Enhanced and More Secure Multipath AODV Routing Protocol to Avoid Black Hole Attack in MANET

Vijay Chhari[1] Rajesh Singh[2]
[1,2]Department of Computer Science & Engineering
[1,2]NITM Gwalior, M.P, India

Abstract— Adhoc network is composed of mobile nodes having dynamic topology .The nodes sends the data packet to the other nodes by forwarding mechanism. The black hole is a malicious node that advertises itself as a node through which the path to the destination is present. The nodes send the data packet to the black hole considering it as a right path. The problem with the black hole is that it drops the packet or sends it to a route away from the destination. In this paper present various aspects of black hole attack that tells the reasons and the problem in the network due to black hole.

Key words: Black hole, RREQ, RR, PDR

I. INTRODUCTION

In the present era, the study in MANETs has gained a lot of interest of researchers due to the realization of the nomadic computing paradigm [1]. Wireless networks can be basically either infrastructure based networks or infrastructure less networks. The coordinating communication, between mobile nodes (host) is possible with the help of using fixed infrastructure [2] based network. The ad hoc networks fall under the class of infrastructure less networks, in which communication between mobile nodes is possible with no any fixed infrastructure between them. A Mobile Ad Hoc Network (MANET) comes under the category of infrastructure less network.

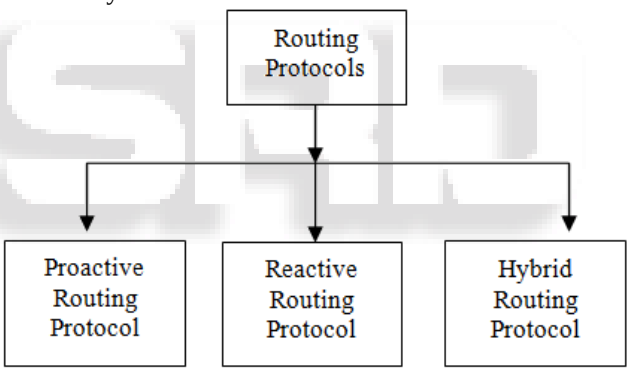
MANET is a set of mobile nodes that perform basic networking functions like routing, packet forwarding and service discovery without the need of an established infrastructure. All the nodes of an ad hoc network depend on one another in forwarding a packet from source to its destination, due to the restricted transmission range of each mobile node's wireless transmissions [3]. There is no centralized administration in ad hoc network. Ad hoc network gives assurance that the network will not stop in providing functionality only because nodes are mobile in nature and hence they travels out of the range of the others. As nodes wish, they should be able to go in and disappear from the network. Multiple intermediate hops are required to communicate to other nodes, due to the limited range of the nodes. In ad hoc network every node must be keen to forward packets for other nodes. In this way, every node performs role of both, a host and a router. The nodes of ad hoc networks have dynamic topological arrangement and changes with time as nodes moves, join or leave the ad hoc network. This unsteadiness of topology wants a protocol to route and run on every node to produce and preserve routes among the nodes.

In Mobile Ad-Hoc Network security of routing protocol is the key factor for the basic functionality of network. MANETs have a lot of protocol such as OLSR (Optimized Link State Routing), AODV (Ad Hoc On-Demand Distance Vector), DSR (Dynamic Source Routing), ZRP (Zone Routing Protocol), [4]DSDV (Destination Sequence Distance Vector) protocol and so on. In this paper, we concentrate on the AODV routing protocol that is widely used in MANET. It gives dynamic link conditions, low network utilization, low control message overhead, low memory overhead, and so on. However, the protocol was not considered security mechanisms. Hence, it is defenseless various types of attacks. The black hole attack is one of the attacks against the AODV routing protocol. The malicious node send the counterfeit reply that it has the freshest and shortest path to the destination node. Then, it absorbs all data packets to the destination. Hence, it disturbs the network and becomes data lost and affects the performance of network.

II. ROUTING PROTOCOLS

MANET routing protocols are categorized into three main categories:

- Table driven/ proactive
- Demand driven/ Reactive
- Hybrid



A. Proactive Routing Protocol:

These protocols are also known as Table Driven protocols as they uphold the information about routing even before it is required [5].All the nodes communicate with other nodes of the network. The information of routing is usually preserved in the direction-finding tables and is occasionally restructured as the system topology varies. There exist some differences between the protocols that come under this category depending on the routing information being updated in each routing table. Furthermore, these routing protocols maintain different number of tables. The proactive protocols are not appropriate for larger networks, as they crucially maintain entries of node aimed at both and each node in the direction-finding desk of all the available node. This results in more conjunction in the routing table resulting in the consumption of more bandwidth.

