Detection of Black Hole Attack using Control Packets in AODV Protocol for MANET

Nidhi Tiwari
Department of Computer Science and Information Technology
Sam Higginbottom Institute of Agriculture, Technology and Sciences (Deemed-to-be-university), Naini, Allahabad, India

Raghav Yadav
Department of Computer Science and Information Technology
Sam Higginbottom Institute of Agriculture, Technology and Sciences (Deemed -to-be-university), Naini, Allahabad, India

ABSTRACT

Mobile ad hoc network (MANET) is a network of mobile nodes in which there is no infrastructure is defined. Mobile nodes transmit their information through intermediate nodes. Since there is no predefine infrastructure, MANET suffers from many internal or external attacks. Black hole attack is one of the security attacks in MANET. In black hole attack, a malicious node replies with having a shortest path to destination and absorb the send packet by the source node instead of forwarding it to the destination node. An approach is presented for the detection of black hole attack using control packets and prevents the network by informing other nodes in network.

Keywords

MANET, black hole, AODV, RREQ, DRREQ, DRREP, DBAODV

1. INTRODUCTION

Mobile Ad-hoc network (MANET) is a collection of mobile nodes that can change their location and configuration at any time. Each node can communicate with the help of the intermediate node between them. In MANET there is no predefined infra-structure, so to make the communication possible between nodes in MANET set of rules has been define that finds the route from source and destination. These set of rules are called routing protocols. The routing protocols [20] for MANET are DSR, DSDV, AODV, OSPF, ZRP etc. AODV is ad-hoc on demand distance vector routing as its name signifies it finds the route or path when there is need to transfer the information.

Due to the absence of the central control over the network, each mobile node takes the help of the intermediate node to transfer the packets. Several attacks such as gray hole, wormhole, sybil attack may affect the communication between nodes in MANET, black hole attack is one of them. So MANET must have a secure way to transfer information over the network. There has been presented many research efforts by the researchers to reduce the security threat in ad hoc network. In this paper we discus about one of the security attack which is called black hole attack. In black hole attack malicious node consumes the packet send by the source node or intermediate node and does not send it to the destination or other intermediate nodes and it interpret itself as a normal node by sending a reply to the sender of the packet with higher sequence number.

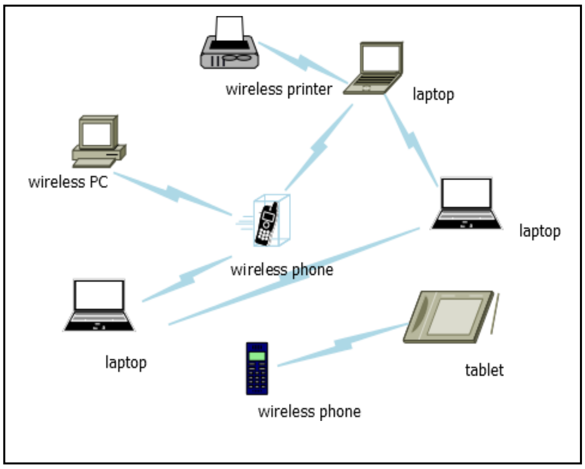


Fig 1: Mobile ad-hoc network

1.1.Black hole Attack in AODV

A black hole attack in AODV occurs due to the presence of a malicious node which advertises itself as having a shortest and fresh route to the destination. This type of malicious node is called as black hole node as it does not forward the data packet to its neighbor nodes; it only drops the packets coming from the source node as shown in figure 2.

Assume P and U is the source and destination node respectively and R is the black hole node. Source node P wants to send some data to the destination and it does not have the route to the destination in its routing table, therefore, it broadcast RREQ packets to its neighbors Q, S and V. On receiving the RREQ packet, nodes S, V searches their cache for find the route, on the other hand node Q send the RREP packet to the source before other nodes with higher sequence number as node R advertise itself having route to U. Source node on receiving RREP assumes that node Q has the route and sends the data packet to it. On receiving data packet black hole node R drops the data packet, while source node assumes that data packet will reach on destination.

