International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 10, Issue 12 (December 2014), PP.13-18

A Survey of various Methods of Preventing and Detecting Attacks on AODV-based MANET

[1]Jagdish J. Rathod, [2]Prof. Amit. M. Lathigra
Student of M.Tech. (C.E.) H.O.D. of CSE, Department of CSE, RKUniversity, Rajkot

Abstract:- Mobile Ad hoc Network (MANET) is constructed from a collection of nodes that can move anywhere and anytime in different areas without any infrastructure that means MANET is infrastructure less. Each node works at the same time as router and host. Lack of a fixed infrastructure, wireless medium and dynamic topology makes MANET vulnerable to different kinds of attacks like Gray hole and Black hole. In this paper, we investigate different mechanisms that have designed to detect or prevent black or gray hole attacks in AODV protocol. We discuss about advantages and disadvantages of the different methods.

Keywords:- MANETs, Security, Attacks, Gray hole Attack, Black hole Attack, AODV**.**

I. INTRODUCTION

Opposed to the infrastructure wireless networks where each user directly communicates with an access point or base station, a mobile ad hoc network, or MANET is a kind of wireless ad hoc network [1]. MANET is a self-configuring network of mobile routers connected by wireless links with no access point. Every mobile device in a network is autonomous, move anywhere any time. The mobile devices are free to move haphazardly and organize themselves arbitrarily.

Ad-hoc On-Demand Distance Vector (AODV) [14] Routing Protocol is used for finding a path to the destination in an ad-hoc network. To find the path to the estimation all mobile nodes work in cooperation using the routing control messages mostly use three parameter. Thanks to these control messages, AODV Routing Protocol are quick adaptation to dynamic network conditions, low processing and memory overhead, low network bandwidth utilization with small size control messages. The most usefull feature of AODV as compared to the other routing protocols is that AODV uses a destination sequence number for each route entry. The destination sequence number is generated by the destination or receiver when a connection is requested from it. Using the destination sequence number ensures loop freedom. AODV makes sure that the route to the destination must loop free and it is the shortest path.

II. AODV ROUTING ALGORITHM

Ad-hoc On-Demand Distance Vector (AODV) [14] Routing Protocol is used for finding a path to the destination in an ad-hoc network. Route Requests (RREQs), Route Replay (RREPs), Route Errors (RERRs) are three control messages used for establishing a path to the destination, sent using UDP/IP protocols. Header information of these control messages are explained in [14]. If source node wants to make a connection with the destination node(to communicate with destination), then it broadcasts an RREQ message. This RREQ message is propagated from the source, received by neighbors (intermediate nodes) of the source node. The intermediate nodes broadcast the RREQ message to their neighbors. This process goes on until the packet is received by destination node or an intermediate node that has a fresh enough route entry for the destination.

III. GRAYHOLE AND BLACKHOLE ATTACKS

Gray hole attacks is an active attack type, which lead to dropping of messages. Attacking node first agrees to forward packets and then fails to do so and behaves like malicious node. Initially the node behaves correctly and replays true RREP messages to nodes that initiate RREQ message. This way, it takes over the sending packets. Afterwards, the node just drops the some or all packets to launch a (DoS) denial of service attack[12].

If neighboring nodes that try to send packets over attacking nodes lose the connection to destination then they may want to discover a route again, broadcasting RREQ messages. Attacking node establishes a route, sending RREP messages. This process goes on until malicious node succeeds its aim (e.g. network resource consumption, battery consumption). This attack is known as routing misbehavior [12].

The difference of Black Hole Attacks [11] compared to Gray Hole Attacks is that malicious nodes never send true control messages initially.it drops all the pcckets. To carry out a black hole attack, malicious node waits for neighboring nodes to send RREQ messages. When the malicious node receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself, assigning a high sequence number to settle in the routing table of the malicious node, before other nodes send a true one. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node.

IV. REVIEW OF THE METHODS

In this section, we present the eight different methods for detection and removal of gray hole and black hole attacks.

4.1 First Method

Detection and removing of black/gray hole attacks processes are [10]:

In proposed AODV protocol, when a node receives a route reply packet (RREP), it checks the sequence number value in routing table; if it is greater than the one in the RREP, the RREP packet is accepted; otherwise it is discarded [10].

the route discovery process in AODV in the presence of a malicious node M. Source node S broadcasts route request packet (RREQ); nodes within its communication range or sort communication range, when intermediate node receive the RREQ and rebroadcasts RREQ to their neighbors until a node having a valid route to the destination or destination D itself receives RREQ [10]. This node sends RREP to the source node on the reverse path of RREQ. The malicious node M sends RREP with higher, but fabricated, sequence number to the source; another RREP is sent by D having genuinely higher sequence number. As malicious node sends RREP with higher sequence number than the normal node, S chooses path through M to transfer data packets and therefore, malicious node can drop some or all received packets which causes degrade the performance of network.

