IJSTE - International Journal of Science Technology & Engineering | Volume 4 | Issue 1 | July 2017
ISSN (online): 2349-784X

Black hole Attack Prevention on AODV in MANET

Mrs. Preeti. A. Aware
M.E Student
Department of Computer Engineering
L.R. Tiwari COE University of Mumbai, India

Mrs. Amarja Adgaonkar
Assistant Professor
Department of Computer Engineering
K.C.College of Engineering and Technology University of Mumbai, India

Mr. Saurabh Suman
Assistant Professor
Department of Computer Engineering
L.R. Tiwari COE University of Mumbai, India

Abstract

Wireless networks provide connectivity to people from different geographical position have. Ad-hoc network is a type of wireless network without an infrastructure. Here network connectivity is maintained with the cooperation of all the network nodes. When the nodes change their locations dynamically, then such ad-hoc network is called as mobile ad-hoc network (MANET). Due to its features like dynamic topology, large degree of freedom, MANET is susceptible to various kinds of attacks like Black hole, Gray hole, Wormhole. A Black hole attack is a most brutal attack against routing protocols in MANETs. It is a malicious node which replies for any route requests claiming to have shortest path to the destination. However in reality it does not have any active route to the specified destination and drops the receiving packets.

Keywords: Black hole attack, Gray hole attack, Routing protocols, AODV, DSDV, DSR, Ad hoc networks, MANET

I. Introduction

Wireless networks use radio frequencies in air to transmit and receive. The nodes in a wireless network consist of routers and host. Nodes in a mobile network move randomly, such a network is called mobile ad hoc networks (MANET). A mobile ad hoc network (MANET) is a group of mobile devices connected by wireless link without the requirement of fixed common infrastructure in place like wireless access point. In MANET nodes enter or disappear from the network quickly.[4] The biggest challenge faced by MANET is attacks on routing protocol. Nodes in MANET communicate with each other to deliver data. When the nodes are out the communication range of each other then the intermediate nodes act as routers to deliver the packet to the destined node. Each node in a MANET acts as host as well as router. In router mode, the node discovers the route and delivers the data with the help of the routing protocol. [5, 6]

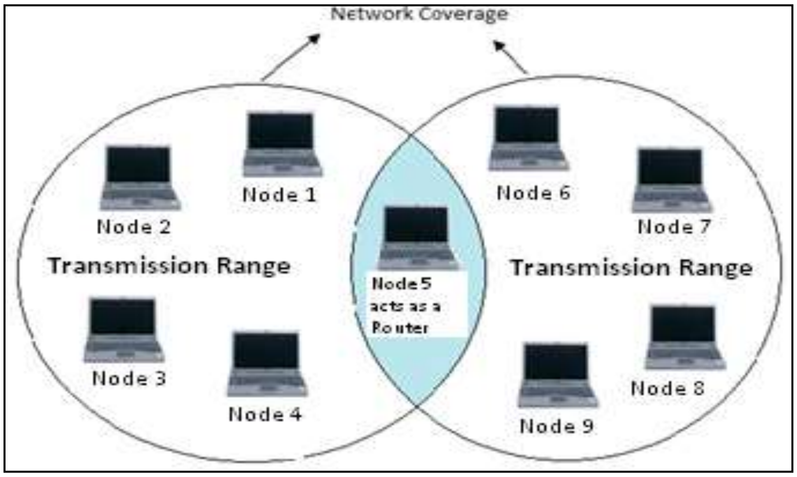


Fig. 1: Mobile Ad-Hoc Network with nine Nodes

Figure 1 shows a simple mobile ad-hoc network with nine nodes. The outer nodes are not within the transmitter range of each other. Here, the middle node i.e. node 5 can forward packets between the outermost nodes. The middle node acts as a router. The eight network nodes along with the router form a MANET [7].

Further paper is divided in to 7 sections, section II Working of AODV routing protocol, section III explains Black hole and cooperative black hole attack in detail, section V explain about related work, section VI explain the proposed method for prevention of black hole attack, section VII describes conclusion.

II. WORKING OF AODV ROUTING PROTOCOL

AODV stands for Ad-hoc on demand Distance Vector. It is the most frequently used routing protocol in MANET. AODV is an on demand routing protocol which means it does not require nodes to maintain routes to destination. It uses various control packets like Route Request, Route Reply to discover links .It uses the Route Error control packet for route maintenance.