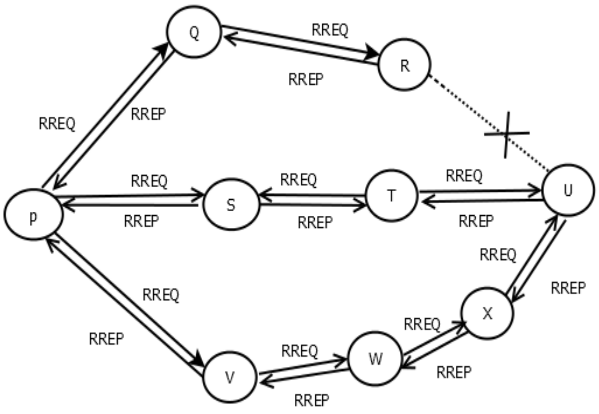


Fig 2: Black hole attack in AODV

The paper is organized as in section II literature of previous work is discussed, the proposed work and algorithm is presented in section III, the result of implementation of proposed work in shown in section IV of this paper and finally conclusion is made in section V.

2. RELATED WORKS

To make the ad-doc network safe from black hole attack many researches had been done. Researchers did their own works to prevent the network using different methods and concepts.

Payal N. Raj et al. [1] proposed a solution against black hole attack. Authors projected DPRAODV to defense against this attack. In this approach authors checks the seq_no in RREP packet. According to the approach if the seq_no in RREP has the higher value as compare to the sequence number in the routing table of sender then the RREP packet is acceptable. For comparing authors defined a threshold value. If the compared value of the seq_no is also higher than the threshold value then the sender of RREP is consider to be malicious and an ALARM message is send to the neighbors by the source node.

Seryvuth Tan et al. [2] proposed a new protocol SRD-AODV (Secure Route Discovery for AODV-based MANET) for detecting black hole nodes. In this protocol, authors defined three thresholds for classifying malicious and normal node in three different environments- small, medium and large environments. In his approach the sequence number of each response is checked with threshold value. If it is greater than that node is black hole node otherwise normal node.

MINseq = 0

MAXseq = 4294967295

Weichao Wang *et al*. [3] proposed a hash based technique for finding the behavior of nodes. This technique is based on the auditing method to discover the collaborative misbehaving nodes. This method of discovering the collaborative attack such as black hole or grey hole used REAct which is audit based method. The audit based REAct is unable to find the collaborative attack. An auditing node is settled by the source node and source node sends sequence numbers for the packet to be sent to the auditing node. The source node adds random number t0 to every packet and sends it. Intermediate node combines its own random number with received packet to find random number t1. Every intermediate node continued this process until destination node will receive the packet.

Marti et al. [4] proposed a method that uses Watchdog and Pathrater to detect black hole attacks. Watchdog enables neighbor nodes to detect malicious nodes. Watchdog detects malicious nodes by finding nodes that are repeatedly discarding packets. Pathrater assigns a default value to each node and then observes the transmitting behavior of each node. After a period of time, if the value for a node is below a certain threshold, the node will be added to the list of black hole nodes. This method cannot handle cooperative attacks.

B. Sun et al. [5] has presented a neighborhood approach for detecting the black hole attack. Once the root discovery process initiated by the source is over, the source node sends a special control packet to request the destination to send its current neighbor set. If the two neighbor sets received by the source at the same time are different enough, it can be considered that they are generated by two different nodes. Thus the difference between the two neighbor set is compared with threshold value. If the difference is larger source node assumes that this network has thee black hole node. But this approach is unable to count the number of black hole nodes present in the current ad hoc network.

