A Model to Prevent Gray Hole Attack in Mobile Ad-Hoc Networks

Thabiso N. Khosa, Topside E. Mathonsi *, and Deon P. Du Plessis
Tshwane University of Technology, Pretoria, South Africa; Email: thabisonicholus@yahoo.com (T.N.K.), duplessisdp@tut.ac.za (D.P.D.P.)
*Correspondence: mathonsite@tut.ac.za (T.E.M.)

***Abstract*—Over the past few years, Mobile Ad-hoc Networks (MANET) has been playing an important role in ubiquitous networks based on its ability to support mobility without depending on infrastructure-based design, dynamic topology, and thus, are known as decentralized environment. One of the advantages of MANET is that its nodes can act both as routers and hosts. This, therefore, implies that its nodes can transmit packets between source to destination nodes. As a result of such and many more advantages, these networks are more vulnerable to different types of network attacks. In the recent past, several secured routing protocols were proposed and implemented for MANET. However, those protocols cannot fully guarantee security within these networks in terms of Denial of Services (DoS) attacks such as black hole and gray hole attacks. The review of the literature showed that existing solutions cannot always ensure true node classification. This is because MANET's cooperative existence sometimes leads to the false exclusion of innocent nodes and/or proper classification of malicious nodes. A new Gray Hole Prevention (GRAY-HP) algorithm for the detection of malicious nodes with the actual high accuracy ratio of node classification is proposed in this paper. The proposed algorithm employs and modifies the gray-attack prevention technique known as Secure Detection Prevention and Elimination Gray Hole (SDPEGH), and the proactive scheme. It has been confirmed by Network Simulator 2 (NS2) computer simulation that the proposed algorithm outperforms the Genetic Algorithm to Bacterial Foraging Optimization (GA-BFO) and Rough Set Theory (RSetTheory) algorithms in terms of throughput, routing overhead and delivery ratio. The proposed GRAY-HP algorithm guarantees the successful elimination of Gray hole nodes, while it also ensures that no legitimate nodes are excluded.**

***Keywords*—wireless network, mobile ad-hoc networks, dynamic source routing, gray hole**

I. Introduction

Mobile Ad-hoc Networks (MANET) is the fast-growing wireless network technology, this is because it supports the communication of mobile network devices without the need for a central control system and infrastructure setup (see Fig. 1). Thus, MANET is used to deliver network traffic in different areas without using any pre-established infrastructure [1]. MANET can be used for air pollution, environmental disasters monitoring among many others [2]. MANET consist of nodes that can communicate altogether without a pre-established network topology thus, each node in MANET can act as both the router and host hence, routing is critically important to enable nodes to communicate to each other in MANET [2].

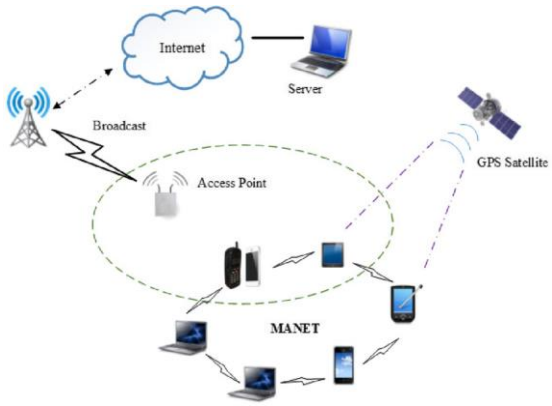

Figure 1. Typical MANET architecture.

Routing is the process of determining the best path to reach the destination from the sender [3]. In MANET three kinds routing protocols exist namely proactive routing which is considered as table-driven. The second one is named reactive protocol, which is considered as an On-demand protocol. Lastly, there is a hybrid protocol, which is the combination of both reactive and proactive protocol. Ad-hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), Temporally Ordered Routing Algorithm (TORA), and Associativity Based Routing (ABR) are reactive protocols that are used in MANET.

MANET is vulnerable to network attacks due to its major characteristics such as open standard, vibrant topology, and shortage of central intensive care devices. There are several network attacks in MANET such as a black-hole attack, a wormhole attack, and a gray hole attack.

Gray hole attack is considered as a one of the severe security threats that not partly drops packets but also affects the procedure of communication in MANET. The source node accepts a reply from the authorized node that offers a direct route that is near to the destination and

Manuscript received July 20, 2022; revised August 26, 2022; accepted September 8, 2022; published June 7, 2023.

malicious node reply to a sender that the data is received. During a gray hole attack in MANET, source gets confused with two replies. The malicious node gets to be a sender node, and complete information is considered by it. During this procedure, the data packet entirely dropped by a source.