A RREQ control packet is sent be a source node which wants to find a path to the destination. The RREQ contains four fields broadcast identifier, source addresses destination address and sequence number. The intermediate nodes on receiving the route request broadcast the Route Request message. When forwarding a RREQ, node stores broadcast identifier, source address and maintains a reverse route. The destination node on receiving the route request will generate the Route Reply. The Route Reply packet will be sent through the reverse path maintained be the intermediate node to reach the source node.[4]

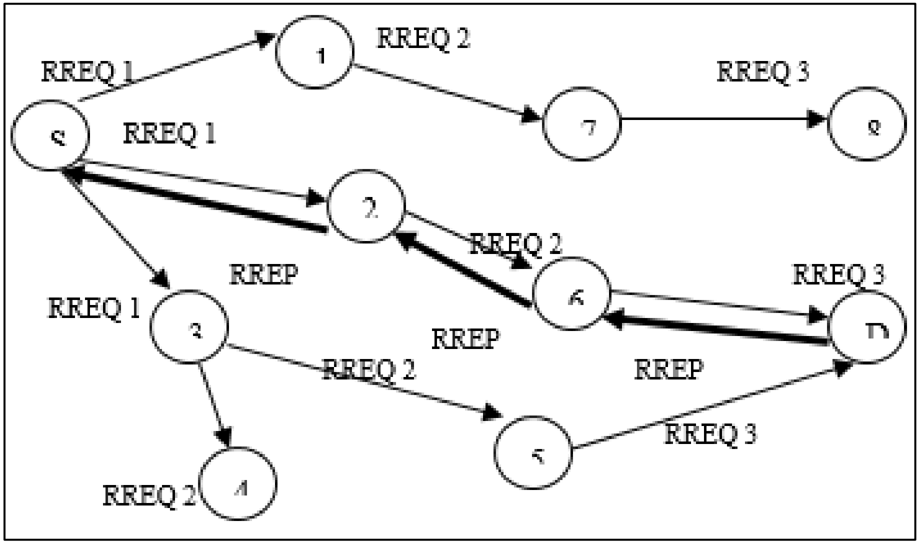


Fig. 2: Route Discovery using AODV protocol

In Figure 2. Source node broadcasts RREQ message. The intermediate nodes create reverse route to the source node. On receiving RREQ packet, the destination node unicasts RREP to the source using the same path that was created during RREQ.

The AODV protocol is most optimal protocol for MANET compared to other protocols like. The sequence numbers avoids loops from being formed.

The table 2 shows the comparative study of different protocols in MANET

Table - 2
Comparative study of routing protocols

S. N.	*Protocol Property*	*DSDV*	*DSR*	*AODV*
1	*Network Suitable for*	*Less number of nodes*	*Up to 200 nodes*	*Highly Dynamic*
2	*Node overhead*	*Medium*	*High*	*Medium*
3	*Network Overhead*	*High*	*Low*	*Medium*
4	*Route Discovery*	*Periodic*	*On Demand*	*On Demand*

From the above table we can conclude that AODV protocol is the most optimal routing protocol for MANET

III. BLACK HOLE ATTACK

The black hole node falsely claims it has the shortest route to the destination. When the source node sends the data packets, the malicious node instead of forwarding the data to the destination, drops the Packets [12]. The situation becomes worse when two or more nodes work as a black hole node.

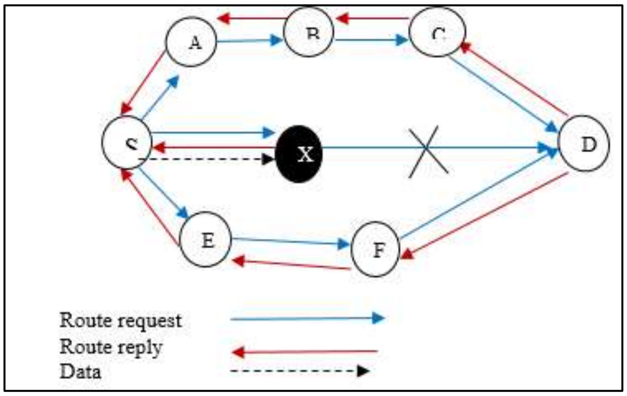


Fig. 3: Black Hole Attack

Fig 3 shows black hole attack, here node “S” is the source node and “D” is the destination node. Node “S” will begin a route discovery process. Here “X” is a malicious node and will give first reply saying it has the shortest route to the destination. Source “S” will discard the later route replies from other node. It will start sending the data packets to node “X” which will drop the received packets.13]

IV. Related work

M. Abdelshafy &J.B. King [1] proposed a solution for resisting black hole attacks in MANET. In this a node will send fake Route Request control packet for a non-existing source and destination. If any node sends route reply then the trust level of the node is changed to threat. The drawback of this method is overhead of false route request packet in the network.

