In MANET Q, the DSR Protocol Has Been Modified To Identify and Remove Selective Black Hole Attacks

Sweta Kumari Barnwal, Assistant Professor

Department of Computer Science, Arka Jain University, Jamshedpur, Jharkhand, India

Email Id- sweta.b@arkajainuniversity.ac.in

ABSTRACT: In an ad hoc network, a black hole attack occurs when hostile nodes forcefully acquire the route from a source to a destination by fraudulently advertising the shortest hop count to reach the target node. A Modified Dynamic Source Routing Protocol (MDSR) is presented in this article to identify and avoid selective black hole attacks. A selective black hole attack is a kind of black hole attack in which hostile nodes selectively discard data packets. To identify the anomalous difference in the amount of data packets sent by a node, we suggested an Intrusion Detection System (IDS) in which the IDS nodes are configured in promiscuous mode only when needed. When an anomaly is discovered, the adjacent IDS node sends out a block message to other nodes in the network, instructing them to work together to remove the malicious node from the network. Glomosim is used in the suggested method to verify the efficacy of the proposed intrusion detection system.

KEYWORDS: Black Hole, Routing, Detection System, Dynamic Source, Malicious.

1. INTRODUCTION:

There are no routers or access points in a wireless Mobile Ad hoc Network (MANET); data is transferred between nodes through several hops. To establish a route, each mobile node serves as both a host and a router. Because packets are transmitted via intermediary nodes when a source node wishes to send data to a destination node, finding and rapidly establishing a route from a source to a destination node is a critical problem for MANETs. The MANET routing protocols that are currently available are primarily divided into proactive and reactive routing protocols[1].

Every node in a proactive routing protocol like DSDV (Destination Sequence Distance Vector) or OLSR (Optimized Link State Routing Protocol) proactively searches for routes to other nodes and exchanges routing messages on a regular basis to keep the routing table formation up-to-date and correct. Because MANET nodes have limited power and bandwidth, frequent transmission of routing messages would cause network congestion. A route is sought and created only when two nodes want to transmit data in a reactive routing protocol like AODV (Ad hoc On-Demand Distance Vector) [1] or DSR (Dynamic Source Routing) [2]. Because most of these routing protocols rely on node cooperation for packet forwarding, a malicious node may launch routing attacks that interrupt regular routing operations or Denial-of-Service (DOS) attacks like the black hole or gray hole that deny service to genuine MANET nodes.

MANETs are commonly used for disaster communication, battlefield communication, and business conferences. As a result, data transfer between two nodes must be secure. The majority of secure routing protocols are designed to protect safety properties like

- authentication and non-repudiation;
- resource availability;
- integrity; and
- Confidentiality and privacy.

These security mechanisms can only protect against external attacks, that is, attacks launched from the outside.

nodes that aren't part of the network Internal assaults such as black hole or gray hole attacks, routing attacks, and worm hole attacks, on the other hand, are very difficult to detect since they are launched by compromised nodes that have been allowed by the target network.

A gray hole attack, also known as a selective black hole attack, is a type of black hole attack that can be launched easily on reactive routing protocols such as DSR or AODV. A malicious node may draw all data packets by falsely claiming a new or quickest route to the target and then absorbs them without forwarding them to the destination in a black hole attack; however, in a gray hole attack, malicious nodes participate properly in the route discovery process. However, once a route is chosen through them to reach a destination, they will selectively drop data packets. Gray hole attacks are more difficult to detect than black hole attacks because only partial data packets are dropped[3].

By monitoring and analyzing the forwarding behaviors of wireless nodes, we propose a non-cryptographic technique for detecting gray hole attacks in this paper. The existence of gray hole attackers in the route is detected by the destination node using a substantial discrepancy between the number of data packets sent by the source node and the number of data packets it actually receives. The IDS nodes are then notified of the suspected nodes, allowing the malicious nodes that launch the selective black hole attack to be isolated from the network. Because the DSR [2] is one of the most widely used reactive routing protocols and has been extensively addressed in research publications, this work installs and analyzes the suggested approach on DSR-based MANETs[4].