3. PROPOSED APPROACH

In this proposed approach route request and reply message is modified in order to find the black hole node along with the route to the destination. The basic idea is that a normal node cannot find the route for invalid IP address where as malicious node respond for invalid destination IP address as it never search routing table for finding the route and never forward the request to other nodes. That is why in this method two destination IP address is specified in route request massage. One is valid destination IP address and second is invalid IP address for detecting the black hole node. This new route request is called here DRREQ (REQuest for Route and Detection). The benefit of adding two destination IP addresses is that only malicious node will send reply for both IP addresses, on the other hand normal or genuine node responds only for desired valid IP address. Route reply packet is changed and it is named as DRREP (Route Reply with Detection). A FLAG field of 2 bits is added in DRREP for understanding the reply. On the basis of values of the FLAG replied node is decided either it is normal or black hole. The values of FLAG are shown in table1.On receiving the reply with FLAG value 01 or 11, source node mark that replying node as malicious in its routing table field BLACK_HOLE_ID and it then broadcast an ALERT message to inform neighbors with ID of black hole node. On receiving the ALERT message neighbors will mark the ID of black hole node in its routing table for future use so that they reject any reply or request from marked nodes. After sending ALERT message source node selects one of the other routes arrived which has higher sequence number and less hop-count value.

Table1. FLAG values

Value	Route information	Decision about node
00	No route for any address	-------------
01	Route for invalid IP	Malicious node
10	Route for valid but nor for invalid IP	Normal node
11	Route for both address	Node is malicious

Thus a node that wants to start communication will broadcast a DRREQ packet. On receiving the DRREP from nodes, source node will first check in its routing table whether the replying node is marked as malicious? If yes, it will simply discard DRREP packet if no will check FLAG value. On the basis of above table1 decision will be taken by source node. This approach is illustrated in figures 3 and 4.

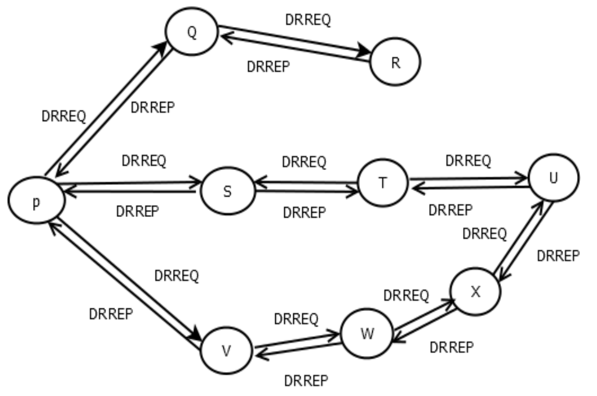


Fig 3: Propagation of DRREQ and DRREP

In above figure 3 suppose P is a source node and U is the destination node and R is the malicious node. To start the communication source node initially broadcast a DRREQ packet with two destination IP addresses. On receiving DRREQ packet black hole node responds by sending the DRREP packet while other nodes forward it to their neighbors if not found the route. The Id of black hole node has been saved in routing table with field BLACK_HOLE_ID when the FLAG value in DRREP would be either 01 or 11. FLAG value replied by any of the normal node would be 10.

Source node P receives three routes P-Q-R, P-S-T and P-V-W-X to reach destination U. Out of these three first route information arrives earlier than other as black hole node immediately send reply. On receiving this information source node check FLAG bit. If the FLAG bit indicate that the reply from malicious node then the IP address in the field last replied node will be saved in routing table and source node will discard this route and consider other route requests having higher sequence number and less hop-count. Now the source node selects either route P-V-W-X or P-S-T-U and sends the data packet to the selected route as shown in figure 4.

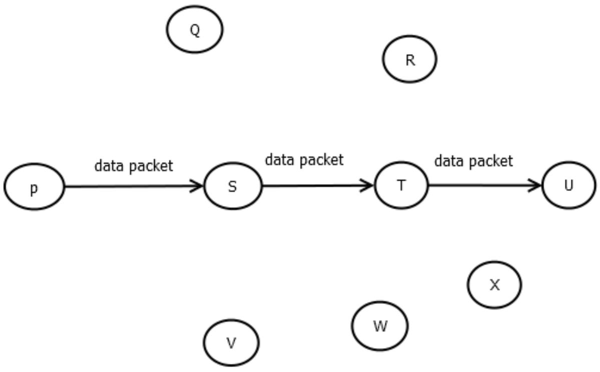


Fig4: Forwarding of data packet

3.1. Formats of Packets

3.1.1. Format of DRREQ packet

This packet is used for route discovery process as well as malicious node detection. Destination IP address1 is the address of desired destination and Destination IP Address2 is the non existing IP address. The number represented in bits.

