International Journal of Engineering & Technology, 7 (3.34) (2018) 305-308

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Reducing the Effectiveness of Gray-Hole Attack in Manet

W.Ancy Breen [1], S.Durga Devi[2], E.Sushmitha[3], V.Suveetha[4]

Assistant Professor[1], Associate Professor[2], UG Scholar[3, 4], Department of Computer Science and Engineering[1,2,3,4]
Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi, Tamilnadu
ancybreen@velhightech.com[1], durgadevi@velhightech.com[2]
[*]Corresponding author E-mail: esushmitha143@gmail.com[3], suveethav@gmail.com[4]

Abstract

MANET is the mobile ad-hoc network. Security is very important especially when transmitting the data packets from one node to another. MANET is constructed by grouping mobile wireless nodes with no fixed infrastructure. In order to forward the packets, all the nodes in the network must cooperate with each other, so that the nodes beyond the radio ranges can communicate. Each node acts as a router and MANET is infrastructure-less networks. Hence, MANET is open to more security attacks such as Gray-hole attack, Black-hole attack and worm-hole attack. Due to the dynamism in network topology, MANETS are highly vulnerable and are prone to malicious attack. Security issue is highly challenging in MANET. Understanding the different form of possible attacks and providing good security solutions is important for secure data transmission between nodes. The most dangerous attack among these attacks is Gray-hole attack. In this paper, it proposed a method for reducing the Gray-hole attack. Our proposed algorithm MAODV identifies the malicious node before the data transmission process and it greatly reduces the dropping of data packets.

Keywords: *AODV, Gray-hole attack, malicious node, MANET, Worm Hole Attack, Vulnerability*

1. Introduction

MANET is a self arranging, infrastructure-less, association less system of portable nodes, in which every node go about as Router. The nodes are associated by remote connections with no unified access point. In the system, every one of the devices are free from each other. These devices can move and arrange themselves arbitrarily. Multi-hop ways are utilized for correspondence in MANET explained by Ms.Amita Pandey [1]. The system topology is changes questionably and powerfully in the remote medium and every one of the nodes share a similar system .As nodes are available to move anyplace in MANET, the communication breaks much of the time. In the MANET, as indicated by applications, the quantity of hubs can be chosen. Military Applications, Emergency Operations, Wireless Mesh Networks, Wireless Sensor Networks are the utilizations of the MANET which was stated by Mr. L Raja,Capt. Dr. S SanthoshBaboo [2]. MANET's are presented to various dangers due to not having any foundation and progressively arrange topology, which prompts distinctive kinds of security assaults like Black gap Attack, Flooding Attack, Gray Hole Attack, Worm Hole Attack, Sinkhole Attack and numerous others[3]

2. AODV Routing Protocol

The Ad-hoc on demand Distance Vector routing protocol among the reactive routing protocol. The memory

Fig 1: Mobile Ad-hoc Network

Required for this simple reactive routing algorithm is very less than the proactive routing algorithm. In AODV, the source node creates a route whenever, it demands. Route request(RREQ),Route reply(RREP) and route error(RERR) are the control packets are used in AODV. RREQ & RREP are used for route discovery and RERR is used for route maintenance. The source node sends the RREQ packet to its neighbour nodes until it reaches its destination. After sometime, source node receives the RREP packet from the other nodes. The source node checks the table whether it has entry in it for destination or not and also checks the sequence number. The source node selects the node which has highest sequence number and make it as a route for transmission of packets. If more than one node has equal sequence number, it selects the minimum hop count route to the destination. If any link breakdown between two nodes then, RERR message is broadcasted to the other nodes in the network

regarding the route failure. If route failure occurs, the new route has to be established by the source node to its destination.

1.1. Attacks on Mobile Ad-Hoc Network:

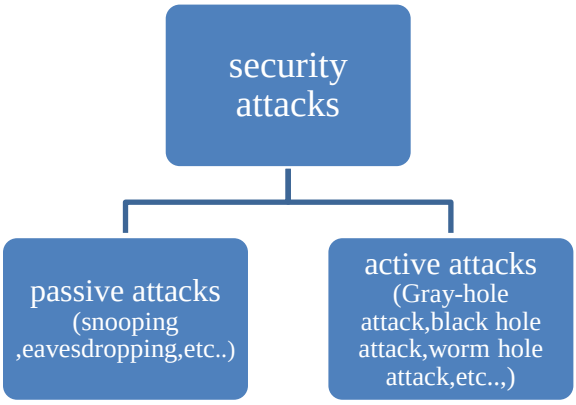


Fig 2: Types of security attacks

1.2. Passive Attacks

Passive attack does not drastically alter the structure of the MANET. An attacker snoops over the data being exchanged in the network; hence the confidentiality of the data is lost. The gathered information through snooping is interpreted and is used for launching attack on the target nodes. Different types of passive attacks are Traffic monitoring, Eavesdropping, traffic analysis, syn flooding [4].