As a result, this paper designed a Gray Hole Prevention (GRAY-HP) algorithm. The proposed GRAY-HP algorithm employs and modifies 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, the proposed GRAY-HP algorithm reduced the chances of eliminating legitimate nodes in MANET. In the proposed 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 has compared the proposed GRAY-HP algorithm against GA-BFO and RSetTheory algorithms in terms of throughput, routing overhead, and delivery ratio.

The rest of this paper is structured as follows: Section II, gives the background of MANET, and protocols security challenges. Section III, provides the related literature. Section IV, presents the proposed algorithm as a solution to the problem. Section V presents the performance evaluation for the GRAY-HP algorithm. Conclusion and future work are presented in Section VI.

II. Backgound and Security Challenges in Manet

MANET gained its popularity because of its rapid deployment, diverse topology, and infrastructure-less network. The traditional procedures and technology is not compatible with MANET so they have to be consolidated with the functionality of MANET in order to function effectively. MANET's topology changes rapidly because of the flexible mobility of nodes linking and disembarking from the network. MANETs routing procedures are grouped into a hybrid, reactive, and proactive depending on how the nodes make and maintain paths [4]. The pyramid of these protocols is illustrated in Fig. 2.

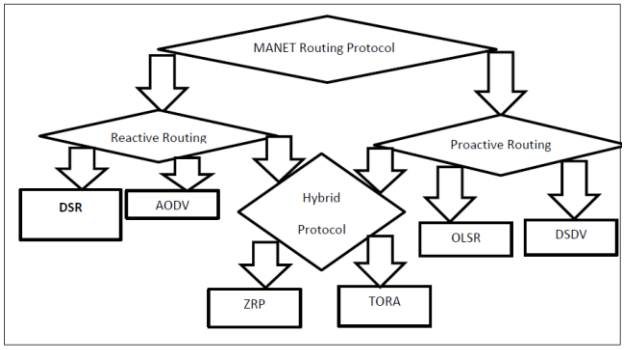

Figure 2. MANET pyramid.

MANET routing protocols are categorized according to their purpose in three different categories:

A. Reactive Routing Protocols

When the nodes need to transfer data to an unknown destination, the route to the destination is determined. If a node wishes to send information, a path detection procedure is initiated in the network. As compared to proactive protocols, reactive protocols have less power overhead. On the other hand, the process of searching the route before transmitting data packets can cause the source node to delay [5].

B. Proactive Routing Protocols

These are routing protocols powered by a routing table to record new and updated network routes. Each node has a table to store the network routing information. The nodes share information about the topology for the purpose of maintaining a consistent network view which informs the nodes about any changes in the topology. When a node wants to send a message, it can get the path to the destination by searching the local route table without any delays [6]. One consequence of the modified topology is the high control overhead in routing tables. Destination-Sequenced Distance-Vector (DSDV) routing protocol and Optimized Link State Routing Protocol (OLSR) are examples of common proactive Routing protocols [6].

C. Hybrid Protocols

The design of hybrid protocols is the combination of strengths of both the reactive and proactive protocols for improved performance [7]. Most of the hybrid routing protocols are arranged hierarchically or are layered. The proactive routing serves the purpose of acquiring all the unknown routing information while reactive routing deals with updating the routing table when there is a topology change. The common hybrid routing protocol is the Zone Routing Protocol (ZRP) [6–11].

D. Security Attacks in MANET

The MANET are exposed to security outbreaks because of their properties such as resource constraints, little physical security, dynamic typology, and lack of infrastructure. MANET security vulnerability is more severe because they are wireless [12]. Each layer in MANET communication has its own vulnerabilities, therefore attacks can also be classified according to the layer of occurrence [13]:

1) Gray hole attack

The Gray hole is different from a black hole attack. In gray hole attack, a nasty node selectively drops the packets [14]. Through route detection procedure, a nasty node pretends to be honorable, but subsequently begins to drop packets. Primarily, a gray hole might choose to reject packets imminent from or planned for specific nodes, but advancing all packets to certain nodes. Furthermore, a gray hole could turn wickedly for a certain time, then later on performance just like any other ordinary nodes. In addition, a gray hole node can abandon packets from precise nodes for a specific period only, and later on, turn normally. It is pretty complex to discover these types of attacks due to this ambiguity [10–15]. The Fig. 3 demonstrates the procedure of the gray hole attack.