Table2. DRREQ format

Type[8]	Reserved [16]	Hop Count[8]
DRREQ ID [32]		
Destination IP Address 1[32]		
Destination IP Address 2[32]		
Destination Sequence Number[32]		
Source IP Address[32]		
Source Sequence Number[32]		

3.1.2. Format of DRREP packet

Table3. DRREP format

Type[8]	Pfx Length[8]	Hop Count[8]
Destination IP Address 1[32]		
FLAG [2]		
Destination Sequence Number [32]		
Source IP Address[32]		
IP Address of node that first generate DRREP [32]		
Life Time [32]		

3.1.3. Routing table format

AODV maintains the routing table [8] for each route even for short lived route. The fields of routing tables are shown in figure 5.

- **Destination IP Address**- IP address of the destination node.
- **Destination Sequence Number**- last sequence number received by the source.
- **Valid Destination Sequence Number flag** – value can be set or unset.
- **Other state and routing flags** – values can be valid, invalid, repairable, being repaired.
- **Network Interface**- stores the interface number that indicates the network interface through which a data packet is sent to a next hop along the path.
- **Hop Count** - number of hops needed to reach destination.
- **Next Hop -** IP address of the next hop.

- **List of Precursors** - contains the list of neighboring nodes to which a RREP packet was forwarded.
- **Lifetime** -expiration or deletion time of the route.
- **BLACK_HOLE_ID** - stores the IP address of the black hole node.

3.2. Proposed Algorithm

Step 1: Initially SN broadcast DRREQ
Step 2: There can be two cases:

    Case1: If IMN is a BHN
        send DRREP immediately with FLAG 01 or 11
    Case 2: If IMN normal node, forwards DRREQ to its neighbor if not finding the route for first destination IP address or send reply with FLG value 10.

Step3: On receiving DRREP

    Case 1: if FLAG value is either 01 or 11, SN discards the route reply and selects route with higher sequence number and less hop count
    Case 2: if FLAG value is 10 the route reply is accepted by SN

Step4: SN then sends the data packet towards the selected route.
Step 5: SN broadcast the ALARM message to inform other nodes.

Notations used:

SN- Source Node

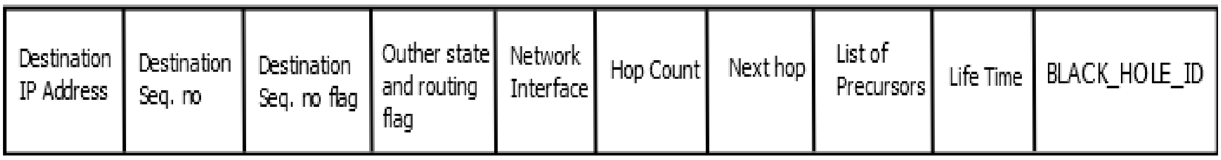
DN-Destination Node

IMN-Intermediate Node

BHN-Black Hole Node

DRREQ-Route REQuest for Detection

DRREP-Route request for Detection



Destination IP Address	Destination Seq. no	Destination Seq. no flag	Outher state and routing flag	Network Interface	Hop Count	Next hop	List of Precursors	Life Time	BLACK_HOLE_ID

Fig 5: Routing table used in proposed work

3.3. Flow Charts

i. Chart first is made to understand the action and reaction of source node after sending DRREQ and receiving DRREP. Chart first is shown in figure 6.

ii. Chart second is for intermediate node and is shown in figure 7.

