International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Enhanced AODV Routing for Secure MANET Using Preventing Gray hole Attack

Jagdish J. Rathod[1], Amit M. Lathigara[2]

[1]PG Scholar, Computer Engineering, School of Engineering, RK University, Gujarat, India

[2]Head of Department, Computer Engineering, School of Engineering, RK University, Gujarat, India

Abstract: ***Ad hock Network is a temporary network set up to share information among nodes. The network is constrained about resources and always has threat from malicious nodes. Gray hole attack is one of the attack in which, attacker node drops some packets and forward some packets and because of its behaviour its difficult to detect and prevent. In this Paper proposed a technique to identify and prevent Gray hole attacks in AODV based MANETs, in proposed approached, using AODV protocol which is widely used in MANETs and it easy to use. In Proposed work by verifying source address in the RREQ control packet named Source Node ID. This field will be used to store the value of the IP of the intermediate node that processes the RREQ. Because it checks destination sequence number and time stamp when any RREP comes from source node or and any attacker nodes. Source node will keep this field empty when it initiates the route request and forward the RREQ packet. It will keep a copy of its own RREQ. Proposed method uses the available control packets i.e. RREQ and RREP to ascertain trustworthiness of a node. Therefore, new packets like acknowledgment packets need not be introduced for proving reliability. Results are present taken with the help of the NS2 simulator, which is widely used in networking field.***

Keywords: Ad hock network, Security, different Attacks, Gary Hole Attack, NS2,AODV.

1. Introduction

Restricted to the framework remote systems where every client straightforwardly speaks with an entrance point or base station, MANET is a sort of remote specially appointed system [1]. MANET is a self-arranging system of portable switches associated with remote connections with no entrance point. Each mobile node in a system is self-governing, move anyplace at whatever time. The Mobile nodes are allowed to move heedlessly and arrange themselves subjectively. Security in (MANETs) is the most essential sympathy toward the fundamental usefulness of the system. The accessibility of the administrations of MANETs can be ensured just by guaranteeing that the security issues have been determined up to in any event some degree. Certain qualities of MANETs, for example, dynamic topologies, attack limitations, constrained physical security [2] and no base which makes its security exceptionally defenseless.It has no focal checking and various Gary Holes which may compromise the availability of management and also no clear line of site. This feature imposes the security threats, and results into various attacks. Which may compromise the availability of the network, Lack of centralized authority causes it to operate on the basis of mutual trust. This attack makes it more powerless against be misused by an attack inside the system.

2. AODV Routing Algorithm

This section investigates AODV convention in purpose of interest. AODV remains for Ad-hoc On Demand Distance Vector. It is a directing convention, which uses the open methodology of routing; It is in view of the DSDV convention clarified in the previous segment. It utilizes the table driven methodology, It finds the routes just when necessary. Any reactive protocol does three capacities in the network as talked about prior.

a) Route Discovery, b) Data Forwarding and c) Route Maintenance [5]. AODV performs these capacities by utilizing three control Packets 1-Route-Request (RREQ) packet,2-Route-Reply (RREP) packet and 3- Route-Error (RERR) packet.

3. Gray hole Attack

The Gray hole attack is most risky and dangerous attack in MANET, it carries on differently as contrasted with all other attacks on the grounds that at some point drop the packets and eventually not. Attacker node first agrees to forward packet and after that fails to do as being what is indicated and not forward the packet to the destination [6]. At first the node demonstrations adequately like bona genuine node and replays veritable RREP messages to node that start RREQ message (send RREP to source node). Thus, it assumes control over the packets send the packets send by the source node. Next the node just drops the packets and reveals to it behave like genuine node to dispatch a DOS attack [7]. In the event that neighboring node attempts to send packets over attacker nodes the it lose the association with destination node, then they may need to send also, look Route once more, again broadcast RREQ messages to all its neighbor nodes [8]. Attacker node again makes a Route, sending RREP messages as authentic node sends. This procedure is run until malignant or attacker node succeeds its point (e.g. system resource utilization, corrupt system execution, and make the traffic). This attack called Gray hole attack [8].