Firstly, source node acts as a normal node and forwards all packets from source node to the target node (destination). Subsequently as shown node M start performing nastily and drops packets intended to destination from source node.

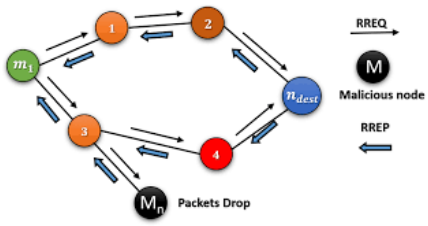

Figure 3. Gray hole procedure.

Gray hole attacks that uses Dynamic Source Routing (DSR) in MANET selectively drops data packets, since DSR does not have a security mechanism. Thus, malicious nodes can perform a gray hole attack simply by failing to comply correctly with DSR rules. In addition, all UDP packets can be dropped by the malicious nodes. In addition, the attacker can also use a statistic method, such as a dropout of just 50% of the packets, which can cause a heavy network destabilisation.

2) Black hole attack

The invader attacks the network by recommending that it's the shortest route to a certain node whose packets they intend on compromising. The packets from the node are then redirected to them and they drop them [13, 16].

III. 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 high computational complexity which does not suit the features of MANET. In addition, the majority of these existing algorithms are designed to detect and prevent attacks in the AODV protocol.

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

Cai and Yi *et al.* [1] proposed a Route Confirmation Request (RCONR) and a Route Confirmation Answer (RCONA) solution to modify the DSR routing protocol. In addition to the RREP to the source node, an intermediate node should send an RCONR to its next-hop node. When the next-hop node receives an RCONR, it searches its cache for an itinerary to the destination. It sends the RCONA to the source when it has a route. The source node can confirm the validity of the path after receiving the RCONA by comparing the path of RREP and that of RCONA. When both agree, the source node considers the route suitable. The disadvantage of this method is that the cooperative gray hole attack cannot be avoided if two consecutive nodes work together since the first node requested its next-hop node to send RCONA to the source. Similarly, the proposed GRAY-HP algorithm will aim to use the same approach, when the next-hop node receives an RCONR, it should search its cache for an itinerary to the destination. However, in GRAY-HP a neighbor's RREQ will be only processed if there is less RREQs received from that neighbor. If the number is greater than Black-List Limit, on the other hand, it will delete the RREQ, and blacklist the specific neighboring note. If the previously received RREQ from this neighbor is more than RREQ LIMIT and less than Black-List Limit, RREQ will be delayed before it will be queued for processing.

The algorithm to allow an RREP node to be checked was developed [5]. The node tests when the number of the RREP sequence is above a threshold. When the number of the RREP sequence is greater than threshold, the sending node is considered malicious, and the node is added to the blacklist. After the nodes detect a malicious node, they will send an ALARM packet to inform their neighbour nodes and ignore all of the RREPs that they have received. Each node updates its threshold value dynamically, as the average difference between RREP packets sequence numbers and the values in their routing table. This solution is primarily designed for a single black hole assault and does not detect cooperative attacks. Updating and transmitting ALARM packages increases over-the-counter routing. An innocent node may be excluded as a black hole by miscalculating the limit value. GRAY-HP adopted this method of node test and run it when the number of the RREP sequence is above a specified threshold.

The study presented a solution that depends on evaluating all acknowledged RREPs [17]. As the source node receives the first RREP, it waits MOS_WAIT_TIME seconds to receive multiple RREPs. The source node saves all the RREPs that have been received in a table during this period. The source node will then analyse the stored table of RREPs and reject a high target sequence number and declare the node malicious. It will then analyse the source node. The rest of the table entries are arranged by number and the node with the highest number is selected. This technology also records the identity of suspected malicious nodes that do not keep a routing entry for that node to dispose of any forthcoming control packs received and/or forwarded from that node. The algorithm leads to a high delay as nodes must wait until several RREPs are established.

The technology for intrusion prevention algorithm was developed [18]. The proposed algorithm suggests that the source node should wait until several RREP messages are sent. The source node stores the sequence number in a table during this period and the arrival time for each RREP received. The proposed algorithm will verify the number of RREP messages in the table when the time expires. This algorithm assumes that only the target node is the trusted node and that the receipt of more than one RREP package shows that the trusted destination node creates one of those packets and malicious nodes create the other messages.