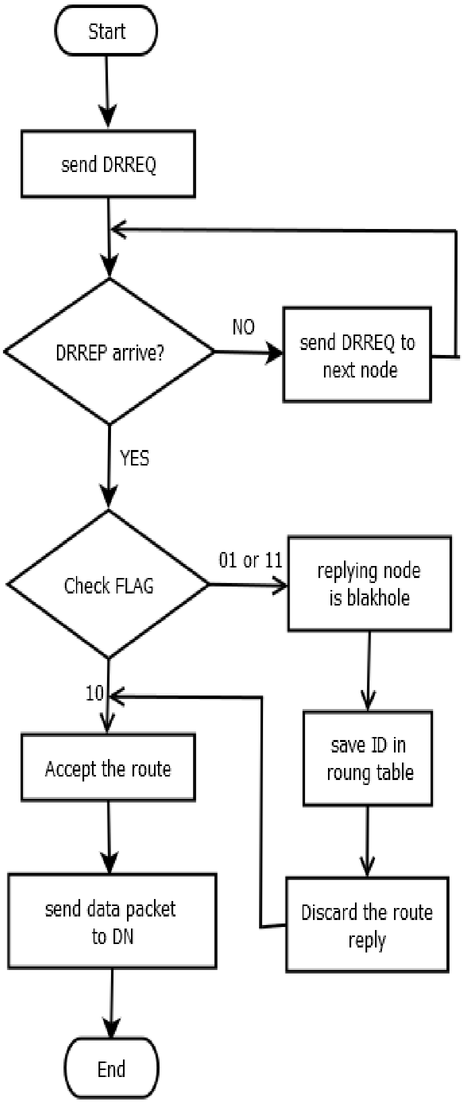


Fig 6: Flow chart for source node

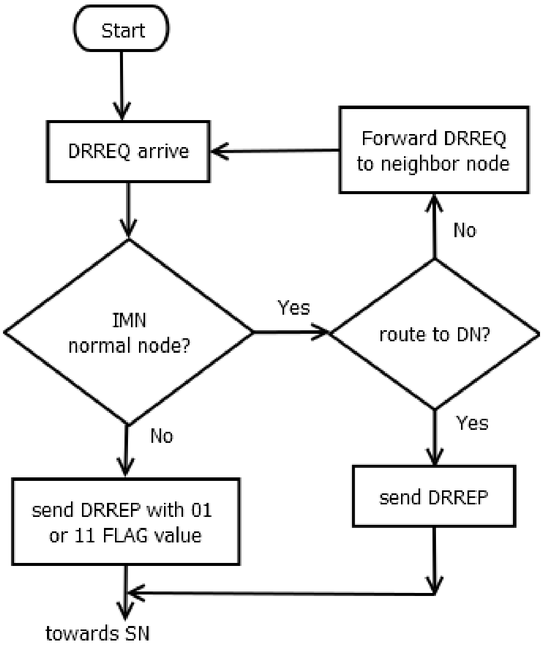


Fig 7: Flow chart for intermediate node

4. RESULTS

The NS2 simulator is used to implement the proposed system. The parameters are used in simulation is shown in table 4 and a output window of simulation is shown in figure 8. The simulation run is performed each time when parameters were changed. To get the values, for each parameter and for different numbers, simulation was performed at least 10 times. These simulations are done for seven pause times and on average 80 simulations were performed. Thus a grand total of 800 simulation run was performed. In simulation initially 5 nodes are made to move after that number of mobile node is increased for the analysis of throughput, end-to-end delay and packet delivery ratio.

