International Journal of Electrical, Electronics and Computer Engineering **4**(1): 57-65(2015) **ISSN No. (Online): 2277-2626**

An Enhancement of Security level under varying Black Hole attacks in Mobile ad-hoc Network

Rashmi Vishwakarma* and Moh. Imran Hashiam**
**Research Scholar, Department of Computer Sciences Engineering, Jawaharlal Nehru College of Technology, Rewa, (MP), India*
***Professor, Department of Computer Sciences Engineering, Jawaharlal Nehru College of Technology, Rewa, (MP), India*

(Corresponding author: Rashmi Vishwakarma)
(Received 04 December, 2014 Accepted 15 February, 2015)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Wireless ad hoc network is extensively useful area in the field of communication. It is autonomous system which can dynamically form the network which has self- configuring capability and infrastructure less network. Due to its dynamic behavior it is more vulnerable to severe threats such as Sybil, wormhole, byzantine, hello flood, denial of services etc. which can influence the performance of the system. It is a group of mobile nodes and each node behaves as router or host. It uses different routing protocol to route the packet from source to destination. In this work, Black hole attack in AODV is discussed. In black hole attack, the malicious node announces itself as having the shortest path to the destination and falsely replies to the route requests, and drops all receiving packets. We propose a novel approach to remove the black hole attacked activities using blacklist criteria as well as miss-activity node identification based method and also IDS node to watch the neighbor node. The simulation of the proposed methodology is done using the network simulator NS-2.34. The analysis and comparison of the proposed method is done using different performance measuring metrics such as PDR, throughput, NRL and end to end delay.

***Keywords*—Attacks, AODV, MANET, Routers, Security Threats**

I. INTRODUCTION

The MANET is widely used filed now days this is because of its infrastructure-less and self-deployment in nature. In this each and every node can communicate with each other by own believes. Although wireless network has several advantages over the wired network but it also faces some of the security issues. This is used in many applications like military, disaster relief, communication and so on. But due to its self-configuring and dynamic capacity this network can be more vulnerable to severe type of attack during the transmission of packets from source to destination. For the transmission of the message or packets different routing protocols are used. The mobile ad hoc routing protocol is classified into three categories: table –driven routing protocol [1], on demand routing protocols [2] and hybrid protocol [3]. In table driven routing protocols the mobile nodes periodically broadcast the routing information to their neighboring nodes. Some of the example of this protocol is DSDV and OLSR etc. In on demand routing protocol, the routing starts when the node is require to transmit the packet some of the example of this routing protocols are: AODV, DSR and TORA etc. In This work we use AODV protocol to minimize the overhead. It uses two routing packet that is RREQ (route request) and RREP (route reply). AODV routing protocol also get influences by the security threat. This paper discussed about blackhole attack in AODV routing protocol. This attack advertises or broadcast that the malicious node has the shortest route to transmit the packet earlier and then it drop the packet.

The organization of the rest of the paper is done as follows: The section II explained about overview of routing protocol. Section III presents black-hole attack in AODV. In Section IV illustrate literature of the techniques for detection of black-hole attack. Section V explains about the proposed method and its algorithm. Section VI presents the experimental details with simulation results and last section gives conclusion about the paper.

II. OVERVIEW OF AODV ROUTING PROTOCOL

The mobile ad hoc network has different routing protocol for the transmission of packet. Generally, it is broadly categorized into three: table driven and on demand routing protocol which are summarized in Fig. 2.