1.3. Active Attacks:

In Active attack is carried by a malicious node trying to compromise the nodes in the network .The compromised nodes perform various attacks on the nodes or the data transmitted by modifying, fabricating, deleting the information Umesh Kumar Singh, KailashPhuleria,Shailja Sharma & D.N. Goswami [3]. Both active and passive attacks are occurred at any layer of the network protocol stack. Both of these attacks can be reduced by using the encryption techniques.

1.4. Gray-Hole Attack:

Gray-hole attack is different from the black-hole attack. In gray-hole attack, the malicious node act as a normal node(honest node)during the route discovery process and then it changes its behavior from normal to malicious. The data packets are dropped by these malicious node. But the detection of these malicious node is very difficult due to its frequent changing behavior. Initially, it acts as a honest node and later it drops packets by changing its state from normal to malicious. The Gray-hole node acts as a honest node but actually it is an attacker. It drops all the UDP packets when TCP packets are forwarding. By this, half of the total data packets are dropped. It destroys the network and it is not detected very easily.

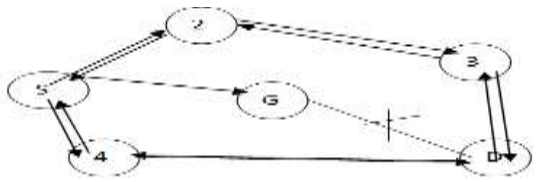


Fig 3: Gray-hole attack in MANET

2 .Literature Survey

Nadav Schweitzer, Ariel Stulman [5] stated that,in this each node uses the internal knowledge collected by the routing information. Gray-hole attack was reduced by using DCFM (Denial Contradiction with Factious node Mechanism)in addition to an improvement algorithm. The source node identifies the malicious node by checking the neighbour node list of each and every node present in the network. If the information present at the neighbour node list is correct,it marks as a normal node else it is marked as a malicious node.

Rutvij H.Jhaveri, Narendra M.Patel [6],in this the malicious node is identified during the route discovery process. This SNBDS is specially designed for AODV protocol. It uses the bait detection mechanism. When the sender node receives RREP from the other node, it marks that as a suspicious node. Then it sends the bait REQ to the suspicious node. If any node reply to the bait REQ ,it marks that as a malicious node.

Shani Makwana, Krunal Vaghela [7],this proposed solution is based on the credit values. If the node forwards message/receive message ,the credit value is increased. If not it will be decreased from the initial credit values. When credit value becomes zero, it compare destination sequence number and source sequence number. If the destination sequence number is higher than the source sequence number, that path is isolated.

Monika, Swati Gupta[8],there are using the digital signature technology. Encryption and decryption are done while sending and receiving the message. Trust Based Server(TBS) stores all the registered node ID's which are unique. TBS verifies the node authentication when the sender node sends the information about the node which sends the RREP. If the node is not authenticable, it identifies that as a malicious node.

Jian Ming Chng, Po Chun Tsou, Hanchieh Chao & Chin Feng Lai[9] explained, it is based on the CooperativeBait Detection Scheme(CBDS).Each source node selects their neighbour node to send a reply to the Bait REQ. The malicious node are identified by receiving the Bait REP from that node.

Schhram Behzad, Reza Fotochi, Fathulah Dadgar[10], RTT are calculated to find the distance between source and destination node. By sending the HELLO message RTT is calculated. The route which holds the maximum difference RTT is selected for sending the data packets. By this, attacks are prevented.

3. Existing System

This solution assumes no explicit node collaboration, with each node using only internal knowledge gained by routine routing information. Gray -hole attack was reduced by using DCFM (Denial Contradiction with Fictious node Mechanism)in addition to an improvement algorithm DCFM was proposed to address the problem of node isolation in OLSR based networks. It identifies potential malicious nodes trying to falsify HELLO messages using only internal information within the victim, without relying on any centralized or external trusted party. Such early detection prevents a possible attack before it can manifest. The source node identifies the malicious node by checking the neighbour node list of each and every node present in the network. If the information present at the neighbour node list is correct, it marks as a normal node else it is marked as a malicious node.

The simulation results greatly minimized the gray-hole attack.