B. Reactive Routing Protocol:

These protocols are also called On Demand routing protocols because they don't compulsorily maintain direction-finding evidence or routing movement at the system nodules in case of no communication. If a node

wants to forward a package to alternative node then this procedure searches for the direction in an on-request way and maintains the connection to forward and obtain the package [6]. The direction discovery frequently ensues by overflowing the route application containers throughout the network. Reactive search procedures can also add a significant amount of control traffic to the network due to query flooding. Because of these weaknesses, reactive routing is less suitable for real-time traffic or in scenarios with a high volume of traffic between a large numbers of nodes.

C. Hybrid Routing Protocol:

This type of protocols combines the advantages of proactive and of reactive routing. The routing is at first well-known with some proactively prospected routes and then serves the order from extra activated nodes by using [7] reactive flooding. The basic 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 maintain routing information. For those nodes outside of its zone, it does not maintain routing information in a permanent base. Instead, on-demand routing strategy is adopted when inter-zone connections are required.

III. BLACK HOLE ATTACK

The black hole attack [8][9]occurs when a malicious node transmission himself for taking the through pathway to the destination node or forging route reply message that is sent to the source node, with no effective route to the destination. For fresh routes hostile node advertises its availability without rechecking its routing table. In this manner attacker node will always shows the availability in responding to the direction request and therefore intercept the documents package and hold it. In protocol based on flooding, the requesting node receives a reply from the malicious node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, the hateful node does not communicate the package and engrosses all documents packet.

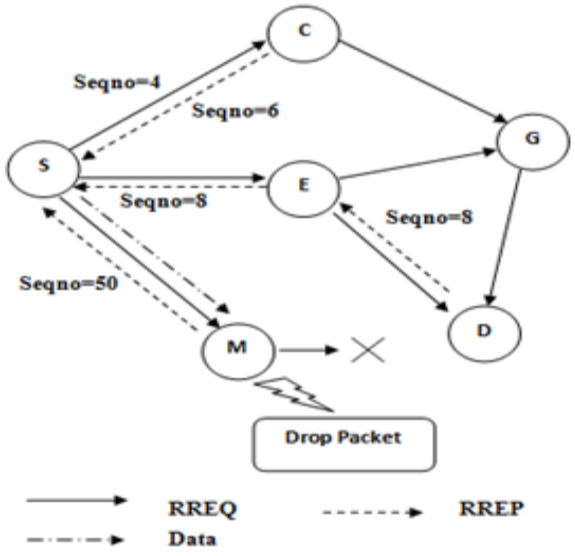


Fig. 1: Black hole attack

As an example, consider the following scenario in Fig. 1. In this scenario, the node 'S' is the source node, 'D' is the destination node and 'M' is assumed the malicious node. When the source node 'S' want to send the data packet to the destination node 'D', it first broadcasts the RREQ message with destination sequence number 4 to the neighboring nodes. So, the neighboring node 'C', 'E' and the malicious node 'M' receive this message. As the node M is a malicious node, it immediately sends back a RREP message to node 'S' with highest sequence number that it has a active route to the destination. The node 'S' assumes that this is the freshest route. So, the node 'S' ignores all other replies and sends the data packets to the destination through it. However, the node 'M' absorbs all the data and thus behaves like a 'Black hole'.

IV. LITERATURE REVIEW

Nital Mistry et. al. has proposed[10] an algorithm to counter Black hole attack against the AODV routing protocol. Observed that the proposed modification to secure AODV is indeed effective in preventing the Black hole attacks with marginal performance penalty. A Black hole attack is one of the active DoS attacks possible in MANETs. In this attack, a malicious node sends a *false* RREP packet to a source node that initiated the route discovery, in order to pose itself as a destination node or an immediate neighbor to the actual destination node.

Jaspal Kumar et. al.[11] the things of Black hole attack on mobile ad hoc direction-finding protocols. Mostly two protocols AODV and Value-added AODV have been well-thought-out. Reproduction has been completed on the basis of presentation strictures and result has been investigated subsequently addition Black-hole nodes in the system. It is an superior version of AODV and is mixture in nature.

Sarita Choudhary et.al. has [12]propose a complete protocol for detection & removal of networking Black/Gray Holes by using OPNET network simulator 14.5; it is the latest version of simulation software. Basically, OPNET allows you to build a network with a range of simulated "real-life" equipment, so different configuration options can be tested. And considering two different networks with 15nodes and 35 nodes in network and evaluating a security attack against MANET as a network, different statistics or performance metrics Packet loss, Packet delivery ratio and Average end to end delay has been used.

Vishnu k et. al.[13] propose a complete protocol for detection & removal of networking Black/Gray Holes. AODV is a source initiated on-demand routing protocol. Every mobile node maintains a routing table that maintains the next hop node information for a route to the destination node. When a source node wishes to route a packet to a destination node, it uses the specified route if a fresh enough route to the destination node is available in its routing table. If not, it starts a route discovery process by broadcasting the Route Request (RREQ) message to its neighbors, which is further propagated until it reaches an transitional node through a renewed sufficient direction to the endpoint node identified in the RREQ, or the destination node itself.