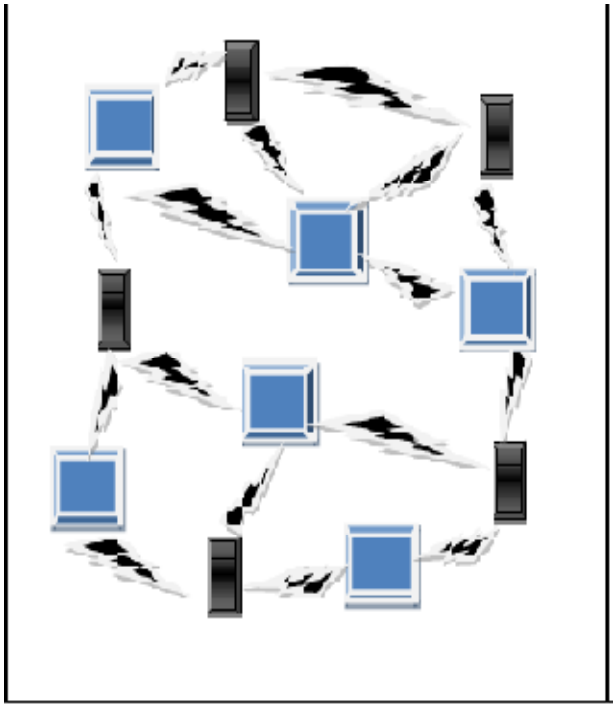

Fig.1. Mobile ad hoc networks.

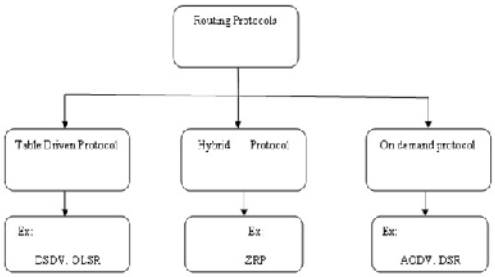

Fig. 2. Tree structure of routing protocols in mobile ad hoc network.

(i) Table driven routing protocol

These protocols are also called as proactive routing protocol since they uphold the routing information even formerly it is desired [1]. All nodes in the network uphold routing information to every other node in the network. Information of the route is normally kept in the routing tables and is intermittently updated as the network topology changes. There subsist definite differences along with the protocols that come under this classification depending on the routing information being updated in each routing table. Furthermore, these routing protocols uphold dissimilar number of tables. The proactive protocols are not suitable for larger networks as they necessitate upholding node entries for each and every node in the routing table of every node. It causes further overhead in the routing table leading to expenditure of superfluous bandwidth. This paper mainly emphasis on AODV (ad hoc on demand) routing protocol.

(ii) On demand routing protocol

These protocols are also called on demand routing protocols since they don't uphold routing information or routing movement at the network nodes if there is no announcement. If nodes wish to send a packet to another node then this protocol investigates for the route in an on-demand method and founds the connection in order to broadcast and acknowledge the packet [2]. The route discovery generally occurs by flooding the route request packets all over the network. Reactive investigate procedures can also add a momentous amount of control traffic to the network due to query flooding because of these weaknesses, reactive routing is less appropriate for real-time traffic or in scenarios with a high volume of traffic between a big numbers of nodes.

(iii) Hybrid Routing Protocol

Hybrid routing protocols combine the advantages of proactive and of reactive routing. This routing is primarily recognized with some proactively prospected routes and then serves the stipulate from furthermore activated nodes through reactive flooding. The fundamental idea is that each node has a pre-defined zone centered at itself in terms of number of hops. For nodes within the zone, it uses proactive routing protocols to preserve routing information. For those nodes exterior of its zone, it does not sustain routing information in a permanent base. Instead, on-demand routing policy is adopted when inter-z are summarized in fig. 2. one connections are required [3].