The Genetic Algorithm to Bacterial Foraging Optimization (GA-BFO) algorithms to detect and black hole and prevent the system from the threat through these

optimization algorithms was proposed [19]. MATLAB was used to simulate, the energy, throughput, bit error rate, packet delivery ratio, and an end to end delay were the parameters used. The algorithm considers the varied features in network connectivity such as type of protocol, destination network service, and connection status to produce type-based rules. This method has challenges when the nodes move randomly among the simulation area. In this study the performance of the Genetic algorithm is compared with the proposed GRAY-HP algorithm

Rough set theory for detecting malicious nodes. The malicious node is detected based on the transmission history in the route cache table of the node. That node in the network preserves its neighboring node's cache table and transmission history. To find out the node transmission history based on measured transmission metrics such as packet delivery ratio, reliability, end-to-end latency, number of packets dropped, and error rate. Based on the values of the transmission history of nodes operating at different speeds, the information table is built. The rules are taken from the table to determine whether the nodes are good or bad. The path with the packet's bad node sends an alternative route in the shortest possible path. Results of the experiment show that the rough set method increases the efficiency of the network such as the packet delivery ratio, and reduces end-to-end delay and throughput, however, the algorithm can blacklist legitimate nodes when poor network performance occurs. This study will compare this algorithm with the proposed GRAY-HP algorithm.

Radha and Rao [20] 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. Apart from that, the proposed GRAY-HP algorithm also looks at the network performance to ensure that the proposed GRAY-HP algorithm does not blacklist legitimate nodes because of issues such as poor network performance.

This scheme 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. Moreover, the scheme 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. Under malicious attack, AODV drops more packets with an increase in the number of attacks. It is found that the performance of the proposed AODV protocol degrades when introducing more malicious nodes but have less routing overhead compared to the normal AODV. This method can lead to blocking legitimate nodes due to a shortage of bandwidth. Furthermore, it can cope with the cooperative malicious nodes. This research paper integrated different techniques to eliminate cooperative attacks.

IV. Proposed Solution

MANET is comprised of wireless mobile nodes forming a temporary network to facilitate the communication and relaying of messages without any central Access Point (AP). This makes MANET more vulnerable to most network attacks. As a result, MANET mostly experiences poor network performance in terms of QoS. 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} defines the total number of nodes and thus |V| = n. Meanwhile, E = {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 move freely 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 malicious nodes 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 and now presents some techniques to curb out the issues of fake RREQ and RREP transmitted by the malicious nodes.

The proposed GRAY-HP algorithm employs one of the most 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 [21].

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 routes discovery process to establish new routes between its source 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, when a 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 assigned them 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-HP algorithm adopted and modified Proactive scheme. This technique was designed and implemented by the research work conducted by [22]. In this paper, the focus 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 GRAY-HP algorithm modifies their algorithm by calculating the network performance before declaring nodes as malicious or misbehaving nodes and ensures that nodes are assigned a key to avoid cooperative malicious nodes attack.

In addition, the GRAY-HP 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 [19]. 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 drop packets 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 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.

As depicted in Fig. 1, 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 and unauthorized 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 makes it 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.

A. System Modeling

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.

This work, therefore, presents the design and implementation of the proposed GRAY-HP algorithm for MANET. 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 proposed GRAY-HP algorithm integrates two existing techniques to detect and prevent 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.

1) SDPEGH algorithm design

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 source constantly 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 a trustworthy node and facilitated to modify its state to spiteful and vice versa. Moreover, any malicious node might release every packet or specific data packets.

This research work focuses on deploying two functions of 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 from sending and receiving messages on the network. The Gray hole attack detection function detects gray hole attacks by determining whether the packets sent from source 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. The blacklisted 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);
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
```

The gray hole attack prevention function prevents gray hole attacks by determining whether each node has its key or not. Thus, the algorithm has to ensure that the key is not a duplicate. This is the main part of this research paper, as this research also wanted to determine nodes with fake or without key addresses while also keeping an eye on the nodes dropping packet messages between sources and destination nodes.

2) Proactive scheme design

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 problems. The same further degrades the network performance. This scheme 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

```
1.  Begin
2.  L= RREQ_RATELIMIT
3.  LT= RREQ_ACCEPT_LIMIT
4.  M= RREQ_BLACKLIST_LIMIT
5.  Upon the receiving the RREQ by a neighbor
6.  Increment RREQ_COUNT for that neighbor
7.  If RREQ_COUNT < LT Then
8.    Process the RREQ
9.  Else
10.   If RREQ_COUNT > M Then
11.   Black list the specified node and declares it is malicious
node
12. If the node behaves as malicious Then
13.   Drop the data packets received by the malicious node.
14. Else
15.   If the RREQ_COUNT > L Then
16.   Ignore all route requests
17. 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.