4. Related Work

Rutvij H. et al. [9] proposed the AODV protocol, works like when an any node gets a route or route answer (RREP), the it first checks the succession number esteem in its own particular directing table; if it is more imperative than the

one in the RREP, the RREP packet is acknowledged; if it less at that point it is disposed of, this is the first condition. The Route finding begins in AODV while the aggressor hub is available. Source node sends the RREQ next gesture get also, again rebroadcast if the destination hub not discovered still it Broadcast the RREQ. At the point when the destination node gets the RREQ then it This node again sends RREP to the originator on the other way the way of the RREQ. Presently the aggressor node shows its conduct and sends the RREP with a higher Destination grouping number of the source node; another RREP is sent by Destination having a truly higher Destination Sequence number. Than the ordinary node or when contrasted with another node, when an assailant gesture collector the packets, then it begin to drop the packet. In that case source node imagines that the packets are going towards the destination, however this suspicion aren't right. In this proposed approach, one estimation is going on and that is to ascertain the Crest value.

Course based method proposed by Deepali Raut et al. [10] in which the node are not able to observe all the nodes, but only observe the next node in present path. By observation and doing some work it possible to say that the same packet are dropped and some of them are not drop so there are Gray hole attack are generated because it drop some of the packets. in which the router will maintain the packet count A history in which it maintains all the record as it forward the downstream node. in this paper the Simulation results show that the proposed method has good performance against Black hole attack without much overhead.

Route Discovery approach Proposed By Rutvij h. et al. [11] in proposing the method start finding of default AODV in the presence of an attacker. Source node S sends data to destination D broadcasts RREQ; and malicious node MN replies back with a RREP containing high destination sequence number misleading S as if it has a fresher route to D; another normal intermediate node IN sends RREP having a higher sequence number. As RREP of the attacker holds higher destination sequence number of all received RREPs, source node find out path and select them to send the data. attacker node create and shows it malicious behaviour and drop some of the data from all the received data and forward some of them. Given proposed method provided and do improvement in route discovery process of AODV protocol to find multiple Black hole and Gray hole nodes. R-AODV provides a simple and easy way to detect and isolate more than one attacker nodes without introduction of any extra control packet.

An Approach discussed by Gundeep Singh Bindra et al. [12] in which the proposed work comprises in following steps: Implementation of Modified EDRI Table and the algorithm towards detecting Gray hole and Cooperative Black hole attacks, Implementation of Negative Acknowledgment (NACK) Algorithm, Eliminating Non-Consecutive Cooperating Black hole and Gray hole attacks. In proposing work there are modifying the existing EDRI table. The EDRI table contains the entries for 'From' 'Through', 'CTR', 'BH' and 'Timer' but this is not sufficient for detecting Gray hole attack, hence by adding three new columns which are 'Packet size at source', 'Packet size at destination' and 'Result' which checks the complete data packet reaches from source to destination or partial data reaches to destination. These three entries are very useful to catch the packet routing problem in MANET. Because of this MEDRI table it is easy to find out the secure path from source to destination in MANET. The MEDRI table also records and maintain the history of previous malicious nodes that is used for the future secure transformation of data from source to destination and to discover a secure path from source to destination.

Onkar V. Chandure et al. [13] proposed an approach in which the new method is used in which the data routing information table is used. there are three nodes in the first node or the initiated nodes are called source node and the neighbour node are called cooperative mode and the attacker node are called suspected node. the source node first find out its neighbour node for transmission of data purpose. The source node sends the information to its neighbour node and In answer to this RREQ message the I Initiator Node or source node will get various RREP messages from its neighbouring nodes. And at the same time it will get the RREP from aggressor node. After getting the RREP from the SN, the IN sends a test packet to the CN through the SN. It likewise takes a shot at TTL it additionally checks the CN whether it get the test packet or not. if the packet are received the test packet or not if yes, they put the section on the DRI table at 1 if not then put 0.

Credit value based approach proposed by Deepali A. Lokare et al. [14] in which initially each and every node assigns a static value for its every neighbour node as the neighbour credit value. This credit value is incremented by when it receives a route request packet (RREQ) and decrement when it receives the route reply (RREP) packet. When a node able to finds credit for one of its neighbours as a negative value, then it identifies the Gray hole node. Also, it removes all existing paths from its routing table going through that node. When the node is found, then it not send the alarm packet, and therefore it reduces the routing overhead. every node maintains its record in its NVRAM. FALSE REPLY is the oak from which is detected as a fake or false from malicious. Every node assigns a credit value that we are sending the route request and subtracting the credit value when we got a reply from them. Credit based approach to mitigate the Gray hole attack.