The suggested protocol has more virtues than previous similar studies; the most significant merit is that it accomplishes packet loss rate decline without any computational complexity. Similarly, IDS nodes only go into promiscuous mode once a network assault is detected. The suggested work's sole restriction is the location of IDS nodes. The IDS nodes should be chosen in such a way that any of the IDS nodes can reach all network nodes, i.e., the suspected nodes should be within range of any of the IDS nodes. In situations when gray hole attackers are beyond the range of all IDS nodes, identification and isolation of gray hole nodes may be impossible if the IDS nodes do not cover the whole network.[5]

The rest of this paper is laid out as follows. In Section 2, prior work on black hole and gray hole attacks in reactive routing protocols is reviewed; in Section 4, we provide the implementation of our MDSR method; in Section 5, we discuss experimental data and analysis using GLOMOSIM; and in Section 6, we offer our findings[6].

Reactive routing schemes like AODV [and DSR are vulnerable to black hole attacks. Many safe routing algorithms have been suggested to prevent single and cooperative black hole attacks, and it has gotten a lot of attention in recent research.

A gray hole attack (selective forwarding attack) is a kind of black hole attack in which the behavior of a rogue node is very unpredictable. The assault may be carried out in three ways by the gray hole nodes: I While forwarding all other packets, the rogue node may drop packets from certain nodes. (ii) A node may act maliciously for a period of time, selectively discarding packets. (iii) Is a hybrid of the two attacks, in which the malicious node drops packets from specified nodes for a limited period before returning to normal behavior Gray hole attacks are difficult to detect because of these features. A gray hole attack may impair network performance by disrupting route finding. On reactive routing systems like AODV and DSR, both black hole and gray whole attacks are simple to launch.

Proposes a novel routing security method for hierarchical ad hoc networks based on reputation assessment. The reputation relationship is based on the node's actions and correlation. It includes an incentive system to encourage cluster members to cooperate in forwarding data packets and to improve cluster members' activity likelihood in the network. Selective forwarding attacks were originally presented by Karloff and Wagner, who stated that multi path forwarding might be utilized to prevent these assaults in sensor networks. The program, on the other hand, fails to provide a technique for detecting and isolating the attackers from the network. The authors of suggest a system in which a portion of the intermediate nodes along a forwarding route is randomly

selected as checkpoint nodes, which are in charge of producing acknowledgments for each packet received. If suspicious activity is identified, an alert packet is generated and sent to the source node. The method, however, has a significant cost since the intermediary nodes must send an acknowledgement to the source node for each packet received. Furthermore, the authors assume that the channel is flawless and that any packet loss is attributable to hostile nodes. To identify and isolate gray hole nodes, the method described in requires all nodes participating in a data forwarding session to produce a proof for receiving the data packets. When a source node detects a misbehavior, the checkup method is used to evaluate intermediary nodes. It uses the Diagnosis algorithm to track out the malicious node based on the results of the checkup algorithm.

The authors of approach [20] dealt with the Byzantine Agreement (BA) issue in order to solve the fault-tolerance problem in distributed systems. The majority of BA problems need all of the healthy processors to reach an agreement in the same round, which is known as an Immediate Byzantine Agreement (IBA). When the fact up (fact is the number of real arbitrary faulty processors; up is the number of tolerable arbitrary faulty processors), another kind of agreement, Eventual Byzantine Agreement (EBA), enables its parties to achieve a common agreement at various rounds. In the MANET, the EBA issue is explored in a dual failure scenario (processors and transmission medium). Early Dual Agreement Protocol is suggested in this method to reach agreement in a MANET while tolerating the greatest number of defective processors and transmission medium with the least amount of message exchanges. It can also effectively manage and arrange the network, even if the processors move around it.

In, the source node sends a prelude message to the destination node to warn it before transmitting any block of data. the traffic flow is monitored by the adjacent nodes. When the transmission is complete, the destination sends a postlude message with the number of data packets received. Initiate the process of identifying and eliminating all malicious nodes by aggregating responses from neighbor nodes of the originating route in the network if the data loss exceeds the acceptable range. Even when there is no attack, all nodes around the nodes in the source route enter promiscuous mode to monitor their data forwarding behavior, resulting in energy loss in individual nodes[7].