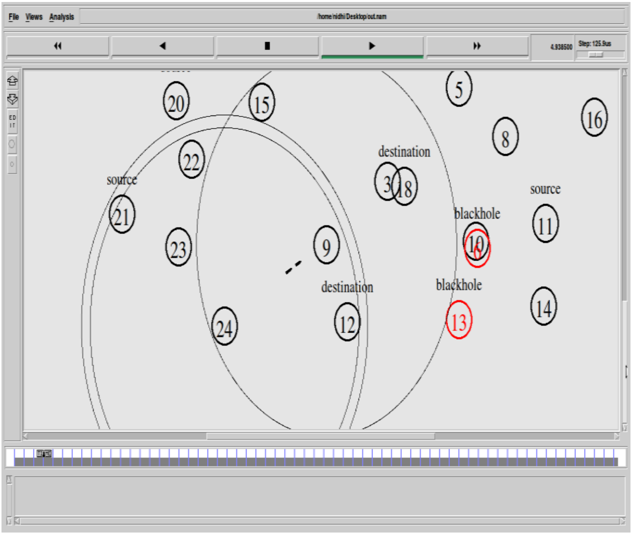


Fig 8: Snapshot of simulation run

Table 4.Simulation Parameters

Protocol used	AODV
Simulation Time	100 ms
Simulation Area (mxm)	900 m x 900 m
Number of Nodes	25
Traffic Type	CBR
Performance Parameters	Throughput, End to End Delay, PDR
Mobility(m/s)	20 m/s
Mobility Model	Two Ray Ground Model
Number of Black hole Node	1,2,3
Number of Mobile Nodes	5, 8, 11, 14, 17, 20, 23,25
Number of Connections	5,8,11

4.1. Packet Delivery Ratio (PDR)

Packet delivery ratio is the ratio of total number of data packet received by the destination node to the total data packet send by the source node. Packet delivery ratio is plotted with respect to the change in number of mobile nodes as shown in figure 9. Initially when moving nodes were less, PDR is higher and approximate 99.9% and on increase in number of moving nodes PDR decrease and then increase. When number of moving nodes was 5 the packet delivery ratio was 99.32% for our approach, it is 99.39 % when moving node were 8. As the moving nodes were increased and 3 malicious nodes were introduced when mobile nodes become 17 the value of PDR is 99.05% in DBAODV due to proposed algorithm black hole node not able to consume the packets. The random change in AODV line is due the affect of malicious nodes and it reduces the delivery ratio whereas in DBAODV line packet delivery ratio shows better value than AODV because of the detection and prevention.

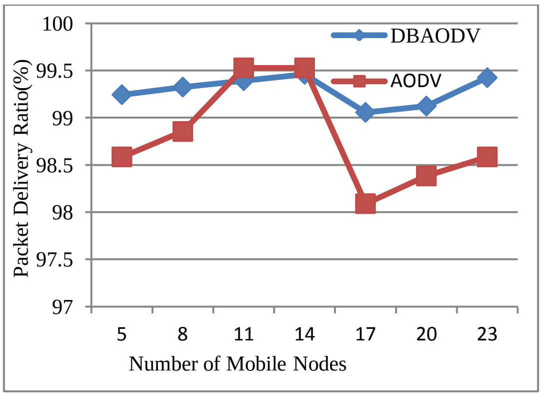


Fig 9: Packet Delivery Ratio of network with 25 nodes

4.2. End-to-End Delay

The Average end-to-end delay is the ratio of the time difference of the arrival time and the send time of the packet to the total number of connection in the network. The lower value of average end-to-end delay means the better performance of the protocol. The graph of end-to-end delay with respect to the number of mobile nodes is shown in figure 10.

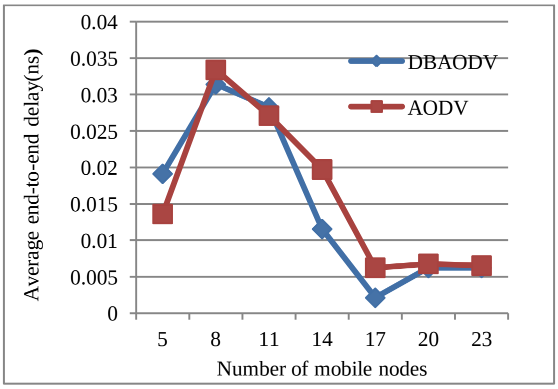


Fig 10: Average end-to-end delay

The shape of graph is so because the end-to-end delivery is affected by the change in number of mobile nodes as delay may possible due to the route finding or due to the link break. Initially graph shows the lower value of delay in AODV than DBAODV as DBAODV involves checking of parameters involve in its packet. As the introduction of 3 black hole nodes after there are 17 numbers of nodes in network, end-to-end delay in DBAODV has lower value than AODV which shows that our approach shows better value with respect to end-to-end delay than AODV in presence of black hole nodes.

