Comparative Analysis of Various Black Hole Detection Techniques

Gurpreet Singh[1], Dr. Raman Maini[2]

[1]*Department of Computer, Punjabi University Patiala, Punjab, India*
[2]*Professor Punjabi University Patiala, Punjab, India*

***Abstract:*- An ad hoc network is combination of mobile nodes that dynamically make the network which are temporarily in nature. There is no need of any central administration hence more chance to attackers. There are various types of protocols used in Ad hoc network like AODV (Ad-hoc on demand distance vector) protocol, DSR protocol. In this attack, a malicious node advertises itself of having the shortest path to the node whose packets it want to intercept. This works analysis the Watchdog mechanism, comparing destination sequence number, detection of black hole using IDS method, and detection of black hole using DRI are different kinds of black hole detection techniques. DRI is the better technique as compared to other techniques as it can detect more than one malicious node in network.**

Keywords: Black hole, ad-hoc network, AODV protocol, malicious node

I. INTRODUCTION

MANETs is usually self –organized and configuring the of mobile –device, which interconnected via wireless links. Ad-hoc, is Latin means “for this purpose”. For moving data or information from one place to another, wired or wireless medium is requiring. Wireless medium is used more often as it can easily transmit email, message, and connect to the internet and so on. In manets there is no need of base station as each device in manets is free to move Independently in any direction and can change their links to other node frequently. It is a system in which network is connected in wireless and in manets topology change rapidly [1]. Black hole attack occur in malicious node which fakes sequence_number that means every node in manets have sequence no. if source find that the Request reply(RREP) comes from that node which have highest sequence no. as compare to other Node then it is suspected that node is a malicious node[2].

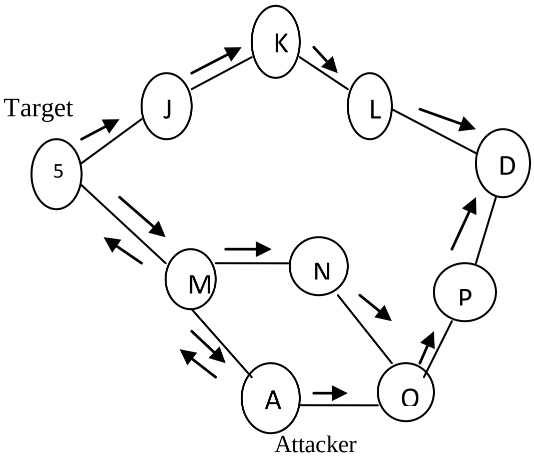

Figure1.Single black hole [2]

In case of AODV, the assailant can launch a false RREP to the starting node, asserting that it has a suitably clean path to the target node and cause the starting node to choose the path that goes by the assailant. Thus, all packets will be passed through the assailant, and , the assailant can exploit or dispose of the packets. Figure1 shows an illustration of such attack, where assailant A launch a false RREP to the starting nodes, asserting that it has a suitable path than others. while the assailant’s advertised sequence_number is more than other nodes' sequence_numbers, the starting node S will select the path that goes by node.

In paper we are going to do analysis different black hole detection techniques which are as follows:-

1. Watchdog mechanism [4]
2. Comparing destination sequence number [5]
3. Detection of black hole using IDS method [6]
4. Detection of black hole using DRI table [7]

The paper is organized as follows section 2 provides different types of black-detection method. Section 3 provides comparative study of various methods reviewed. Section 4 performance metrics & Section 5 provides conclusion & future work.

II. BLACK HOLE DETECTION METHODS

There are different types of detection techniques which are as follows:-

2.1 Watchdog mechanism [4]

In this method, it keep record of two tables first is node rating table and second is pending packet table. The node rating table is used for maintaining the rating of node, address of node, dropping packet, packet which are to be transferred to next node & last field calculate the ratio of dropped packet. If the dropped packets given threshold value then this is 1 which means it is malicious node otherwise it is 0.

Advantages:

- It is a simplest method because one node only monitors its next node in the route.

Disadvantages:

- In this method, only one node monitor one node at a time.

- Source node should trust the other node's information about one node's misbehavior.
- There is no predefined limit to differentiate malicious nodes and increases the numbers of mistakes to find black hole attack.