3) GRAY-HP algorithm design

The employed algorithm ensures a fair distribution of resources among all contending neighbors [22, 23]. Incoming RREQs are processed only when the number of RREQs from the said neighbor is below RREQ_ACCEPT_LIMIT. This parameter specifies a value that ensures uniform usage of a node's resources by its 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 its requests 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 in their 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 Fig. 4, the wireless network is formed and the accessibility of each node is established. The communication of the source with other mobile nodes is the 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 then the 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, the route discovery phase then begins.

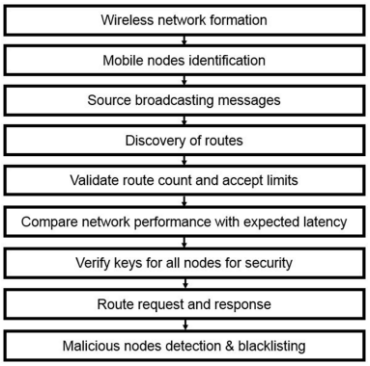

Figure 4. GRAY-HP algorithm design flow.

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 this process is done, the prevention and blacklisting of malicious attacks using the proposed GRAY-HP algorithm take place. This process will be iterated until all the malicious nodes have been prevented and blacklisted explained previously.

The proposed Gray-HP algorithm is demonstrated using Algorithm 4.

Algorithm 4: Gray Hole Prevention (Gray-HP)

1. **Begin**
2. L = RREQ_RATE_LIMIT
3. LT = RREQ_ACCEPT_LIMIT
4. M = RREQ_BLACKLIST_LIMIT
5. MS = MESSAGE SIZE
6. B = BANDWIDTH
7. EL = EXPECTED_LATENCY
8. NL = NETWORK_LATENCY
9. Set nm[i][j]; // where i = node at 'x', and j=node 'y' position
10. Set source=sn;
11. Set key[]=nm; // nm denotes number of mobile nodes
12.
13. **While** RREQ_COUNT ≠ 0
14. $NL = \frac{MS}{B}$ //To calculate the current network latency to determine and monitor network performance to ensure that nodes are not blacklisted because of poor network performance.
15.
16. **If** RREQ_COUNT < LT **Then**
17. Process the RREQ
18. Receive another RREQ and increment RREQ_COUNT by 1
19. //Upon receiving the RREQ by a neighbor node
20. //Increment RREQ_COUNT for that neighbor
21. **Else**
22. **For each** i = 1 **to** nm **step** 1
23. **For each** j = 1 **to** nm **step** 1

24. **If** nm[i][j]packets.equals(drop) **Then**
25. **If** RREQ_COUNT > M && NL < EL **Then**
26. **If** key.equals(null) && ipaddress.equals(redundant) **Then**
27. Blacklist(nm[i][j]); //Blacklist the specified node and declare it as a malicious node
28. **Else**
29. **If** key.equals(null) && ipaddress.equals(unique) **Then**
30. Send(nm[i][j]); //Send packets to the legitimate sink node
31. **Else**
32. Sink node cannot receive packets
33. Continue the process of RREQ
34. **End if**
35. **End if**
36. **End if**
37. **End if**
38. **Next j**
39. **Next i**
40. **End if**
41. **Do**
42. **If** the node is declared as malicious **Then**
43. Resend the RREQ to other neighbor nodes (excluding malicious nodes)
44. **Else**
45. **If** RREQ > L **Then**
46. Ignore all route requests
47. **End if**
48. **End if**
49. **Until** all malicious nodes are blacklisted
50. **Loop**
51. **End**

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 and declared 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.

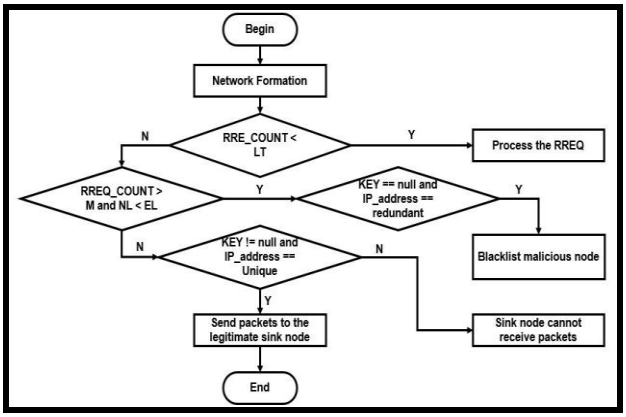

Figure 5. GRAY_HP flowchart.