4.3. Throughput

Throughput is the ratio of actual number of packets send by the source node to the total time taken to send those packets. The time consumed to send the data packet is the actual transmission time and the sum of the time spent in the route finding process and flow control mechanism. The throughput is calculated for two scenarios for the proposed approach, first when there is five numbers of connections between mobile nodes and second, when there is eight numbers of connections between mobile nodes in simulation environment.

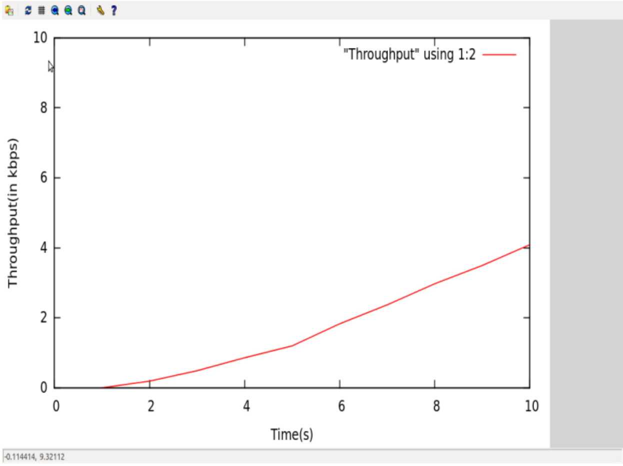


Fig 11: Throughput with 5 connections

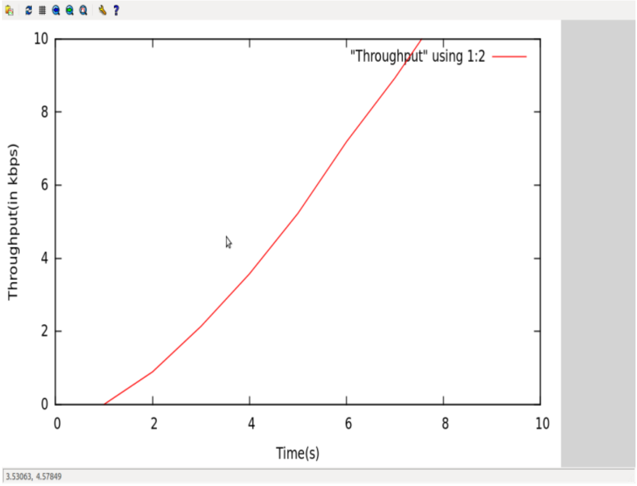


Fig12: Throughput with 8 connections

5. CONCLUSION

In this paper the security of MANET is focused as the information being transmitted is more important than the other parameter of the network. The proposed approach is capable to detect the black hole nodes using the packet flow and by informing other nodes, it prevents the network from attack. Further in future the control packets can be modified in such a way that other attacks may also be detected in AODV without forwarding extra control packets which may create overhead.

6. REFERENCES

[1] Payal N. Raj and Prashant B. Swdesh (2009), DPROADV: A dynamic leaning system against black hole attack in AODV based MANE, International Journal of Computer Science Issues (IJSI), Vol 2 pp. 54-59.

[2] Seryvuth Tan and Keecheon Kim (2013), Secure Route Discovery for Preventing Black Hole Attacks on AODV-

based MANETs, IEEE International Conference on High Performance Computing and Communications & IEEE International Conference on Embedded and Ubiquitous Computing. 1027- 1032.