In proposed approach, an intermediate node dynamically calculates a PEAK value after fixed time interval [10] that uses three parameters for calculation: RREP sequence Number, routing table sequence number and number of replies Received during the time interval. The PEAK value is the Maximum possible value of sequence number that any RREP can have in the current state. RREP received from malicious node is marked as

DO_NOT_CONSIDER.

With the proposed algorithm, when an intermediate node receives RREP having sequence number higher than the calculated PEAK value, it is marked as DO_NOT_CONSIDER; the node sending RREP is marked as malicious node in the routing table and RREP is then forwarded to the source node via reverse path. Meanwhile, each node receiving the forwarded RREP updates route entry for the malicious node. Source node sending RREQ also appends a list of malicious nodes to inform other nodes in the network about the existence of attackers. Thus, malicious nodes remain isolated from normal nodes.

4.1.1 Advantages

1-in this proposed method there is no extra control packets added in the proposed Algorithm, there would be negligible difference in Routing Overhead which is the ratio of the number of routing related Transmissions to the number of data related transmissions.

2-as the malicious nodes would be isolated, Packet Delivery Ratio (PDR) would be improved greatly; PDR is the ratio of number of received data packets to the number of sent data packets.

4.1.2 DisAdvantages

1-If the node receiving RREP from a malicious node doesn't have the node marked as malicious in the routing table, the proposed algorithm adds a little computational overhead to that node as it has to calculate the PEAK value.

4.2 Second Method

In [1] the proposed algorithm is based on a course based scheme. That is, a node does not observe every node in the neighbor, but only observes the next hop in current route path. The proposed algorithm is represented for finding the intentional selective dropping attack by a node and if all the packets are dropped will identify the attack as a black hole attack by checking the forwarding of packets by the immediate neighbor

downstream node to which the data is sent.

In the algorithm at each node, the router will maintain a packet count history of the number of packets it has forwarded to the downstream node and also the number of packets it has overheard for the forwarded packets. This algorithm is divided into three steps:

i) When a router forwards a packet to the downstream node, the number of packet sent is incremented and also buffers the packet up to certain time period. Then it overhears the packet which is forwarded by the downstream node and compares with the packet in the buffer.

ii) When a match is found the number of packets forwarded by downstream node is increased. Once the match is found or if the time period is over the packet is deleted from the buffer.

iii) If the packet forwarding is not heard within the time period the algorithm assumes that the packet is dropped by the downstream node.

4.2.1Advantages

1-in this paper the Simulation results show that the proposed method has good performance against Black hole attack without much overhead.

2-This solution holds good for gray hole attack also.

4.2.2 Disadvantages

1-it is only used for Black hole and Gray hole Attack only.

4.3 Third Method

In [8] the proposed method start route discovery process of default AODV in the presence of an attacker. Source node S

Wishes to send data to destination D broadcast RREQ;

a malicious node MN replies back with RREP containing unusually high destination sequence number misleading S as if it has a fresher route to D; another normal intermediate node IN sends RREP having legitimately higher sequence number. As RREP of the attacker holds higher destination sequence number of all received RREPs, source node unknowingly selects path through MN to transfer data packets and therefore, (malicious node)MN intercepts and drops some or all of the received packets that causes denial-of-service in the network. This issue states the requirement of a variation of AODV protocol that efficiently discovers a secure route to the destination.

4.3.1 Advantages

1- In this paper, the proposed method provided improvement in route discovery process of AODV protocol to find multiple Black hole and Gray hole nodes.

2- The mechanism provides high packet delivery rate with noticeable normalized routing overhead and acceptable average end-to-end delay under attack.

3-R-AODV provides a simple and efficient way to detect and isolate multiple malicious nodes without introduction of any new control packet.

4.4 Fourth Method

In [6] The proposed work comprises in following steps:

1. Implementation of Modified EDRI Table and algorithm towards detecting Gray hole and Cooperative Black hole attacks.
2. Implementation of Negative Acknowledgement (NACK) Algorithm.
3. Eliminating Non-Consecutive Cooperating Black hole and Gray hole attacks.

In proposed 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.

4.4.1 Advantages

1- The MEDRI table also record and maintain the history of the previous malicious nodes that is used for the future secure transformation of data from source to destination and to discover secure path from source to destination.

2-The proposed solution can be also applied to

1. Identify multiple black/gray hole nodes cooperating with each other in a MANET.
2. Discover secure paths from source to destination by avoiding multiple black/gray hole nodes acting in cooperation.