(iv) AODV routing protocol

AODV is a reactive routing protocol that does not recline on active paths neither upholds any routing information nor contributes in any periodic routing table exchanges. In additional, the nodes do not have to determine and uphold a route to another node until the two needs to communicate, unless former node is offering its services as an intermediate forwarding station to sustain connectivity between other nodes [4]. AODV has borrowed the concept of destination sequence number from DSDV [5] to sustain the most recent routing information among nodes. Every time a source node needs to communicate with another node for which it has no routing information, Route Discovery method is initiated by broadcasting a Route Request (RREQ) packet to its neighbors. Each neigh boring node either responds the RREQ by sending a Route Reply (RREP) backside to the source node or rebroadcasts the RREQ to its own neighbours after increasing the hop_count field. If a node cannot reply by RREP, it keeps record of the routing information in order to implement the reverse path setup or forward path setup [6]. The destination sequence number indicates the freshness of a route to the destination before it can be acknowledged by the source node. Ultimately, a RREQ will arrive to node that possesses a new route to the destination. If the intermediate node has a route entry for the required destination, it concludes whether the route is fresh by comparing the destination sequence number in its route table entry with the destination sequence number in the RREQ received. The intermediate node can use its recorded route to respond to the RREQ by a RREP packet, only if, the RREQ's sequence number for the destination is greater than the recorded by the intermediate node. Instead, the intermediate node rebroadcasts the RREQ packet. If a node accepts more than one RREPs, it updates its routing information of routing table and propagates the RREP only if RREP surrounds either a larger destination sequence number than the preceding RREP or similar destination sequence number with a lesser hop count. It surrounds all other RREPs it receives. The source node starts the data broadcasting as soon as it receives the first RREP and then afterwards updates its routing information of better route to the destination node. Each route table entry encloses the subsequent information:

-Destination node
-Next hop
-number of hops
-Destination sequence number
-Active neighbors for the route
-Expiration timer for the route table entry

The route discovery method is reinitiated to set up a new route to the destination node if the source node moves in an active assembly. As the link is busted and node receives a announcement and Route Error (RERR) control packet is being sent to all the nodes that uses this broken link for further communication. And then, the source node restarts the discovery process. Since the routing protocols normally assume that all nodes are cooperative in the synchronization process malicious attackers can effortlessly interrupt network operations by disobeying protocol arrangement. This paper discusses about black hole attack and provides routing security in AODV by eradication the threat of black hole attacks.

III. BLACK HOLE ATTACK IN AODV

In Black hole attack a malicious node broadcasts about the shortest path to the node whose packets it wants to seize [7]. In following figure, imagine, M is malicious node. When node A broadcasts a RREQ packet, nodes B, D and M receive it. Node M, being a malicious node, this node does not check up with its routing table for the requested route to node E. Hence, it immediately sends back a RREP packet, claiming that it has a route to the destination. Node "A" receives the RREP from M ahead of the RREP from B and D. Node A assumes that the route through M is the shortest route and sends any packet to the destination through it. When the node A sends data to M, it absorbs all the data and thus behaves like a Black hole.

In AODV there are two type of black hole attack [8], these are following.

A. Internal Black hole attack. This type of black hole attack has an internal malicious node which fits in between the routes of given source and destination, when it gets the chance this malicious node makes itself an active data route element. Now this node is capable of conducting attack with the start of data transmission. This is an internal attack because node itself belongs to the data route.

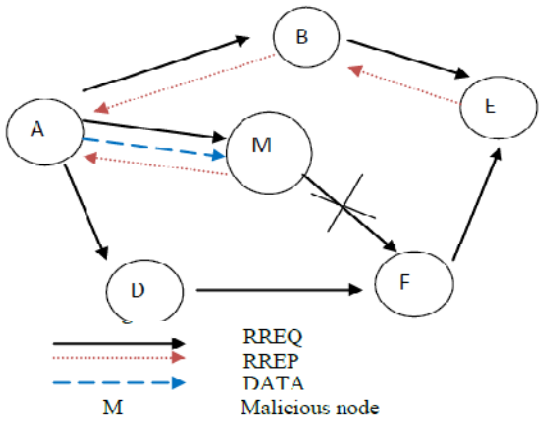

Fig. 3. Black-hole attack in AODV routing protocol.

B. External black hole attack. External attack physically stays outside of the network and denies access to network. External attack can become a kind of internal attack when it take a control of internal malicious node and control it to attack other nodes in MANET. External black hole attack can be summarized as following points:

1. Malicious node detects the active route and notes the destination address.
2. Malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value is set to lowest values and the sequence number is set to the highest value.
3. Malicious node send RREP to the nearest available node which belongs to the active route. This can also be send directly to the data source node if route is available.
4. The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node.
5. The new information received in the route reply will allow the source node to update its routing table.
6. New route selected by source node for selecting data.
7. The malicious node will drop now all the data to which it belong in the route.