[3] Wang W, Bhargava B, Linderman M (2009) Defending against Collaborative Packet Drop Attacks on MANETs. Paper presented at the 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009) (in Conjunction with IEEE SRDS 2009).

[4] Mistry N, Jinwala DC, IAENG and Zaveri M (2010). Improving AODV Protocol against Black hole Attacks, the International Multi Conference of Engineers and Computer Scientists, Hong Kong 17-19.

[5] B. Sun, Y. Guan, J. Chen and U.W. Pooch (2003). Detecting black-hole attack in mobile ad hoc networks, presented at 5th European Personal Mobile Communications Conference, Apr. 2003, 490-495.

[6] Jiao Wen-Cheng, Peng Jing And Zheng Jain-Ling (2010) "Research and Improvement of AODV Protocol in Ad Hoc Network", Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference, 1-3.

[7] Al-Shurman M, Yoo S-M, Park S (2004). Black Hole Attack in Mobile Ad hoc Networks. The 42nd Annual ACM Southeast Regional Conference (ACM-SE'42), Huntsville, Alabama, 2-3.

[8] C. Perkins, E. Belding Royer and S. Das (2003). Ad-Hoc on Demand Distance Vector Routing, (pdf) Request for Comments (RFC):3561 .Available at <https://www.ietf.org/rfc/rfc3561.txt >.

[9] Ehsan H. Khan, F.A (2012). Malicious AODV: Implementation and Analysis of Routing Attacks in MANETs by Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference, 1181 – 1187.

[10] Hemanth Narra, Yufei Cheng,Egemen K. Çetinkaya, Justin P. Rohrer and James P.G. Sterbenz (2011), Destination-Sequenced Distance Vector (DSDV) Routing Protocol Implementation in ns3. Information and Telecommunication Technology Center Department of Electrical Engineering and Computer Science The University of Kansas, Lawrence, KS 66045, USA ,439-446.

[11] Jing Xi, Luis Girons Quesada and Yuming Jiang (2007). A Threshold based Hybrid Routing Protocol for MANET. Published in ISWCS 2007, 4th International Symposium Publisher:IEEE, 622 - 626.

[12] Kozma W. and Lazos L.(2009). REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits. Paper presented at the Second ACM Conference on Wireless Network Security, Zurich, Switzerland, 16-18.

[13] Mansoor Mohsin and Ravi Prakash (2002).IP Address Assignment in a Mobile Ad Hoc Network, the University of Texas at Dallas Richardson, TX, MILCOM CCR-0093411.

[14] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah (2010). MANET Routing Protocols and Wormhole Attack against AODV: IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010.

[15] Radhika Saini and Manju Khari (2011).Defining Malicious Behavior of a Node and its Defensive Techniques in Adhoc Networks, Journal of Smart Sensors and Adhoc Networks (IJSSAN) Volume 1, Issue-1 18-21.

[16] Subash Chandra Mandhata and Dr.Surya Narayan (2011). A counter measure to Black hole attack on AODV- based Mobile Ad-Hoc Networks: International Journal of Computer & Communication Technology (IJCCT), Volume-2, Issue-VI, 37-42.

[17] S. Marti, T. J. Giuli, K. Lai, and M. Baker (2000). Mitigating routing misbehavior in mobile adhoc networks, in proceedings of the 6th Annual International Conference on Mobile Computing and Networking, 255-265.

[18] Surendra H. Rout and Hemant P. Ambulgekar (2013). Proactive and Reactive protocol, in multihope. Inernational Journal of Advance Research in Computer Science and Software Engineering, 152-157.

[19] Sheikh R. Singh Chande and M. Mishra, D.K (2010) Security issues in MANET. Wireless and Optical Communications Networks (WOCN), 1-4.

[20] Su M-Y (2011). Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks Through Intrusion Detection Systems. IEEE Computer Communications 34(1):107-117.

[21] Tamilselvan L, Sankaranarayanan V (2007). Prevention of Blackhole Attack in MANET, the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, 27-30.