fake routing messages to another node in the network, appealing that it has a direct route from a particular destination node. The attacker often uses a higher metric or cost value to make the advertised route seem more attractive. As other nodes update their routing tables accordingly, they forward traffic to the attacker's node. The attacker can intercept, modify, or drop the traffic before delivering it to the intended destination. To prevent sinkhole attacks, several mechanisms have been proposed. Trust-based routing protocols found belief among nodes by exchanging reputation or trust values. These values can then be used to make routing decisions based on each node's reliability level. In this way, a node with a high reputation or trust value is more likely to be selected as the next hop toward a destination node. This approach helps prevent sinkhole attacks by making it difficult for attackers to advertise themselves as trustworthy nodes falsely.

DOI: https://doi.org/10.52756/10.52756/ijerr.2023.v31spl.016

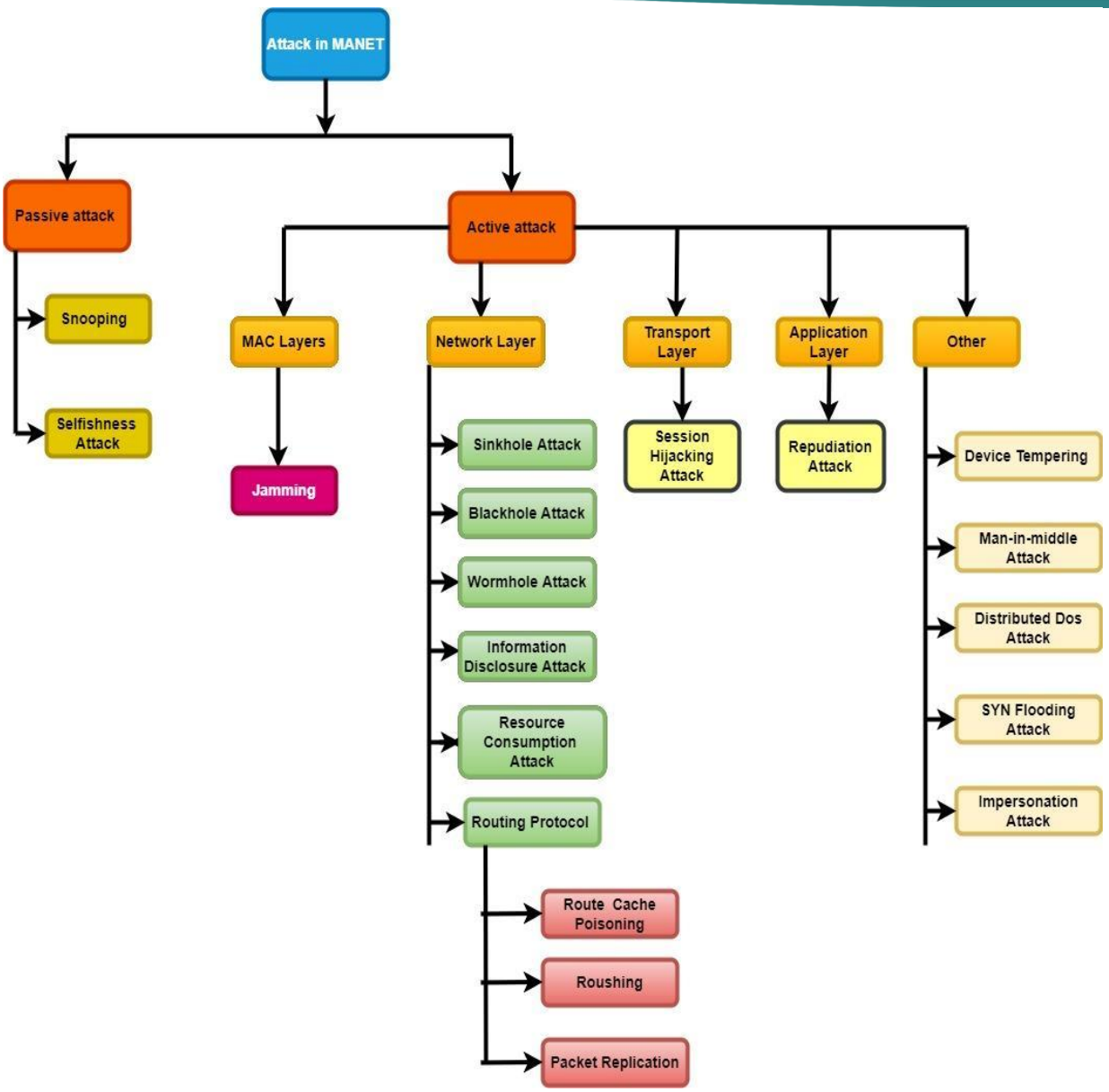

Figure 1.Types of Attack

IDS are another mechanism to avoid sinkhole attacks. IDS monitors the network traffic for unusual behavior, such as a sudden increase in traffic to a particular node, which may indicate a sinkhole attack. When an IDS detects such behavior, it can alert the network administrator or take action to prevent the attack from succeeding. IDS are effective at preventing sinkhole attacks but can be resource-intensive and require significant processing power. Overall, sinkhole attacks are a substantial hazard to the Safety and confidentiality of MANET. As such, it remains essential to have robust security mechanisms in place to prevent such attacks and ensure the safe and efficient operation of the network. Trust-based routing protocols and IDS are two effective mechanisms that can be used to avoid sinkhole attacks in MANETs. However, they must be implemented correctly and continuously updated to be effective against evolving attack strategies.

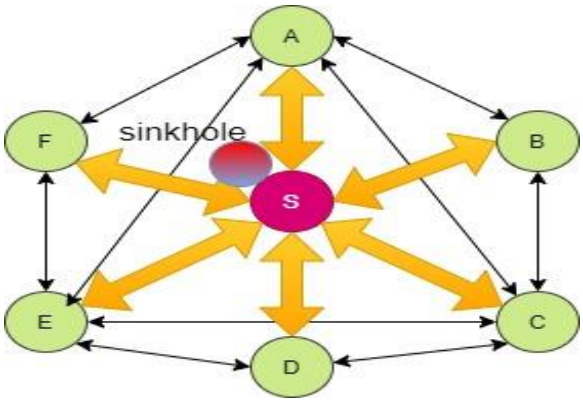

Figure 2. Sinkhole attack

The above passage describes the concept of a sinkhole attack on a MANET, where a particular node, referred to as "S," has been compromised and is controlled by a malicious entity.

DOI: https://doi.org/10.52756/10.52756/ijerr.2023.v31spl.016

In an SHA, the compromised node S sends fake or incorrect routing data to the extra nodes in the network. This misleading information directs other nodes to route their packets toward the compromised node S. The other node in the networks assumes that the routing data provided by node S is authentic and legitimate. However, the packages sent to node S are not transmitted further to their destination. Instead, node S drops these packets intentionally, resulting in a depletion of network resources and energy. To better understand the attack, reflect a scenario where nodes A, B, C, D, E, and F are connected in a network, as depicted in Figure 2. In this situation, node S has been hacked and transmitting fake routing information. As a result, the packets intended for other nodes are sent along the bogus route defined by node S. The transmission of these packets consumes the energy of the nodes on the fake route, leading to a depletion of network resources. The sinkhole attack is a significant danger to the Safety of MANETs, as it allows malicious entities to conciliate the truthfulness and accessibility of the network. To protect against such attacks, it is essential to implement security measures, such as encryption, authentications, and IDS, to sense and avoid malicious nodes after infiltrating the networks.