Ira Nath et al. [15] proposed BHAPSC, a scheme in which clusters of nodes are made to detect Gray hole nodes. It uses so many tables and one of them is Friendship table, trust estimator and a control packet called False-Packet. Friendship table provides the relationship between the cluster head and its neighbour node. Calculates the trust value if trust value is too much higher than this information is provided by other nodes. To calculate the trust value of a stranger the trust estimator is called here. S first sends fake packets to the stranger. The malicious node will show its behaviour by acting as a black hole or Gray hole. In such scenario the transmission are stopped and not transmitted. if the next node are not Gray hole, then false packets are returning back and it's clear that there are not an attack. But attack is founded then there are drops of packet are possible.

A Method proposed by Shalini et al. [16] In which there are such a large number of routes through which it demonstrates

to the best practices to recognize and detect Gray hole or black hole attack: first system are by the source node. To distinguish the attack 1-Dividing information packet in same or k equivalent amounts of parts, 2-send the message to the destination, 3-disseminate this message to Remaining all neighbour nodes, 4-After beyond any doubt that destination node discovers check of messages, the source begins to send the information, 5-Setting up a clock still information got by destination, 6-If number of pronounced information packets from destination is not as much as a gave farthest point, begin evacuating the procedure of Black/Gray hole attack.

5. Proposed and Implemented Approach

A novel solution has been suggested for this problem by introducing three new procedures during the route discovery phase:

1- Source Node ID: The Proposed method to verify source address in the RREQ control packet named Source Node id filed. This field will be used to store the value of the IP of the intermediate node that processes the RREQ. The source node will add own filed when it initiates the route request and forward the RREQ packet. It will keep a copy of its own RREQ.

***2. Broadcast received RREQ*:** If the node is an intermediate node, it is required to send the RREQ back to the originator node by adding the value of its IP address to the field named SN_ID. This process is to be done by all the source node and intermediate nodes. Figure 5.1 shows how Source Broadcast the RREQ.

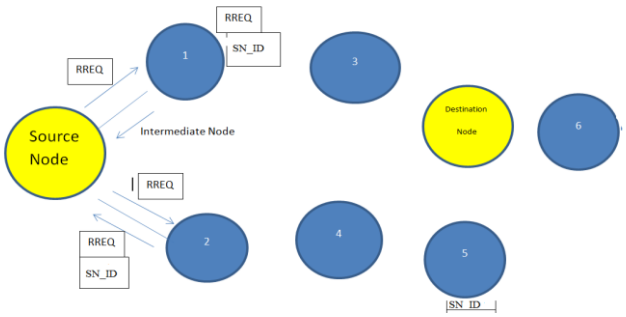

Figure 5.1
Source Broadcast the RREQ

3. Storage in cache memory: The source node and the intermediate nodes will store the values of the received RREQ viz, Destination sequence Number, Destination IP address, and Timestamp in its own cache memory if it is a new RREQ. If the RREQ has already been processed, it will discard it. Figure 5.2 shows How node stores the value In Cache table.

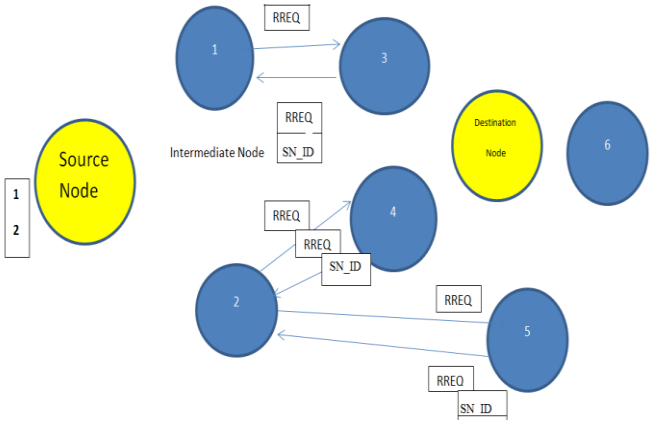

Figure 5.2: Schematic Representation of proposed approach

4. Compare with received RREP: Once the RREQ reaches destination node, it will send the RREP back by unicasting. The nodes which get back the RREP will compare the values of the already stored RREQ fields in the cache, i.e. Originator IP address, Originator Sequence Number, Destination Sequence number, Destination IP address and Timestamp with the values in the RREP. If it matches, the nodes can be sure that a secure route is established and all the nodes are trustworthy. Figure 5.3 shows the reception of the RREP.