2.2 Comparing destination sequence number [5]

Pooja jaiswal and Dr.Rakesh Kumar proposed method for black hole detection. In this source node collect the entire request reply message which is also known as RREP from different intermediate nodes. First entry marked as first entry in Route Reply Table (RRT). The sequence_number of target node compared with the source node sequence_number. The sequence number of destination node is very large than source node require node is suspected to be the malicious node and it is entry removed from RRT. The data packets path is selected on the bases of all entries which exist in the RRT table.

Advantages:

- Easy to implement

Disadvantages:

- Malicious node can act as source and break security

2.3. Detection of black hole using IDS method [6]

In this technique intrusion detection method is used where IDS nodes all set in promiscuous mode only when it is required to find any abnormal difference between the numbers of packet which are forward by it. If any abnormal difference happened then IDS node transmit the block packet to all nodes in network to separate the assailant node from network.

IDS node's actions for RREQ, RREP packets:-

RREQ: First IDS checks if there is an entry in its table for destination & source .IDS adds source, destination and all nodes which are going to broadcast nodes in table. These broadcasting nodes ID are used for detection of attack.

RREP: It stops to checking if the source is destination. If answer is no then it check if there is an entry for this node in its table as broadcasting node or not. If it is not last broadcast node then it starts a counter and named that node as inactive. If it cross the maliciousness over a predefined value, marks that node as active and sends messages to n/wk that called block and announces that is malicious node.

Advantages:

- It uses new nodes which called IDS. It gives more trustful reporting of black hole attacks.
- It is used for decreasing the overhead for monitoring on all nodes.
- There are less chances of mistake in detecting the malicious node.

Disadvantages:

- It needs some active and constant nodes which are always active in network.
- This scheme only detects black hole not gray hole attack.

2.4. Detection of black hole using DRI table [7]

This Method DRI (Data Routing Info) tables are used in which there are two fields: From and through. 'From' means that from this node gets a routing message and 'through in which from this current node sends a message to that node .In this source tries to find route from source sends RREQ packets to destination. If destination sends back the RREP, source trusts to its answer. If intermediate node returns RREP that node should also send its DRI Table & ID of the next neighbor in route to source. If source previously sent a message to that node. It is trustable node for source and start data transfer packet to that destination. If source does not know about that node then it sends packet to next node of marked node and ask for DRI table and also ID of next node. Same process continues until source receives a DRI table of a Trustable node. Then stop this process and just check DRI table of both neighbor nodes to find maliciousness by checking from and through field of them. If source find any difference in two neighbors DRI table announces all the nodes in N/WK about maliciousness.

Advantages:

- This method finds any co-operative black-hole attack.

Disadvantages:

- If there is no any attack in N/WK then this process consume lot of time and create overhead.
- It does not check gray hole attack.

III. PERFORMANCE METRICS

There are different kinds of metrics which are as follows:-

3.1 Throughput

The throughput is the amount of bytes sent or received in unit of time. The throughput is symbolized by T,[8]

Throughput=received node/simulation time

$$x = \frac{\sum_{i=1}^{n} N_i^r}{\sum_{i=1}^{n} N_i^s} \text{ X } 100\% \ldots\ldots\ldots.(1)$$

Where, Nr=average receiving node, Ns= average sending node, and *n* = number of applications.

3.2 Average end-to-end delay

It characterizes the time required to move the packet from the source node to the destination node. E-2-E delay [packet_ id] = received time [packet_ id]– sent time [packet_ id] The average end-to-end delay can be calculated by adding the times taken by all received Packets divided by its total numbers [8]

$$D = \frac{\sum_{i=1}^{n} d_{\dot{i}}}{N} \text{ X } 100\% \ldots\ldots\ldots\ldots\ldots.(2)$$

Where, di= average end to end delay of node of ith application and n=number of application

3.3 Dropped Packets:

It corresponds to the number of packets that aresent by the starting node and does not reaches the destination node [8].