3.1 Disadvantages:

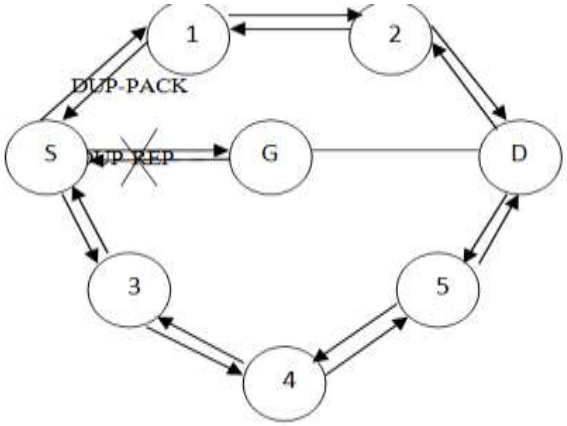
- routing overhead, delay and throughput are high, as the number of nodes increases.
- Detecting the cooperative attack is difficult.
- Existing system failed to detect the cooperative attacks.
- The speed for detecting the malicious node is very high .so, the data loss is high.
- During monitoring ,each node consumes lot of energy and network overhead is high.

4. Proposed System

The solution is proposed to detect and reduce the Gray-hole attack in MANET. Initially, the malicious node exhibits the normal behavior and after the route discovery process that same node act as a attacker. Our proposed method provides a solution to identify the malicious node before the route discovery process and isolate that particular path. It is mainly proposed for AODV protocol. In AODV, each node sends the RREQ to their neighbour node to discover the route. If the node receives the RREQ, it replies with RREP message. Then the source node selects the shortest route path to send the data packets to its destination. Each and every node maintains the routing table which holds sequence number of source & destination,neighbour node _list. Each node identifies the neighbour node from the routing information.

Our proposed solution included some mechanism in addition to AODV protocol.

Each node sends the Duplicate_packets to all their neighbour nodes that are selected from the neighbour node_list. If the normal node receives the Duplicate_packets, it does not reply to its received Duplicate packets, With the help of their acquired knowledge and analyzing its ID's, the normal node identifies it as a unauthorized packets. Hence, it does not send reply to its sender. The malicious node receives those Duplicate_packets because the attacker always wish to receive the available data's and information. Then the source node stimulate the malicious node to send the D_REP (reply message) to it. After accepting the packets Mal_node send a D_REP to the source node.Source node identifies the malicious node by accepting the D_REP from the malicious node and also identifies its ID's from the routing information. After identifying the attacker, source node blocks that route path and also it advertise about the malicious node to all other nodes present in the entire network. It makes other node to know about the attacker. By using these information, other nodes also do not use that isolate path for transferring the packets. After identifying the Malicious node ,Data packets are transferred to its destination through the smallest, alternative route path.



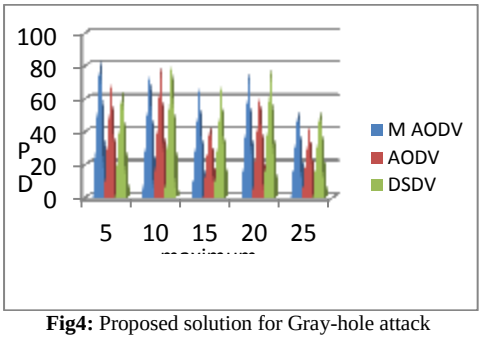


Fig4: Proposed solution for Gray-hole attack

5. Simulation Parameters

Table1: Simulation Parameters for Ad-hoc Network.

Simulator	NS 2.35
Simulation time	200(s)
Number of nodes	25
Area	250m *250m
Traffic	CBR
Routing protocol	AODV
Transport protocol	TCP & UDP
Packet size	512 bytes

6. Experimental Results

6.1. Packet Delivery Ratio

The MAODV algorithm has higher packet delivery ratio than AODV and DSDV.

6.2. Packet Loss

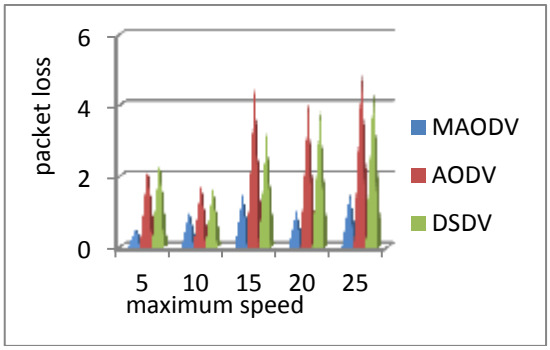


Fig 5: packet loss

In the above fig 5, the MAODV has less packet loss than AODV and DSDV.

