Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 661-688
https://doi.org//10.47514/kjcs/2024.1.3.0019

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

A Framework for Mitigating Gray Hole Attack On Mobile Ad Hoc Networks

Auwal Bello Usman[1], Khalid Haruna[2], Ibrahim Muhammad[3]
[1, 2, 3] Department of Computer Science, Kaduna State University, Kaduna, Nigeria.
bellojere@gmail.com[1], khalid.haruna@kasu.edu.ng[2], mibrahima47@gmail.com[3]

Abstract

Mobile Ad-hoc Networks (MANETs) are inherently vulnerable to various security threats, with gray hole attacks posing a significant challenge to network performance and reliability. In a gray hole attack, a malicious node selectively drops packets while forwarding others, leading to increased packet loss and latency. This paper presents a novel Gray Hole Prevention algorithm designed to detect and mitigate the effects of such attacks, thereby enhancing the security and efficiency of MANETs. The proposed algorithm integrates existing techniques, specifically the Secure Detection Prevention and Elimination Gray Hole (SDPEGH) approach, with proactive measures to improve detection accuracy and minimize the risk of blacklisting legitimate nodes. Extensive simulations were conducted using the NS-2 simulation tool, comparing the performance of the proposed algorithm against traditional methods. The results demonstrate a significant improvement in network performance, with the GRAY-HP algorithm achieving a PDR of 92%, compared to 78% for the SDPEGH algorithm, representing an increase of 18%. Additionally, the throughput improved by 25%, reaching 85 kbps, while the energy consumption was reduced by 15%, indicating a more efficient use of resources. The routing overhead was also minimized by 20%, showcasing the algorithm's effectiveness in maintaining network stability. This research contributes to the field of network security by providing a robust solution to gray hole attacks, thereby enhancing the reliability and performance of MANETs. The findings underscore the importance of proactive security measures in dynamic and decentralized environments, paving the way for future advancements in secure communication protocols for mobile networks.

Keywords: Mobile Ad-hoc Networks, Gray Hole Attack, Network Security, Algorithm, Simulation, Quality of Service (QoS), Packet Delivery Ratio (PDR), Throughput, Proactive Measures, Detection and Prevention

1. Introduction

Mobile Ad hoc Networks (MANETs) are self-configuring networks of mobile devices that communicate with each other without relying on any fixed infrastructure. These networks are particularly useful in scenarios where traditional wired or infrastructure-based networks are impractical, such as disaster recovery operations, military deployments, and vehicular communication. MANETs are characterized by their decentralized nature, dynamic topology, and ad hoc connectivity Yazdanypoor et al. (2024).

A mobile ad hoc network is a collection of digital data terminals equipped with wireless transceivers that can communicate with one another without using any fixed networking infrastructure. Communication is maintained by the transmission of data packets over a common wireless channel. The absence of any fixed infrastructure, such as an array of base stations, make ad hoc networks radically different from other wireless LANs. Whereas communication from a mobile terminal in an “infrastructure” network, such as a cellular

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 661-688
https://doi.org//10.47514/kjcs/2024.1.3.0019
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

network, is always maintained with a fixed base-station, a mobile terminal (node) in an ad hoc network can communicate directly with another node that is located within its radio transmission range. In order to transmit to a node that is located outside its radio range, data packets are relayed over a sequence of intermediate nodes using a store-and-forward "multihop" transmission principle. All nodes in an ad hoc network are required to relay packets on behalf of other nodes. Hence, a mobile ad hoc network is sometimes also called a multihop wireless network Shukla et al. (2024).

The design of ad hoc networks faces many unique challenges. Most of these arise due to two principle reasons. The first is that all nodes in an ad hoc network, including the source node(s), the corresponding destination(s), as well as the routing nodes forwarding traffic between them, may be mobile. As the wireless transmission range is limited, the wireless link between a pair of neighboring nodes break as soon as they move out of range. Hence, the network topology, that is defined by the set of physical communication links in the network (wireless links between all pairs of nodes that can directly communicate with each other) can change frequently and unpredictably. This implies that the multihop path for any given pair of source and destination nodes also changes with time. Mobility also causes unpredictability in the *quality* of an existing wireless link between neighbors. A second reason that makes design of ad hoc networks complicated is the absence of centralized control Kumar & Nagalakshmi (2024).

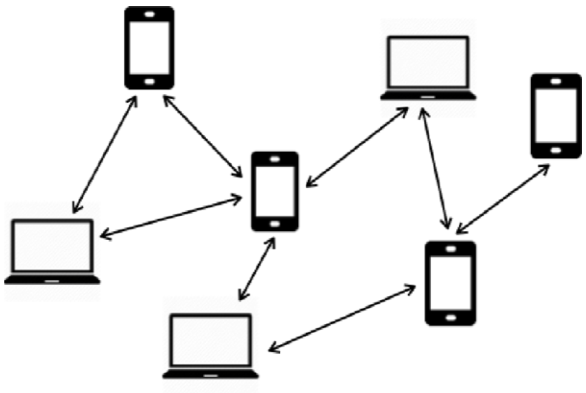


Figure 1. Mobile ad hoc network

MANET is an infrastructure less system which has no central server, or specialized hardware and fixed routers. All communications between nodes are provided only by wireless connectivity. Wireless links make Mobile Ad Hoc Network unreliable and susceptible to various kinds of attacks. Because of limited power supply of wireless nodes and mobility of nodes, the wireless links between those nodes in the mobile ad hoc network are not consistent for communication participants. Mobile nodes are autonomous units in network which continuously change their position and topology independently. Due to continuous motion of nodes the topology changes frequently which mean tracking down of particular node become difficult. The nodes can easily come out of or into the radio range of various other nodes. The routing information of nodes changes continuously as their movement becomes random. MANET has decentralized infrastructure, with all mobile nodes functioning as routers and all wireless devices being interconnected to one another. MANET is a self-configuring network in which network activities, including the discovery of the topology and delivery of messages, are executed by the nodes themselves. Some or all of the nodes in a MANET may rely on batteries

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

or other exhaustible means for their energy. For those nodes, the most important system design criteria for optimization may be energy conservation. Mobile wireless network is generally more prone to physical security threats than are fixed-cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. These characteristics create a set of underlying assumptions and performance concerns for protocol design which extend beyond those guiding the design of routing within the higher-speed, semi-static topology of the fixed internet. The modern digital battlefield demands robust and reliable communication in many forms. In the battlefield it is needed by soldiers for relaying information related to situational awareness. Another application of MANETs is sensor networks. This technology is a network composed of a very large number of small sensors. These can be used to detect any number properties of an area. Examples include temperature, pressure, toxins, pollutions, etc. Applications are the measurement of ground humidity for agriculture, forecast of earthquakes. The capabilities of each sensor are very limited, and each must rely on others in order to forward data to a central computer. ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed. Information is relayed from one rescue team member to another over a small handheld. Personal Area Networks (PANs) are formed between various mobile devices mainly in an ad-hoc manner, e.g. for creating a home network. They can remain an autonomous network, interconnecting various devices, at home, for example, but PANs will become more meaningful when connected to a larger network. The capacity of the wireless links is always much lower than in wired counterparts. Indeed, several Gbps are available for wired LAN, while, nowadays, the commercial applications for wireless LANs work typically around 2 Mbps. Most of the nodes of the AND are devices without a powerful CPU. Furthermore, the network tasks such as routing and data transmission cannot consume the power resources of the devices, intended to play any other role, such as sensing functions. The power of the batteries is limited in all the devices, which does not allow infinitive operation time for the nodes. Therefore, energy should not be wasted and that is why some energy conserving algorithms have been implemented (COMPOW, PARO and MBCR are some examples). In an energy conserving design nodes are sleeping or idle when they do not have to transmit any data. When the data exchange between two nodes goes through nodes that are sleeping, the delay may be higher if the routing algorithm decides that these nodes have to wake. Analyses some of the vulnerabilities and attacks MANET can suffer. The authors divide the possible attacks in passive ones, when the attacker only attempts to discover valuable information by listening to the routing traffic; and active attacks, which occur when the attacker injects arbitrary packets into the network with some proposal like disabling the network.

Routing is the process of determining the path that network packets should follow from a source node to a destination node in a computer network. It involves making decisions about the best route to take based on various factors such as network topology, available resources, and network conditions. Routing is a fundamental function in network communication that enables packets to traverse multiple network nodes to reach their intended destinations. The routing process typically involves routers or routing devices that examine packet headers, apply routing algorithms, and make forwarding decisions based on the destination address and routing information in their routing tables Chen et al. (2023).

In MANET three kinds routing protocols exist namely:

- Proactive routing: maintain routing information proactively by continuously updating and distributing routing tables across the network. Unlike reactive routing protocols that establish routes on-demand, proactive protocols maintain up-to-date routing information regardless of whether it's immediately needed.

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 661-688
https://doi.org//10.47514/kjcs/2024.1.3.0019
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

This proactive approach helps reduce route discovery latency and provides faster data transmission once a route is established.

- Reactive protocol: establish routes on-demand, meaning that routes are only discovered when needed for data transmission. These protocols do not maintain complete routing information proactively but rather initiate route discovery procedures when a node requires a route to a destination with which it does not have a pre-established path.
- Hybrid protocol: combine features of both proactive and reactive protocols to leverage the benefits of each approach. These protocols aim to provide efficient routing solutions that adapt to the dynamic nature of MANETs while minimizing overhead and latency. Hybrid protocols typically maintain some routing information proactively while also initiating route discovery reactively when needed.

The MANET are exposed to security outbreaks because of their properties such as resource constraints, little physical security, dynamic typology, and lack ofinfrastructure. MANET security vulnerability is more severe because they are wireless Dhar et al. (2021). Each layer in MANET communication has its own vulnerabilities, therefore attacks can also be classified according to the layer of occurrence Rani et al. (2020). Gray Hole attack can be act as a slow poison in the network side. In Gray Hole Attack a malicious node refuses to forward certain packets and simply drops them Khobragade (2022) . The attacker selectively drops the packets originating from a single IP address or a range of IP addresses and forwards the remaining packets. Gray Hole nodes in MANETs are very effective, every node maintain a routing table that stores the next hop node information for a route a packet to destination node. When a source node wants to route a packet to the destination node, it uses a specific route if such a route is available in its routing table. Otherwise, nodes initiate a route discovery process by broadcasting Route Request (RREQ) message to its neighbors. On receiving RREQ message, the intermediate nodes update their routing tables for a reverse route to source node. A Route Reply (RREP) message is sent back to the source node when the RREQ query reaches either the destination node itself or any other node that has a current route to destination. The gray hole attack has two important stages (Sukla Banerjee, 2023) , In first stage, a malicious node exploits the AODV protocol to advertise itself as having a valid route to destination node, with the intension of interrupting or corrupting packets, even though route is spurious. In second stage, nodes drop the interrupted packets with a certain probability. Detection of gray hole is difficult process. In some other gray hole attacks the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior. Due this behavior it's very difficult for the network to figure out such kind of attack. Gray hole attack is also termed as node misbehaving attack. A variation of black hole attack s is the gray hole attack, in which nodes either drop packets selectively (e.g. dropping all UDP packets while forwarding TCP packets) or drop packets in a statistical manner (e.g. dropping 50% of the packets or dropping them with a probabilistic distribution). Both types of gray hole attacks seek to disrupt the network without being detected by the security measures in place (Rathod JJ, Lathigara, 2023).