Pooja DCSA & R.K. Chauhan [2] proposed an assessment based approach for detecting black hole attack in MANET. In this hint value is calculated depending upon the connection start and connection end time between neighboring nodes. This hint value is then compared with a threshold value. If the hint value is greater than the threshold value then there is a black hole node in the network. The drawback of this method is the calculation of the hint value between the neighbouring nodes.

Ashish Jain & Vrinda Tokekar [3] proposed a solution to prevent Black hole attack by using RREP packet caching mechanism. In this solution the all the RREPs are cached. The first RREP is discarded as there is a possibility that the route reply is from a black hole node. The disadvantage of this method is the caching of the RREP packets of the entire network.

M. Dasgupta, D. Santra [5] proposed a solution to prevent black hole attack. In this a CPN model is used wherein the IDS nodes are placed in the network to sniff the packets. The traffic patterns are analyzed and if a match is found with a malicious pattern, a black hole node is detected. The drawback of this method is placement of the IDS throughout the network.

Meenakshi Patel, S. Sharma[6] proposed a solution for detection and prevention of flooding attacks in MANET using SVM. The system gathers the activities of every node in the network. It then compares this data with the predefined threshold to detect the malicious node. The disadvantage of tis method is that much time is wasted in data gathering.

Supriya Tayal, Viniti Gupta [7] proposed survey of attacks on routing protocols. They proposed that AODV is best suitable for MANET, but it is prone to many security threats like active and passive attacks. One of the active attack is the black hole attack.

V. The proposed method

The source node will search for an optimal path to the destination. It will send a Route Request packet. If there is a malicious node in the network, it will send the first route reply claiming it has the shortest path to the destination. So in our proposed scheme the source node will gather all the route replies. It will discard the first route reply. It will take second route reply path for sending the message. For each message it will do hash authentication. If the sender’s and the destination node’s hash value is same, then that path is selected else discarded.

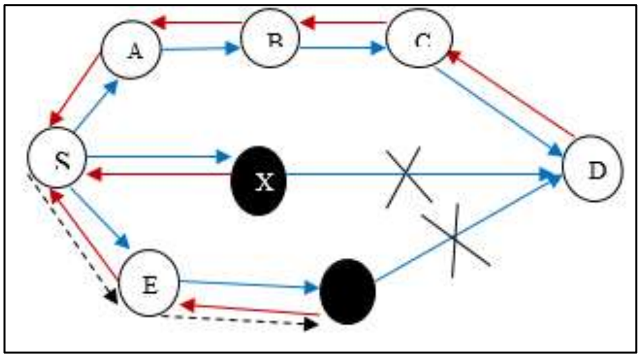


Fig. 4: proposed solution for avoiding black hole attack.

As shown in the fig the source node ‘S’ will send route request packet to find the path to the destination ‘D’. In this network node ‘X’ is the malicious node, it will not forward the route request packet. Node ‘X’ will send the first Route reply saying it has the shortest path to the destination. The source node ‘S’ will gather all the route replies. It will discard the first route reply as it will always be from a black hole node in the network. It will take the path of the second route reply. The source node will compute the hash value of the message and send it along with the message. At the destination ‘D’ the hash value is again recomputed. If the hash value is different, then the path is discarded as there is a black hole node in the path. So the path ‘S-E-F-D’ will be discarded. If the hash value calculated at the source and the destination is same, then that route is used for data transmission.