Black hole attack

BHA categories of security attacks that can arise in MANETs (Suma and Harsoor, 2022; Pullagura and Dhulipalla, 2023). In such attacks, malicious nodes, also known as blackhole nodes, attempt to entice all network traffic near themselves by falsely advertising that they take an actual and effective path to reach out destination. Once the traffic is redirected to the blackhole node, it can be dropped or modified, depending on the attacker's motives. A MANET's nodes are mobile and interconnect separately supplementary without a central structure. The communication between the nodes is established using wireless links, and the routes between them are discovered and maintained by a routing protocol. When a node requests to send a data packet to alternative nodes, it forwards the packet to its neighbor with the best path toward the destination, and so on, until the packet reaches its destination. However, in a blackhole attack, the attacker sends false routing information to the neighboring node, advertising that it has a direct or most efficient path to the destination. The adjacent nodes, unaware of the attacker's malicious intent, start to use the attacker as the next hop toward the destination, causing all the packets to be redirected to the attacker. The attacker can then dewdrop or alter the data packets, leading to a DoS attack or tampering. The BHA can be executed by exploiting vulnerabilities in the directing protocols used in the MANET. For example, the attacker may forge route discovery messages, modify routing tables, or even impersonate other legitimate nodes to convince the neighboring nodes that it has an excellent path to the destination. Various countermeasures are used to defend against blackhole attacks, such as secure routing protocols, trust-based mechanisms, and intrusion detection systems. Secure routing protocols can ensure that only legitimate nodes participate in the route discovery and prevent attackers from advertising false routing information. Trust-based mechanisms can establish a trust level for each network node based on its behavior and reputation, which can be used to evade direction-finding through untrusted nodes. Intrusion detection systems can detect black hole nodes by analyzing network traffic and behavior patterns and taking appropriate actions to isolate or remove them from the network.

Blackhole attacks seriously threaten the Security and reliability of MANET. It is crucial to apply effective countermeasures to avoid and lessen the impact of such attacks. A BHA occurs in MANET when a malicious node pretends to take the direct route to the destination's node and intercepts all acknowledged messages from other network nodes. Once an attacker receives the packets, it can drop or modify them to disrupt communication or steal sensitive information without being detected by other nodes. To prevent blackhole attacks, several mechanisms have been proposed. One of these is secure routing protocols, designed to avoid attackers falsely advertising themselves as the next hop toward the destination. This is achieved by requiring nodes to authenticate their identity and routing messages before they are accepted. Another mechanism is IDS, which can monitor network traffic and detect any unusual behavior, such as sudden drops in traffic to a particular node. IDS can detect and mitigate suspicious activity by comparing traffic patterns with normal traffic behavior. Blackhole attacks pose an essential threat to the Safety and confidentiality of MANET, as they can cause significant damage and compromise the privacy and truthfulness of the communicated data. It is, therefore, important to have robust security mechanisms in place to prevent such attacks and ensure the safe and efficient operation of the network. Overall, preventing blackhole attacks in MANET is crucial for maintaining the data's confidentiality, integrity, and availability. Secure routing protocols and intrusion detection systems effectively prevent these attacks and ensure the network's Security.

DOI: https://doi.org/10.52756/10.52756/ijerr.2023.v31spl.016

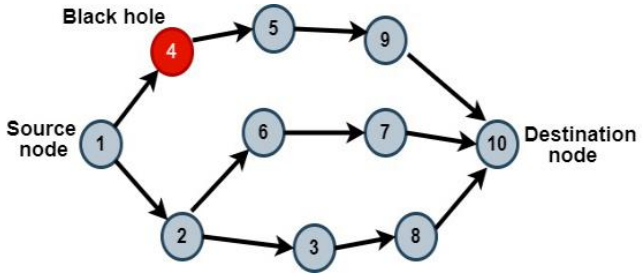

Figure 3. Black Hole Attack (Source: Ankita Kumari et al., 2023)

In the diagram depicted in Figure 3, a network of ten nodes is interconnected through dynamic topology. A source node and a destination node are also present.

The sender node broadcasts an (RREQ, Route request) message to send data to the intended recipient. The RREQ aims to find the direct route to the destination node. However, a malicious node known as a "black hole node" sometimes intercepts the RREQ. In such cases, the black hole node may send fake route reply (RREP) messages to the sender node (in this example, node 1) instead of forwarding the RREQ to its intended recipient. In this scenario, node 4 is the black hole node. Subsequently, node 1 uses the routing the fake RREP message provides to transmit data packets. The black hole node, node 4, receives and then drops the data packets, leading to network degradation.

Here are two categories of BHA: simple black hole attacks and cooperative black hole attacks. These attacks can pose a significant threat to the network's security and should be addressed appropriately to ensure the proper functioning of the network.

Wormhole attack

A WHA (Wormhole attack) is a network attack involving collaboration between two or more malicious nodes (Tahboush and Agoyi, 2021; Shukla et al., 2021; Alghamdi and Bellaiche, 2023). This attack aims to create a tunnel in the network that can be used to redirect traffic and compromise network security. In a wormhole attack, the malicious nodes work together to intercept an RREQ communication from a legitimate source node. Once they have blocked this message, they create a fake routing reply (RREP) data message and send it back to the source node. However, malicious nodes have not calculated a legitimate path to the destination node. When the source nodes send data packets to the destination nodes, malicious nodes use a tunnel they created to redirect the packets to other network nodes. By doing so, the malicious nodes can intercept and potentially modify or destroy the transmitted data, thus compromising the network's security and integrity. Wormhole attacks can be dangerous and difficult to detect because they involve multiple malicious nodes working together. Moreover, they can launch another attack, such as DoS or man-in-the-middle attacks. So, it is critical to implement adequate safety measures to avoid wormhole attacks and protect the network's integrity.

An investigation into various forms of attacks on MANETs

A sinkhole attack is when the attacker alters the data packets and transmits them into the network (Tseng et al., 2005). Form prevents it after attacking. This paper presents an intrusion detection system introduced with an indicator that helps indicate the sinkhole attack in MANET. While watching, the current scenarios in the MANET indicator are proposed. They proposed two indicators ideas that help hint at the attack, named a sinkhole intrusion indicator system (SIIS). In this system, two indicators are proposed: if the seq_num_discountity is high, there is a chance of an SHA, and if route_add_ratio is also high, there is the possibility of a sinkhole attack. The indicator idea can be used in other related problems that help the sender find a good path for sending and receiving data in the MANET. Using the indicator consumes lots of energy from nodes which can cause the degradation of the network.

A DDA (Distributed Detection Approach) is proposed to automatically detect fake routing requests (RREQs) from sinkhole attackers (Shim et al., 2010). In the distributed detection system, cluster analysis is used to extract the exact feature of nodes based on their behavior. One indicator indicates the false route request (RREQ) messages in MANET. The cluster analyzes the nodes' features and decides the C.H. makes the C.H. It starts transmitting information in the network. Future work focuses on finding more additional features of nodes so that while receiving route request (RREQ) messages, it will know that RREQ is the fake or original message from the sender. This will help the routing protocol to detect and block the attacker from the network.

The authors Kim et al. (2010) proposed a cooperative sinkhole detection system. The MANET sinkhole attacks are short of a routing protocol attack that alters the original data packet and sends them to their adjacent network nodes. The technique was premeditated to improve the presentation regarding sinkhole attack detection rate and detection time. The projected algorithms are compared with SIIS (sinkhole intrusion indicator system), which shows that the proposed algorithms are higher than the SIIS. The SIIS (sinkhole intrusion indicator system) can only detect about 45% of the malicious node, while the cooperative sinkhole

DOI: https://doi.org/10.52756/10.52756/ijerr.2023.v31spl.016

detection method can detect accurately only when the attack is strong. The algorithms are more effective in detecting sinkhole attacks in MANET. Future work will lower the network consumption of energy so that nodes of the network will stay for a more extended period and give more results.

The authors Nagai et al. (2007) presented an original process for sensing sinkhole attacks in WSNs. The algorithms help to discover the network's assumed nodes, checking data uniformity on the basics of that they effectively identify the malicious node. The algorithm is also used to determine the network's multiple malicious nodes. They have analyzed the algorithms through both numerical analyzations as well as simulation, which gives the accuracy and effectiveness of the algorithms. The proposed algorithms also help the sender node identify the hidden malicious node, which does not perform malicious activity in the network. The algorithm helps discover the series of malicious nodes in the network. The procedure uses much less energy from nodes, which is very feasible. In future work, they are trying to improve their algorithm to give a more accurate result for finding the malicious node/sinkhole attack in a WSN.