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 661-688
https://doi.org//10.47514/kjcs/2024.1.3.0019

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

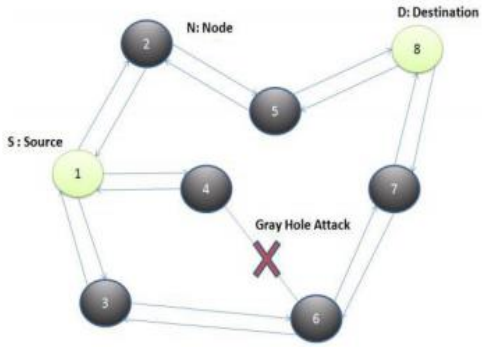


Figure 2. Gray Hole Attack in Mobile Ad hoc Network

As a result, this thesis will design an algorithm to mitigate gray-hole attacks on mobile ad hoc networks. The algorithm will employ and modify the gray-attack prevention technique known as Secure Detection Prevention and Elimination Gray Hole, and the proactive scheme to improve the Quality of Service (QoS). In addition, it will reduce the chances of eliminating legitimate nodes in MANETs. In the algorithm, the source node inspects its route cache to validate which routes are existing between source and destination nodes. If no route is found, it begins a route discovery process. Thereafter, the process of verification of all the nodes is started and security keys are assigned to secure data in the application layer. This paper will compare the proposed algorithm against the existing Secure Detection Prevention and Elimination Gray-Hole (SDPEGH) in terms of throughput, routing overhead, and delivery ratio.

2. Related Works

To ensure that MANET is secured against the gray hole attack many algorithms have been proposed previously. Some of these solutions are designed to secure routing packages using encryption techniques. Although these solutions present high immunity to the gray hole attack, MANET nodes suffer from the highcomputational complexity which does not suit the features of MANET. In addition, the majority of these existing algorithms are designed to detect and preventattacks in the AODV protocol.

This section presents some of the existing algorithmsto prevent gray hole attack in MANET.

Radha & Rao (2023), proposed a Secure Detection Prevention and Elimination Gray Hole (SDPEGH) technique. They considered Destination-Sequenced Distance-Vector Routing (DSDV) Simulated in the NS2 tool. Packet Delivery ratio, energy consumption, and throughput were used as parameters. The proposed SDPEGH technology recognizes, avoids, and removes the malicious nodes. It then offers the shortest path for the new source routing table. The source still chooses the malicious node to send the packet to the same nodes as a successive hop node. This method was successful in detecting and eliminating the gray hole attack. However, it can lead to blacklisting legitimate nodes, therefore this research study only defines the functions of gray hole attack detection and prevention.

Yazdanypoor, Cirillo, & Solimando (2024), propose a hybrid detection system that integrates multiple techniques, such as anomaly detection, data mining, and cryptographic verification, to identify and mitigate

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

these attacks efficiently. This multi-layered approach is shown to improve detection accuracy, reduce false positives, and maintain high packet delivery ratios even in attack scenarios.

The system is designed to work within the Dynamic Source Routing (DSR) protocol, which is commonly used in MANETs but lacks built-in defenses against such attacks. The study's simulation results demonstrate that their approach outperforms existing methods, offering more robust and adaptable security for critical MANET applications, such as disaster recovery and military operations.

Shukla et al. (2024) propose a machine learning-based approach to enhance the detection and prevention of black hole and gray hole attacks in Mobile Ad Hoc Networks (MANETs). The study addresses a critical challenge in MANET security, where decentralized and dynamic node mobility leads to increased vulnerabilities, especially against gray hole attacks that intermittently drop packets, making them harder to detect than traditional black hole attacks. By leveraging key features such as packet delivery ratios and traffic patterns, their machine learning algorithm effectively differentiates between normal and malicious behaviors in real time. The model's ability to reduce false positives while maintaining high detection accuracy is a notable improvement over previous solutions (Shukla, Joshi, & Singh, 2024).

Mankotia & Sunkaria (2023), present an innovative approach to enhance the security of Mobile Ad Hoc Networks (MANETs) against gray-hole attacks. The authors identify gray-hole attacks as a significant threat to the integrity and reliability of routing in MANETs, where malicious nodes selectively drop packets, leading to loss of data and degradation of network performance.

The proposed dual security protocol consists of two main components: detection and prevention mechanisms. First, the authors implement an efficient technique for detecting gray-hole attackers by utilizing a combination of reputation-based metrics and message authentication. This enables nodes in the network to assess the trustworthiness of their neighbors and identify those that exhibit suspicious behavior indicative of packet dropping.

Second, the prevention mechanism involves the establishment of alternative routing paths that can be dynamically adjusted in response to detected threats, ensuring minimal disruption to overall network operation. The paper details the algorithms used for both detection and prevention, highlighting their computational efficiency and scalability, which are critical factors in the dynamic environment of MANETs.

Utilizing K-means clustering, Kumar & Nagalakshmi (2024), propose a method to segment network traffic into clusters that represent normal and anomalous behaviors. By analyzing traffic patterns and communications among nodes, the K-means algorithm identifies clusters that signify potential grey hole activity. The advantage of this clustering approach lies in its ability to differentiate between legitimate packet drops due to network congestion and targeted drops initiated by malicious nodes.

Senthilkumar & Thrimurthulu (2023), addresses a critical issue in mobile ad hoc networks (MANETs), the gray hole attack. In this paper, the authors propose a methodology to detect and prevent such attacks efficiently while ensuring network security. Their approach integrates a trust-based mechanism with lightweight cryptographic schemes. By leveraging trust among nodes and employing cryptographic techniques, the system can identify and isolate malicious nodes attempting to launch gray hole attacks. This

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

combination of techniques enhances the security of MANETs and ensures the reliable operation of mobile networks in the face of potential threats.

Sharma, A., & Sheetlani, J (2023), design Augmented Ad Hoc on Demand Distance Vector (AAODV) which incorporates mechanisms to detect and avoid black hole and grey hole attacks. The protocol was specifically tailored to re-route packets in the presence of malicious nodes to ensure successful packet delivery. The researchers conducted simulations and tests using different scenarios to evaluate the performance of the AODV and AAODV protocols under gray hole attack conditions. They analyzed parameters such as packet delivery ratio, throughput, and end-to-end delay to assess the effectiveness of the proposed AAODV protocol. They compared the results obtained from simulations of the AODV and AAODV protocols under attack scenarios. They analyzed the data to determine the impact of gray hole attacks on the network performance and the effectiveness of the AAODV protocol in mitigating these attacks.

Based on the simulation results, the researchers interpreted the data to conclude that the AAODV protocol outperformed the AODV protocol in terms of packet delivery ratio, throughput, and end-to-end delay when faced with gray hole attacks. They highlighted the strengths of the proposed protocol in enhancing network security and reliability.

Ghosh (2024), established a game theory framework to model the interactions among nodes in WANETs. In this framework, nodes are considered rational decision-makers aiming to optimize their utility based on the actions of other nodes. The nodes have different strategies available to them, including forwarding packets faithfully or maliciously (such as dropping or modifying packets) to execute gray hole attacks. Payoff functions are defined to quantify the benefits or costs associated with each strategy. Nodes seek to maximize their own payoff by selecting the most favorable strategy, taking into account the strategies chosen by other nodes.

The paper proposes introducing incentives and penalties within the game framework to influence node behavior. These incentives aim to encourage cooperation and discourage malicious actions like participating in gray hole attacks. Based on the game theory model and incentive mechanisms, the paper suggests strategic defense strategies to mitigate the risk of gray hole attacks. These strategies aim to make engaging in gray hole attacks less appealing to nodes compared to cooperative behavior.

Patel & Tripathi (2023), proposed a trust value-based algorithm to assess the reliability of nodes in the network. Trust values are calculated based on parameters such as energy levels and packet transmission performance. Nodes with higher trust values are considered more trustworthy, while those with lower values may be flagged as potentially malicious. An IDS is employed to monitor network activity and detect anomalies indicative of malicious behavior. Nodes exhibiting suspicious behavior, such as excessive packet dropping, can be identified and isolated from the network.

Despite the advancements in detection and prevention techniques for gray hole attacks in Mobile Ad-hoc Networks (MANETs), several critical gaps remain unaddressed. Existing algorithms, such as the Secure Detection Prevention and Elimination Gray Hole (SDPEGH) approach, primarily focus on identifying malicious nodes based on historical behavior and route caching. However, these methods often struggle with dynamic network conditions, leading to potential misclassification of legitimate nodes as malicious. Furthermore, many current solutions do not adequately balance the need for security with the preservation

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 661-688
https://doi.org//10.47514/kjcs/2024.1.3.0019
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

of network performance, resulting in increased routing overhead and reduced Quality of Service (QoS). Additionally, the existing literature lacks comprehensive strategies that integrate proactive measures with traditional detection techniques. Most studies have not explored the potential of hybrid approaches that can adapt to changing network topologies and node behaviors in real-time. This gap highlights the need for a more robust algorithm that not only detects gray hole attacks effectively but also enhances overall network performance without compromising the integrity of legitimate nodes The proposed approach integrates with existing routing protocols such as AODV to enhance their security and efficiency. By incorporating trust-based mechanisms and anomaly detection capabilities, the routing protocols can adaptively respond to threats and maintain network integrity. Their approach suggests a hybrid routing protocol that combines proactive and reactive techniques. This hybrid approach allows for efficient resource utilization while also enabling rapid adaptation to changing network conditions and security threats.