4.4.2 Disadvantages

1- A limitation of this solution is that the malicious nodes have to be consecutive while acting in cooperation to be identified by the algorithm.

4.5 Fifth Method

In [7] the security procedure is invoked by a node when it identifies a suspicious node by examining its DRI table. by call the node that initiates the suspected node recognition procedure as the Initiator Node (IN). The IN first chooses a Cooperative Node (CN) in its neighborhood based on its DRI records and broadcasts a RREQ message to its 1-hop neighbors requesting for a route to the CN. In reply to this RREQ message the IN will receive a number of RREP messages from its neighboring nodes. It will certainly receive a RREP message from the Suspected Node (SN) if the latter is really a gray hole (since the gray holes always send RREP messages but drop data packets probabilistically). After receiving the RREP from the SN, the IN sends a probe packet to the CN through the SN. After the time to live (TTL)(time duration is expire) value of the probe packet is over, the IN checks the CN whether it has received the probe packet or not. If the reply to this query is affirmative, (i.e., the probe packet is really received by the CN) then the IN updates its DRI table by making an entry „1" under the column „Check Bit against the node ID of the SN. However, if the probe packet is found to have not reached the CN, the IN increases its level of suspicion about the SN and activates the suspected node recognition procedure.

4.5.1 Advantages

PDR & e2e term & also analyze the impact of gray hole attack on ad hock network, with their PDR & e2e value.

4.6 Sixth Method

In [2] this proposed approach, in which initially each and every node assigns a static value for its every neighbor node as the neighbor 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 neighbors 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 gets detected, it would not send any alarm packet. Hence it is reduces routing overhead. Every node maintains a data structure in their local RAM which acts as a black list cum FALSE REPLY list of the nodes in the network. FALSE REPLY is the replies which are detected as a fake 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.

4.6.1 Advantages

1-This paper presents good performance in terms of better throughput and minimum packet loss percentage over AODV without attack and AODV with attack.

4.6.2 Disadvantages

1- in this algorithm static value is used for assigning credit for every node. A dynamic value can also be generated for assigning credit.

4.7 Seventh Method

In [5] proposed approach Identification of relationships between cluster head neighbors in ad hoc network In an ad hoc network, the relationship of a cluster head node i to its neighbor node j can be any one of the following types

i) cluster head node i is a stranger to neighbor cluster head node j:

Cluster head node i has never sent/received messages/few messages to/from node j. Their trust levels between each other will be very low. Any new node entering an ad hoc network will be stranger to its entire neighbor. There are high changes of malicious behavior from stranger nodes.[26]

ii) Cluster head node i is a friend to neighbor node j: existing paths from its routing table going through that node.

4.7.1 Advantages

1-the propose solution presents good performance in terms of black hole node detection time requirements as well as routing overhead with increasing mobility in an already formed cluster.

4.8 Eight Method

Detection and removing of black/gray hole attacks processes are [14]:

- Detection process for gray hole /black hole attack by source node:

1-Dividing data packets into *k* equal parts.

2- Sending a message to destination containing number of messages.

3- Broadcasting messages to all neighbors of route.

4- After ensuring that destination node knows count of messages, source begins sending of data.

5- Setting up a timer until getting number of data packets that destination receives.

6- If number of announced data packets from destination is less than a limit, initiates removing process of black/gray hole attack.

7- Also if after terminating of timer, did not get any message from destination, starts removing process of black/gray hole attack.

- Detection process for black/gray hole attack by destination node:

After knowing the number of data packets that are sent from source node, setting a timer to zero and starts counting data packets. After a timeout, returns data packet numbers to source node.

- Detection process for black/gray hole attack by neighborhood nodes:

By getting monitoring message from source node, each node starts a counter for counting number of data packets of its neighbors.

- Remove process for black/gray hole attack by source node:

1- Source node gets vote of one node's neighbors about the maliciousness.

2- According to the votes of neighbors, starts counter for malicious node in Find Malicious table.

3- If votes of neighbors about maliciousness exceeds from a limit, source enters that node in Gray/Black hole table and finds a new route to destination. Also announces to the network that node is a malicious one.

- Remove process for black/gray hole attack by neighbor nodes:

When they get monitoring message, they start counting numbers of packets that malicious node sends. If number of passed messages is less than a limit, inform about it to source node.

4.8.1 Advantages

1-Using a limit for identifying malicious nodes, decreases number of mistakes in identifying black/gray hole attack. This threshold value is the probability of packet dropped by a node through no mistake of its own. Packet dropping may occur due to overhead, lack of CPU cycles, buffer space or bandwidth, congestion or collusion to forward packets.