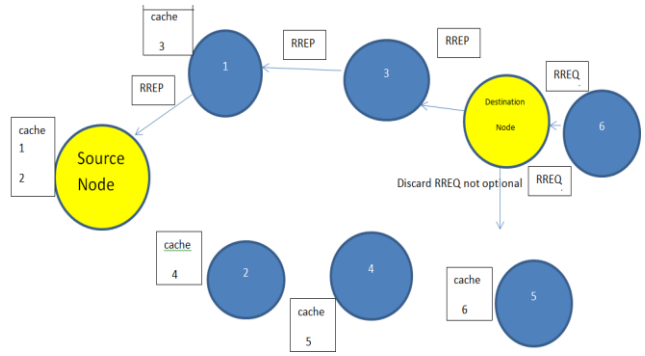

Figure 5.3: Schematic representation of reception of RREP

5. Detection of Gray hole: If a Gray hole node is detected, because of its behaviour, the data packets are not forwarded to it and either a new route Discovery is initiated or next available node having an optimal path is used to forward the data. Figure 5.4 shows working of proposed work in presence of Gray hole.

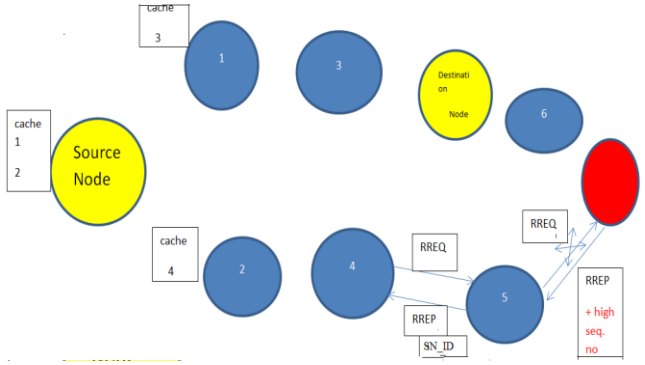

Figure 5.4: Working of proposed work in presence of Gray hole

In the initial stage where the RREQ message is forwarded in a multi hop scenario, it will be forwarded to all the nodes one

by one. As shown in the Figure 5.4. The immediate neighbours of the nodes send the RREQ back along with the Source node Identifier (SN_ID) of the respective node. This is a phase of neighbour discovery, so as to know which neighbour is near to it.

Below Figure 5.5 shows the flow chart for Sender Node in which First Broadcast the the RREQ. Next node receive the RREQ with source node id, and check if it is already received by previous node then discard otherwise store the value in cache table.

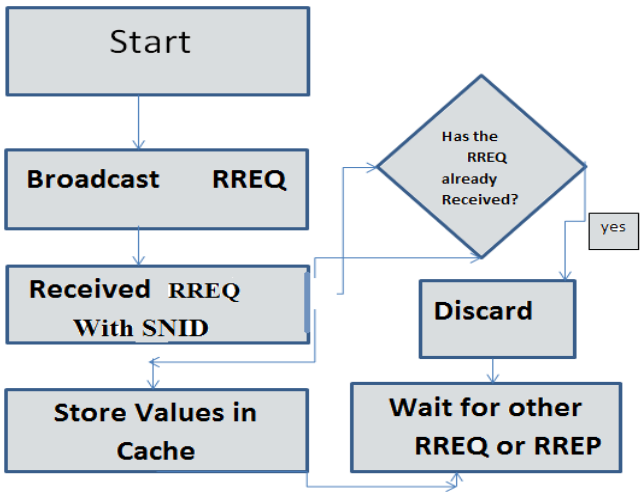

Figure 5.5: Flowchart for sender node

Below Figure 5.6 shows the Flow chart for intermediate node in which intermediate node check that it has already received the RREQ with source node id if yes then discard otherwise store the value in cache table and forward the RREQ.