2. DISCUSSION:

DSR is a source routing mechanism that runs on demand. Because routes are found when a source delivers a packet to a destination for which it does not have a cached route, it is an on-demand protocol. Route discovery and route maintenance are the two primary functions of DSR. The protocol's fundamental strategy during the goal of the route discovery phase is to create a route by flooding the network with Route Request (RREQ) packets. The final destination node is When it receives an RREQ packet, it sends a Route Reply (RREP) packet back to the source, reversing the route information in the RREQ packet. Any intermediary node may transmit the RREP back to the source node after receiving the RREQ.if it knows how to go to the destination

The connection breakdowns are dealt with during the Route maintenance phase. When any intermediary node that is connected to the main node breaks the connection, it is called a link break. Travels out of the transmission range of its upstream neighbor during the packet forwarding process. If a node farther upstream fails, when a packet is sent to the next node in the route path, it detects a link break and returns a route error (RERR) message. Contact the source, notifying it of the broken connection the source either attempts another accessible path or starts the route discovery process[8].

If node A is inside node B's transmission range, node B is also within A's transmission range. (b) In addition, our approach requires that all nodes are authenticated and can communicate, i.e., that all nodes are authorized nodes.(c) By default, the source, destination, and IDS nodes are considered trustworthy nodes. (d) All IDS nodes have been configured. Only use promiscuous mode when absolutely necessary, and an IDS node will always be neighbors with another IDS node. d) Because there are because there are many routes from a source to a destination, the source node must cache the other routes to reduce the overhead. Throughout the process of discovering new routes The source node must broadcast the RREQ packet to discover a route to the desired destination, according to the DSR protocol. The desired destination, or any intermediary node with the route, may respond to the source node with a reply. As

The malicious nodes that carry out gray hole attacks participate properly in the route discovery process, They send the RREQ packets just like any other DSR node. When the route via this malicious node is chosen, To go to the destination, it loses data packets one by one, as illustrated in Fig. 1b. When the destination nodes receive data packets from the source node, they begin the process of detecting the existence of any gray holes in order to counteract gray whole attacks. The path's nodes when the source node has data packets to transmit to the destination, it splits the data to be sent in our method. The data is split into separate chunks and sent to the destination one block at a time. It also tells you how many data points there are. Before sending the data, it sends a block of packets to the target over a different route.

The number of packets transported from source node S to destination node D in a block is denoted by the letter NS. Let's call the nodes a0, a1, and a2The source route or data forwarding path between source node S and destination node D ire presented by a3,..., an. Any ai node inAs NFPai, ai+1, the route must keep track of the amount of packets it sends to its downstream node ai+1. When the destination node gets data packets from the source, it begins a counter to keep track of how many data packets it has received in a block. Let ND stand for the number of packets received at the destination node, and then the probability of packets arriving at the source node.

If PD > TPL, the destination node begins the process of determining if the route contains any malicious nodes. If not, the source node receives an affirmative acknowledgment from the destination node. The packet is represented by TPL in this case. The destination node begins the gray hole detection in our methodology, and it accepts values between 0 and 0.2.When the data packet loss exceeds 20% of the total packets transmitted by the source node, the procedure is initiated. Only after getting a positive acknowledgment from the destination or an ALARM packet from a neighboring IDS node does the source node begin sending the next block of data. The activity of the source and destination nodes during transmission is shown in Procedure 1.involves the transmission and receipt of data packets

The gray hole node detection process begins when the destination node notices that the actual number of data packets it gets from its previous hop node is substantially fewer than the number of data packets the source node transmits. First and foremost, it transmits a QUERY REQUEST (QREQ) packet at a 2-hop distance to the node in the source route (data forwarding path). If The source path is represented as S, a0, a1, a2,..., an3, an2, an1, an, D, and node D transmits a QREQ packet to node an1 at 2-.[3]

Procedure 1: During data forwarding, the source and destination take action. If the source node is the number of data packets in a block of data is intimate to the destination. Send one block of data through the route discovered during the route discovery procedure. Otherwise, if the target node Compare the number of data packets received to the number of data packets indicated by the source.As PD, determine the likelihood of packets arriving at the target node.PD TPL PD TPL PD TPL PD TPL PD TPL PD T (the value of TPL is between 0 and 0.2) Return to the source node a positive acknowledgment.ElseStart the discovery process for the Gray Hole Attack. If it's over