V. Related Simulations and Experimental Results

Several simulations were conducted to assess the performance of the proposed GRAY-HP algorithm against RSetTheory and GA-BFO algorithms. RSetTheory and GA-BFO were previously proposed to improve the original DSR, AODV, and DSDV protocols therefore, in this paper, it is anticipated that both RSetTheory and GA-BFO have better performance than the original DSR, AODV, and DSDV. Throughput, routing overhead, and delivery ratio were used to compare GRAY-HP, RSetTheory, and GA-BFO algorithms.

In this research paper, the NS-2 simulation tool was used as an experimental platform for the proposed GRAY-HP. The model is used for creating mobility scenarios on a random basis. The random waypoint model is the simplest mobility model, generating completely random movement patterns. It was designed for simulations in which the movement patterns of mobile nodes are completely unpredictable. Since many entities in nature move in extremely unpredictable ways, the Random waypoint model is developed to mimic this erratic movement. The Random waypoint with a set of tools is created. The saddest' application in the directory is a third-party application of NS; /ns-2.35/indep-utils / cmu-scen-gen / setdest. Randomly creates node positions in the network with the speed and pause time specified. Table I below present the simulation parameters used in this paper.

TABLE I. Simulation Parameters

Parameters	Values
1. Network Area	100m × 100m
2. Number of nodes	100
3. Packet Rate	2,4,6,8,10,12,14, and 16 bit/s
4. Packet Size	512 bytes
5. Traffic Type	TCP
6. Number of Malicious Nodes	0–10
7. Node Speed	0–30 m/s
8. Simulation Time	100s

A. Throughput

The number of data bits that are delivered in unit time measured in bps in the application layer of destination Nodes. This is the amount of data transferred successfully in a given period from one place to another and measured by kilobit per second (kbps), megabits per second (Mbps), or gigabits per second (Gbps). The simulation results for the throughput for all three algorithms is shown in Fig. 6 below.

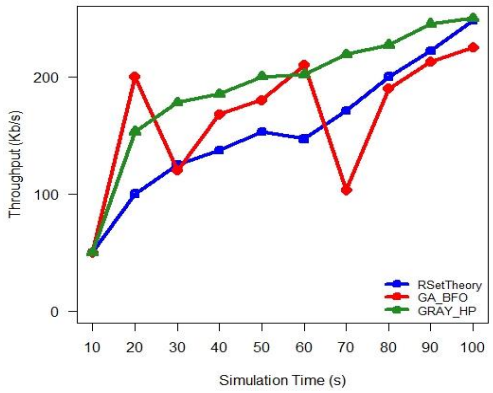

Figure 6. Network throughput.

The proposed GRAY-HP algorithm produced improved average network throughput as compared to that of RSetTheory and GA_BFO algorithms. These promising results have been clearly shown in Fig. 6. The main reason is that the proposed GRAY-HP algorithm introduced the process of excluding and blacklisting malicious nodes. Furthermore, the proposed GRAY-HP algorithm calculated the network performance to avoid blacklisting legitimate nodes due to poor network performance. The simulation results showed an improved average network throughput by appropriately 90.9% as compared to that of RSetTheory and GA_BFO algorithms.

B. Delivery Ratio

Thee The packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources. The simulation results for the packet delivery ratio for all three algorithms is portrayed in Fig. 7 below.

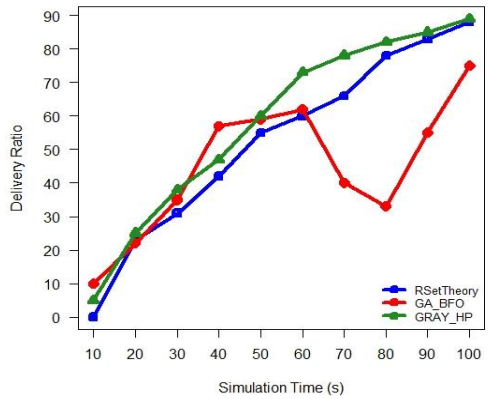

Figure 7. Network throughput.