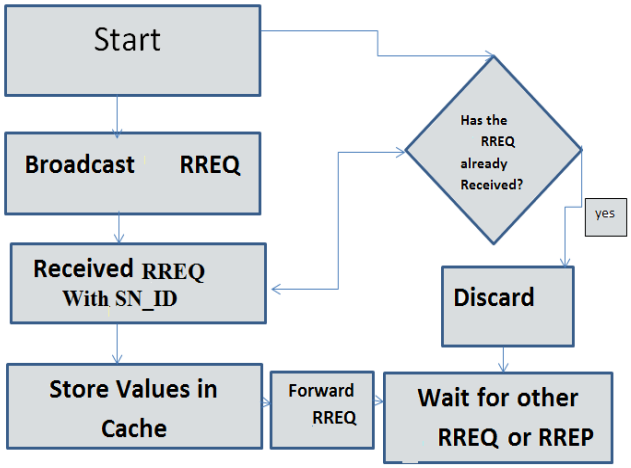

Figure 5.6: Flowchart for intermediate node

Below Figure 5.7 shows the Flow chart for receiving node in which when destination node receive the RREQ then it send RREP, if there are any optional path is not available then Discard it.

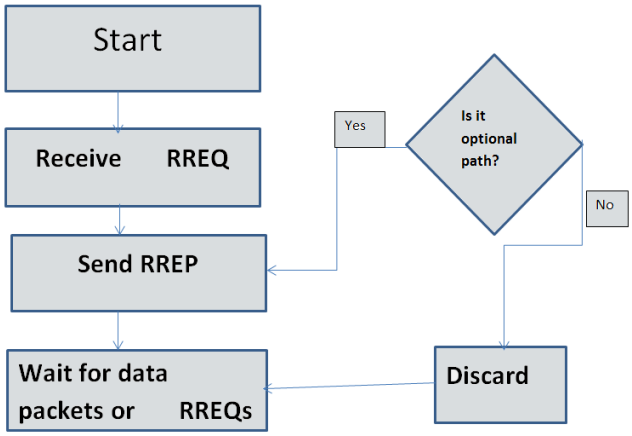

Figure 5.7: Flowchart for receiving node

Figure 5.8 shows that How to bypass the Gray hole attack it checks the Destination sequence number and Timestamp. Based on this both if sequence number are too much high then it discard the RREP.

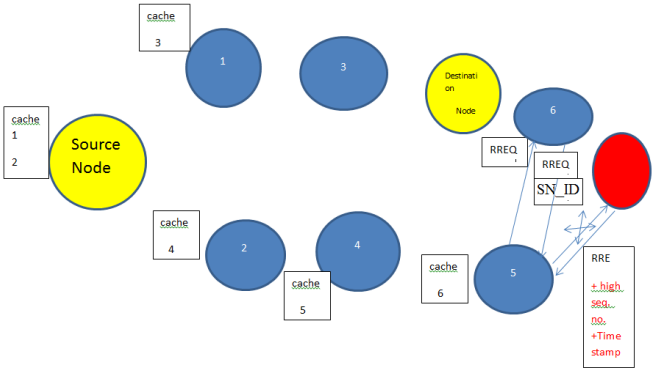

Figure 5.8: Bye- pass the Gray hole node

- This method uses the available control packets, i.e. RREQ and RREP to ascertain trustworthiness of a node. Therefore, new packets like acknowledgement packets need not be introduced for proving reliability.
- Originator IP address, Destination Sequence number, Destination IP address and Timestamp.
- Fields of RREQ stored in the cache will ascertain that the RREQ was processed.
- The field SN_ID will provide the information about the neighbouring node. Therefore a node will know its neighbour's so that if any error is encountered, the node can be blacklisted.
- If a malicious node enters the realm, then it will not know about this process going on between the nodes. So it can be trapped by its behaviour. This method can be used to mitigate Gray hole and also other such as Black hole using the same approach.

6. Simulations and Results

Simulation test bed in ns-2(Ver. 2.35) simulator [17] is based on a 500 x 5000 meter flat space with 10 to 100 mobile nodes. IEEE 802.11 MAC layer is utilized with bearer sense and back-off components and the transport layer utilized is User Datagram Protocol (UDP). Nodes move as indicated by the irregular waypoint mobility model. Accepting that the mobility of the ad-hoc networks is contrarily relative to the

delay time, in proposed work simulated the mobility by utilization of pause time. The more extended the pause time,, the less the mobility. In Proposed 50-second simulations, a pause time of 2 seconds have been taken and with a packet size of 512 bytes. Besides, the proposed AODV protocol is implemented as an answer for defeat with Gray hole attack and proposed AODV. Simulation parameters are introduced in Table 1**.**