Akanksha Saini et. al Their [14] paper explains the behavior of the Black Hole node considered under different scenarios. Black Hole AODV protocol has been judged by changing the number of all the available mobile nodes and black hole nodes. The protocol is studied on various performance metrics like packet loss, PDR and average end

to end delay. It is noted that the result on packet loss is much inferior as compare to effect on delay. An ad hoc network is collection of mobile nodes that dynamically form a temporary network and have no fixed infrastructure. A black hole is a wicked node that incorrectly replies the route requests that it has a clean route to destination and then it mislead or drops all the obtained packets. The damage will be serious if malicious nodes work together as a group. This attack is called as cooperative black hole attack.

V. FLOW CHART OF PROPOSED WORK

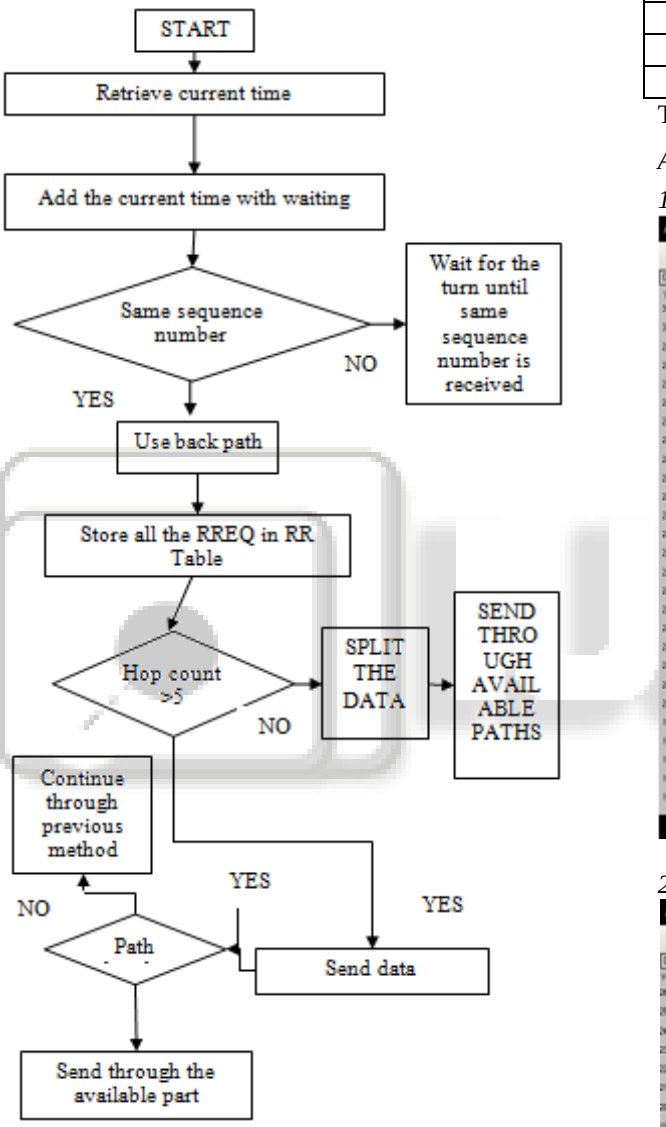


Fig. 2: Flow Chart

A. *Proposed Work:*

In this paper we present the working of Aodv in black hole with the help of flow chart.

1) Start with initial node to retrieve the current time of node.
2) Add the current time with waiting, because node check the path with RREQ and find whether the sequence number is matched or not. If matched then store the RREQ into RR table, else wait for same sequence number.
3) Now check the hop counts whether it is greater or smaller. If it is greater then send the data or not split the data and send it also through different available paths.
4) Send data with path if it is yes then send through available path, if not then continue with the previous method.

VI. EXPERIMENTAL RESULTS

In simulation result we calculate packet delivery ratio and throughput. For simulation we take 7, 14 and 21 nodes.

Node	Attack condition	Simple Aodv	Proposed work
7	0.4508	0.6850	0.5491
14	0	0.9688	0.4692
21	0.1691	0.9836	0.7107