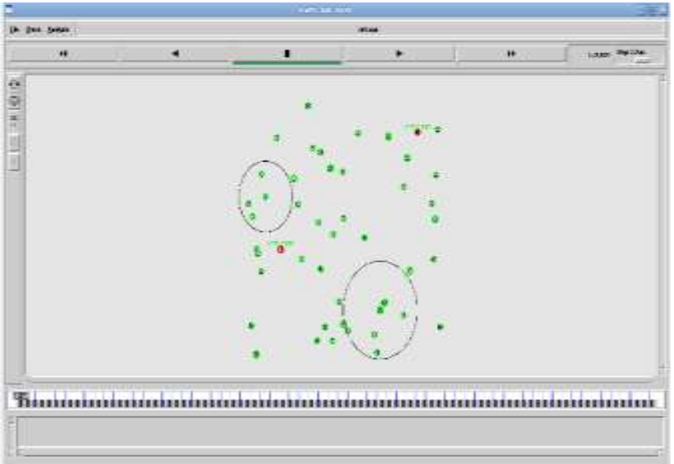
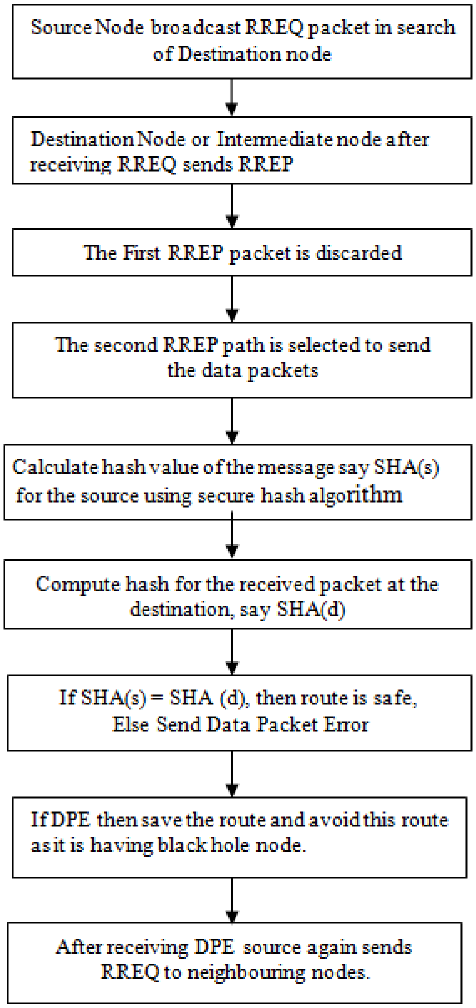


Fig. 5: Showing the mobility of nodes in the network

A. *Flowchart of the proposed system:*

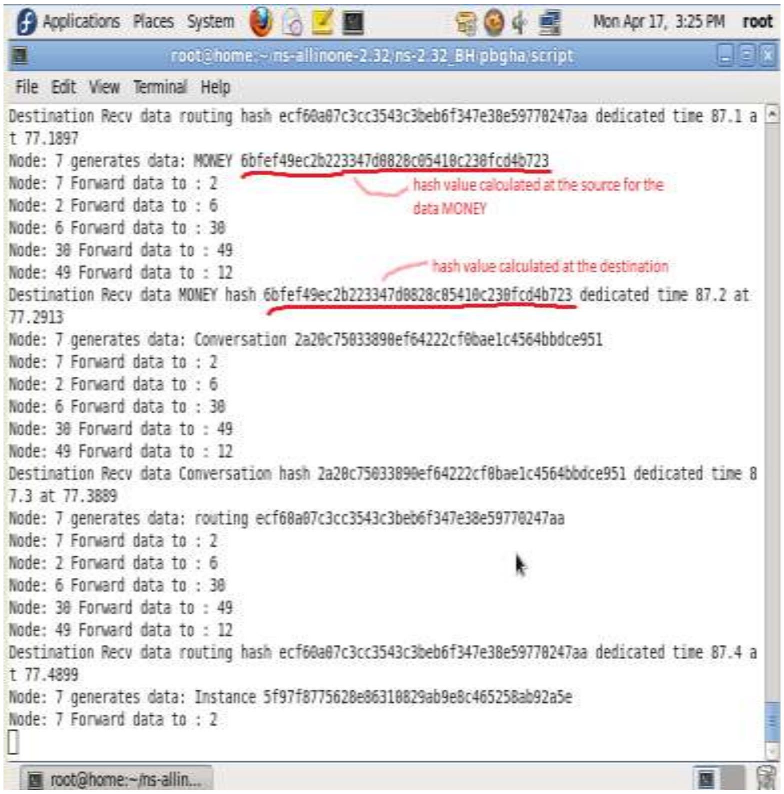

Source Node broadcast RREQ packet in search of Destination node
Destination Node or Intermediate node after receiving RREQ sends RREP
The First RREP packet is discarded
The second RREP path is selected to send the data packets
Calculate hash value of the message say SHA(s) for the source using secure hash algorithm
Compute hash for the received packet at the destination, say SHA(d)
If SHA(s) = SHA (d), then route is safe, Else Send Data Packet Error
If DPE then save the route and avoid this route as it is having black hole node.
After receiving DPE source again sends RREQ to neighbouring nodes.