Table 1: Simulation Parameters

Parameter	Value
Network Simulator	NS2.35
Terrain Area	500 m x 500 m
Simulation Time	50 s
MAC	IEEE 802.11
Application Traffic	CBR (UDP)
Routing Protocols	AODV
Transmission Range	250m
Data Payload	512 Bytes/Packet
Pause Time	2.0 s
Speed	50 m/s
Number of Nodes	10 to 100

Impact of Number of Nodes: The number of nodes varies on different performance metrics is depicted in below the Figure 6.1 to 6.4. Keeping on all parameters is the same shown in Table 1. As shown below in each graph, the number of nodes varies from 10 to 100 with all other configurations are fixed including pause time and mobility.

Packet Delivery Ratio

It's a proportion of the number of packets got by the destination to the number of packets send by the source. This represents the level of delivered data to the destination. The more packet delivery data to the destination means better execution of the protocol [18].

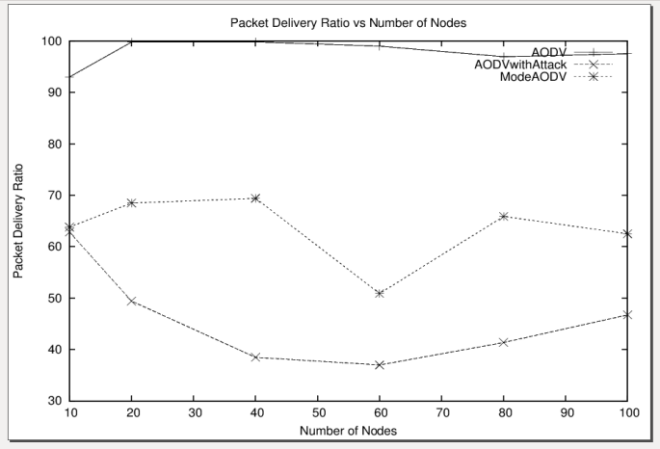

Figure 6.1: Packet Delivery Ratio v/s Number of Nodes

Figure 6.1 shows the effect of the number of nodes on packet Delivery Ratio and performance comparison of AODV, AODV with attack and Proposed or ModeAODV under varying network size between 10 to 100 nodes and keeping pause time 2.0 seconds and Maximum speed as 50 m/sec. As Gray hole node intercepts and drops some packets,PDR of AODV drops significantly less number of packets so the Packet Delivery Ratio of simple AODV has higher Packet Delivery Ratio. And the second observation is that ModeAODV protocol has a high packet delivery ratio presently as compared to AttackerAODV. since it takes more secure and attack free route for data delivery. The ModeAODV does not contain any attacker node so there is no any misbehavior are there and there is secure and reliable path for data delivery. The Third observation is that, AODV with attack having less packet delivery ratio. Since it doesn't have any mechanism to keep from prevent from data loss. By observation it is clear that the packet delivery ratio is high even though the number of nodes is increasing.

Throughput

Throughput is the number of data packets conveyed from source to destination per unit of time. Throughput is calculated as received throughput in bit every second at the traffic destination [18].

Below Figure 6.2 exhibits the effect of the number of nodes on throughput for protocols AODV and AODV with Gray hole attack including our Proposed or ModeAODV. The first observation from the Figure 6.2 is that AODV with attack protocol experience the more effects of the Gray hole attack since this protocol don't have any procurement that avoid helpful to prevent gray hole attack. Besides, the throughput of AODV with attack goes down under regardless of the number of nodes in the network. The second observation is that our protocol ModeAODV gives higher and enhanced throughput than AODV with attack and its near to the performance of plain AODV (without attacking) protocol. The explanation for the change is that the ModeAODV strongly prevents gray hole attack based on the proposed solution and thus, save packets drops that gray hole does regularly. Besides, ModeAODV gives higher throughputs contrasted with different protocols, even the number of nodes is more which has more chance of attacks.