6.3. Throughput

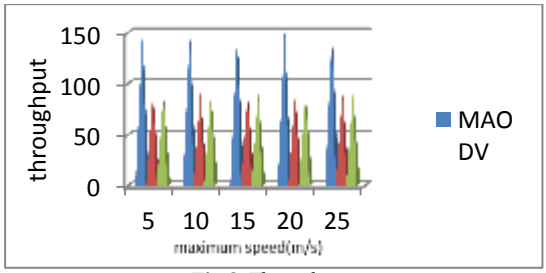


Fig 6: Throughput.

In the above fig 6 , the MAODV has higher throughput than AODV and DSDV.

7. Conclusion

This paper proposed a method to identify the malicious node(Attacker) before the data transmission process. It detect and reduce the Gray-hole attack in MANET. This proposed method provides a solution for securing the routing protocols. The performance of the proposed method is evaluated by using the simulation of Gray-hole attack and simulation of proposed method. According to the obtained results throughput is increased and average end to end delay & packet loss are decreased . It provides high Packet Delivery Ratio with less end to end delay.

References:

[1] Ms.Amita Pandey,"Introduction to Mobile Ad-hoc Network", *International Journal of Scientific and Research Publications*, Volume 5, Issue 5, May 20151ISSN 2250-3153.

[2] Mr. L Raja,Capt. Dr. S SanthoshBaboo," An Overview of MANET: Applications, Attacks and Challenges",*International Journal of Computer Science and Mobile Computing*, Vol.3 Issue.1, January-2014.

[3] Umesh Kumar Singh, KailashPhuleria,Shailja Sharma & D.N. Goswami," An analysis of Security Attacks found in Mobile Ad-hoc Network", *International Journal of Scientific & Engineering Research*, Volume 5, Issue 5, May-2014.

[4] Rupali Sharma," Gray-hole Attack in Mobile Ad-hoc Networks : A Survey ",*International Journal of Computer Science and Information Technologies*, Vol. 7 (3) , 2016.

[5] Nadav Schweitzer, Ariel Stulman, Member, IEEE, Roy David Margalit, and AsafShabtai," Contradiction Based Gray-Hole Attack Minimization for Ad-Hoc Networks", *IEEE Transactions on mobile computing*, vol. 16, no. 8, august 2017.

[6] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, Member, IEEE*,"* Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach", IEEE *Systems journal*, vol. 9, no. 1, march 2015.

[7] ShahramBehzad, Reza Fotohi, FathulahDadgar," Defense Against the Attacks of the Black Hole, Gray Hole and Wormhole in MANETs Based on RTT and PFT, *International journal of Computer Science & Network Solutions*, Volume 3.No.3,March.2015.

[8] Rutvij H. Jhaveri, Narendra M. Patel," A Sequence Number Based Bait Detection Scheme to Thwart Grayhole Attack in Mobile Ad-hoc Networks*",Wireless networks*,vol-21,april-2015.

[9] ShaniMakwana,KrunalVaghela,"Detection and Elimination of Gray Hole Attack using Dynamic Credit based Technique in MANET", *International Journal of Computer Applications* (0975 – 8887) Volume 125 – No.4, September 2015.

[10] Monika , Swati Gupta," Detection and Prevention of Black Hole & Gray hole attack in MANET using Digital signature Techniques", *International Journal Of Engineering And Computer Science* ISSN:2319-7242 Volume 4 Issue 7 July 2015.

[11] Bhimsingh Bohara1,Varun Sharma" Analysis and Prevention of effects of gray hole attacks on Routing Protocol in Mobile Ad-hoc Networks", *International Journal of Advanced Research in Computer and Communication Engineering* Vol. 2, Issue 6, June 2013.

[12] Bhupendra B Patel, Prof Chirag S Thaker, Nidhi R Jani," Analysis and Implementation of Malicious Node in AODV Routing Protocol", *Computer Engineering and Intelligent Systems* ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)Vol.4, No.13, 2013

[13] Ashok M.Kanthe ,Dina Simunic&Ramjee Prasad,"A Mechanism for Gray Hole Attack Detection in Mobile Ad–hoc Networks", *International Journal of Computer Applications* (0975 –8887)Volume 53–No.16, September 2012.

[14] G.S. Mamatha and Dr. S. C. Sharma," A Highly Secured Approach against Attacks in MANETS", *International Journal of Computer Theory and Engineering*, Vol. 2, No. 5, October, 2010 .

[15] Alex Hinds, Michael Ngulube, Shaoying Zhu, and Hussain Al-Aqrabi,"A Review of Routing Protocols for Mobile Ad-Hoc Networks (MANET) ",*International Journal of Information and Education Technology*, Vol. 3, No. 1,February .2013