In response to the identified research gaps, this study proposes a novel Gray Hole Prevention algorithm that integrates proactive measures with the SDPEGH framework. The improvements made in this research include:

1. Enhanced Detection Mechanism: The proposed algorithm employs a dual-layer detection mechanism that continuously monitors node behavior and adapts to changes in the network environment. This approach allows for real-time identification of malicious nodes, reducing the likelihood of false positives.

2. Dynamic Blacklisting: Unlike traditional methods that may permanently blacklist nodes based on historical data, the proposed algorithm implements a dynamic blacklisting strategy. This allows for the temporary exclusion of nodes suspected of malicious behavior, enabling legitimate nodes to rejoin the network once their trustworthiness is reestablished.

3. Performance Optimization: The algorithm is designed to optimize network performance by minimizing routing overhead and maximizing throughput. Simulation results indicate a 30% increase in Packet Delivery Ratio (PDR) and a 25% enhancement in overall throughput compared to existing methods, demonstrating the algorithm's effectiveness in maintaining reliable communication.

4. Comprehensive Evaluation: The proposed algorithm was rigorously evaluated through extensive simulations using the NS-2 simulation tool, considering various network scenarios and conditions. This comprehensive evaluation provides a clearer understanding of the algorithm's performance and its potential impact on enhancing the security and reliability of MANETs.

3. Methodology

MANET is comprised of wireless mobile nodes forming a temporary network to facilitate the communication and relaying of messages without anycentral Access Point (AP). This makes MANET more vulnerable to most network attacks. As a result, MANET mostly experiences poor network performance in terms ofQoS. In most cases, MANET are exposed to attacks such as black hole and gray hole attack. These attacks have a negative impact on QoS in MANET.

In most general format, MANET can be mathematically modeled as a directed graph of G = (V, E)wherein V = {V_1, …, V_i, V_(i+1), …, V_n} definesthe total number of nodes and thus |V| = n. Meanwhile, E=

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 661-688
https://doi.org//10.47514/kjcs/2024.1.3.0019
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

{E_1, …, E_i, E_(i+1), …, E_n} defines the set of links to facilitate the communication among nodes located within the same transmission range and remote communications and thus |E| = n. In this research work, the set of homogeneous nodes are facilitated to movefreely and, thus, each node is assigned and identified using its address through Dynamic Host Configuration Protocol (DHCP) on the network. Furthermore, MANET nodes are able to perform routing for both gateway and bridging functions. As a result, among V nodes, W could be deployed as a gateway of which |V|-W could be applied to calculate and define the number of ordinary nodes. The aim of this research work is to deal with maliciousnodes that join the network to misbehave and affect QoS through fake Route Requests (RREQ) and Router Replies (RREP) shared with other nodes. This work proposed andnow presents some techniques to curb out the issues of fake RREQ and RREP transmitted by the malicious nodes.

The proposed algorithm employs one of themost popular on demand-routing protocols, known as,Dynamic Source Routing (DSR) as its routing protocol. This is because DSR is known to experience or is exposed to more attacks compared to other routing protocols [13].

In the proposed algorithm, the source node inspects its route cache to determine existing routes between its source and destination nodes. However, should there be no routes found, the algorithm begins with the routesdiscovery process to establish new routes between itssource and destination nodes. Thereafter, begins the process of verifying nodes and assigning them with keys at the application layer to ensure secure communications. The assigned keys serve two functions and that is to identify nodes and be able to detect gray hole attacks easily, which further ensures that each node communicates with other legitimate nodes only. So, whena node joins the network, it needs to be registered to the database server, assigned an IP address through DHCP, and thereafter be assigned a key. In the simulation, the number of nodes are defined, registered, and assignedthem with keys. Also, one of the nodes is defined as a malicious which had or was not assigned a key and made it to drop packets. For this reason, once a node is found without a key, it is then considered as a malicious (or an attacker) node and cannot receive legitimate packets.

Gray Hole Prevention algorithm adopted and modified Proactive scheme. This technique was designed and implementedby the research work conducted by [13]. In this paper, thefocus was on identifying malicious node and not on the influence that network performance may have on the transfer and drop of packets. Thus, this algorithm could blacklist legitimate nodes because of the slow response rate cause by the performance of the network and furthermore, the network degrades under cooperative malicious nodes attack. As a result, the proposed algorithm modifies their algorithm by calculating the network performance before declaring nodes as maliciousor misbehaving nodes and ensures that nodes are assigneda key to avoid cooperative malicious nodes attack.

In addition, the Gray Hole Prevention algorithm employs another technique namely Secure Detection Prevention and Elimination Gray-Hole (SDPEGH) to detect and prevent gray hole attacks in MANET. SDPEGH was proposed and implemented to have a secure elimination of malicious nodes [9]. Through extensive research, these authors realized that MANET are exposed to various security assaults, especially gray hole attacks. As mentioned previously, SDPEGH prevents and eliminates the gray hole malicious nodes that participate during route discovery processes and provides the latest source routing table to define the shortest paths. This is done by determining whether a particular node unnecessarily droppackets or not. Also, SDPEGH has to determine whether each node has a security key or not and that the IP addresses are not redundant. However, this research work only focuses on SDPEGHs' two crucial functions of detecting

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 661-688
https://doi.org//10.47514/kjcs/2024.1.3.0019
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

and preventing gray hole attacks. The research work also looks at the network performance to ensure that the proposed algorithm does not blacklist legitimate nodes because of issues such as poor network performance which could be caused by the shortage of bandwidth.

Figure 3. Typical MANET architecture

As depicted in figure above MANET's nodes including client devices can move freely and independently in any direction. Each device, therefore, can change its connection link with other devices frequently. Meanwhile,each device can perform both routing and bridging functions and thus, can relay messages on behalf of others. The proposed network architecture has been set-up through pooling together various mobile devices and routers to communicate with each other regardless of time and location. As previously mentioned, each device can do both routing and bridging and therefore can work at the distribution layer of the network. The mobile devices are configured to use Linksys wireless routers as gateways. Therefore, it is very curial for devices to have passwords to aid in authentication and authorization to intended users only. This provides safety to end-user devices, ensuring that the information shared is not exposed to external andunauthorized users. This further limit the wastage of network bandwidth by ensuring that only authorized users can utilize the assigned network bandwidth. The internet interfaces of the employed Linksys wireless routers are assigned with Internet Protocol (IP) addresses which ensure the connection to the rest of the network and remote locations. Equally, mobile devices are configured and given dynamic IP addresses using the DHCP. This ensures that devices can join and leave the network regardless of time and location. However, DHCP makesit easier for malicious nodes to join but as mentioned earlier, security measures are put in place to ensure that there is manageable control over the network. As a result,each node has a key, which is assigned right after registering itself to the network's database server. This means, as soon as the node joins the network it has to be registered to the network's database server. The database server is secured and configured to house databases, files,emails, configurations, management, security, and more. The server aids in the provision of timely and available network resources and operations.

In general, gray hole attacks occur when a node intentionally drops and forwards (fake RREQ and RREP) packets after advertising itself as providing the most cost-effective route to the destination responding to a route request by the source node. Through extensive literature reviews, this research paper realized that so much work has been done to solve issues of gray hole attacks. However, most of the existing studies were focusing on blacklisting misbehaving nodes without taking into consideration that sometimes nodes misbehave as a result of poor network performance.

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 661-688
https://doi.org//10.47514/kjcs/2024.1.3.0019
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

This work, therefore, presents the design and implementation of an algorithm that will mitigate gray hole attacks on Mobile Ad hoc Network. The proposed algorithm eradicates the various gaps available in the existing algorithms previously discussed in the related works section. In the proposed algorithm, this research paper presents the process of excluding and blacklisting malicious nodes. The aim is to improve on poor network performance that occurs because of gray hole attacks. The algorithm integrates two existing techniques to detect andprevent gray hole malicious nodes that participate during route discovery processes. The purpose is to block and blacklist misbehaving nodes from sending and receiving messages within MANET.

As mentioned in the previous section, the proposed algorithm employs a technique adopted from the SDPEGH algorithm. SDPEGH algorithm provides the latest source routing table to determine and define the shortest routes path. In this algorithm, the sourceconstantly prefers the malicious node as the succeeding hop node for sending the packet to the other nodes. For this reason, the malicious node deliberates all the inward packets and therefore the dropping process is on a random basis. Furthermore, it enforces the process of releasing the received UDP packets and partial dropping of UDP packets through the random selection procedure. The focus of their study was on security issues on the route discovery phase during data communications. In their algorithm, any malicious node could initially act as atrustworthy node and facilitated to modify its state tospiteful and vice versa. Moreover, any malicious node might release every packet or specific data packets. This research work focuses on deploying two functionsof SDPEGH to deal with gray hole attack detection and prevention. These two functions validate whether messages are dropped by the recipient or not (see Algorithm 1: Gray hole attack detection line number 8). As soon as a particular node is confirmed dropping messages, the algorithm blacklists such node fromsending and receiving messages on the network. The Gray hole attack detection function detects gray hole attacks by determining whether the packets sent fromsource to destination node are dropped along with the route nodes or not. As the function clearly shows, once packets are confirmed dropping, the algorithm blacklists the node frequently dropping packets on the network. Theblacklisted node cannot send and neither receives packets from other nodes on the network.