In their study, Shafiei et al. (2014) proposed a novel approach to recognising and preventing sinkhole attacks in Wireless Sensor Networks (WSNs). They were achieved by utilising a centralised strategy to identify and locate malicious nodes that were present within the network. They are using a geostatistical hazard model to identify the malicious node. The proposed distributed monitoring approach for finding the malicious behavioral nodes in the network. This model monitors the network traffic and analyzes every network node's performance. When a particular node is flooding more messages in the network, that shows some malicious activity. Monitoring the traffic helps the model mitigates the malicious node from the networks. In future work, the model needs to improve by the optimization time and energy of the nodes.

An SHA detection technique was proposed by the authors Zhang et al. (2014). They can identify the sinkhole attack within the WSN with the use of an algorithm. AnSHA is performed in the network layer. Most attacks are performed in the network layer. They used three processes to establish the path to detect the sinkhole attack. One is RREQ; another is route reply and route formation. In creating the WSN scenario, establishing the network in the node is static and arbitrarily distributed. Sinkhole detection algorithm based on multiple path selection. One way to express this statement could be: "Using Dijkstra's algorithm enables the computation of the most efficient route to the intended endpoint.". The proposed algorithm finds the multiple paths that help the sender select the best path for data sending to their respective neighborhood in the network. They simulated their algorithm to check its feasibility, which is very good. In forthcoming work, they will try to improve the algorithm and focus on more problems in wireless sensor networks.

Anticipated is an agent-based approach for detecting SHA in WSNs (Hamedeidari et al., 2013). The agent is mobile, which helps the network to find the attackers. The agent uses the AODV routing protocol for data transmission. They used different sets of nodes like 100 nodes, 200 nodes, 300 nodes, and 400 nodes. All nodes present in the network are simulated and analyzed on many parameters like average energy consumption, the average number of uncovered nodes, the accuracy of intruder identification, packet loss rate, agent packet overhead, and throughput. As a result, it is analyzed based on different parameters that show that the proposed algorithms are better than the AODV. The proposed approach has many advantages like memory overhead being increasingly reduced. The energy of nodes is fixed, so the agent is suitable for detecting an intruder; no other expense is used for exchanging public and private keys. The proposed algorithms are good for mobile nodes. The future aspect of this algorithm is to increase its performance and try to diminution the normal of revealed nodes by emerging it through a different technique, such as clustering.

A swarm intelligence-based approach detects SHA (Sreelaja et al., 2014). By using swarm intelligence, the classical rule-matching technique is used. Using ACO (Ant Colony Optimization), they proposed an ACO-AD algorithm for sensing SHA in WSN. The sensor node has somewhat number of adjacent nodes in the networks. The voting technique detects intruder/ malicious nodes in networks. Comparison is made with the binary search and the proposed work, i.e., ACO- attack detection. The result of compared algorithms is good. The ACO-AD algorithm is improved than the binary and sequential search methods for sensing SHA in WSN.

The authors (Sanchez-Casado et al., 2015) propose a method for detecting SHA in a network. The technique involves using contamination borders to identify malicious nodes and mark them as containment borders. This alert signal informs the sender that the network has potentially malicious nodes. The sinkhole attack targets the AODV protocol, and the proposed method leverages its features. The sequence number determines the presence of contamination zones and border nodes. The

DOI: https://doi.org/10.52756/10.52756/ijerr.2023.v31spl.016

contamination border is identified using a heuristic that monitors network activity for signs of malicious activity. The simulation of the proposed method was conducted using OMNeT++ (Varga). In future research, the authors plan to extend the contamination border approach and explore the use of trust-based schemes as a reply device for collision circumstances in the network.

The authors (Jahandoust et al., 2017) proposed an ASA algorithm for WSN. In ASA algorithm help it to detect the sinkhole attack. It allows the sender to discover a reliable route from source to destination. The projected algorithm uses probabilities to find the more trusted path. By using probability, they design the model, which is adaptive to detect the SHA. The model too detects the byzantine malicious node in the network. The false-positive and false-negative results can also reduce network coverage area. The idea can be projected in future work to detect extra attacks in MANET, like WHA, BHA, and grey hole attacks.

The authors (Liu et al., 2018) propose a design and analysis of how to discover IoT devices. They are probing the route of a sinkhole attacker and trying to block them from the network. The PRDSA (probing route defence sinkhole attacks) is validated through OMNeT++. It is a defensive scheme based on a route probe in which every node in the network is deployed. PRDSA can detect and locate sinkhole attacks on the network, which help the genuine nodes. The benefit of this project work is that it can bypass the sinkhole attack in the network. In future work, intelligent cities, edge computing, and fog computing will rectify the attack in MANET. Some penetrating data packet will be sent to the network so the attacker node says, "I am the attacker node," and then it can easily be removed from the network.

Vigenesh et al. (2019), routing attacks are major consent these days. They degrade the quality of networks for detecting sinkhole attacks in MANETs. ESRSPA (efficient steam region sink position analysis) model is introduced. With the help of this model, they try to detect whether a sinkhole attack is possible. This model decreases the routing overhead by 50% with 96.86% throughput. When an attack is detected in the network, which increases several parameters, grows the network's entire presentation, and determines the data packet delivery ratio. There are still chances to improve the proposed model's throughput in the future, which will help the network improve its security and performance.

The authors (Gothawal et al., 2019) proposed RPL in WSNs. For the implementation, they used the Contiki operating system to simulate and validate the proposed work. In this proposed work, the sender node broadcasts each message in the network when all the genuine nodes send the acknowledgment to the sender node. This marks that the nodes are genuine, and that node that does not send an acknowledgment message marks the node as a malicious node in the network. They check the latency of the packet delivery. When they checked the latency for the different numbers of data packets like 30, 50, and 100, the latency for the other numbers of packets was different, i.e., 41 % latency for 30% of packets, 50% latency for 55.8% latency, and 63.3% latency for 100% of packets, but when they analyzed, they see that the overall latency is improved the efficiency of RPL so that consumes less energy of nodes. An effective process also needs to sense and mitigate attacks from the network.

Babaeer and Al-Ahmadi (2020) proposed a secure model for sensing and avoiding sinkhole attacks in WSNs. The proposed approach utilizes homomorphic encryption and watermarking techniques to enhance the network's security. The model involves the TEEN protocol and the base station, which change dynamically as the cluster formation changes. To confirm the validation of data packets, the researchers used watermarking and pseudo-random number generators. The data packets were watermarked before being sent to the network. If any manipulation was detected in the watermarked data packets, the receiver node could identify the tampering and inform the sender node in the network. Homomorphic encryption techniques enhanced the watermarking process, ensuring data packets could not be manipulated. The simulation outcomes evidenced that the projected system achieved 100% successful security against data packet manipulation.

Khatoon et al. (2021) proposed a fuzzy-based Q-learning method for FQ MEC. In this, they monitor the behavioral activity of nodes. They also used Chebyshev's inequality principle for load balancing of nodes and more efficiency of nodes. Then they simulated in NS2. After implementing the proposed work, they set the fuzzy instructions for clustering nodes. They compared their work with reinforcement learning (R.L.). The result is obtained after the comparison that it improves the network lifetime, packet delivery ratio, average end-to-end delay, and energy consumption cluster head has a major responsibility to enhance the network lifetime; Chebyshev's inequality helps the cluster head maintain the network because it always balances the cluster head to get degraded and re-clustering as in the future work they have thought of using SARSA learning methodology to be applied in MANET to improve the network security routing and clustering.