VI. Simulations Results

The network simulation is done using NS-2, to analyze the performance of MANET by varying the mobility of the nodes. For wireless LANs this solution makes use of Distributed Coordination Function (DCF) of IEEE 802.11 for simulation of the MAC layer. The traffic source is set as Continuous Bit Rate (CBR). The simulation models 50 to 100 mobile nodes and the speed of nodes is varied from 0-20m/s

Table - 2
Simulation Constraints

Constraint	*Value*
Simulator	*NS-2*
Number of Mobile Nodes	*50 to 100*
Topology Space	*1000m X 800m*
Mobility Model	*Random waypoint*
MAC layer Protocol	*IEEE 802.11*
Routing Protocol	*AODV*
Placement of nodes	*Random*
Packet Size	*512 bytes*


Applications Places System
Mon Apr 17, 3:25 PM root
root@home:~/ns-allinone-2.32/ns-2.32_BH/pbgha/script
File Edit View Terminal Help
hash value calculated at the source for the data MONEY
hash value calculated at the destination
root@home:~/ns-allin...

```
Destination Recv data routing hash ecf60a07c3cc3543c3beb6f347e38e59770247aa dedicated time 87.1 a
t 77.1897
Node: 7 generates data: MONEY 6bfef49ec2b223347d0828c05410c230fcd4b723
Node: 7 Forward data to : 2
Node: 2 Forward data to : 6
Node: 6 Forward data to : 30
Node: 30 Forward data to : 49
Node: 49 Forward data to : 12
Destination Recv data MONEY hash 6bfef49ec2b223347d0828c05410c230fcd4b723 dedicated time 87.2 at
77.2913
Node: 7 generates data: Conversation 2a20c75033890ef64222cf0bae1c4564bbdce951
Node: 7 Forward data to : 2
Node: 2 Forward data to : 6
Node: 6 Forward data to : 30
Node: 30 Forward data to : 49
Node: 49 Forward data to : 12
Destination Recv data Conversation hash 2a20c75033890ef64222cf0bae1c4564bbdce951 dedicated time 8
7.3 at 77.3889
Node: 7 generates data: routing ecf60a07c3cc3543c3beb6f347e38e59770247aa
Node: 7 Forward data to : 2
Node: 2 Forward data to : 6
Node: 6 Forward data to : 30
Node: 30 Forward data to : 49
Node: 49 Forward data to : 12
Destination Recv data routing hash ecf60a07c3cc3543c3beb6f347e38e59770247aa dedicated time 87.4 a
t 77.4899
Node: 7 generates data: Instance 5f97f8775628e86310829ab9e8c465258ab92a5e
Node: 7 Forward data to : 2
```

Fig. 6: Transmission of Data

Fig. 6 shows data is transmitted from the source node 7 to destination node 12. As node 7 and 12 are not in the transmission range of each other, the data is transmitted through the intermediate nodes. The hash value is calculated using SHA_{128} at the source and the destination. If the two hash values match then path is selected for further transmission of the data packets. Otherwise the path is discarded.

A. *Packet Delivery Ratio*

It is the ratio of total number of packets received by the destination to the total number of packets sent by the source. The solution provided helps us to detect the black hole and gray hole node and hence the packet delivery ratio increases as shown in the graph.