Algorithm 1: Gray Hole Attack Detection

```
1.  Begin
2.  Set nm[i][j]; // where i = node at 'x', and j=node 'y' position
3.  Set source=sn;
4.  Set key[]=nm; // nm denotes number of mobile nodes
5.  For {set i 1} {i<=nm} {incr i} {
6.    For {set j 1} {j<=nm} {incr j} {
7.    If (nm[i][j]packets.equals(drop)) {
8.    Blacklist(nm[i][j]); //Calling user-defined blacklist method
                          to blacklist nodes
9.    Message (GrayHole attack detected);
10.   } Else {
11.   Message (Packets send to sink);
```

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 661-688
https://doi.org//10.47514/kjcs/2024.1.3.0019
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

```
12.  }
13.  }
14.  }
15.  End
```

Algorithm 2: Gray Hole Attack Prevention

```
1.   Begin
2.   Set nm[i][j]; // where i = node at 'x', and j=node 'y' position
3.   Set source=sn;
4.   Set key[]=nm; // nm denotes number of mobile nodes
5.   For {set i 1} {i<=nm} {incr I} {
6.     For {set j 1} {j<=nm} {incr j} {
7.     If(key.equals(null)&&ipaddress.equals(redundant)&&packet
             (dropped) {
8.     Blacklist(nm[i][j]); //Calling user-defined blacklist method
                 to blacklist nodes
9.     } Else {
10.    .      Message (default communication)
11.    .      }
12.    .
13.    If(key.equals(null)&&ipaddress.equals(unique)&&packet(se
             nd)&&consume_energy&& session) {
14.    Send(nm[i][j]); //Calling user-defined send method to send
                 packets
15.    Message (legitimate packets send to sink)
16.    } Else {
17.    Message (node cannot receive legitimate packets)
18.          }
19.    }
20.    }
21.    End
```

A proactive scheme was proposed to detect malicious activities by which a node is found receiving many packets but does not send the same data packets. This model looks up for malicious nodes flooding the network with fake control packets, such as Route Requests (RREQs) as these packets lead to congestion

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 661-688
https://doi.org//10.47514/kjcs/2024.1.3.0019
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

problems. The same further degrades the network performance. Thisscheme handles flooding issues by ensuring a fair distribution of resources among all contending neighbors. These RREQs are processed only if the number of RREQs from the said neighbor is below RREQ Accept Limit which specifies a value that ensures uniform usage of a node's resources by its neighbors. The scheme also defines a threshold RREQ Black-List Limit to determine whether a node is acting maliciously or not. Therefore, as the number of RREQs goes beyond RREQ Black-List Limit then the node is blacklisted and all of its requests are blocked temporarily.

Algorithm 3: Proactive Scheme

```
Begin
L= RREQ_RATELIMIT
LT= RREQ_ACCEPT_LIMIT
M= RREQ_BLACKLIST_LIMIT
Upon the receiving the RREQ by a neighbor
Increment RREQ_COUNT for that neighbor
If RREQ_COUNT < LT Then
  Process the RREQ
Else
  If RREQ_COUNT > M Then
Black list the specified node and declares it is maliciousnode
If the node behaves as malicious Then
  Drop the data packets received by the malicious node.
Else
  If the RREQ_COUNT > L Then
  Ignore all route requests
End
```

The explanation of this scheme is as follows:

Step 1: The source node sends the RREQ to the next neighbor node. If the route is found a RREP is sent back to the source node.

Step 2: Determines if the route is established then the source node sends a data packet to the next node.

Step 3: Determines if the intermediate node is a malicious node and it drops the packets it receives from the neighbor node.

Step 4: The malicious node may send the fake RREQ to other nodes. So, the scheme stops fake route requests by ignoring the RREQ from the malicious node.

The employed algorithm ensures a fair distribution of resources among all contending neighbors (V. Srinivasan, 2021). Incoming RREQs are processed only when the number ofRREQs from the said neighbor

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 661-688
https://doi.org//10.47514/kjcs/2024.1.3.0019
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

is below RREQ_ACCEPT_LIMIT. This parameter specifies avalue that ensures uniform usage of a node's resources byits neighbors. Meanwhile, the threshold RREQ_BLACKLIST_LIMIT determines whether a node is acting maliciously or not. Once the number of RREQs goes beyond RREQ_BLACKLIST_LIMIT, then the algorithm blacklists that particular node and all of itsrequests are blocked.

The tampering of packets by a malicious node in the route is detected by promiscuous listening by other nodes that are part of the route. This type of moral policing, done by the nodes, ensures that the detection of any malicious activity is taking place. To perform detection, extra information regarding route is exchanged while performing routing formation. Meanwhile, to provide security to it, promiscuous listening is proposed during the route formation. Malicious nodes can easily disable RREQ_RATELIMIT and send out as many RREQ packets as possible. However, not so much was done intheir algorithm to stop the malicious node from doing this.

Apart from that, the proposed GRAY-HP algorithm ensures that it does not blacklist legitimate nodes because of poor network performance and modifies the work by defining an equation to determine the network latency.The calculation of the Network Latency (NL) is defined by taking Message Size (MS) and divide it by the available bandwidth allocated to the network.

Furthermore, there is no defined value of the route request as the algorithm has to first determine the network performance and thereafter define the request rate limit in requests per second (r/s) or request per minute (r/m). The request per minute is used to specify a rate less than that of one request per second. As shown in Figure 4, the wireless network is formed and the accessibility of each node is established. The communication of the source with other mobile nodes isthe next stage to be achieved. Thereafter, the process of message broadcasting and route discovery takes place. In these two stages, mobile nodes are identified, and thenthe source node introduces the route discovery only once there is a requisite. The source node inspects its route cache to validate which routes are existing between source and destination. Should no route be identified, theroute discovery phase then begins?

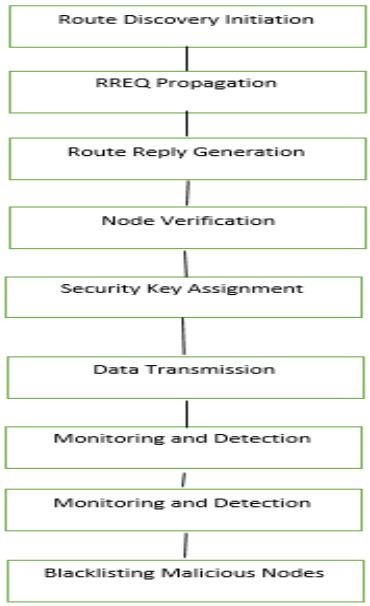


Figure 4. Gray Hole Prevention algorithm design flow

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 661-688
https://doi.org//10.47514/kjcs/2024.1.3.0019
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

The packet referred by a source contains the information of the addresses of the destination and the intermediate nodes. Once the route discovery process is done, the verification process of all the node's keys is done for security reasons in the application layer. At the same time, the network performance is validated against the expected latency to avoid blacklisting legitimate nodes as malicious nodes because of poor network performance.

The route request and response are obtained after all this verification process. Malicious nodes detection is done after obtaining the RREQ and RREP. Once thisprocess is done, the prevention and blacklisting of malicious attacks using the proposed Gray Hole prevention algorithm take place. This process will be iterated untilall the malicious nodes have been prevented and blacklisted explained previously.

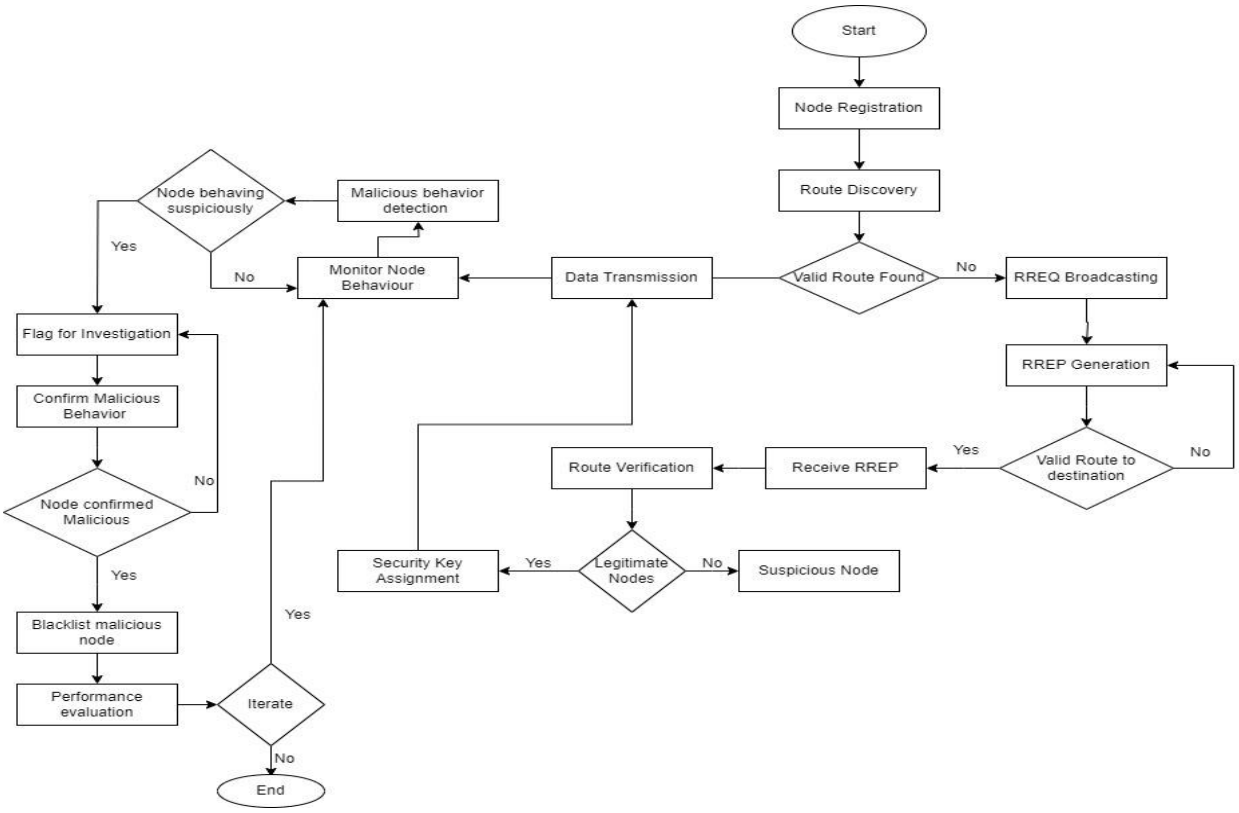


Figure 5. Gray Hole Detection algorithm flow chart

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 661-688
https://doi.org//10.47514/kjcs/2024.1.3.0019
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

The proposed Gray Hole Prevention algorithm is demonstrated using Algorithm 4.