DOI: https://doi.org/10.52756/10.52756/ijerr.2023.v31spl.016

In the research by Tamilselvan et al. (2007), an ad-hoc network is used for short data transmission. It is wireless and infrastructure-less. There are two routing protocols used. A BHA is executed in AODV protocol. BHA, a malicious node, responds to the source node, which is a direct path from this side. The source node trusts on message and sends the data packets that way. They used the wait-and-check method for the prevention of BHA. When any node sends the data packets to its neighbors, it checks when the message is sent and received. They used GLOMO Sim to review their proposed work's performance. By using a simulator, a metric is generated. The matrix has different parameters to analyze the network's performance.

Chang et al. (2014) proposed a defense mechanism for sensing BHA in MANET, i.e., CBDS. CBDS is based on both reactive and proactive routing protocols. They compared the CBDS approach with DSR based on restrictions like packet delivery ratio, routing overhead, throughput, and end-to-end delay. They found that CBDS is performing improved than the DSR routing protocol. In the CBDS approach, they catch the malicious nodes in the network, but in DSR, there is no mechanism for sensing the malicious node in the networks. In upcoming efforts, they focus on the network's possibility of identifying the coordinated attacks in MANETs. Another work is to make s secure routing framework to transfer the data in the network.

Dhaka et al. (2015) introduced the Rseq packet and code Cseq. When any other node sends Cseq to all its adjacent nodes in the networks, all adjacent nodes send the Rseq packet to their corresponding neighborhood nodes. When the Cseq and Rseqmatch, the requested node is matched, and the requested node is acceptable to join the networks. It discards the demand to join the network if it does not reach them. To check the proposed work, they have simulated in NS-2 software for more authentication and validation. The result of the projected work improves the PDR and routing overhead, which shows that the proposed work is the efficient identification of BHA in MANETs. In future work, they are trying to improve the parameters of the proposed work.

Ranjan et al. (2015) proposed utilizing MANET for temporary data transmission and studied several routing algorithms to transport data throughout the network. However, malicious activities, such as black hole attacks, can cause impairment to the networks. In BHA, a malicious node collects data packets and dewdrops them from the networks, depleting its strength and performance. Multiple malicious nodes work together in a cooperative BHA to cause more damage.

To prevent black hole attacks, several surveys have been conducted. The authors (Chavan et al.) 2016 paper compared the AODV and DSR routing protocols and found that AODV performed better in every parameter except when subjected to a BHA. In such cases, the packet delivery ratio and throughput decreased to zero, highlighting the need for modification to avoid BHA.

In 2017, Khamayseh et al. in their article revealed an OBSA method that might get around BHA in MANETs. The OBSA has two components: the source node and the observation node. The observation node monitors the network's traffic and data flow and proposes a solution when a new message needs to be sent. The proposed algorithm was simulated and verified using the Qualnet simulation package. It significantly improved the PDR and throughput in condensed and sparse networks, reducing packet drops in dense and sparse networks by 75% and 63%, respectively. However, the simulation was limited to low-mobility and high-density networks. Future research will focus on calculating and transmitting data packets based on the node's energy level to improve network efficiency further.

Rani et al. (2018) proposed a lightweight reputation-based approach to senseBHA in MANETs. The approach included a reputation table of nodes and multi-hop acknowledgment. The nodes' reputation increased or decreased based on simulation and reflection in the conditions. The proposed method could detect coordinated and simple black hole attacks and outperform the concurrent protocol in terms of detection ratio and network transmission overhead.

Gaurav et al., 2020 used deep learning and artificial neural networks to protect MANETs from dual black and grey hole attacks. The paper utilized swarm-based artificial bee colonies (ABC) to detect and mitigate attacks, and ABC was used to separate the nodes created on their possessions. After simulation and evaluation, the projected method to improve networks performances in terms of PDR values, throughput, and delays compared with the previous model of MANET.

Nagalakshmi et al. (2020) used, different machine learning classifiers to detect BHA in MANETs. They studied six machine learning algorithms and made groups based on their work. The paper found an ineffective intrusion detection system without feature extraction techniques. After analyzing the system with feature extraction, the system was more accurate and efficient in detecting BHA in MANETs.

DOI: https://doi.org/10.52756/10.52756/ijerr.2023.v31spl.016

The authors in their research predicted a secure backbone structure to shield MANET from various attacks (Hammanouche et al., 2021). The network was separated into clusters, and cluster heads were selected based on a low-cost analysis. The proposed model could also detect malicious nodes and generate alert messages when such nodes were found. The researchers found that their model consumed less energy from nodes, which helped them stay active for extended periods. Additionally, the proposed model was more efficient than the BTRES approach. However, it could not detect multiple malicious nodes simultaneously, and the researchers plan to improve their algorithm and reduce the false positive rate in the future.

The SEC-DSR protocol analyses the RREQ and RREP messages to prevent black hole attacks. If any issues are detected with these messages, the node responsible is removed from the network.

When the presentation of the SEC-DSR protocol was assessed, it was found to have better packet delivery ratios and end-to-end delay than other models. However, an increase in network dynamics may lead to a higher number of RREQs and increased network overhead, necessitating frequent updates to the routing table.

Simpson et al. (2021) implemented a fuzzy-based system to tackle the cooperative blackmailing attack in MANET-IoT. In the proposed work, they have set fuzzy rules and created a trustworthy environment for the smart city on edge computing. In a cooperative blackmailing attack, a malicious node is on the direct route to the destination node. The cooperative blackmailing attack decrees the constancy of the network, which leads to the destruction of the network. The attack is made simultaneously, indicating other compromised nodes to attack in the network. The malicious activity is performed on many levels, so they used the fuzzy-based model to evaluate the network routine to identify the malicious node. When there is malicious activity in network performance, the throughput, and PDR change when there is malicious movement in the networks. When the fuzzy-based system is applied in a network to prevent a cooperative blackmailing attack, the throughput increases, reduces packet drop from the network, less delay in message sending, and increases the network resistance. In the future, there are going to try to protect IoT from different categories of attacks.

Reddy et al. (2021) proposed that AODV-BS (built-in Security) has used an N.S. simulator of version 2.3. They have used different nodes like 30, 50, 70, 90, and 110. The simulation time for all the nodes is 200s. After simulation then, it was compared by the AODV routing protocol. They found the resulting parameters delivery ratio, average end-to-end delay, normalized routing overhead, and throughput. The comparison result shows that it is improved than the AODV routing protocol. In forthcoming work, there are going to enhance the Security of internal Security and External Security of MANET.

Li et al. (2011) proposed a new approach to detecting wormhole attacks. Physical layer network coding is used to notice WHA. The mechanism works on a physical layer network. When two sender nodes send the data packet simultaneously, the source node checks the origin of the packet it sends from and checks the message's sequence number. To find the best solution for detecting wormhole attacks, they studied literature and analyzed them to find a false alarm rate that rings the alarm ring when there are no network attacks. When an attack is performed, one drawback is that sometimes alarms ring when there is no attack in the network. The proposed work has two extensions. One is checking how much efficiency software gives to sense the wormhole attack in MANET. Another technique is the software-defined ratio. They implement the software, provide the environment, and observe how they react when their nay attack is performed in the network. All these are performed in the physical layer to detect another stealth attack in MANETs.

To identify and avoid wormholes, Singh et al. (2015) and the BHA Authors' Collaborative have proposed a trust-based AODV routing algorithm in which a trusted database is built for each node in the network. The node has a high trust value table in the network. They simulated their trust value in the table using NS-2 software for validation. When they increase the message-sending time, it consumes more nodes' energy, which impacts MANET. The throughput of the AODV trust table is compared with a wormhole attack and a collaborative black hole which shows the throughput and delivery ratio are improved. In future work, they have planned to calculate the trust value of other attacks in MANET.