The proposed GRAY-HP algorithm seems to have improved delivery ratio as compared to RSetTheory and GA_BFO algorithms. This improvement has been achieved by employing the Gray-Attack prevention technique 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 GRAY-HP 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 proposed GRAY-HP algorithm results showed that it outweighs other algorithms with an increase of average delivery ratio with about 89%.

C. 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 for the Overhead Routing for all three algorithms is portrayed in Fig. 8 below.

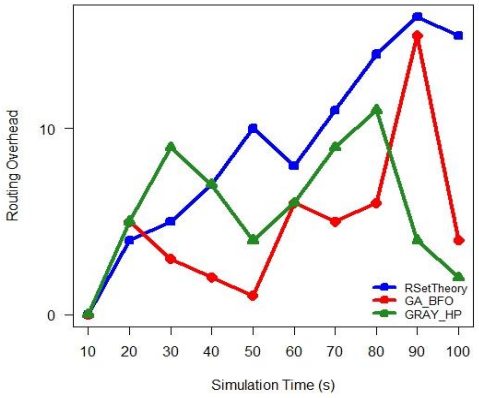

Figure 8. Routing overhead.

Fig. 8 compares, as obtained through multiple simulations, the routing overhead by the proposed GRAY-HP algorithm with that of RSetTheory and GA_BFO algorithms. Fig. 8 clearly shows that the GRAY-HP algorithm reduced the routing overhead compared to the others. This was achieved as a result of reducing congestion problems through blocking and blacklisting malicious nodes. The proposed GRAY-HP 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 proposed Gray-HP algorithm determined the network performance to ensure that legitimate nodes are not blocked and blacklisted because of poor network performance. The proposed GRAY-HP algorithm results showed that it outweighs other algorithms with an increase in routing overhead with an appropriate 5.7%.

VI. Conclusion and Future Work

Symbols This paper designed and implemented an algorithm that effectively detects and prevents a gray hole attack in MANET by implementing the GRAY-HP

algorithm. The SDPEGH and Proactive scheme were integrated to produce the GRAY-HP algorithm which was compared with RSetTheory and GA-BFO algorithms. The integration of these algorithms successfully detects and prevents the gray hole attack, and maintains the QoS efficiency, delay constraint, and overhead routing.

The GRAY-HP algorithm proposed in this paper successfully detects and prevents a gray hole attack in MANET while satisfying the throughput, deliver ratio, and routing overhead. The proposed GRAY-HP algorithm was implemented and evaluated using NS2 simulation. The SDPEGH and the Proactive scheme were integrated when designing the proposed GRAY-HP algorithm to advance the performance of the MANET. The number of drawbacks for MANET algorithms were highlighted and indicated that better results could be obtained by combining these algorithms. Nonetheless, not all algorithms yield better results when combined and therefore diversity measures were used to help discover the algorithms that can produce better results.

The simulation results showed an improved average network throughput by appropriately 90.9% as compared to that of RSetTheory and GA_BFO algorithms. The proposed GRAY-HP algorithm results showed that it outweighs other algorithms with an increase of average delivery ratio with about 89%, and routing overhead with appropriate 5.7%. These results show that the proposed GRAY-HP algorithm is better than RSetTheory and GA_BFO algorithms. This was achieved as a result of reducing congestion problems through blocking and blacklisting malicious nodes while not compromising the QoS.

Some research ideas can be taken from these investigations, such as implementing different algorithms to address other attacks on MANET such as the Black hole, Selfish, Wormhole, and Jellyfish attack.

CONFLICT OF INTEREST

The authors state that there are no conflicts of interest in the publication of this research.

AUTHOR CONTRIBUTIONS

Thabiso N. Khosa carried out the research, wrote the paper, design of the algorithm, simulated, and evaluated the results. Topside E. Mathonsi have been involved in revising the manuscript for important intellectual content. Deon P. Duplessis have contributed to the manuscript's creation and critical revision for key intellectual substance. All authors approved the final version.

ACKNOWLEDGMENT

The authors would like to thank the Tshwane University of Technology with their support.

REFERENCES

[1] J. Cai, P. Yi, J. Chen, Z. Wang, and N. Liu, "An adaptive approach to detecting black and gray hole attacks in ad-hoc network," in *Proc. 2010 24th IEEE International Conference on Advanced Information Networking and Applications*, 2010, pp. 775–780.