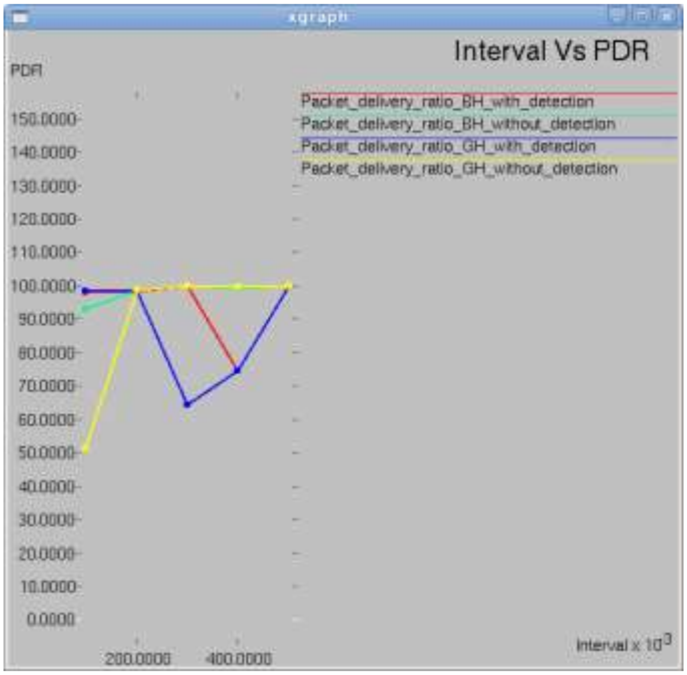


Fig. 7: Interval Vs Packet delivery ratio

B. *Interval vs Control Overhead*

The number of control packets being sent such as RREQ, RREP in a given time interval determines the control overhead. As the black hole nodes are detected the control overhead eventually reduces as seen in the graph.

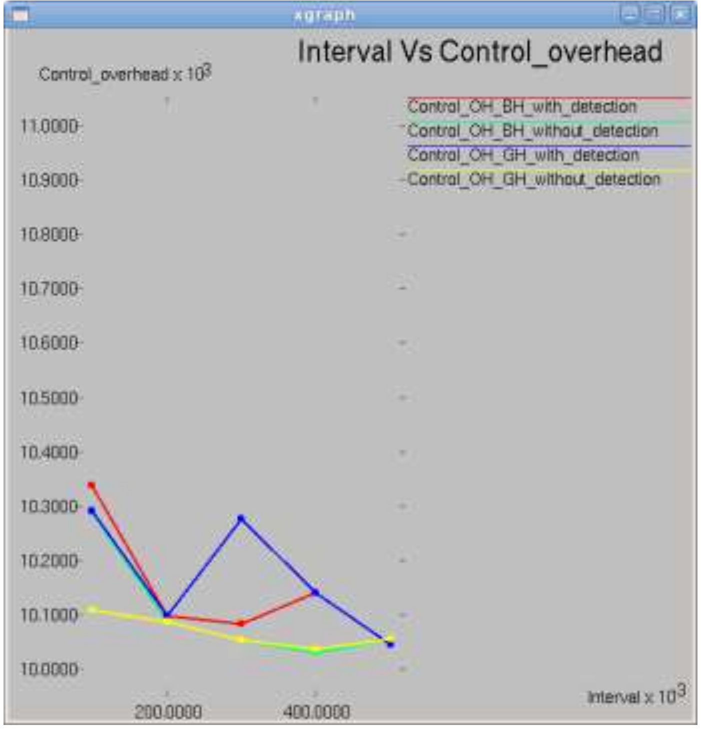


Fig. 8: Interval Vs Control overhead

C. *Throughput*

Throughput is the average number of packets sent successfully over a communication channel. As seen in the graph of fig 9. The throughput with the black hole detection is more compare to the throughput without the black hole detection.