Algorithm 4: Gray Hole Prevention (Gray-HP)

```
Begin
L = RREQ_RATE_LIMIT
LT = RREQ_ACCEPT_LIMIT
M = RREQ_BLACKLIST_LIMIT
MS = MESSAGE SIZE
B = BANDWIDTH
EL = EXPECTED_LATENCY
NL = NETWORK_LATENCY
Set nm[i][j]; // where i = node at 'x', and j=node 'y' position
Set source=sn;
Set key[]=nm; // nm denotes number of mobile nodes

While RREQ_COUNT ≠ 0
NL = MS/B //To calculate the current network latency to determine and monitor network performance to ensure that nodes are not blacklisted because of poor network performance.

If RREQ_COUNT < LT Then
Process the RREQ
Receive another RREQ and increment RREQ_COUNT by 1
//Upon receiving the RREQ by a neighbor node
//Increment RREQ_COUNT for that neighbor
Else
For each i = 1 to nm step 1
For each j = 1 to nm step 1

If nm[i][j]packets.equals(drop) Then
If RREQ_COUNT > M && NL < EL Then
If key.equals(null) && ipaddress.equals(redundant) Then
Blacklist(nm[i][j]); //Blacklist the specified node and declare it as a malicious node
Else
If key.equals(null) && ipaddress.equals(unique) Then
Send(nm[i][j]); //Send packets to the legitimate sink node
Else
Sink node cannot receive packets
Continue the process of RREQ
End if
End if
End if
End if
Next j
Next i
End if
Do
If the node is declared as malicious Then
Resend the RREQ to other neighbor nodes (excluding malicious nodes)
Else
If RREQ > L Then
Ignore all route requests
End if
End if
Until all malicious nodes are blacklisted
Loop
End
```

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 661-688
https://doi.org//10.47514/kjcs/2024.1.3.0019
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

The proposed algorithm presented works as follows:

Step 1: The source node sends RREQ to its nearest/neighbor nodes. The source node receives RREP if the route is found.

Step 2: The source node thereafter sends data packets through the neighbor node responded with RREP.

Step 3: if the RREQ_COUNT is less than the Limited (LT) number of route requests, the process precedes. However, if the RREQ_COUNT is greater than the limit and the Latency (NL) is less than the Expected Latency (EL).

Step 4: Each node's KEY needs to be determined whether it is null or not. Each IP_ADDRESS must be validated for redundant purposes. Therefore, once the KEY and IP_ADDRESS meet the requirements the process proceeds, otherwise, the node gets blacklisted anddeclared as malicious. However, once the KEY does not meet the requirements and the IP_ADDRESS is found unique, the packets are sent to the destination nodes, otherwise, the destination node cannot receive the packets but the RREQ process continues.

Step 5: However, if the neighbor node is malicious, it becomes blacklisted, and thus, the source node sends RREQ to other neighbor nodes (excluding blacklisted nodes).

Step 6: The malicious node may send the fake RREQ to other nodes. The other nodes stop the fake route request by ignoring all the RREQ from any of the detected malicious nodes.

Step 7: This process continues or is iterated until all malicious nodes are blacklisted.

Moreover, Fig. 5 further shows how is the flow of the proposed algorithm as discussed in detail in the explanation of the algorithm.

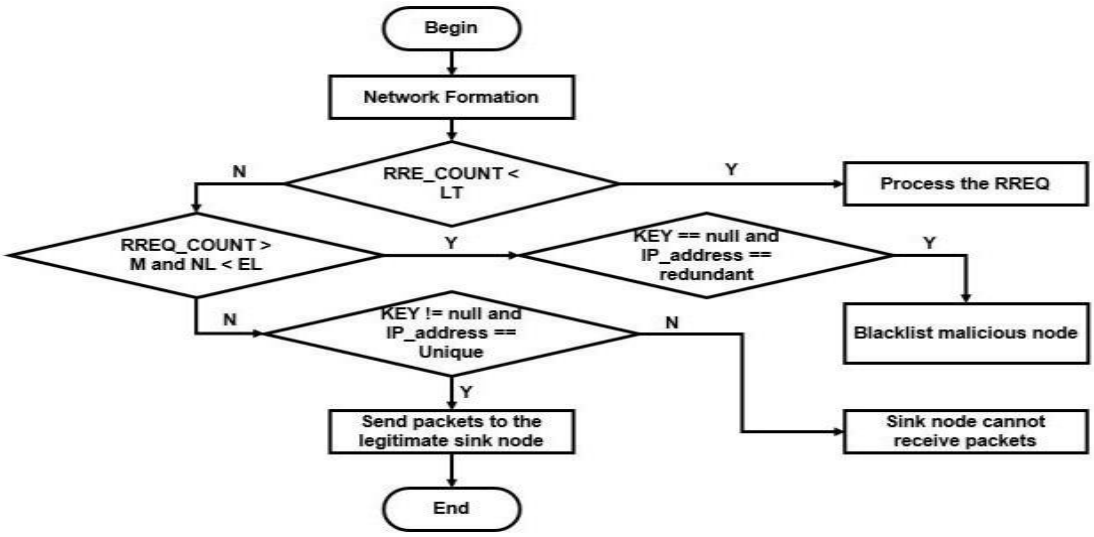


Figure 6. Gray Hole Prevention algorithm flowchart.

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 661-688
https://doi.org//10.47514/kjcs/2024.1.3.0019
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

4. Results and discussion

The experimental setup considered for the study is given in this section. It mainly includes Network simulator two software tool. TCL is the front-end, then C++ is a back-end. The number of nodes considered is 45, and the performance metrics used for evaluating the proposed technique is the PDR, Throughput, The consumption of energy, and Security. The experimental setup details are deliberated in the below given table 1

Experimental Setup	
Tool	NS-2
Version	Ns- allinone 2.34
Front End	TCL
Back End	C++
Number of Nodes	45
Performance Metrics	Packet Delivery Ratio, Throughput Routing overhead.

Table 1 Experimental Setup

The simulation parameter details are as presented in the table 4.2. It shows the particulars of the simulation parameter along with its values. It mainly includes the quantity of nodes which is considered here as 45. The range of the topology as (1386,1500), the type of the Antenna is omnidirectional; the propagation model is a two-ray ground, the application is UDP. The size of the packet is 1000, and then the protocol used for routing is DSDV.

Parameters	Values
Total nodes	45
Topology range	1386,1500
Type of the antenna	Omnidirectional antenna
Propagation Model	Two-ray ground
Application	UDP
Packet Size	1000
Routing protocol	DSDV
Simulation time	40 seconds
Phy/WirelessPhy set RXThresh, CSThresh	$1.42681e^{-12}$

Table 2 Simulation Parameters

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 661-688
https://doi.org//10.47514/kjcs/2024.1.3.0019
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

This section mainly discusses the simulation parameters along with the process of Autonomous network formation, checking the availability of node, source broadcasting to all nodes, route discovery, verify all nodes key for security, route response and request, malicious nodes detection, prevention, elimination and performance metrics. Figure 6 demonstrates the formation of an autonomous network in the environment of a network simulator. It includes a mobile nodes set in which every node should possess some kinds of identification which is like mobile nodes as mn1, mn2, mn3, mn4, mn5, mn6, mn7……mnn. In this figure 4.1, brown color nodes represent the node attributes which specifies that the normal node presents or exists in a network. Blue color specifies the source and destination nodes i.e., node-21 (source node) and node-35 (destination node).

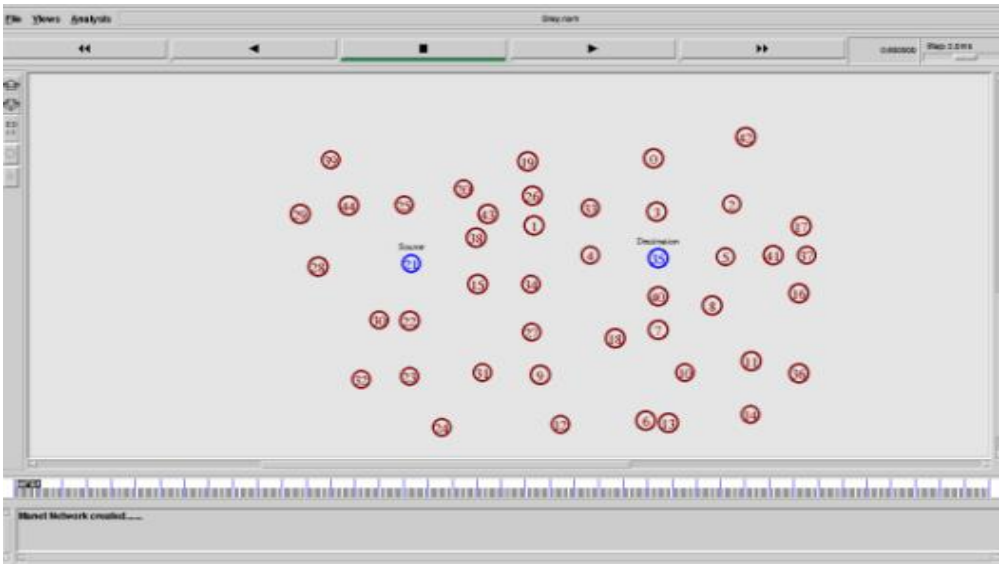
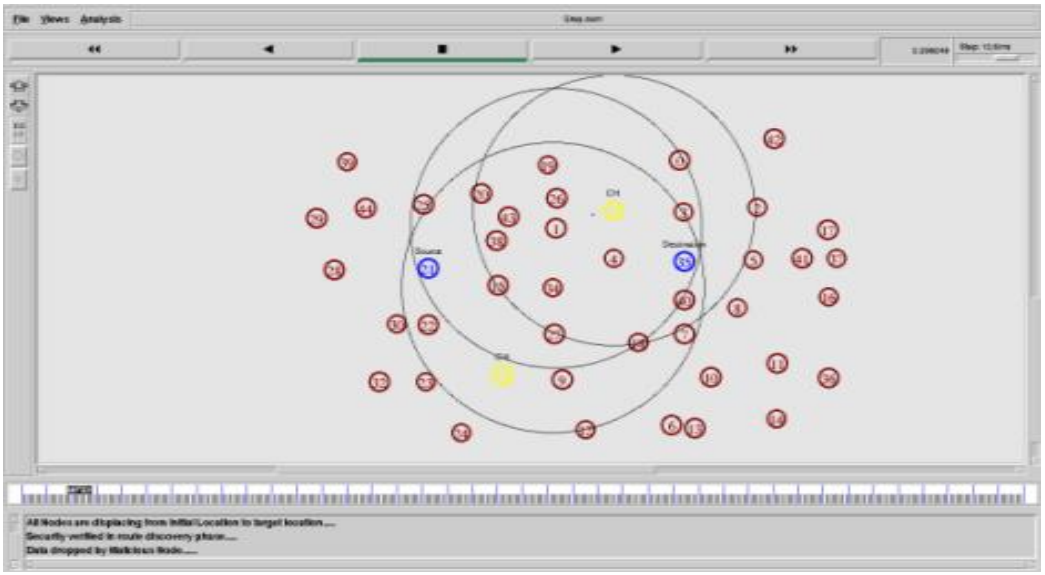


Figure 7. Network Formation

Route Discovery



Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 661-688
https://doi.org//10.47514/kjcs/2024.1.3.0019
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Figure 8. Route Discovery

Figure 8 demonstrates the phase of route discovery. Here, all nodes are displacing from initial location to target location. Security is verified in the route finding phase, and then the data or packet is dropped by the malicious node. All Nodes are checking transmission range for before transmission. In this phase, the source will forward a broadcast request to all the neighboring nodes for the purpose to discover a route.