FPGA was suggested by Kumar et al. (2015) to detect BHA and wormhole attacks in MANET. They have created different scenarios through which they analyzed in what conditions the attack is taken place and how much damage was done to the network. For testing the software, they have three scenarios first one is in which MANET is created of two nodes, N1 and N3 are placed in a range line and are tested in normal communication. The second scenario was N1 and N3 are nodes of MANET, the range line is out from the range, and

DOI: https://doi.org/10.52756/10.52756/ijerr.2023.v31spl.016

communication is normal. The packet gets loosed because the nodes are not in range. In the third scenario, two nodes, N1 and N3, are placed in a line, but it is out of range, and in between N1 and N3, N2 is set. So, in this condition, N1 and N3 communicate with each other through one hop count, but the communication is usually taking place. In the fourth scenario, N2 is replaced with a malicious node without MANET properties. When the node sends the data packet, it gets dropped by the malicious node, which quickly gets detected and marked as a malicious node in the network.

Jamali et al. (2017) introduced an improved variety of the AODV routing protocol, which helps detect the wormhole attack immune routing protocol. The projected protocol is DAWA, based on fuzzy logic and artificial immune systems to protect from WHA in MANET. The proposed work is replicated in an NS-2 simulator. The fuzzy logic is based on a few parameters, such as the residue energy of nodes, the path's hop count of their neighboring node, and the path's distance of different stable routes of nodes. Artificial intelligence helps to check the immune of nodes, bypass the genuine nodes, and detect the malicious node through its previous experiences. Then they compared DAWA with COTA and worm planar algorithm. The result of the proposed work, i.e., DAWA's overall performance, is improved over COTA by 20%, and worm planar DAWA is better in terms of packet delivery ratio, wormhole detection, false-positive ratio, false-negative ratio, and packet drop ratio. The DAWA I is more effective in detecting wormhole attacks in MANET.

Qazi et al. (2018) discussed about De1PHI, in which multi-rate transmission is performed. They proposed the M-De1PHI protocol, which protects the network from multi-rate transmission attacks. When the De1PHI protocol is used to secure the AODV for multiple data transmissions, it protects it from wormhole attacks in MANET. The proposed M-De1PH is compared with De1PHI. The wormhole exposure rate is 90% in both incoming and out-of-band tunnels, in which the false-positive rate is 10%.

In the study conducted by Govindasamy et al.(2018), various routing protocols in WSNs were compared to detect wormhole attacks. The study used the IEEE802.15.4-based Qualnet 5.0 simulator to investigate the recital of AODV, OLSR, and ZRP. The performance of these protocols was evaluated using a performance matrix of 50 nodes, considering metrics such as throughput, average end-to-end delay, and energy consumption by each node. The study utilized several parameters, such as transmitted, received, idle, and sleep nodes, to determine the performance of different routing protocols. ZRP exhibited the highest throughput among the three routing protocols, while OLSR had the lowest average end-to-end delay. Based on the analysis of these protocols, the study concluded that there is a need to design a more energy-efficient routing protocol to avoid excessive energy consumption by nodes.

In an effort to reduce false alarms of wormhole detection in MANET and safeguard its resources, Tiruvakadu et al. (2018) suggested the Wormhole Attack Confirmation (WAC) system. MANET has no central administration, so the security issues are more. The attack tree is also proposed in which the sender identifies the attack, where it is performed, and how much damage is given to the network. The idea of the honeypot is also used there to attract the malicious by interacting with malicious nodes. It also distracts the malicious from performing malicious activity in the network. When the WAC performance is evaluated and compared with DPS (Detection Prevention System), they find that WAC works well in identifying malicious nodes and giving an alarm when they encounter any malicious Wormhole attack in the network. The performance is evaluated based on PDR, throughput, and message delay.

Bai et al. (2019) suggested a MaXIS-based method for identifying wormhole attacks in 3D networks using only the connectivity information. They improved the MaXIS construction by using a simple greedy algorithm which helped to see the wormhole attack in MANET. They have analyzed their proposed work on different types of parameters. They first chose the parameters for the wormhole detection rate. The result shows that the performance improved its detection rate more by using the forbidden substructure, which improved the performance by up to 88%. If the nodes' density of the nodes 1.39 and 2.5, then the routine increases to 100%. If the network deployment is random, then the detection rate of a wormhole attack is 100%. MaXIS construction is easy to implement and simulates for detecting MANET wormhole attacks.

Hua et al. (2020) used the LLDP to mislead the attacker to attack the network. They have used three network topologies to check the network's performance and efficiency. The three topologies they used are Ncol, Nsfcnet, and Shentel. They compared results based on different parameters. The parameters are packet loss rate, throughput, and PDR. The topology is selected randomly. The total packet loss rate of all three topologies is 168.42% which is very high. They used Mininet 3.3.od4 and open flow 1.5 for simulation to detect wormhole

DOI: https://doi.org/10.52756/10.52756/ijerr.2023.v31spl.016

attacks. They have also proposed a detection algorithm for wormhole detection in SDN networks.

The research by Nguyen et al. (2008) analyses the influence of various security threats on multicast sessions in Mobile Ad hoc Networks (MANETs). The study considers black hole attacks, neighbor attacks, and jellyfish attacks. The results demonstrate that the performance of multicast sessions is heavily influenced by the number and position of attackers and the number of multicast senders and receivers. In particular, when the number of attackers increases, the damage inflicted on multicast sessions, measured by packet delivery ratio and delay, also increases. Rushing attackers have a higher chance of gaining access to the forwarding group, especially when the number of senders is small, and the number of receivers is large. Attackers should gather in groups near receivers or around the mesh center to maximize success rates. Black hole and neighbor attacks result in similar degradation of packet delivery ratio, comparable to jellyfish attacks' impact on end-to-end delay. Small multicast groups suffer more severely under these attacks, whereas larger groups with more senders and receivers can sustain better performance due to more alternative routing paths. Attackers near the senders pose the most damage, as they intercept packets early, while attackers at the mesh center cause the most packet losses or delay when their number is smaller than the multicast senders. The paper presents the first study of multicast vulnerability and performance in MANETs under various security threats.

The study by Nguyen et al. (2012) analysed the influence that security attacks have on connection points inside Mobile Ad hoc Networks (MANETs). It considers blackhole, neighbor, and jellyfish attacks, studying their effects on packet delivery ratio, delay, and delay jitter. The simulation results show that the number of attackers, along with factors like the number of flows, node mobility, traffic load, and attack positions, heavily influences the performance of connections. Higher numbers of attackers lead to more damage to flow performance. Both blackhole and neighbor attacks cause similar packet loss rates and throughput damage, while jellyfish attacks primarily increase end-to-end delay and delay jitter. Despite different attacking mechanisms, blackhole and neighbor attacks affect packet delivery ratio and throughput similarly to how jellyfish attacks impact end-to-end delay and jitter. Networks with dense connections are more susceptible to attackers, while mobile nodes may offer some defence against intrusions due to changing paths. However, excessive mobility can negatively affect network performance through frequent link breaks. Attackers near the senders cause the most damage, aligning with earlier findings. Overall, the study sheds light on the vulnerability of connections in MANETs under different attack scenarios.

Eltahlawy et al. (2023) explored the effectiveness of packet forwarding in Mobile Ad hoc Networks (MANETs) and the significance of selecting a suitable simulation tool to set up the MANET environment. Additionally, the authors highlight the relevance of selecting an appropriate simulation tool to build up the MANET environment. Researchers use MANET simulation tools for various purposes, such as performance analysis, evaluating routing protocols under attack, studying the impact of environment parameters on performance, and assessing newly introduced protocols. The authors present a survey of 50 recent papers, summarizing the literature contributions in this field. It overviews simulation, routing, and attack parameters that control MANET behavior. NS-2 is identified as the most popular simulator for MANETs. The survey indicates that small networks typically have a defined area of 200 m × 200 m, while extensive networks do not exceed 2500 m × 2500 m. Simulation times range from 5 seconds to 1 hour, and mobility speeds vary from static nodes (0 m/s) to 50 m/s. The number of network nodes ranges from 3 to 50 for small networks and 600 for extensive networks, with varying numbers of malicious nodes. The authors also present commonly used evaluation metrics to assess network performance in MANETs. The study emphasizes the significance of understanding and controlling the parameters influencing MANET behavior for accurate evaluations and research in this area.