IV. RELATED WORK

Shalini Jain *et al.* [9] proposed a method accomplished of detecting and removing the malicious nodes launching two types of attacks. Their method consists of an algorithm which works as follows. Instead of sending the total data traffic at a time they separate the total traffic into some small sized blocks. Hence, malicious nodes can be detected and removed in between the transmission of two such blocks by ensuring an end-to-end checking. The source node sends an overture message to the destination node prior to start of the sending any block to attentive it regarding the arriving data block. Flow of the traffic is monitored by the neighbors of the each node in the path. Subsequent to the end of the transmission destination node sends an acknowledgement through a postlude message containing the no of data packets received by destination node. Source node uses this information to check whether the data loss during transmission is within the unobjectionable collection, if not then the source node instigate the process of detecting and removing malicious node by aggregating the answer from the monitoring nodes and the network. Harsh Pratap et al. [10] proposed a method in which broadcast synchronization (BS) and relative distance (RD) method of clock synchronization is used to prevent the black hole nodes. In this internal and external clock node compare with the threshold clock if both the clock time is greater than the threshold then it is found that the node is malicious. This method can easily detect and prevent the block-hole node. Taranpreet Kauret et al.[11] they proposed a clustering behaviour based reputation mechanism to recognize the flooding malicious nodes in military battlefield network. Since in battlefield situation; mainly Group Mobility model is followed so grouping of nodes in clusters have a variety of advantages. Reputation (appraisal of its behavior in the network) of a node is calculated at cluster heads. This approach has double nature, therefore it efficiently fix the false detection of genuine nodes as malicious ones. The performance of new method is compared with AODV protocol based on different performance measures it is noticed that proposed strategy has better performance in terms of various measures. Neelam Khemariya *et al.* [12] proposed a secure efficient algorithm for the detection of the Black hole attack is described. This algorithm firstly identifies the black hole node in the given Mobile Ad hoc Network and then removes the entries for that node from the routing table. The algorithm is implemented in a fashionable reactive routing protocol called AODV (Ad hoc On demand Distance Vector Routing). The loveliness of the proposed algorithm is that it employs in both the cases when there is no announcement (i.e., a node is inactive) and when a node is announcement (node is not inactive). This algorithm can detects both the single Black hole attack and the cooperative black hole attack. Payal N. Raj *et al.* [13] proposed DPRAODV (detection, prevention and reactive AODV) to thwart the black hole attack by informing the other nodes about the malicious node. When the value of RREP sequence number is initiated to be higher than the threshold value, the node is assumed to be malicious and it adds the node to the black list. As the node detected an anomaly, it sends a new control packet ALARM to its neighbors.

The ALARM packet has the black list node as a constraint so that, the neighboring nodes know that RREP packet from the node is to be leftover. Additional, if any node obtains the RREP packet, it looks over the list if the answer is from the blacklisted node; no processing is done for the similar. The threshold value is the average of the difference of destination sequence number in each time slot between the sequence number in the routing table and the RREP packet. Yiebeltal Fantahun Alem et al. [13] Proposed an Intrusion Detection using Anomaly Detection (IDAD) technique to prevent the black hole attack. IDAD assumes every activities of a user or a system can be monitored and anomaly activities of an intruder can be identified from normal activities. Hence, by identifying anomaly activities of an adversary, it is possible to detect a possible intrusion and isolate the adversary. To do so an IDAD needs to be provided with a pre-collected set of anomaly activities, called audit data. Once audit data is collected and is given to the IDAD system, the IDAD system can compare the every activity of a host with the audit data on a fly. If any activity of a host (node) resembles the activities listed in the audit data, the IDAD system isolates the particular node by forbidding further interaction. It minimizes the extra routing packets which in turn minimizes the network overhead and facilitates faster communication.