Dropped packets = sent packets– received packets.

$$L = \sum_{i=1}^{n} (N_i^s - N_i^r) - \sum_{i=1}^{n} (N_i^s \_ N_i^r) \ldots\ldots\ldots(3)$$

Ns , Nrnode sent by the sender & the number of application data node received by the receiver, respectively for the *i*th application, and *n* is the number of applications.

3.4 Packets delivery fraction (PDF):

It can be calculated by dividing the received packets at the target node to the packets sent by the starting node [8].

PDF = (number of received_packets / number of sent_packets) * 100

$$PDF = \frac{\sum_{i=1}^{n} (N_i^s - N_i^r)}{\sum_{i=1}^{n} N_{i\cdot}^{s}} \text{ X } 100\% \ldots\ldots\ldots\ldots.(4)$$

Ns Nrnode sent by the sender and the number of application data node received by the receiver, respectively for the ith application, and n is the number of applications

IV.COMPARATIVE STUDY OF VARIOUS METHOD REVIEWED

Method	Black hole Nodes	Routing Protocol	Limitations	Result
Watchdog Mechanism[4]	Single	AODV	Do not detect more than one suspect node.	Improve the date security in mobile Ad –Hoc network.
Comparing destination sequence number[5]	Single	AODV	End to end delay, if sequence number is not extremely high then this method will not able to detect black hole.	High packet delivery ratio.
Detect black hole by IDS system[6]	Single	DSR	High overhead, difficult to set IDS node in network.	Detect and isolate the network from black hole.
Detect black hole by DRI table[7]	Collaborative	AODV	It does not check gray hole attack	It is used for detect the collaborative black node in network

V. CONCLUSION & FUTURE WORK

MANETs is fastest growing area of research today. Because of its dynamic nature, it is open to many attacks. This paper firstly discusses the brief introduction of Manets and different black hole detection techniques. Watchdog mechanism provides more security as compare to other methods. Comparing sequence number method give the highest packet delivery ratio as compared to other methods and IDS provides decreasing overhead. It also provides quick reporting of black hole compared to other methods. Future work includes intend to develop simulator to analyze the performance of the various black hole detection techniques.

REFERENCES

[1]. Shradhha Raut & SD Chede,"Detection and removal of black hole in mobile Ad hoc network (manets)", VOL-1, ISSUE-4, 2231-5284, 2012

[2]. Yashpal Singh, Dr.P.K.Singh, Jay prakash, "A survey on detection and prevention of black hole attack in AODV based manets", VOL-02,ISSUE-02,2013

[3]. Romia Sharma, Rajesh Sharma,"Modified AODV Protocol to prevent black hole attack in mobile Ad-hoc network",VOL-14,ISS-3,2014

[4]. Heta Changela, Amit Lathigara, "A survey on different existing techniques for detection of black-hole attack in manets", VOL-4,ISS-1,2015

[5]. Sakshi Jain, "Review of prevention and detection methods of black hole attack in AODV based on mobile ad-hoc network", VOL-4,ISSUE-4,PP:381-388,2014

[6]. M.Mohanapriya,IIango Krishnamurthy, "Modified DSR protocol for detection and removal of selective black hole attack in manets",2013

[7]. Marjan Kuchaki Rafsanjani, Zahra Zahed Anvari, Shahla Ghasemi, " Methods of preventing and detecting black , gray hole attack on AODV-based manets",2011

[8]. Ms.Gayatri Wahane, Prof.Ashok kanthe, "Techniques of detection of cooperative Black hole attack in manets." 2014

[9]. Robinpreet Kaur & Mritunjay Kumar Rai, A novel review on routing protocols in MANETS, Undergraduate academic research journal, VOL-1,ISSUE-1,2278-1129,

[10]. Swati saini and Vinod sarona,"Analysis and detection of black-hole attack in manets", International journal of science & research, VOL-2, ISSUE-5, 2013.

[11]. A.S.Mulla&Dr.B.T.Jadhav,"Networksecurity parameter analysis using simulation approach", VOL-4, ISSUE-4, 2015.

[12]. T.Manikandan,S.shitharth,C.Senthilkumar,C.Sebastinalbina,N.Kamraj,"Removal of selective black hole attack in MANET by AODV protocol",VOL-3,ISSUE-3,2014