The authors in their research discussed the importance of MANETs, which stand for mobile ad hoc networks, are decentralised wireless networks that operate without any preexisting infrastructure (Sankar et al., 2023). To counter common threats and attacks in MANETs, intrusion detection is advised. Existing solutions to defeat attack nodes often require additional hardware, suffer from delivery delays, and consume more energy. The Safe Routing Approach (SRA) was developed in response, utilizing behavior analysis to track and monitor attackers. The proposed method conceals trusted nodes in the routing pathway and assigns paths promptly based on node strength values. SRA outperforms AIS, ZIDS, and Improved AODV regarding Packet Delivery Ratio (PDR), residual energy, and network throughput. It extends the network's lifespan and reduces packet loss, ensuring enhanced security.

DOI: https://doi.org/10.52756/10.52756/ijerr.2023.v31spl.016

Solutions for different types of attacks in MANET

Sl. No.	Papers name	Authors Name	Year of publications	Attacks	Solutions
1	Sinkhole Intrusion In Mobile Ad Hoc Networks	Tseng et al.	2005	Sinkhole attack	Sinkhole Intrusion Indicator System (SIIS)
2	An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks	Ngai et al.	2007	Sinkhole attack	Sinkhole Detection Algorithm
3	A distributed sinkhole detection method using cluster analysis	Shim et al.	2010	Sinkhole attack	Distributed Detection System and Cluster Analysis
4	A cooperative-sinkhole detection method for mobile ad hoc networks	Kim et al.	2010	Sinkhole attack	Cooperative Sinkhole Detection
5	A novel agent-based approach to detect sinkhole attacks in wireless sensor networks	Hamedheidari and Rafeh,	2013	Sinkhole attack	An Agent-Based Approach for Detection
6	Detection and mitigation of sinkhole attacks in wireless sensor networks	Shafiei et al.	2014	Sinkhole attack	A Detection and Mitigation Technique
7	Sinkhole attack detection based on redundancy mechanism in wireless sensor networks	Zhang et al.	2014	Sinkhole attack	A Sinkhole Attack Detection Algorithm
8	Swarm intelligence-based approach for sinkhole attack detection in wireless sensor networks.	Sreelaja et al.	2014	Sinkhole attack	Swarm Intelligence-Based Approach
9	Identification of contamination zones for sinkhole detection in MANETs	Sanchez-Casado et al.	2015	Sinkhole attack	Contamination borders through which they mark the Malicious node
10	An adaptive sinkhole-aware algorithm in wireless sensor networks	Jahandoust et al.	2017	Sinkhole attack	ASA Algorithm for Wireless Sensor Network
11	Design and analysis of probing route to defense sinkhole attacks for Internet of Things security	Liu et al.	2018	Sinkhole attack	PRDSA (Probing Route Defense Sinkhole Attacks)
12	An efficient stream region sink position analysis model for routing attack detection in mobile ad hoc networks	Vigenesh et al.	2019	Sinkhole attack	ESRSPA (Efficient Steam Region Sink Position Analysis)
13	Intrusion detection for enhancing RPL security	Gothawal et al.	2019	Sinkhole attack	Routing Protocol for Low Power And Lossy Network

DOI: https://doi.org/10.52756/10.52756/ijerr.2023.v31spl.016

14	Efficient and secure data transmission and sinkhole detection in a multi-clustering wireless sensor network based on homomorphic encryption and watermarking	Babaeer et al.	2020	Sinkhole attack	Homomorphic Encryption and Water Marking Techniques
15	FQ-MEC: Fuzzy-Based Q-Learning Approach for Mobility-Aware Energy-Efficient Clustering in MANET.	Khatoon et al.	2021	Sinkhole attack	Fuzzy Based Q Learning Approach for Mobility Aware Energy Efficient Clustering (FQ MEC)
16	Prevention of blackhole attack in MANET.	Tamilselvan and Sankaranarayanan,	2007	Black hole attack	Used For Short Period of Time for Data Transmission.
17	Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach	Chang et al.	2014	Blackhole attack	CBDS (Cooperative Bait Detection Scheme).
18	Gray and black hole attack identification using control packets in MANETs.	Gray and black hole attack identification using control packets in MANETs.	2015	Blackhole attack	Introduced The Response Sequence (Rseq) Packet And Code Sequence Packet (Cseq).
19	Security issues of black hole attacks in MANET.	Ranjan et al.	2015	Blackhole attack	Black Hole Detection Mechanism
20	Performance analysis of AODV and DSDV routing protocol in MANET and modifications in AODV against black hole attack.	Chavan et al.	2016	Blackhole attack	They Have Compared The AODV And DSR Routing protocolsbased on Their Performance Analysis.
21	Ensuring survivability against Black Hole Attacks in MANETS for preserving energy efficiency.	Khamayseh et al.	2018	Black hole attack	OBSA
22	Lightweight reputation-based approach against simple and cooperative blackhole attacks for MANET	Hammamouche et al.	2018	Blackhole attack	A lightweight reputation-based approach is proposed
23	Mitigation of black hole and grey hole attacks using a swarm-inspired algorithm with artificial neural network	Rani et al.	2020	Blackhole attack	They have used deep learning and artificial neural network to protect manet from dual attacks like black hole attack and grey hole attacks.

DOI: https://doi.org/10.52756/10.52756/ijerr.2023.v31spl.016

24	Machine learning models to detect the blackhole attack in wireless Adhoc network	Nagalakshmi et al.	2021	Black hole attack	They have compared different types of machine learning classifiers K-mean cluster algorithm, SVM, decision tree, and random forest.
25	A systematic comparison of mobile Ad-hoc network security attacks.	Syed,	2021	Blackhole attack	They Have Compared The Security On Different Parameters.
26	A novel approach using elliptic curve cryptography to mitigate Two-Dimensional attacks in mobile Ad hoc networks	Shuklaand Joshi,	2021	Blackhole attack	Introduced Scalable-Dynamic Elliptic Curve Cryptography and AODV Protocol Is Named As ECCAODV
27	Lightweight approach for secure backbone construction for MANETs.	Gaurav and Singh,	2021	Blackhole attack	The Proposed A Secure Backbone Construction For Securing MANET From Different Types Of Attack.
28	Detection and elimination of black hole attacks in mobile ad hoc networks	Mohanapriyaand Santhosh,	2021	Blackhole attack	Light Weight Solution Called SEC-DSR Protocol.
29	A fuzzy-based Cooperative Blackmailing Attack detection scheme for Edge Computing nodes in a MANET-IoT environment.	Simpsonand Nagarajan,	2021	Blackhole attack	Implemented A Fuzzy Based System To Tackle The Cooperative Black Mailing Attack In MANET-IoT.
30	The AODV routing protocol with built-in Security to counter blackhole attacks in MANET.	Reddyand Dhananjaya,	2022	Blackhole attack	The Proposed AODV-BS (Built-In Security)
31	Detecting wormhole attacks with physical-layer network coding	Li et al.	2011	Wormhole attack	A physical layer coding technique
32	Detection and avoidance of unified attacks on MANET using trusted secure AODV routing protocol.	Singh et al.	2016	Wormhole attack	Trusted AODV Routing Algorithm
33	Worm hole-black hole attack detection and avoidance in Manet with random PTT using FPGA	Kumar, K.A.	2016	Wormhole attack	FPGA for wormhole detection and avoidance
34	Defending against wormhole attacks in MANETs by using fuzzy logic and an artificial immune system.	Jamaliand Fotohi,	2017	Wormhole attack	Defending against wormhole attack
35	MultirateDelPHI to secure multi-rate ad hoc networks against wormhole attacks.	Qazi et al.	2018	Wormhole attack	M-De1PHI protocol, which protects the network from multi-rate transmission attacks.