V. PROPOSED METHODOLOGY

A. Problem statement

Technology is growing day by day and Mobile Ad-hoc network is here very challenging field because number of various region one measure challenge is topology control, and rather than that other region is data drop through miss-activities, an-authorized access, varying attacker node, MAC error .

B. Proposed Algorithm

Here we proposed a novel approach to remove the black hole attacked activities using blacklist criteria as well as miss-activity node identification based method. The work is enhances the performance of the mobile ad-hoc network in the respect of overall performance like high PDR and minimum routing load maintenance. In the novel approach, initially we set IDS node that watch the all neighbor node activities and broadcasting node generate random packet sequence number while transmitting packets after defined intervals, and here if IDS get found any suspicious activities in nearby range so it keep watching the particular node behavior. But if attacker node/s receives the packet but not forward to the next hope so it simply state that node is to be set as attacker node so it will be blocked, another thing is that if any node continues sends the routing packets to the any particular node, so that will also set as attacker node, and it will be blocked, after the successful blocking of the suspected nodes, we change the route and packet sequence number randomly then transmit data safely to the destination node. And finally observed that the commonly used measurement parameters like: PDR, Throughput, Delay calculation and Network load.

Algorithm follows the following major steps:

IDS for finding Blackhole Attacker Node

```
Set mobile node = M                    //Total Mobile Nodes
Set Sender node = S                    //S □ M
Set Receiver Node = R                  // R □ M
Set Routing Protocol =AODV             //Set Routing Protocol
Start simulation time = t0             //Initial time
Set radio range = rr;                  //initialize radio range
Set sequence number = sqno; //Set packet sequence number
AODV-RREQ_B(S, R, rr, sqno)
{
   If ((rr<=550) && (next hop > 0))
        {
          Hope Count ()
                {
      rtable->insert(rtable->rt_nexthop);   // next hop to RREQ source
  rtable1->insert(rtable1->rt_nexthop);     // nexthop to RREQ destination
if (dest==true)
        {
        Sqno = no-changed;
        Send ack to source node with rtable1 and sqno;
Data_packet_send(sqno, nexthop, type)
        }
        Else
                {
                Destination node not found;
                }
                }
        }
                Else
                {
                Destination mobile is not-reachable;
                }
        }

RREQ_Limit_Check (S, R, M, sqno)
{
      If ((node € M) && (RREQ < 20 pkts/s && (incoming =-true && outgoing ==true))
        {
                RREQ accepted by neighbor;
                RREQ_Accept_limit();
                Calculate PDR
                Calculate Delay/Interval
                If (time-interval > 10)
                        Sqno = rand (new sqno);
        }
              Else
                 {
                 RREQ_Blacklist()
                      {
```

Rejected by neighbor node; **Then**
Block RREQ sender;
Sqno = rand (new sqno);
Set PDR = 0.0;
}
}
}
.