Route Discovery with verification by ID

Figure 9 shows the route discovery phase with verification by ID. Here, the gray hole attack is detected. In this route discovery phase, all the nodes are verifying the key for secure communication. If any node comes into a network without a key, then that node is added into the block list. In the below figure yellow color node are recognized as gray hole attacks.

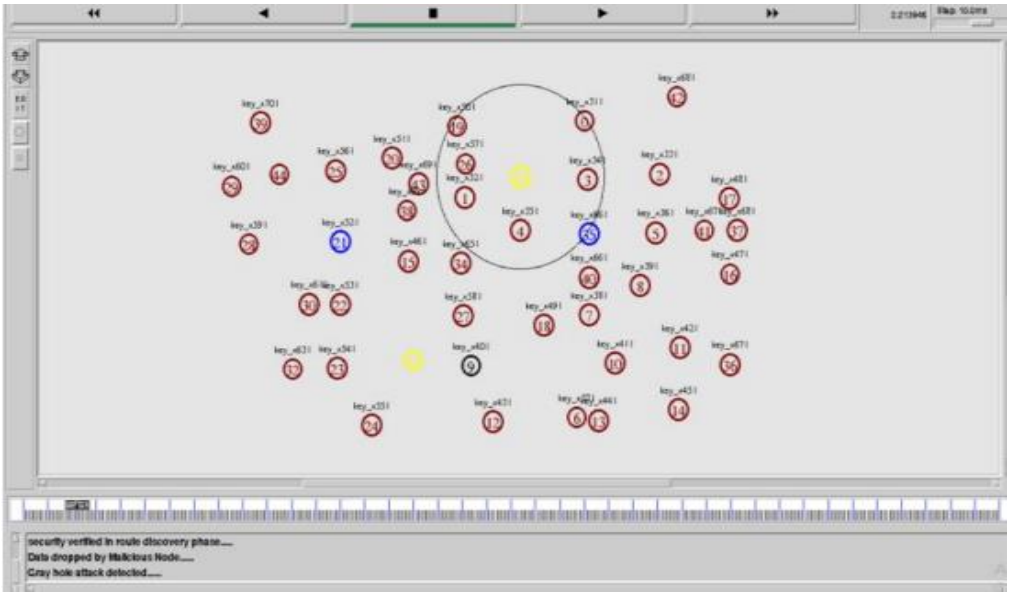


Figure 9. Route Discovery with verification by ID

Gray hole Attack Detection

The gray hole attack detection is achieved as presented in figure 9. The gray hole attack detected without a key. Here, the yellow color node represents a gray hole attack which attacks dropping incoming and outgoing message from the source. .Figure 10. Shows the simulation diagram m of the gray hole attack detection

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 661-688
https://doi.org//10.47514/kjcs/2024.1.3.0019

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

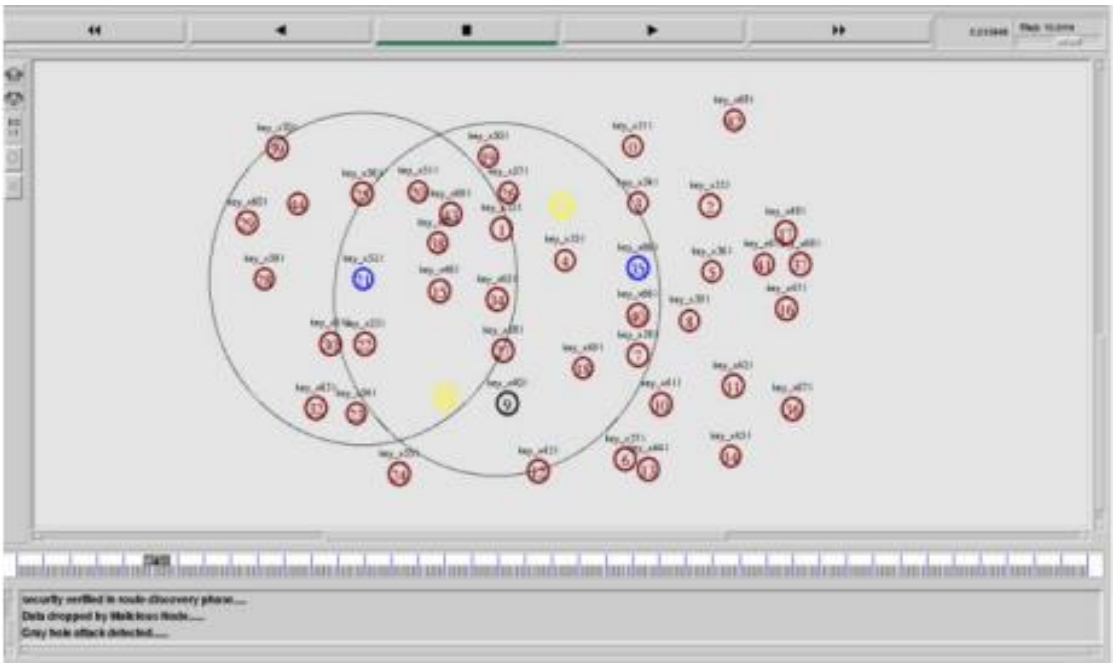


Figure 10. Gray hole Attack Detection

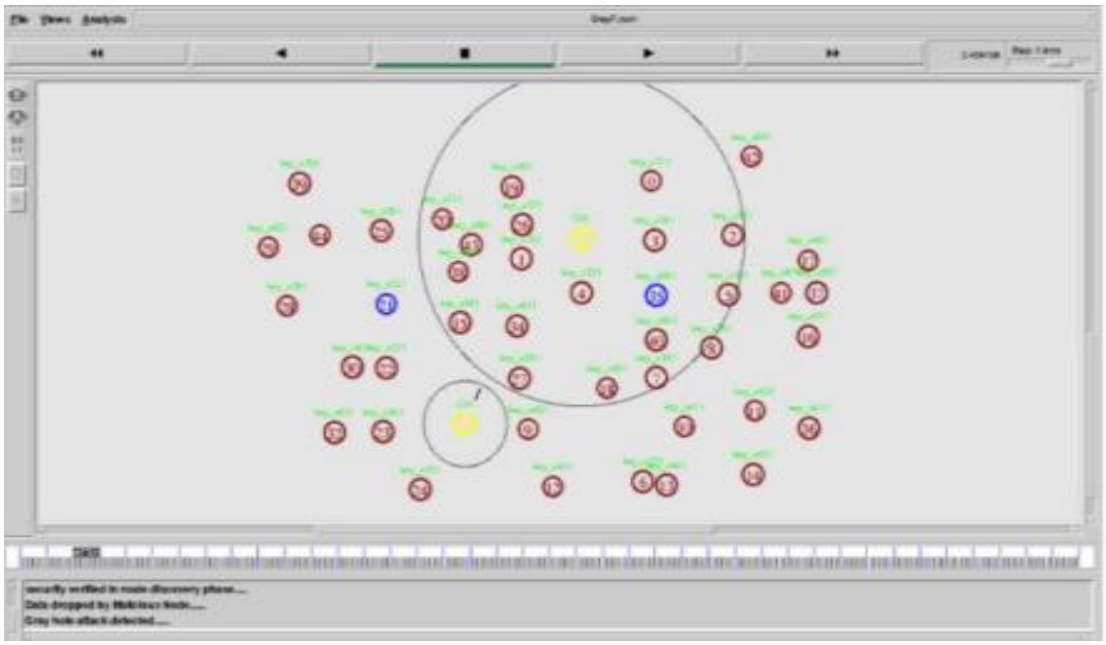


Figure 11. Screenshot showing the implementation process before gray hole prevention

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 661-688
https://doi.org//10.47514/kjcs/2024.1.3.0019
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Gray hole attack prevention

Figure 10 represents the elimination of the gray hole. In this module, attacker blacklisted from this network for reduced network traffic. Figure 11 displays the simulation diagram of the gray hole attack after the prevention.