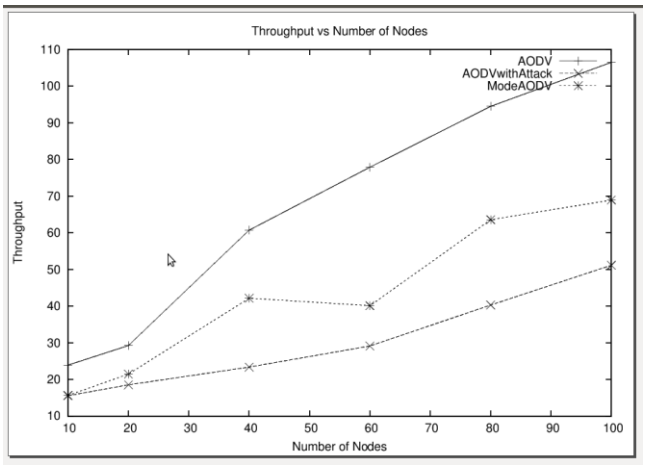

Figure 6.2: Throughput v/s Number of Node

Average End to End Delay

It is defined as normal time taken by information packets to propagate from source to destination over a MANET. This includes all possible delays caused by buffering during routing discovery latency, queuing at the interface queue, and retransmission delays at the MAC, propagation and exchange times. The lower estimation of end to end delay means the better execution of the protocol [18] .

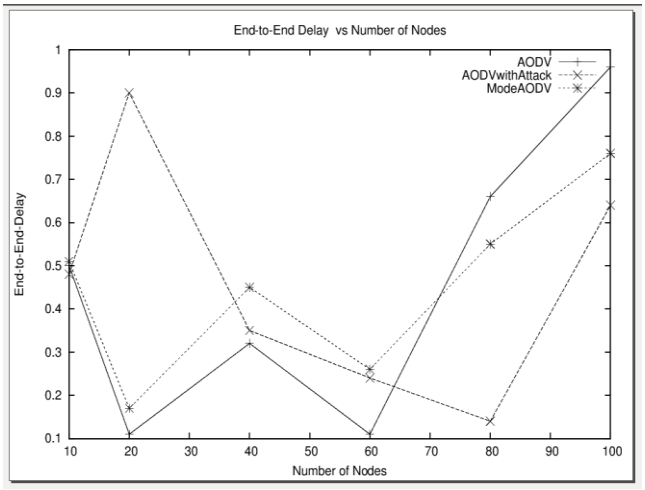

Figure 6.3: Average End to End Delay v/s Number of Nodes

Above Figure 6.3 Shows the effect of the number of nodes on end-to-end delay. As the network size varies from 10 nodes to 100 nodes the Average End to End to Delay of Simple AODV are less as compared to both AODV with attack and Mode AODV. The Second Observation is that in Mode AODV the End to End Delay are to much high because it takes more time to find out a safe and attack free route. and the third observation is that AODV with Attack contains near about Mode AODV End to End Delay because attacker shows its behavior.

Routing Load

The number of routing packets transmitted per information packets conveyed at the destination. Every hope-wise transmission of a packet is considered one transmission [18].

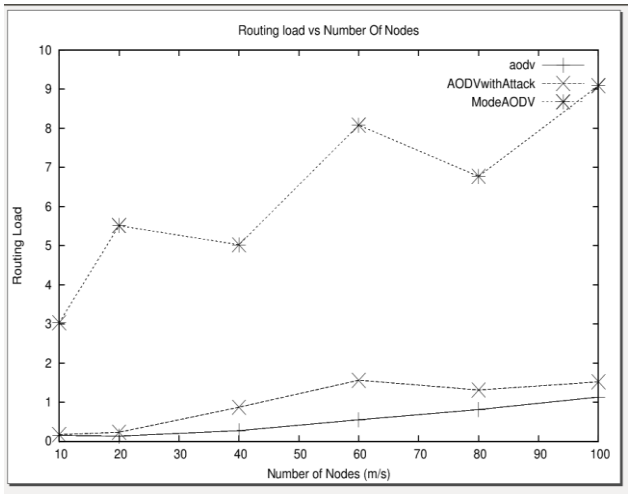

Figure 6.4: Routing Load v/s Number of Nodes

Above Figure 6.4 demonstrates the impact of the number of nodes on Normalized routing overhead. As the network size increase from 10 nodes to 100 nodes the Normalized Routing Load. Varies in simple AODV, ModeAODV and AODV with Attack. The first observation is that the AODV without attack introduces the least overhead since it does not use any additional requests for deciding secure routes. if there is no any additional RREQ or RREP or packets then it shows less Normalized Routing Load, It also decreases the Normalized Routing Load. when the number of nodes increases. The second observation is that the solution proposed by us, ModeAODV increases the amount of routing load because it checks so many routes and modes. And AODV with attack also has a higher Routing load as compared to AODV without attack.