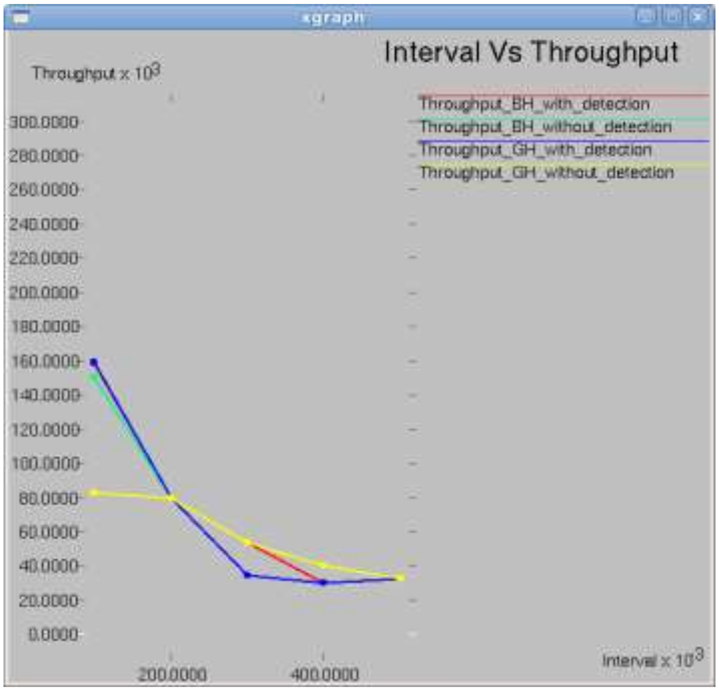


Fig. 9: Interval Vs Throughput

VII. SECURITY ANALYSIS

The black/gray hole node falsely claims it has the shortest route to the destination. So in this solution, the first route is discarded and hence the black hole node is avoided. Here the data integrity is also checked with the hash calculation. So the safest path is selected for the transmission of the data.

VIII. CONCLUSION

MANET has many routing protocols of which AODV is the best. However it is vulnerable to active attacks of which black/gray hole or the most severe attacks. Many authors have provided solutions to prevent black hole attack. Each solution provided has its own drawback.

The black hole node drops the packet and the behavior of the gray hole node is unpredictable. In this solution with hash value calculation both the black hole and gray hole node is detected and the data takes the safest route to reach the destination.

In the future work the proposed scheme will be enhanced and will be further improved to minimize delay and to provide a system which will be of paramount importance for MANET.

REFERENCES

[1] Mohamed A. Abdelshafy, Peter J.B. King "Resisting Black hole attacks on MANET," IEEE Annual Consumer Communication and networking conference, May 2016.

[2] Pooja D, R.K Chauhan, "An Assessment Based Approach to detect Black Hole attack in MANET," IEEE International Conference on Computing, Communication and Automation, May-2015

[3] Ashish Kumar Jain , Vrinda Tokekar " Mitigating the Effects of Black hole Attacks on AODV Routing Protocol in Mobile Ad Hoc Networks, "IEEE International Conference on Pervasive Computing (ICPC) ,May 2015.

[4] Preeti A. Aware, Amarja Adgaonkar "Black hole attack prevention on AODV in MANET" "International Conference on Emanations in Modern Technology and Engineering (ICEMTE-2017, Volume: 5 pp192 - 195, Feb-2017

[5] M. Dasgupta, D. Santra, "Network Modeling of a Black hole Prevention mechanism in MANET," IEEE International Conference on computational intelligence and communication networks, pp. 734-738, Nov-2012.

[6] Meenakshi Patel, S. Sharma. "Detection and Prevention of Flooding Attack Using SVM," IEEE International Conference on communication systems and Network Technology, pp.533-537, May-2013

[7] SupriyaTayal, Viniti Gupta. "A Survey of Attacks on MANET Routing Protocols," International Journal of Innovative Res. in Computer Science Eng. and Technology, Vol.2, Pg. 2280-2285, June-2013.

[8] M. Khalili, H. Taheri, S. Vakilinia, "Preventing black hole attack in AODV through use of hash chain", in Proc. of 19th Iranian Conference Electrical Engineering (ICEE), Iran, pp. 1- 6, 2011

[9] M. Khalili, H. Taheri, S. Vakilinia, "Preventing black hole attack in AODV through use of hash chain", in Proc. of 19th Iranian Conference Electrical Engineering (ICEE), Iran, pp. 1- 6, 2011

[10] Renu Mishra, Dr.Sanjeev Sharma. "Vulnerabilities and security for ad-hoc networks"IEEE International Conference on networking and information technology, pp. 192-196, May-2010

[11] LathaTamilselvan and Dr. V Sankaranarayanan, "Prevention of Black hole Attack in MANET" 2nd IEEE International Conference on Wireless Broadband and Ultra-Wideband Communications, pp. 21, 2007

[12] Piyush Agrawal and R. K. Ghosh: Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks www.stanford.edu/~piyushag/docs/icuimc08.pdf
[13] Y. Hu, A. Perrig and D. Johnson, Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols, in Proceedings of ACM MobiCom Workshop - WiSe'03,2003
[14] J.Chen; U.W. Pooch, "Detecting Black-hole Attack in Mobile Ad Hoc Networks," 5th European Personal Mobile Communications Conference, pp. 490-495, 2003.
[15] H. Deng, W. Li and D.P.Agrawal, "Routing security in wireless ad hoc networks," IEEE Communications Magazine, vo1.40, no. I 0, pp. 70- 75, Oct. 2002.