2-This method can detect both black and gray hole attacks and also can detect selfish node.

4.8.2 Disadvantages

1-In this method, all nodes should always monitor each other; in this case, the network has a high overhead and also each node consumes a lot of energy for monitoring.

2- Detection speed for malicious nodes is low, a lot of data lost until malicious node can be detected.

V. CONCLUSION

Gray hole and Black hole attacks are the most important security problems in MANET. Black hole starts in route discovery phase and gray hole as an attack which drops packets in transmitting step. Detection of gray hole is more difficult than black hole, because the attacker works as normal node then starts dropping of data. In this paper, we introduced some of the proposed methods in detecting Gary and Black hole attacks, pointed out some of the advantages and disadvantages of the method. .we observe that Most of these algorithms suffer from overload and low speed which is a research area for developing a detection system against these attacks. Protection against both attacks in one detection system and decreasing number of errors in detection can be other topics for developing black and gray hole detection systems.

REFERENCES

[1]. Deepali Raut, Kapil Hande "Detection and Prevention of Gray Hole and Black Hole Attack in MANET", IJCA 2014.

[2]. Deepali A. Lokare, A.M Kanthe, Dina Simunic" Cooperative Gray Hole Attack Discovery and Elimination using Credit based Technique in MANET", IJCA 2014.

[3]. C. Siva Ram Murthy, B.S. Manoj, "Ad Hoc Wireless Networks : Architectures and Protocols", Prentice Hall PTR, May 2004, New Jersey, USA

[4]. 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.

[5]. Ira Nath ,Dr. Rituparna Chaki "BHAPSC: A New Black Hole Attack Prevention System in Clustered MANET", IJARCSSE 2012.

[6]. Gun deep Singh Bindra, Ashish Kapoor, Ashish Narang, Arjun Agrawal "Detection and Removal of Co-operative Blackhole and Grayhole Attacks in MANETs", IEEE 2012.

[7]. Onkar V.Chandure,V.T.Gaikwad "Detection Prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol", IJCA 2012

[8]. RUTVIJ H. JHAVERI, SANKITA J. PATEL,DEVESH C. JINWALA "Improving Route Discovery for AODV to Prevent Blackhole and Grayhole Attacks in MANETs", INFOCOMP 2013.

[9]. P. Yau and C. J. Mitchell, Security Vulnerabilities in Adhoc Network

[10]. Rutvij H. Jhaveri, Sankita J. Patel, Devesh C. Jinwala "A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad-hoc Networks", IEEE 2012.`

[11]. 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

[12]. S. Marti, T. J. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehavior in Ad Hoc Networks",in Proc.of 6th Annual Intl. Conf. Mobile Comp. and Net., Boston, MA. pp. 255-265. August 2000.

[13]. www.itrainonline.org/.../04_en_mmtk_wireless_basic-infrastructuretopology_slides.pdf

[14]. 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.

[15]. G. Vigna, S. Gwalani and K. Srinivasan, An Intrusion Detection Tool for AODV- Based Ad hoc Wireless Networks, Proc. of the 20th Annual Computer Security Applications Conference (ACSAC04).

[16]. www.computingunplugged.com/issues/issue200508/00001598001.html.

[17]. compnetworking.about.com/cs/wireless80211/a/aa80211standard.html

[18]. users.tkk.fi/~msarela/texts/cs/military/node11.html

[19]. 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

[20]. C.Perkins, (RFC) 3561, "Category: Experimental(Practical), Net work", Working Group", July 2003

[21]. The Network Simulator, ns-2. http://www.isi.edu/nsnam/ns/.

[22]. D. Johnson, D. Maltz and J. Broch, DSR the Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks. Ad Hoc networking, Chapter 5, page 139- 172. Addison- Wesley, 2001.

[23]. F. Stajano and R. Anderson, The Resurrecting Duckling: "Security Issues for Ad- Hoc Wireless Networks, Security Protocols", 7th International Workshop Proceedings, Lecture Notes in Computer Science, 1999. University of Cambridge Computer Laboratory.

[24]. P. Ning and K. Sun, How to Misuse AODV: A Case Study of Insider Attacks Against Mobile Ad-Hoc Routing Protocols, Proc.of the 2003 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY., June 2003.

[25]. library.uws.edu.au/adtNUWS/uploads/approved/adtNUWS20060125.131604/public/12Chapter11.pdf

[26]. D.G.Raimagia, S.Nagar, "Identification and Elimination of Selfish Nodes in Adhoc Network" International Journal of Engineering Research and Development, pISSN: 2278-800X, www.ijerd.com, Volume 10, Issue 4 (April 2014), PP.29-34