Table 1: Comparison of PDR when nodes have movement

A. *Results with Node 7 in Movement:*

1) *End To End For Node 7:*

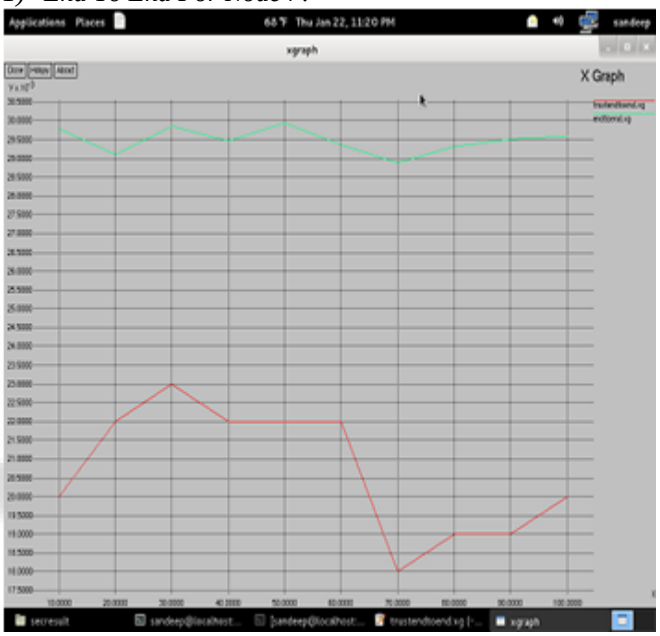


Fig. 3: End to end for node 7

2) *For Sending Node 7:*

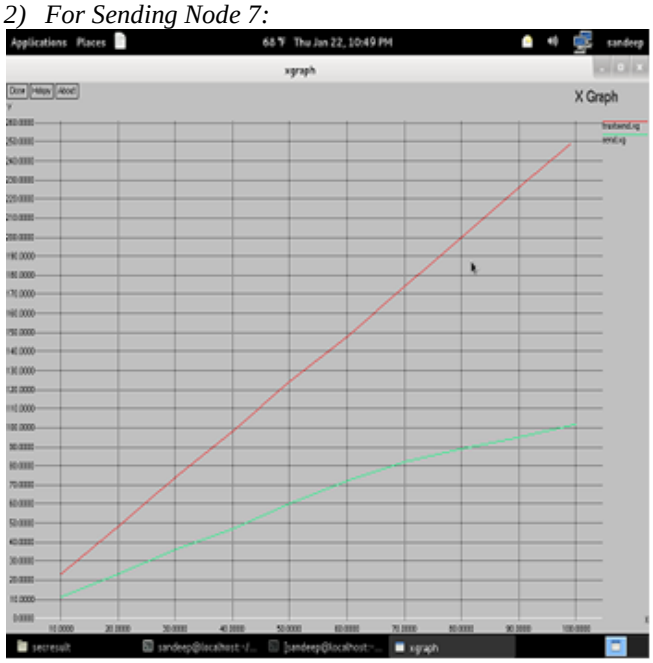


Fig. 4: For Sending node 7

3) For Forward Node 7:

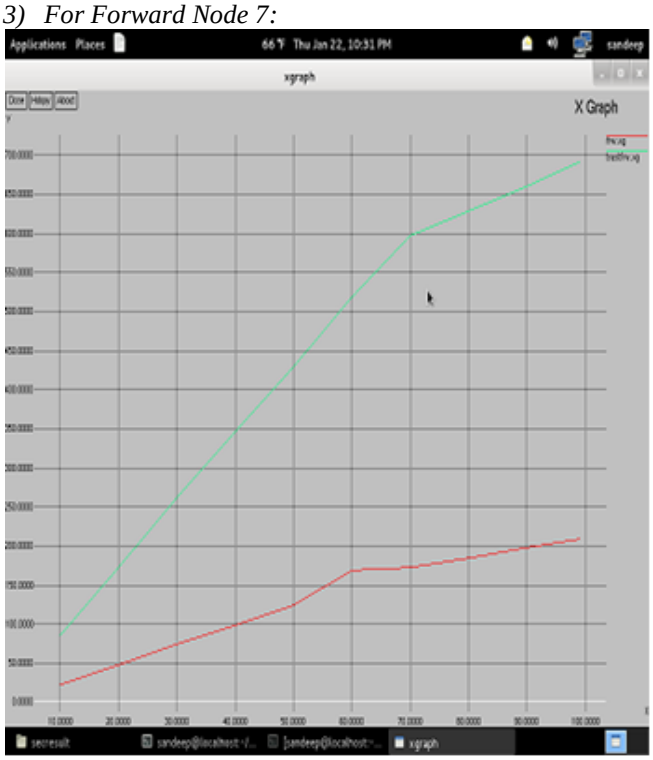


Fig. 5: For Forward node 7

4) For Receive Node 7:

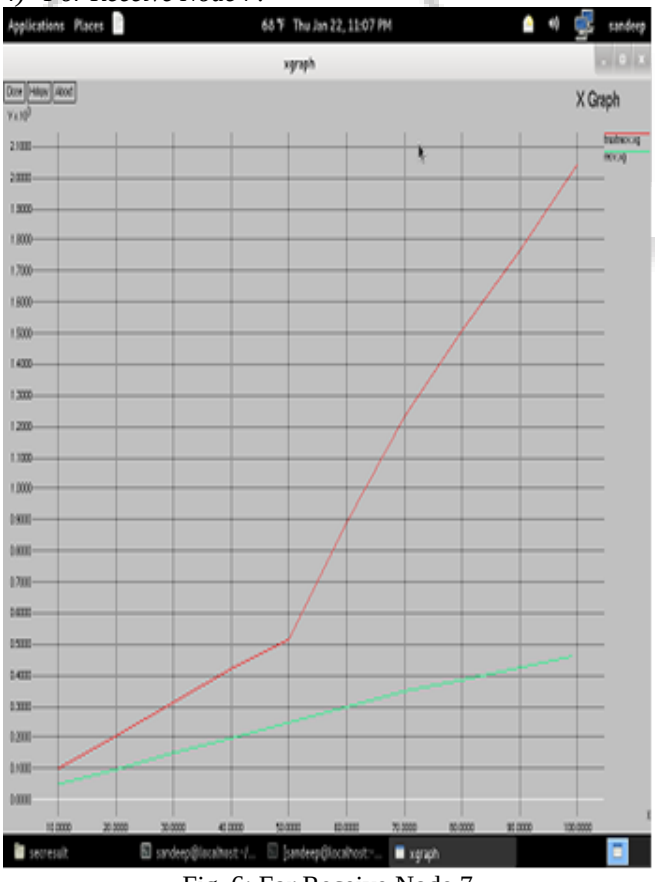


Fig. 6: For Receive Node 7

B. Result with Node 14 in Movement:

1) End To End For Node 14:

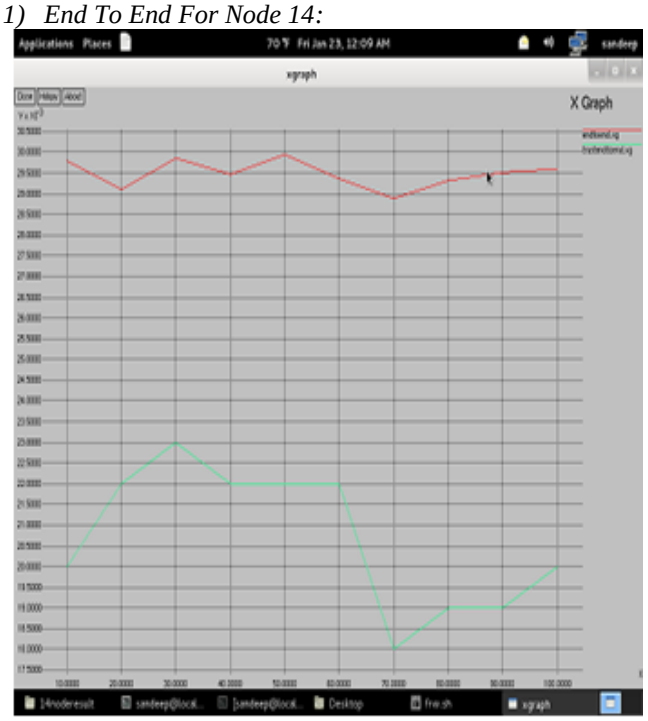


Fig. 7: End to End for Node 14

2) For Send Node 14:

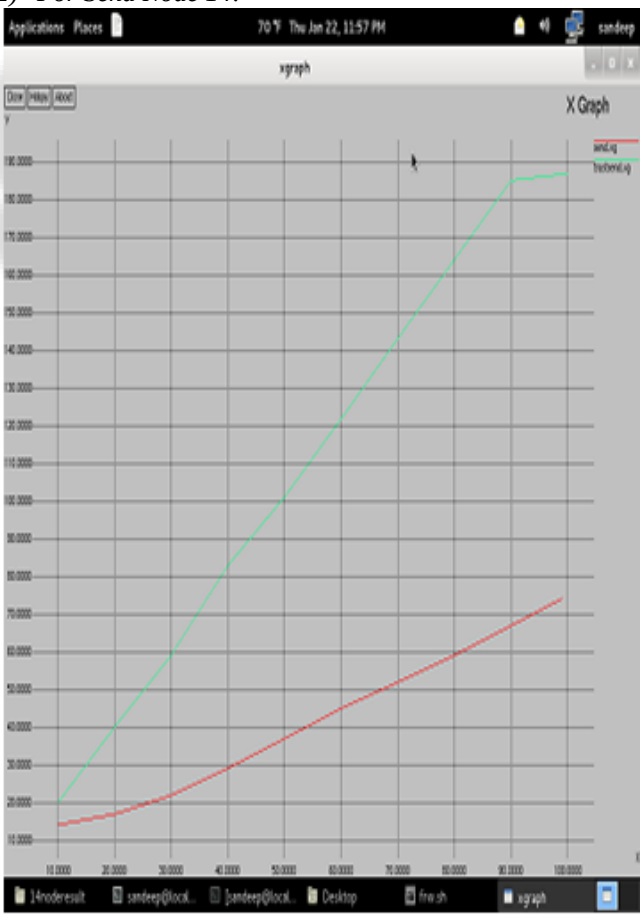


Fig. 8: For Send node 14

3) For Forward Node 14:

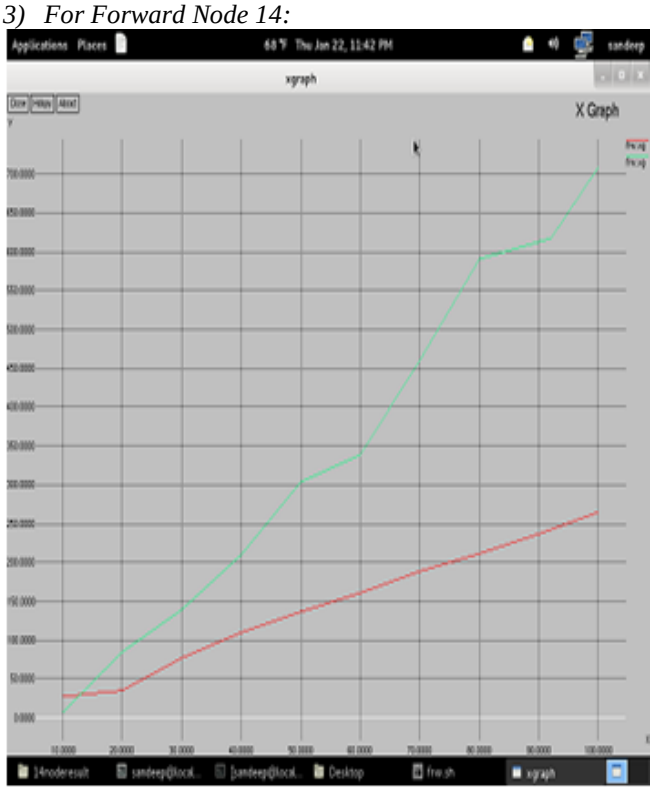


Fig. 9: For Forward Node 14

4) For Receiving Node 14:

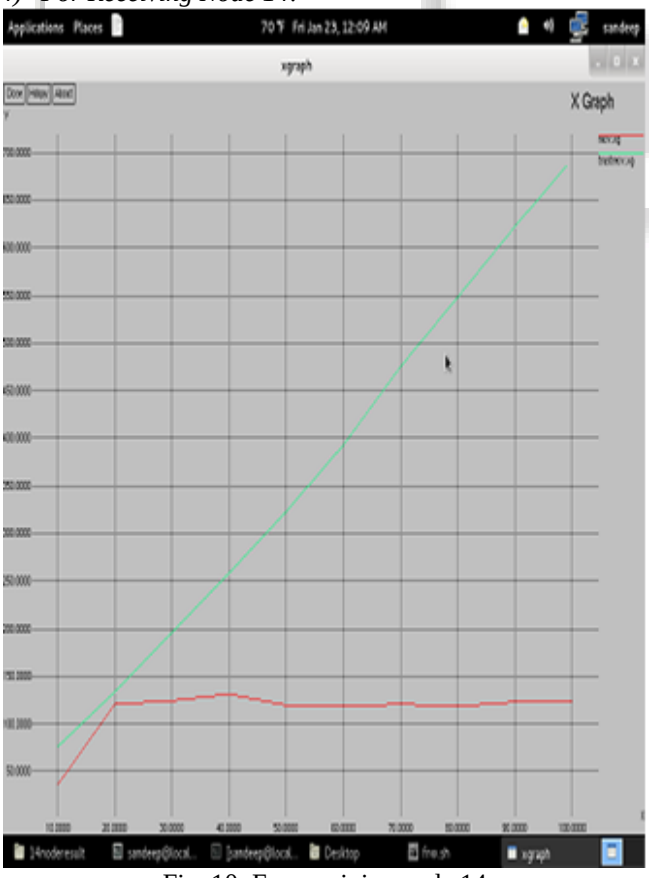


Fig. 10: For receiving node 14

C. Result With Node 21 in Movement:

1) End To End For Node 21:

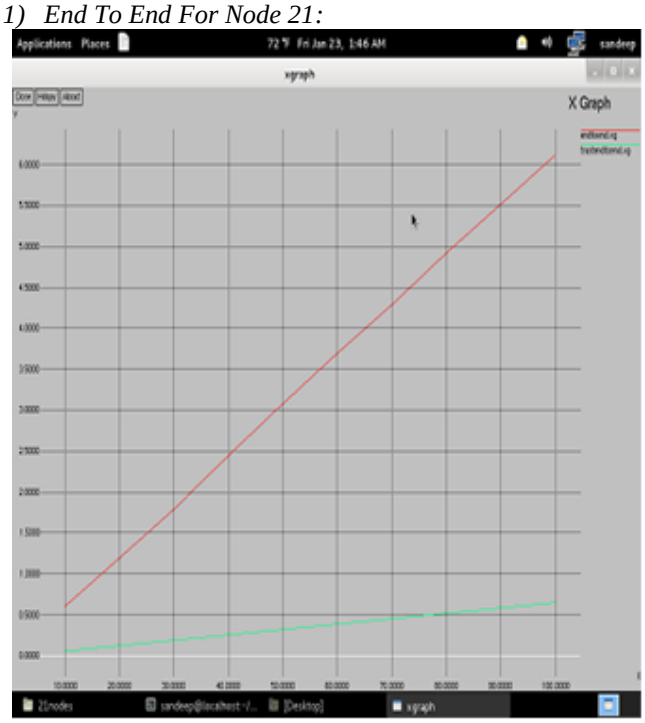


Fig. 11: End to End for node 21

2) For Sending Node 21:

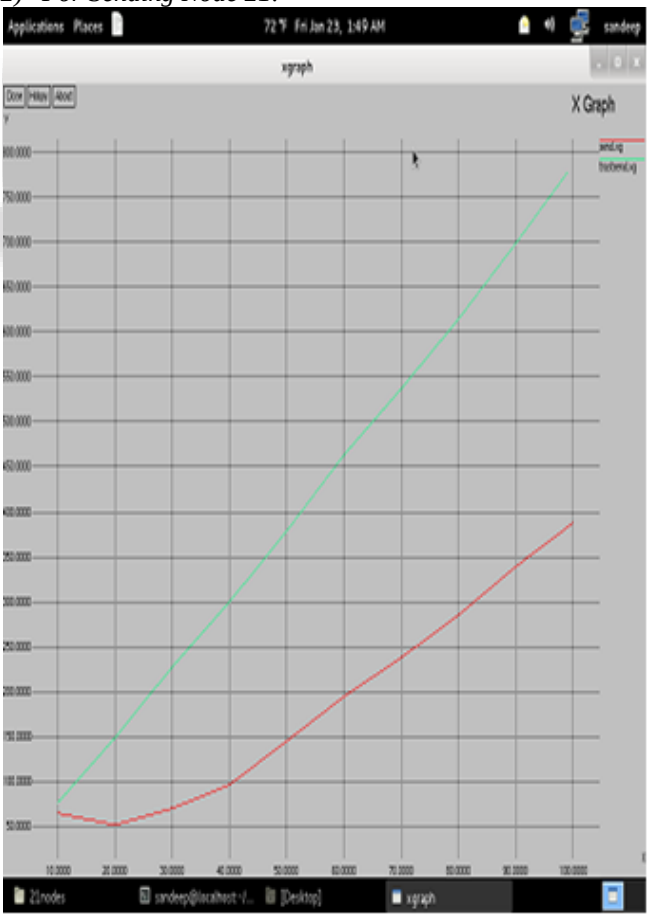


Fig. 12: For sending node 21

3) For Forward Node 21:

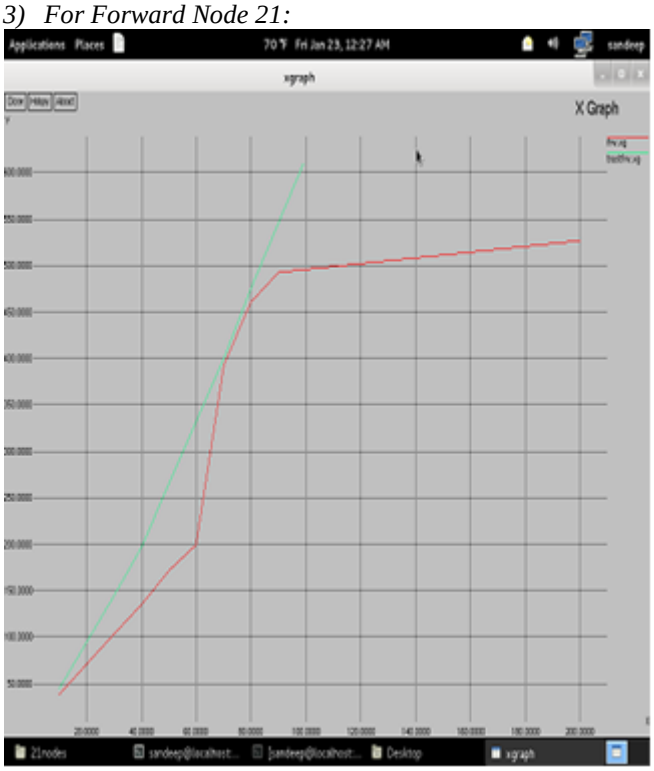


Fig. 13: For Forward Node 21

4) For Receiving Node 21:

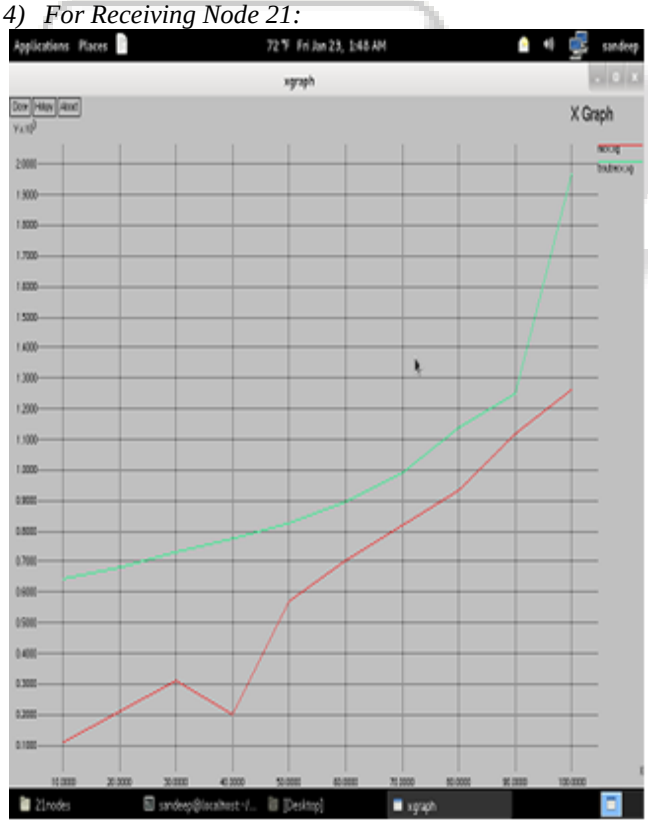


Fig. 14: For receiving node 21

VII. CONCLUSION

Black hole is a malicious node that drops the packet or re routes the packet to the wrong destination. It is a node that disturbs the overall functioning of the network. This paper explains about the method through which this node create hurdle in the network and faces the network .Collaborative black hole attack is also explained in this paper along with the procedure and method by which it is implemented in the network. The nodes must be aware of the method to identify and ignore the black hole.

REFERENCES

[1] Gianni A. Di Caro, Frederick Ducatelle, Luca M. Gambardella. "A simulation study of routing performance in realistic urban scenarios for MANETs". In: Proceedings of ANTS 2008, 6th International Workshop on Ant Algorithms and Swarm Intelligence, Brussels, Springer, LNCS 5217, 2008.

[2] Latha Tamilselvan, Dr. V Sankara narayanan "Prevention of Co-operative Black Hole Attack in MANET" JOURNAL OF NETWORKS, VOL. 3, NO. 5, MAY 2008.

[3] Bhoomika Patel et al, "Improving AODV Routing Protocol against Black Hole Attack based on MANET" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3586-3589.

[4] Ei Ei Khin, and Thandar Phyu "Mitigating Scheme for Black Hole Attack in AODV Routing Protocol" International Conference on Advances in Engineering and Technology (ICAET'2014) March 29-30, 2014 Singapore.

[5] Charles E. Perkins. Ad Hoc Networking. Addision Wesley, 2001.

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

[7] 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.

[8] Hongmei Deng, Wei Li, and Dharma P. Agarwal, "Routing security in wireless ad hoc networks", University of Cincinnati, IEEE Communications magazine, vol.40, no.10, October 2002.

[9] Gaurav Sandhu, Moitreyee Dasgupta, "Impact of black hole attack in MANET", International J. of Recent Trends in Engineering and Technology, vol. 3, no. 2, May 2010.

[10] Mistry N, Jinwala DC, IAENG, Zaveri M (2010) Improving AODV Protocol Against Blackhole Attacks. Paper presented at the International MultiConference of Engineers and Computer Scientists, Hong Kong, 17-19 March, 2010

[11] Jaspal Kumar, M. Kulkarni, Daya Gupta," Effect of Black Hole Attack on MANET Routing Protocols", Published Online April 2013 in MECS (http://www.mecs-press.org/), I. J. Computer Network and Information Security, 2013, 5, 64-72

[12] Sarita Choudhary, Kriti Sachdeva," Discovering a Secure Path in MANET by Avoiding Black/Gray Holes",published in International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-1, Issue-3, August 2012.

[13] Vipan Chand Sharma, Atul Gupta, Vivek Dimri," Detection of Black Hole Attack in MANET under AODV Routing Protocol", Volume 3, Issue 6, June 2013 International Journal of Advanced Research in Computer Science and Software Engineering.
[14] Akanksha Saini, Harish Kumar," Effect Of Black Hole Attack On AODV Routing Protocol In MANET", International Journal of Computer Science and Technology.