DOI: https://doi.org/10.52756/10.52756/ijerr.2023.v31spl.016

36	A comparative study of reactive, proactive, and hybrid routing protocol in wireless sensor networks under wormhole attack.	Govindasamyand Punniakody,	2018	Wormhole attack	Comparative study of AODV, OLSR, and ZRP.
37	Confirmation of wormhole attack in MANETs using honeypot. *Computers & Security*	Tiruvakadu and Pallapa,	2018	Wormhole attack	Wormhole attack confirmation (WAC) system.
38	Detecting wormhole attacks in 3D wireless ad hoc networks via 3D forbidden substructures.	Bai et al.	2019	Wormhole attack	MaXIS- based for the detection of wormhole attacks in 3D networks by using only connectivity information
39	Wormhole attack in software-defined networking via building in-band covert channel.	Hua et al.	2020	Wormhole attack	Used link layer discovery protocol (LLDP) to mislead the attacker to attack the network.

Conclusion

In this research, we analysed a wide range of previous publications that have previously explored the topic of Mobile Ad hoc Networks (MANETs) and looked at several types of attacks. We classified attacks into groups and analyzed defenses against them. Some solutions, however, have flaws and vulnerabilities. The damage done to networks by these attacks is substantial. Wormhole, black hole, and sinkhole attacks are only a few of the ones that were studied, and they all have a major negative impact on network throughput and reliability. Because of its hostile character, the wormhole attack has emerged as a particularly dangerous threat in MANETs. Mobile ad hoc networks (MANETs) are a relatively new and promising kind of localised networked communication. Intruders looking to take advantage of vulnerabilities in their security mechanisms have therefore become more interested in them. Intruders use a variety of attack types with the long-term goal of depleting nodes and undermining network stability. Despite the broad assessment of potential defences in this comprehensive study, our research underscores the dynamic nature of attack, with attackers always inventing novel strategies to overcome old tactics. Future efforts in this sector must thus address the following imperative aspects:

- A compelling need for the deployment of a highly robust and trustworthy real-time attack detection system capable of rapidly identifying and thwarting new threats in MANET.
- The construction of a centralised audit authority, precisely built to meet the intrinsic security demands of MANET, assuring the network's integrity and trustworthiness.
- Pioneering the creation of a novel, lightweight encryption approach designed exclusively for MANET deployment. This type of innovation tries to reduce the significant energy consumption of nodes, hence conserving their battery life.
- The imperative pursuit of an optimum and dependable strategy for the selection of cluster heads inside MANET, a critical activity that has a considerable influence on the network's overall robustness and performance.

Conflict of interests

None

DOI: https://doi.org/10.52756/10.52756/ijerr.2023.v31spl.016

References

Alghamdi, R., & Bellaiche, M. (2023). A cascaded federated deep learning based framework for detecting wormhole attacks in IoT networks. *Computers & Security*, *125*, 103014.

Babaeer, H.A., & Al-Ahmadi, S.A. (2020). Efficient and secure data transmission and sinkhole detection in a multi-clustering wireless sensor network based on homomorphic encryption and watermarking. *IEEE Access*, *8*, 92098-92109. https://doi.org/10.1109/ACCESS.2020.2994587

Bai, S., Liu, Y., Li, Z. & Bai, X. (2019). Detecting wormhole attacks in 3D wireless ad hoc networks via 3D forbidden substructures. *Computer Networks*, *150*, 190-200. https://doi.org/10.1016/j.comnet.2019.01.008

Chang, J.M., Tsou, P.C., Woungang, I., Chao, H.C., & Lai, C.F. (2014). Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. *IEEE Systems Journal*, *9*(1), 65-75. https://doi.org/10.1109/JSYST.2013.2296197

Chavan, A.A., Kurule, D.S., & Dere, P.U. (2016). Performance analysis of AODV and DSDV routing protocol in MANET and modifications in AODV against black hole attack. *Procedia Computer Science*, *79*, 835-844. https://doi.org/10.1016/j.procs.2016.03.108

Dhaka, A., Nandal, A., & Dhaka, R.S. (2015). Gray and black hole attack identification using control packets in MANETs. *Procedia Computer Science*, *54*, 83-91. https://doi.org/10.1016/j.procs.2015.06.010

Eltahlawy, A. M., Aslan, H. K., Abdallah, E. G., Elsayed, M. S., Jurcut, A. D., & Azer, M. A. (2023). A Survey on Parameters Affecting MANET Performance. *Electronics*, *12*(9), 1956. https://doi.org/10.3390/electronics12091956

Gaurav, A., & Singh, A.K. (2021). Lightweight approach for secure backbone construction for MANETs. *Journal of King Saud University-Computer and Information Sciences*, *33*(7), 908-919. https:// doi.org/10.1016/j.jksuci.2018.05.013

Gopinath, S., Vinoth Kumar, K., & Jaya Sankar, T. (2019). Secure location aware routing protocol with authentication for data integrity. *Cluster Computing*, *22*(Suppl 6), 13609-13618.

Gothawal, D.B., & Nagaraj, S.V. (2019). Intrusion detection for enhancing RPL security. *Procedia Computer Science*, *165*, 565-572. https://doi.org/10.1016/j.procs.2020.01.051

Govindasamy, J., & Punniakody, S. (2018). A comparative study of reactive, proactive, and hybrid routing protocol in wireless sensor networks under wormhole attack. *Journal of Electrical Systems and Information Technology*, *5*(3), 735-744. https://doi.org/10.1016/j.jesit.2017.02.002

Hamedheidari, S., & Rafeh, R. (2013). A novel agent-based approach to detect sinkhole attacks in wireless sensor networks. *Computers & Security*, *37*, 1-14. https://doi.org/10.1016/j.cose.2013.04.002

Hammamouche, A., Omar, M., Djebari, N., & Tari, A. (2018). Lightweight reputation-based approach against simple and cooperative blackhole attacks for MANET. *Journal of Information Security and Applications*, *43*, 12-20. https://doi.org/10.1016/j.jisa.2018.10.004

Hua, J., Zhou, Z., & Zhong, S. (2020). Flow misleading: Wormhole attack in software-defined networking via building in-band covert channel. *IEEE Transactions on Information Forensics and Security*, *16*, 1029-1043. https://doi.org/10.1109/TIFS.2020.3013093

Jahandoust, G., & Ghassemi, F. (2017). An adaptive sinkhole aware algorithm in wireless sensor networks. *Ad Hoc Networks*, *59*, 24-34. https://doi.org/10.1016/j.adhoc.2017.01.002

Jamali, S., &Fotohi, R. (2017). DAWA: Defending against wormhole attacks in MANETs using fuzzy logic and an artificial immune system. *The Journal of Supercomputing*, *73*(12), 5173-5196. https://doi.org/10.1007/s11227-017-2075-x

Joardar, S., Sinhababu, N., Dey, S., & Choudhury, P. (2023). Mitigating DoS attack in MANETs considering node reputation with AI. *Journal of Network and Systems Management*, *31*(3), 1-34.

Khamayseh, Y.M., Aljawarneh, S.A., & Asaad, A.E. (2018). Ensuring survivability against Black Hole Attacks in MANETS for preserving energy efficiency. *Sustainable Computing: Informatics and Systems*, *18*, 90-100. https://doi.org/10.1016/j.suscom.2017.07.001

Khatoon, N., Pranav, P., & Roy, S. (2021). FQ-MEC: Fuzzy-Based Q-Learning Approach for Mobility-Aware Energy-Efficient Clustering in MANET. *Wireless Communications and Mobile Computing*, *2021*, 1-12. https://doi.org/10.1155/2021/8874632

Kim, G., Han, Y., & Kim, S. (2010). A cooperative-sinkhole detection method for mobile ad hoc networks. *AEU-International Journal of*

Electronics and Communications, *64*(5), 390-397. https://doi.org/10.1016/j.aeue.2009.01.008

Krishnakumar, V., & Asokan, R. (2023). An energy efficient and QoS routing protocol for MANET realised over multi-objective red deer algorithm (RD-MOCER) in support of emergency disaster management. *International Journal of Communication Systems*, *36*(1), e5349.