The QREQ is used to determine how many data packets a node has forwarded to its next hop node. The node's name isTo the destination node D, an1 sends a QUERY REPLY (QREP) packet. In the source route, the QREP includes the number of data packets sent by a node to its next hop neighbor. The destination node derives its information from the QREP it gets. checks that its previous hop neighbor (for example, node an) is properly forwarding all data packets received from it.its preceding node (node an1). If the destination node is incorrect, both nodes an1 and an are added to the suspicious list. Incorrect indicates that the two nodes are properly engaging in data forwarding. As a result, the destination sends another message.new QREQ to node an3 in the source route, which is two hops away from node an1. The destination node checks if those two nodes, an3 and an2, are transmitting all of the data packets they get from the QREP it receives.received. This procedure continues until the QREQ reaches a node at 2-hop that hasn't had a prior hop node. in the source route's distance Computers and Electrical Engineering 40 (2014) 530–538 533 M. Mohanapriya, I. KrishnamurthiProcedure 2: During the gray hole attack discovery phase, the target node takes action. When a destination node suspects the existence of a gray hole attack, it takes the following steps.1. Send a QREQ packet to a node in the source path, say X, that is two hops away.2. Node X sends you a QREP packet.3. Count the number of data packets sent by

all nodes from node X to itself using the QREP packet.4[9]. If the number of data packets sent matches,Rep step 1 to a node, say Y, in the source route that is at a 2-hop distance from node X.

Steps 2, 3, and 4 should be repeated.

Otherwise, if the number of data packets sent does not match, Add the source route's next node, as well as the node that transmits QREP, to the suspicious list.Put a stop to it.A first level of verification of data forwarding behavior of intermediary nodes in the source is performed using QREP packets. The destination will carry out the route. If the number of packets sent between any two intermediates differs[8]

When a node's monitoring threshold value is exceeded, the destination node flags both intermediate nodes as suspicious. Between any two nodes, the probability of malicious behavior, Pmb, is computed as follows:

(2) NFPan2, an1 indicates the number of data packets forwarded from node an2 to node an1. If Pmb > Tm, then any node may be used. A malicious node is node an2 or node an1. Tm denotes the monitoring threshold, which may range from 0 to 0. Procedure No. 2displays the destination node's behavior during the gray hole attack discovery phase.After the source node 1 transmits a block of data to the destination node 8 the destination validates the number of bytes sent. It received a certain number of data packets. Node 1 informs node 2 of the number of data packets it is sending in a block.destination node before beginning the actual packet transmission procedure. If the destination receives data packets[10]

3. CONCLUSION:

To identify gray hole nodes in MANET, we developed a light-weight solution approach that is a simple acknowledgment mechanism. It can work with any current ad hoc routing protocols on demand. The suggested method identifies hostile nodes in the source path, and with the aid of an intrusion detection system, the destination node recognizes them. Malicious nodes are cut off from the rest of the network. In addition, our IDS nodes will become promiscuous listeners only in the presence of other IDS nodes. Our approach is appropriate for resource limited features since it reduces the number of suspicious nodes, resulting in reduced energy loss. MANET is a network of networks. The simulation results indicate that our proposed work has a lower proportion of data packet loss than DSR.Multiple gray hole nodes are present[3].

REFERENCE:

[1] I. D. Soares, “A boosted Kerr black hole solution and the structure of a general astrophysical black hole,” *Gen. Relativ. Gravit.*, 2017.

[2] J. L. Bernal, A. Raccanelli, L. Verde, and J. Silk, “Signatures of primordial black holes as seeds of supermassive black holes,” *J. Cosmol. Astropart. Phys.*, 2018.

[3] P. Bueno and P. A. Cano, “Universally stable black holes,” *Int. J. Mod. Phys. D*, 2017.

[4] D. Gaiotto, A. Strominger, and X. Yin, “5D black rings and 4D black holes,” *J. High Energy Phys.*, 2006.

[5] I. D. Novikov, “Black holes,” *Surveys in High Energy Physics*. 2003.

[6] X. Calmet and R. Casadio, “What is the final state of a black hole merger?,” *Mod. Phys. Lett. A*, 2018.

[7] W. Z. Chao, “Quantum black hole,” *Gen. Relativ. Gravit.*, 1998.

[8] J. Zhang, “Black hole quantum tunnelling and black hole entropy correction,” *Phys. Lett. Sect. B Nucl. Elem. Part. High-Energy Phys.*, 2008.

[9] J. van Dongen and S. de Haro, “On black hole complementarity,” *Stud. Hist. Philos. Sci. Part B - Stud. Hist. Philos. Mod. Phys.*, 2004.

[10] Z. Xu, X. Hou, and J. Wang, “Possibility of identifying matter around rotating black hole with black hole shadow,” *J. Cosmol. Astropart. Phys.*, 2018.