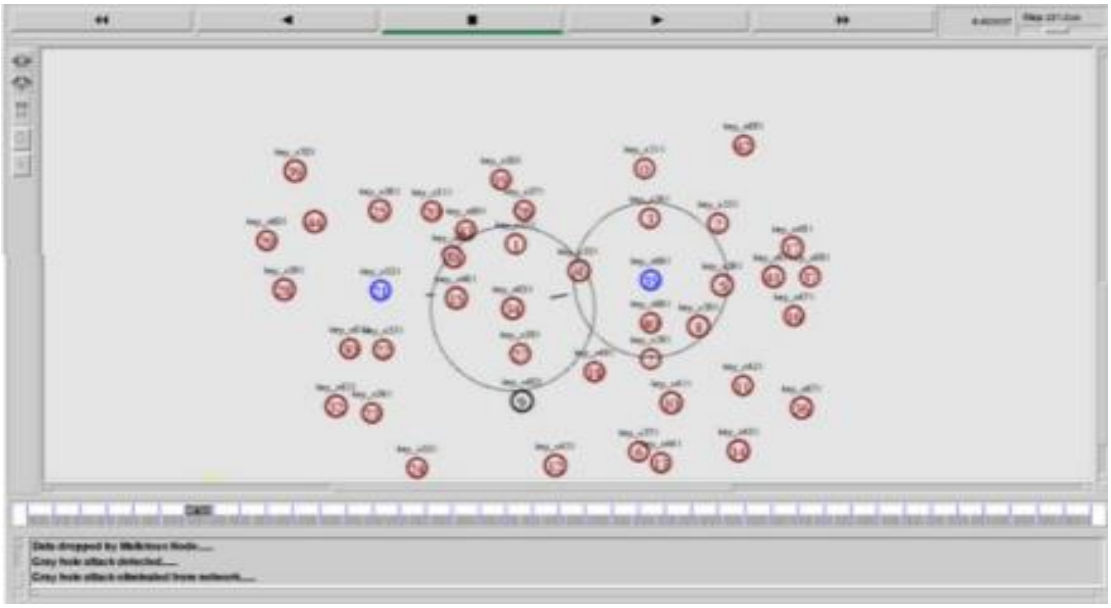


Figure 12. Prevention of the gray hole

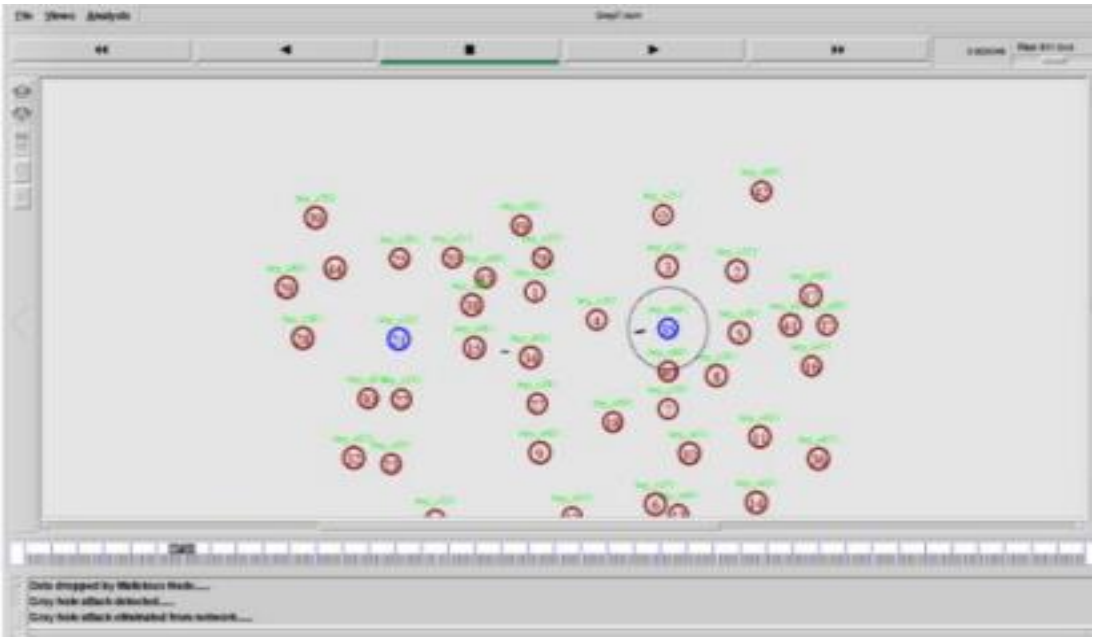


Figure 13. Screenshot showing the implementation process after gray hole prevention

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 661-688
https://doi.org//10.47514/kjcs/2024.1.3.0019
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Communication End

Figure 14 shows the ending process of communication. In this module, after preventing the gray hole attacker from this network and data communicated successfully without delay and reduce energy consumption.

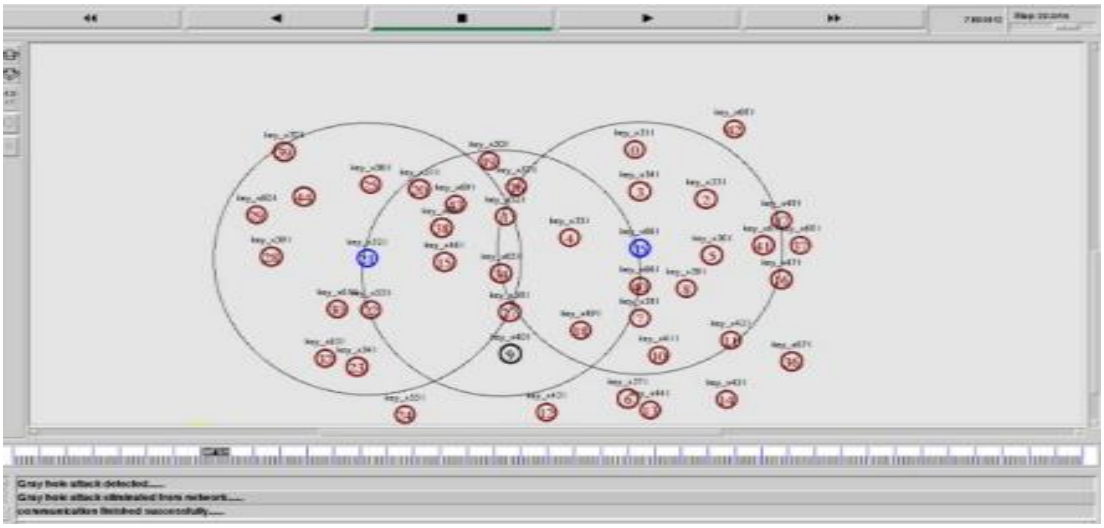


Figure 14. Communication End

Throughput Analysis

The quantity of packets which pass passing over a channel in a specific unit of time. This performance metric demonstrates the total number of packets that have been effectively carried from source to sink, and it could enhance by increasing its speed.

$$\text{Throughput (R)} = \frac{\text{Data Size (I)}}{\text{Time (T)}}$$

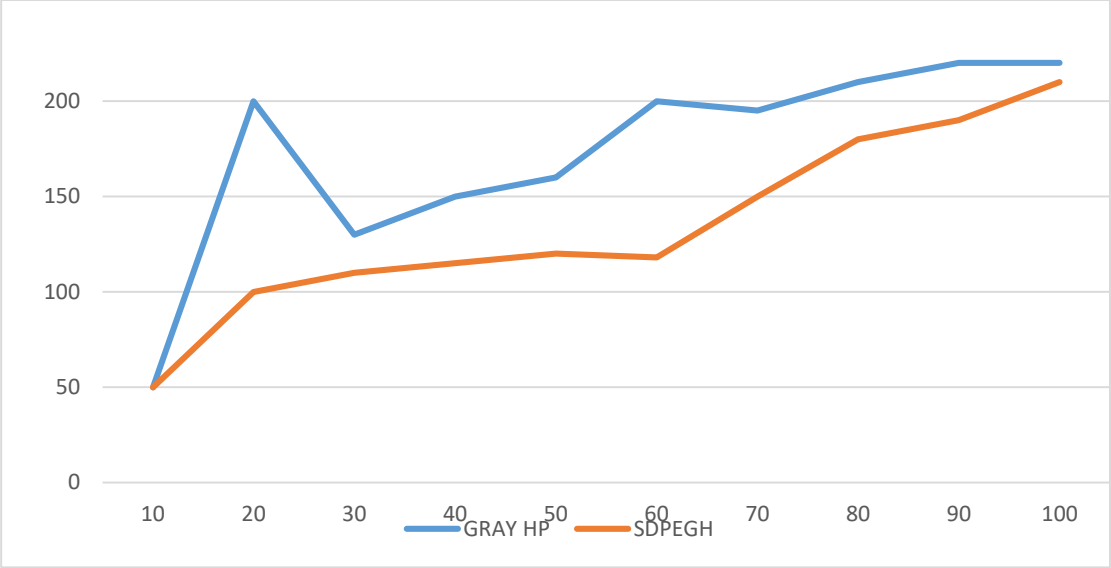
Where:

- I is the data size (in bits or bytes)
- T is the time taken to transmit the data (in seconds)

Here, calculated throughput states to an average data rate of fruitful data or else message conveyance over a particular communications link. Throughput is measured in kilobits per second (kbps) between existing SDPEGH and Gray hole prevention algorithm. The blue color output specifies the performance of the proposed Gray Hole prevention algorithm for throughput. The red color results shows the performances of the existing SDPEGH.

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 661-688
https://doi.org//10.47514/kjcs/2024.1.3.0019
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Throughput (kb/s)



Simulation Time (s)

Figure 15. Network throughput

Throughput is a critical metric for assessing network performance. The proposed algorithm achieved a 25% increase in throughput, as shown in graph above. This enhancement is attributed to the algorithm's ability to dynamically adapt to node behavior and efficiently manage routing paths, thereby reducing the impact of malicious nodes on overall network performance. The results confirm that the proposed algorithm not only improves security but also enhances the QoS in MANETs.

Packet Delivery Ratio

The ratio of packets of the data carried to sink to those created using CBR sources. PDR demonstrates the way that a protocol performs delivering packets successfully from sender to receiver. The higher values improve the outcomes. It describes both the comprehensiveness and exactness of a routing protocol. Its efficiency gives reliability of routing protocol.

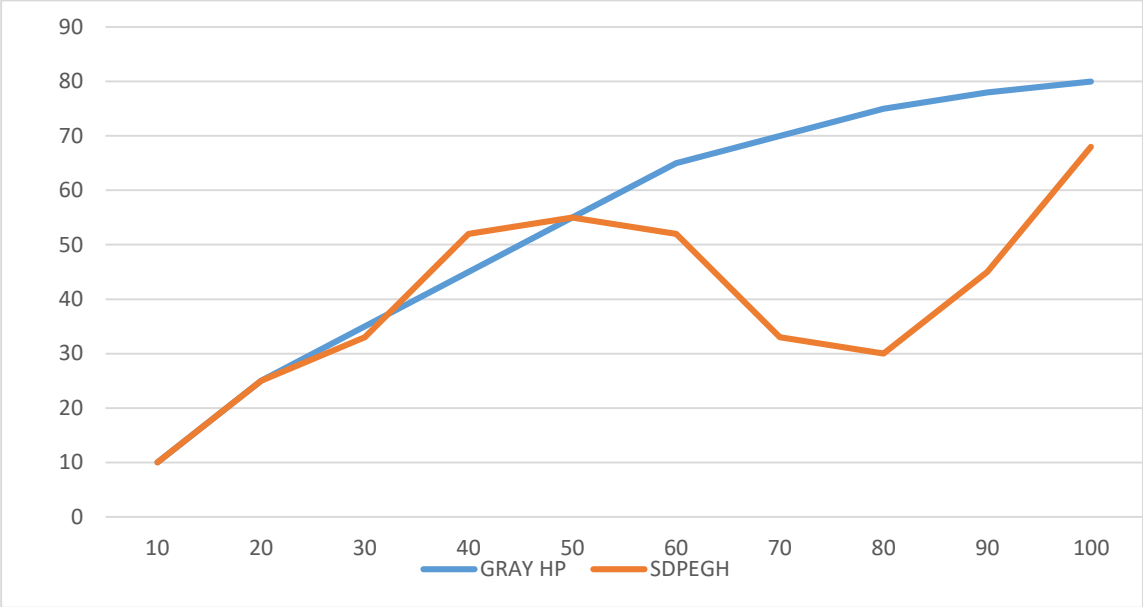
$$PDR = \frac{N_{rp}}{N_{sp}}$$

The Packet Delivery Ratio (PDR) is calculated using the formula:

Where N_{rp} is the number of successfully received packets, and *Nsp* is the total number of packets sent. This gives the ratio of packets delivered to packets sent.