Kumar, K.A. (2016). Worm hole-black hole attack detection and avoidance in Manet with random PTT using FPGA. IEEE, In *2016 International Conference on Communication Systems and Networks (ComNet)*, pp. 93-98. https://doi.org/10.1109/CSN.2016.7823993

Kumari, A., Dutta, S., & Chakraborty, S. (2023). Use of Node credibility and Andrews plot to detect and prevent BHA in MANET. *International Journal of Experimental Research and Review*,*30*, 282-295. https://doi.org/10.52756/ijerr.2023.v30.026

Li, Z., Pu, D., Wang, W., & Wyglinski, A. (2011). Forced collision: Detecting wormhole attacks with physical layer network coding. *Tsinghua Science and Technology*, *16*(5), 505-519. https://doi.org/10.1016/S1007-0214(11)70069-4

Liu, Y., Ma, M., Liu, X., Xiong, N.N., Liu, A., & Zhu, Y. (2018). Design and analysis of probing route to defense sinkhole attacks for Internet of Things security. *IEEE Transactions on Network Science and Engineering*, *7*(1), 356-372. https://doi.org/10.1109/TNSE.2018.2881152

Nagalakshmi, T.J., Gnanasekar, A.K., Ramkumar, G., & Sabarivani, A. (2021). Machine learning models to detect the blackhole attack in wireless ad-hoc networks. *Materials Today: Proceedings*, *47*, 235-239. https://doi.org/10.1016/j.matpr.2021.04.129

Ngai, E.C., Liu, J., & Lyu, M.R. (2007). An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks. *Computer Communications*, *30*(11-12), 2353-2364. https://doi.org/10.1016/j.comcom.2007.04.025

Nguyen, H. L., & Nguyen, U. T. (2008). A study of different types of attacks on multicast in mobile ad hoc networks. *Ad Hoc Networks*, *6*(1), 32-46. https://doi.org/10.1016/j.adhoc.2006.07.005

Nguyen, H. L., & Nguyen, U. T. (2012). A study of different types of attacks in mobile ad hoc networks. *In 2012 25th IEEE Canadian Conference on Electrical and Computer Engineering* (CCECE), pp. 1-6. https://doi.org/10.1109/CCECE.2012.6335025

Pullagura, J. R., & Dhulipalla, V. R. (2023). Black-hole attack and counter measure in ad hoc networks using traditional routing optimization. *Concurrency and Computation: Practice and Experience*, *35*(9), e7643.

Qazi, S., Raad, R., Mu, Y., & Susilo, W. (2018). Multirate DelPHI to secure multi-rate ad hoc networks against wormhole attacks. *Journal of Information Security and Applications*, *39*, 31-40. https://doi.org/10.1016/j.jisa.2018.01.005

Rani, P., Verma, S., & Nguyen, G.N. (2020). Mitigation of black hole and gray hole attack using swarm-inspired algorithm with the artificial neural network. *IEEE Access*, *8*, 121755-121764. https://doi.org/10.1109/ACCESS.2020.3004692

Ranjan, R., Singh, N.K., & Singh, A. (2015). Security issues of black hole attacks in MANET. IEEE, In *International Conference on Computing, Communication & Automation*, pp. 452-457. https://doi.org/10.1109/CCAA.2015.7148419

Reddy, B., & Dhananjaya, B. (2022). The AODV routing protocol with built-in Security to counter blackhole attacks in MANET. *Materials Today: Proceedings*, *50*, 1152-1158. https://doi.org/10.1016/j.matpr.2021.08.039

Sanchez-Casado, L., Macia-Fernandez, G., Garcia-Teodoro, P., & Aschenbruck, N. (2015). Identification of contamination zones for sinkhole detection in MANETs. *Journal of Network and Computer Applications*, *54*, 62-77. https://doi.org/10.1016/j.jnca.2015.04.008

Sangaiah, A. K., Javadpour, A., Ja'fari, F., Pinto, P., Ahmadi, H., & Zhang, W. (2022). CL-MLSP: The design of a detection mechanism for sinkhole attacks in smart cities. *Microprocessors and Microsystems*, *90*, 104504.

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*.

Shafiei, H., Khonsari, A., Derakhshi, H., & Mousavi, P. (2014). Detection and mitigation of sinkhole attacks in wireless sensor networks. *Journal of Computer and System Sciences*, *80*(3), 644-653. https://doi.org/10.1016/j.jcss.2013.06.016

Sharma, V., Singh, H., Kaur, M., & Banga, V. (2013). Performance evaluation of reactive routing protocols in MANET networks using GSM based voice traffic applications. *Optik*, *124*(15).

Shim, W., Kim, G., & Kim, S. (2010). A distributed sinkhole detection method using cluster

analysis. *Expert Systems with Applications*, *37*(12), 8486-8491.
https://doi.org/10.1016/j.eswa.2010.05.028

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.

Simpson, S.V., & Nagarajan, G. (2021). A fuzzy-based Cooperative Blackmailing Attack detection scheme for Edge Computing nodes in a MANET-IOT environment. *Future Generation Computer Systems*, *125*, 544-563.
https://doi.org/10.1016/j.future.2021.06.052

Singh, U., Samvatsar, M., Sharma, A., & Jain, A.K. (2016). Detection and avoidance of unified attacks on MANET using trusted secure AODV routing protocol. In *2016 Symposium on Colossal Data Analysis and Networking (CDAN)*, pp. 1-6.
https://doi.org/10.1109/CDAN.2016.7570908

Sreelaja, N.K., & Pai, G.V. (2014). Swarm intelligence-based approach for sinkhole attack detection in wireless sensor networks. *Applied Soft Computing*, *19*, 68-79.
https://doi.org/10.1016/j.asoc.2014.01.015

Suma, S., & Harsoor, B. (2022). An approach to detect black hole attack for congestion control utilizing mobile nodes in wireless sensor network. *Materials Today: Proceedings*, *56*, 2256-2260.

Tahboush, M., & Agoyi, M. (2021). A hybrid wormhole attack detection in mobile ad-hoc network (MANET). *IEEE Access*, *9*, 11872-11883.

Tamilselvan, L., & Sankaranarayanan, V. (2007). August. Prevention of blackhole attack in MANET. *The 2nd International Conference on Wireless Broadband and Ultra-wideband Communications (AusWireless 2007)*, pp. 21-21.
https://doi.org/10.1109/AUSWIRELESS.2007.61

Tiruvakadu, D.S.K., & Pallapa, V. (2018). Confirmation of wormhole attack in MANETs using honeypot. *Computers & Security*, *76*, 32-49. https://doi.org/10.1016/j.cose.2018.02.004

Tseng, H.C., & Culpepper, B.J. (2005). Sinkhole intrusion in mobile ad hoc networks: The problem and some detection indicators. *Computers & Security*, *24*(7), 561-570.
https://doi.org/10.1016/j.cose.2005.07.001

Vigenesh, M., & Santhosh, R. (2019). An efficient stream region sink position analysis model for routing attack detection in mobile ad hoc networks. *Computers & Electrical Engineering*, *74*, 273-280.
https://doi.org/10.1016/j.compeleceng.2019.02.005

Zhang, F.J., Zhai, L.D., Yang, J.C., & Cui, X. (2014). Sinkhole attack detection based on redundancy mechanism in wireless sensor networks. *Procedia Computer Science*, *31*, 711-720.
https://doi.org/10.1016/j.procs.2014.05.319

How to cite this Article:

Ankita Kumari, Sandip Dutta and Soubhik Chakraborty (2023). A comparative study of different security issues in MANET. *International Journal of Experimental Research and Review*, *31*, 168-185.

DOI : https://doi.org/10.52756/10.52756/ijerr.2023.v31spl.016