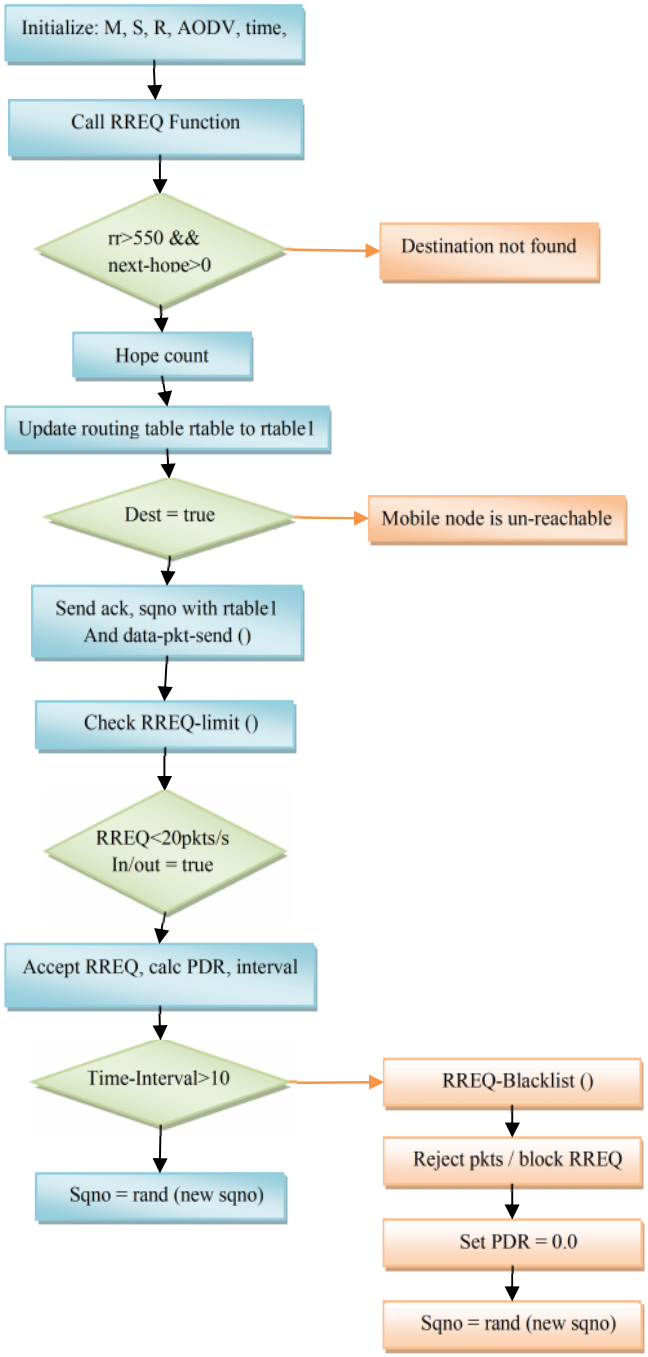

Fig.4. Block diagram of proposed methodology.

VI. EXPERIMENTAL RESULTS ANS ANALYSIS

The simulation of the proposed methodology is done using the well known network simulator NS-2.34.
It is an open-source object-oriented discrete-event simulator for network research. The simulator is written in C++, with an OTcl (Object Tool Command Language) interpreter used as the command interface. The C++ part constitutes the core of the simulator, where detailed protocol implementation and the simulation engine are located.
Performance Metrics
The performance of the WSN can be measured by using different parameter such as Throughput, Packet delivery ratio, end to end delay, routing load.

1. Throughput: It is the average rate of successful message delivery over a communication channel. $Throughput \leq \frac{RWIN}{RTT}$

2. Packet delivery ratio: Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources.
Mathematically, it can be defined as:

PDR= S1÷ S2

3. End to end delay: The average time it takes a data packet to reach the destination. This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue. This metric is calculated by subtracting time at which first packet was transmitted by source from time at which first data packet arrived to destination.
Mathematically, it can be defined as:

Avg. EED=S/N

4. Normalized Routing Load (NRL): It is defined as the total number of routing packet transmitted per data packet. It is calculated by dividing the total number of routing packets sent (includes forwarded routing packets as well) by the total number of data packets received.
Scenario Setup
The implementation of an algorithm is done in well known network simulator NS-2.34 [15]. The simulation environment is setup to simulate the algorithm in which we take an area of 900x900 to transmit the packet TCP/FTP, UDP/CBR protocol AODV is used and the channel wireless operation mode 802.11, mobility model random waypoint with least frequency 50 Hz is used for the simulation time period of 400 sec. In this work, mainly focuses for providing better security by consuming less energy. The comparison of above is done using different parameter such packet delivery ratio, throughput, routing load, delay etc. The simulation parameters are shown in table 1.

Table 1: Simulation Setup.

Parameter	Value
Area	900x900
Nodes	30
Packet	TCP/FTP, UDP/CBR
Channel ireless	802.11
Mobility model	Random Waypoint
Simulation Time	400
Protocol	AODV
Least Frequency	50 Hz

We have simulated the network using AODV routing protocol. It shows the performance in terms of packet delivery ratio in which the method better result than the existing method. The analysis is done by varying the simulation time of the nodes.