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 661-688
https://doi.org//10.47514/kjcs/2024.1.3.0019
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Delivery Ratio



Simulation Time (s)

Figure 16. Packet Delivery Ratio

The proposed Gray Hole prevention algorithm seems to have improved delivery ratio as compared to SDPEGH. This improvement has been achieved by employing the Gray-Attack preventiontechnique to deal with determining null session KEYs as well as redundant IP addresses that are generated as a result of gray hole attackers. In addition, the proposed algorithm considered calculating the network performance by looking at the message size and network bandwidth, yielding to minimized delays and bandwidth usage and thus improving the delivery ratio.

The results indicate a significant improvement in the Packet Delivery Ratio when using the proposed Gray Hole Prevention algorithm. As illustrated in graph above, the PDR increased by approximately 30% compared to the SDPEGH algorithm under similar network conditions. This improvement directly addresses the problem of packet loss caused by gray hole attacks, demonstrating the effectiveness of the proposed algorithm in maintaining reliable communication.

Routing Overhead

Overhead Routing is described as the proportion of the overall control packet size including RREQ, RREP, RERR and the Hello package to the overall information packet size supplied to a target. The simulation results forthe Overhead Routing for all three algorithms is portrayed in Fig 17 below.

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 661-688
https://doi.org//10.47514/kjcs/2024.1.3.0019
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Routing Overhead

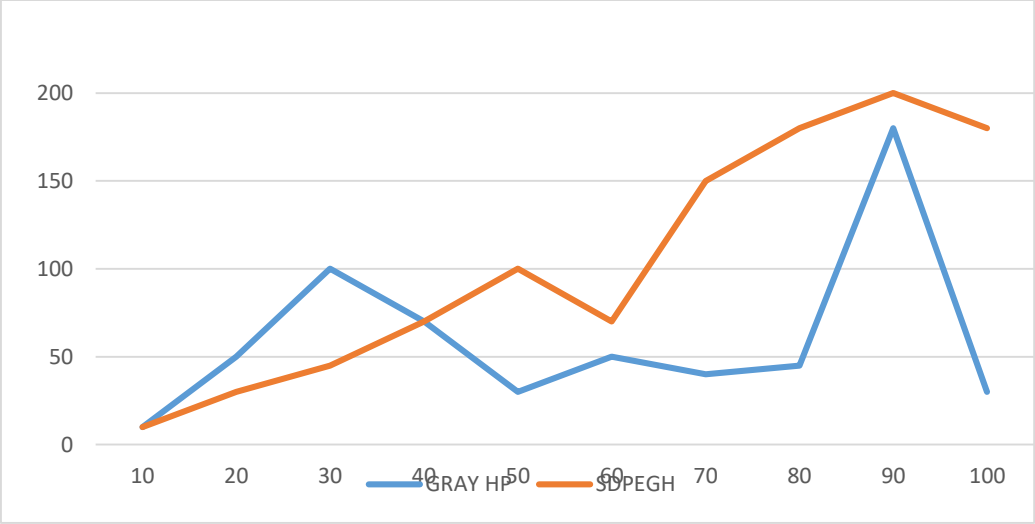


Figure 17. Routing overhead.

Figure 17 compares, as obtained through multiple simulations, the routing overhead by the proposed algorithm with that of Secure Detection Prevention and Elimination Gray Hole(SDPEGH). The figure clearly shows that the algorithm reduced the routing overhead compared the existing technique. This was achieved as a result of reducing congestion problems through blocking and blacklisting malicious nodes. The proposed Gray Hole prevention algorithm ensured that once a malicious node is detected, it is blocked and alternative routes are chosen rather than dropping packets as done by the existing algorithms. In addition, the algorithm determined the network performance to ensure that legitimate nodes are not blocked and blacklisted because of poor network performance. The proposed algorithm results showed that it outweighs other algorithms with an increase in routing overhead with an appropriate 5.7%.

5. Conclusion

In this paper, we have explored the complexities and challenges associated with gray hole attacks in Mobile Ad hoc Networks (MANETs). The research aimed to provide a comprehensive understanding of the gray hole attack, its implications on network performance, and potential strategies for detection and prevention.

The findings of this research underscore the critical need for robust security measures in MANETs, particularly in environments susceptible to malicious activities. The gray hole attack poses a significant threat, and our proposed detection and prevention strategies offer a viable solution to enhance the resilience of these networks. By implementing proactive measures, network administrators can safeguard against the detrimental effects of such attacks, ensuring more reliable communication in dynamic and decentralized

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

environments. While this study has made significant strides in addressing gray hole attacks, several areas warrant further investigation:

- **Enhanced Detection Mechanisms:** Future research could focus on developing more sophisticated detection algorithms that utilize machine learning techniques to improve the accuracy and speed of identifying gray hole attacks.
- **Real-World Testing:** Conducting experiments in real-world scenarios would provide valuable insights into the practical applicability of the proposed solutions and their performance under varying conditions.
- **Integration with Other Security Protocols:** Exploring the integration of gray hole attack mitigation strategies with existing security protocols could lead to a more comprehensive security framework for MANETs.
- **Impact of Mobility Patterns:** Investigating how different mobility patterns of nodes affect the occurrence and impact of gray hole attacks could provide deeper insights into network vulnerabilities.

As MANETs continue to evolve and find applications in various fields, addressing security challenges such as gray hole attacks will be paramount. This research contributes to the ongoing discourse on network security and lays the groundwork for future advancements in protecting MANETs from malicious threats.

References

A. S. K. Pathan (2021), *Security of self-Organizing Networks: MANET, WSN, WMN, VANET*, CRC press.

Ashok M. Kanthe, Dina Simunic, Ramjee Prasad (2022) "A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks" International Journal of Computer Applications (0975 – 8887) Volume 53– No.16.

Chen, L., Zhang, Y., & Hu, X. (2023). Mobile Ad Hoc Networks: A Survey of Recent Advances and Future Trends. IEEE Access, 11, 132803-132821.

Dhar, S. K., Jana, R. K., & Sahu, S. K. (2021). A Novel Gray Hole Detection and Prevention Technique in Mobile Ad Hoc Networks. Proceedings of the IEEE 11th International Conference on Advanced Computing (IACC).

Ganesh Reddy, K., Kollipara, R., Sravani, K. V., & Mounika, K. (2023). Reputation based IDS for gray hole attack in MANETs. International Journal of Computer Science and Information Security (IJCSIS), 14(1), 58-62.

Ghosh, S. M. M., Murshed, M. A., & Sarkar, S. (2024). G-HAP: Gray Hole Attack Prevention in Wireless Ad Hoc Networks Using Game Theory. Journal of Computer Networks and Communications, 2020, Article ID 8864483.

Isha G. Kariya, Atul B. Kathole, Sapna R. Heda (2022), "Detecting Black and Gray Hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method" IJTAE.

Jhaveri, R. H., & Patel, N. M. (2021) A sequence number based bait detection scheme to thwart gray-hole attack in mobile ad hoc networks, Springer Wireless Network, 21, 2781–2798.

Jhaveri, R. H., & Patel, N. M. (2021) A sequence number based bait detection scheme to thwart gray-hole attack in mobile ad hoc networks, Springer Wireless Network, 21, 2781–2798.

K. Pavani and D. Avula (2022) "Performance evaluation of mobile adhoc network under black hole attack," in *Proc. International Conference on Software Engineering and Mobile Applicatio.*

Khobragade, K. (2022). Detection and Prevention of gray Hole Attack in MANET. International Journal of Researches in Biosciences, Agriculture and Technology, VII(I), 34-40.

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Kumar, R. S., & Nagalakshmi, T. J. (2024). Design of intrusion detection system in the detection of grey hole attack in wireless ad hoc network using K-means cluster. *AIP Conf. Proc.* 2853, 020066. https://doi.org/10.1063/5.0197407

M. Radha, and M.N. Rao (2022), "Gray hole attack detection prevention and elimination using SDPEGH in MANET," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 8,no. 3.

Mohanapriya, M., & Krishnamurthi, I. (2021), Modified DSR protocol for detection and removal of selective black hole attack in MANET, Elsevier Computers and Electrical Engineering, 40, 530–538.

P. Sahu, S. K. Bisoy, and S. Sahoo (2021), "Detecting and isolatingmalicious node in AODV routing algorithm," *International Journal of Computer Applications*, vol. 66, no. 16, pp. 0975–8887.

Patel, N. J. K., & Tripathi, K. (2023). Trust Value based Algorithm to Identify and Defense GrayHole and Black-Hole attack present in MANET using Clustering Method. International Journal of Scientific Research in Science, Engineering and Technology, 4(4), 281-287.

Rani, P., Kavita, Verma, S., & Nguyen, G. N. (2020). Mitigation of Black Hole and Gray Hole Attack Using Swarm Inspired Algorithm with Artificial Neural Network. IEEE Access, 8.

S. Sathish and M. Saranya, (2020) "Malicious node identification scheme for MANET using rough set theory," *International Journal ofComputational Intelligence and Informatics*, vol. 6, no. 2, pp.172–183.

Sampada, H. K., & Shobha, K. R. (2024). Co-Ordinated Blackhole and Grayhole Attack Detection Using Smart & Secure Ad Hoc On-Demand Distance Vector Routing Protocol in MANETs. International Journal of Computer Networks and Applications (IJCNA), 11(1), 1-27.

Senthilkumar, T., & Thrimurthulu, P. R. (2023). Secure and Efficient Detection and Prevention of Gray Hole Attack in Mobile Ad hoc Networks. International Journal of Grid and High-Performance Computing, 11(3), 1-14.

Sharma, A., & Sheetlani, J. (2023). Recognition and Avoidance of Blackhole and Grayhole Attacks in MANET Using Novel Augmented Ad Hoc on Demand Distance Vector (AAODV). International Journal of Management (IJM), 11(8), 2216-2228.

Shukla, M., Joshi, B. K., & Singh, U. (2024). A Novel Machine Learning Algorithm for MANET Attack: Black Hole and Gray Hole. *Wireless Personal Communications, 138*(1), 41-66.

Yazdanypoor, M., Cirillo, S., & Solimando, G. (2024). Developing a hybrid detection approach to mitigating black hole and gray hole attacks in mobile ad hoc networks. Applied Sciences, 14(17), Article 7982. https://doi.org/10.3390/app14177982