7. Conclusion

Due to the absence of any centralized authority the mobile ad-hoc network suffers from many kinds of security attacks as the wireless connection is available to all. There are many types of attacks which are belong to inside or outside that occur on the MANETs. Between all attacks the Gray-hole attack is extension of the Black hole attack, It is a more dangerous attack because it drop some packets and forward some of the packets. The proposed algorithm is expected to work better in case of Throughput, PDR, End to End Delay and Routing load. In this proposed solution source node and the intermediate nodes will store the values of the received RREQ viz, Destination sequence Number, Destination IP address, SN-ID and Time stamp in its own cache memory if it is a new RREQ. If the RREQ has already been processed, it will discard it. The field SN-ID will provide the information about the neighboring node. Therefore a node will know its neighbors so that if any error is encountered, the node can be blacklisted. If a malicious node enters the realm, then it will not know about this process going on between the nodes. It can be trapped by its behavior. This method can be used to mitigate Gray hole and also other attacks such as a Black hole attack using the same approach. By using this proposed method the MANETs Performance are increasing. The PDR and Throughput are increasing and prevent Gray hole attack are increasing. The PDR and Throughput are increasing and prevent Gray hole attack.

References

[1] Arti and Dr. S. S. Tyagi "Study of MANET: Characteristics, Challenges, Ap-plication and Security Gary Holes" International Journal of Advanced Research in Computer Science and Software Engineering (Volume 3, Issue 5 , May 2013ISSN: 2277 128X).
[2] www.itrainonline.org/.../04-en-mmtk-wireless-basic infrastructuretopology-slides.pdf
[3] compnetworking.about.com/cs/wireless80211/a/aa80211standard.html
[4] C. Siva Ram Murthy, B.S. Manoj, "Ad Hoc Wireless Networks : Architectures and Protocols", Prentice Hall PTR, May 2004, New Jersey, USA
[5] C. E. Perkins and E. M. Royer, The Adhoc On-demand distance vector protocol, In C. E. Perkins, editor, adhoc Networking, Addison-Wesley, 2004, pp. 173-219
[6] www.computingunplugged.com/issues/issue200508/00001598001.html.
[7] P. Yau and C. J. Mitchell, Security Vulnerabilities in Adhoc Network
[8] P. Agrawal, H. Deng, W. Li and D,- Routing Security in Wireless Ad Hoc Networks(MANETs). University of Cincinnati, IEEE Communication Magazine,October 2002. 43.34

[9] Rutvij H. Jhaveri, Sankita J. Patel, Devesh C. Jinwala "A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad-hoc Networks", IEEE 2012.
[10] Deepali Raut , Kapil Hande "Detection and Prevention of Gray Hole and Black Hole Attack in MANET", IJCA 2014.
[11] Rutvij H. Jhaveri, Sankita J. Patel, Devesh C. Jinwala "Improving Route discovery forr AODV toprrevent Blackhole and Grayhole Attack in MANTEs", INFOCOM March 2012.
[12] Gundeep Singh Bindra, Ashish Kapoor, Ashish Narang, Arjun Agrawal "Detection and Removal of Co-operative Blackhole and Grayhole Attacks in MANETs", IEEE 2012.
[13] Onkar V.Chandure,V.T.Gaikwad "Detection Prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol", IJCA2012
[14] Deepali Raut , Kapil Hande "Detection and Prevention of Gray Hole and Black Hole Attack in MANET", IJCA 2014.
[15] Ira Nath ,Dr. Rituparna Chaki "BHAPSC: A New Black Hole Attack Prevention System in Clustered MANET", IJARCSSE 2012.
[16] Shalini Jain, Mohit Jain, Himanshu Kandwal, "Advanced Algorithm for Detection and Prevention of Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Network" ,in proc. Of IJCA 2010.
[17] The Network Simulator, nshttp://www.isi.edu/nsnam/ns/.
[18] Pankaj Rohal, Ruchika Dahiya, Prashant Dahiya "Study and Analysis of Throughput, Delay and Packet Delivery Ratio in MANET for Topology Based Routing Protocols (AODV, DS and DSDV)", IJARET March 2013.