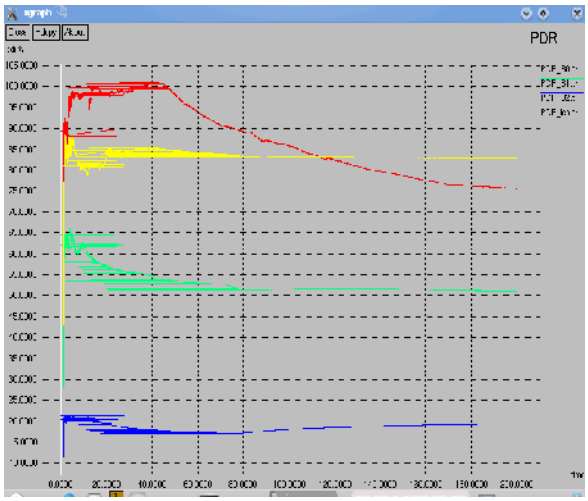

Fig. 5. Comparison of simulation time Vs PDR% with existing and proposed methodology.

Next the analysis of the proposed method is done using the performance metric end to end delay by varying the simulation time and the simulation result shows that delay of the node is very less than the existing method. Then again next, the performance metric throughput is used for analyzing the proposed work and our method enhances the throughput of the network.

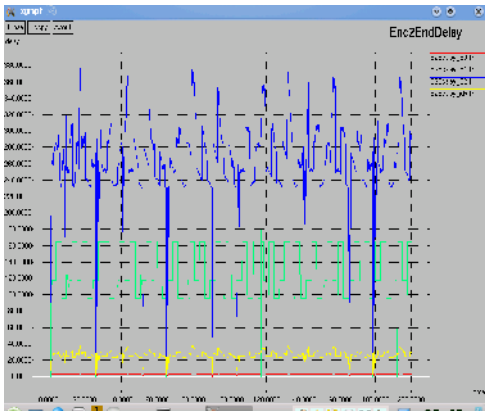

Fig. 6. Comparison of simulation time Vs End to End delay with existing and proposed methodology.

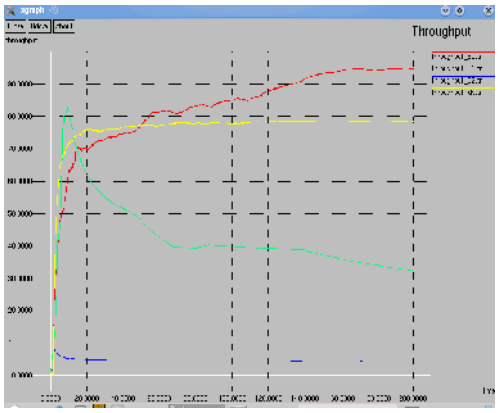

Fig. 7. Comparison of simulation time Vs Throughput with existing and proposed methodology.

The normalized routing load of the existing and proposed methodology differs as we increase the simulation time. The routing load of any network must be low and find that the existing method has more routing load than the proposed methodology which as shown in fig. 8.

VII. CONCLUSION AND FUTURE WORK

In this paper, proposes a novel method to detect and find a secure route against Black hole attack in ad hoc network. Black hole attacks are serious problems that need to be addressed in wireless network security. Although significant research has been done to defend black hole attacks, with use of this method one can detect black hole nodes in wireless ad hoc network.

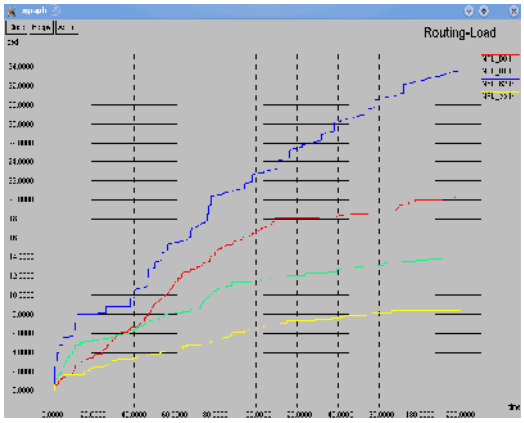

Fig. 8. Comparison of simulation time Vs Routing Load with existing and proposed methodology.