[2] S. K. Sarkar, T. G. Basavaraju, and C. Puttamadappa, *Ad-hoc Mobile Wireless Networks: Principles, Protocols and Applications*, Auerbach publications, 2007.

[3] J. Abdullah, "QoS route search for mobile ad-hoc network using genetic algorithm," *Nature-Inspired Networking: Theory and Applications*, pp. 183–230, 2018.

[4] J. Kaur and G. Singh, "MANET routing protocols: A review," *International Journal of Computer Sciences and Engineering (ICSE)*, vol. 5, no. 3, pp. 60–64, 2017.

[5] M. Er-Rouidi, H. Moudni, H. Mouncif, and A. Merbouha, "An energy consumption evaluation of reactive and proactive routing protocols in mobile Ad-hoc network," in *Proc. 2016 13th International Conference on Computer Graphics, Imaging and Visualization (CGiV)*, 2016, pp. 437–441.

[6] Y. Bai, Y. Mai, and N. Wang, "Performance comparison and evaluation of the proactive and reactive routing protocols for MANETs," in *Proc. 2017 Wireless Telecommunications Symposium (WTS)*, 2017, pp. 1–5.

[7] G. A. Walikar and R. C. Biradar, "A survey on hybrid routing mechanisms in mobile ad-hoc networks," *Journal of Network and Computer Applications*, vol. 77, pp. 48–63, 2017.

[8] S. Shruthi, "Proactive routing protocols for a MANET-A review," in *Proc. 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2017, pp. 821–827.

[9] S. Fauzia and K. Fatima, "Performance evaluation of AODV routing protocol for free space optical mobile Ad-hoc networks," in *Proc. the International Symposium on Intelligent Systems Technologies and Applications*, 2017, pp. 74–83.

[10] S. B. Sharma and N. Chauhan, "Security issues and their solutions in MANET," in *Proc. 2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE)*, 2015, pp. 289–294.

[11] N. Kumari, S. K. Gupta, R. Choudhary, and S. L. Agrwal, "New performance analysis of AODV, DSDV and OLSR routing protocol for MANET," in *Proc. 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, 2016, pp. 33–35.

[12] A. S. K. Pathan, *Security of self-Organizing Networks: MANET, WSN, WMN, VANET*, CRC press, 2016.

[13] K. Pavani and D. Avula, "Performance evaluation of mobile adhoc network under black hole attack," in *Proc. International Conference on Software Engineering and Mobile Application Modelling and Development (ICSEMA 2012)*, IET, 2012, pp. 1–6.

[14] M. C. K. Reddy and B. Sripriya, *A Study on Gray-Hole Attacks in Mobile Ad-hoc Networks*, 2017, pp. 1634–1636.

[15] S. Jain and A. Khuteta, "Detecting and overcoming blackhole attack in mobile adhoc network," in *Proc. 2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, 2015, pp. 225–229.

[16] A. Patel, N. Patel, and R. Patel, "Defending against wormhole attack in MANET", in *Proc. 2015 Fifth International Conference on Communication Systems and Network Technologies*, 2015, pp. 674–678.

[17] M. Mohanapriya, and I. Krishnamurthi, "Modified DSR protocol for detection and removal of selective black hole attack in MANET," *Computers & Electrical Engineering*, vol. 40, no. 2, 2014, pp. 530–538.

[18] G. Singh, "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security," *International Journal of Computer Applications*, vol. 67, no. 19, 2013.

[19] K. Bawa and S. B. Rana, "Prevention of black hole attack in MANET using addition of genetic algorithm to bacterial foraging optimization," *Int. J. Curr. Eng. Technol*, vol. 5, no. 4, 2015.

[20] M. Radha, and M.N. Rao, "Gray hole attack detection prevention and elimination using SDPEGH in MANET," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 8, no. 3, 2019.

[21] S. Sathish and M. Saranya, "Malicious node identification scheme for MANET using rough set theory," *International Journal of Computational Intelligence and Informatics*, vol. 6, no. 2, pp. 172–183, 2016.

[22] P. Sahu, S. K. Bisoy, and S. Sahoo, "Detecting and isolating malicious node in AODV routing algorithm," *International*

Journal of Computer Applications, vol. 66, no. 16, pp. 0975–8887, 2013.

[23] V. Srinivasan, "Detection of black hole attack using honeypot agent-based scheme with deep learning technique on MANET," *Information Systems Engineering*, vol. 26, no. 6, 2021, pp. 549–557.