In this thesis, a secure and flexible technique is proposed using the blacklist criteria as well as miss-activity node identification based method which can be tuned to meet desired security and performance constraints. These methods are performed well with low operating cost and resist the described attack. The simulation result the proposed methodology is done by using different performance metrics parameter in which the work shows that it enhances the performance of the mobile ad-hoc network in the respect of overall performance like high PDR and minimum routing load maintenance.

In future work, this method can also be implemented for the detection of wormhole/grayhole attack detection and prevention in MANETs.

REFERENCE

[1]. Charles E. Perkins “Ad Hoc Networking” ,Addision Wesley, 2001.

[2]. Tseng Y.C., Shen C.C, and Chen W.T. “Mobile IP and ad hoc networks: An integration and implementation experience” Technical report, Department of Computer Sci. and Inf. Eng., Nat. Chiao Tung Univ., Hsinchu,, Taiwan, 2003.

[3]. Vipan Chand Sharma, Atul Gupta, Vivek Dimri, “Detection of Black Hole Attack in MANET under AODV Routing Protocol”, *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume **3**, Issue 6, June 2013

[4]. Charles E. Perkins and Elizabeth M. Royer “Ad-Hoc On-Demand Distance Vector Routing”. In *Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications (WMCSA’99)*, pages 90–100, February 1999.

[5]. C. Perkins and P. Bhagwat, “Routing over multi-hop wireless network for mobile computers”. SIGCOMM ’94: *Computer Communications Review*: 234-244, Oct. 1994.

[6]. Payal N. Raj, Prashant B. Swadas, "DPRAODV: A Dynamic Learning System Against Blackhole Attack In AODV Based MANET", *IJCSI International Journal of Computer Science Issues*, Vol. **2**, 2009 ISSN (Online): 1694-0784.

[7]. Latha Tamilselvan and Dr. V Sankaranarayanan "Prevention of Blackhole Attack in MANET", 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 2007.

[8]. Irshad Ullah, Shoaib Ur Rehman, "Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols" in Thesis no: MEE 10:62 in June, 2010.

[9]. Shalini Jain "Advanced Algorithm for Detection and Prevention of Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks*" International Journal of Computer Applications* (0975 – 8887) Volume **1** – No. 7

[10]. Harsh Pratap Singh, Rashmi Singh, "A mechanism for discovery and prevention of cooperative black hole attack in mobile ad hoc network using AODV protocol", *International Conference on Electronics and Communication Systems (ICECS) 2014* , Page(s):1 - 8 Print ISBN:978-1-4799-2321-2

[11]. Taranpreet Kaur, Amanjot Singh Toor, Krishan Kumar Saluja, "Defending MANETs against Flooding Attacks for Military Applications under Group Mobility", Proceedings of 2014 RAECS VIET Panjab University Chandigarh, 06 - 08 March, 2014

[12]. Neelam Khemariya, Ajay Khuntetha, "An Efficient Algorithm for Detection of Blackhole Attack in AODV based MANETs", International Journal of Computer Applications (0975 – 8887) Volume **66**,No.18, March 2013

[13]. Payal N. Raj, Prashant B. Swadas, "DPRAODV: A dynamics learning system against Black-hole Attack in AODV Based MANET", *IJCSI International Journal of Computer Science Issues*, Vol. **2**, 2009, ISSN (Online): 1694-0784 ISSN (Printed): 1694-0814

[14]. Yiebeltal Fantahun Alem, Zhao Chenh Xuan, " Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection", *2nd International Conference on Future Computer and Communication, IEEE*, Volume **3**, 2010 .

[15]. Jianping Wang "ns-2 Tutorial Exercise", Multimedia Networking Group. Partially adopted from Nicolas's slides.