Performance Evaluation and Comparison of On Demand Multicast Reactive Routing Protocols under Black Hole Attack in MANET

E. A. Mary Anita anitareginald@yahoo.co.in
Research Scholar
Anna University
Chennai, India

V. Vasudevan drvvmca@yahoo.com
Senior Professor and Head / IT
A. K. College of Engineering
Virudunagar, India

Abstract

One main challenge in the design of routing protocols is their vulnerability to security attacks. This is mainly due to the wireless and dynamic nature of ad hoc networks. A black hole attack is a severe attack that can be easily employed against routing in mobile ad hoc networks. In this attack a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept thereby exploiting the proper functioning of the protocol. In this paper the performance of multicast on demand routing protocols such as Multicast Ad-hoc On Demand Distance Vector (MAODV) protocol and On Demand Multicast Routing Protocol (ODMRP) are evaluated and analyzed under black hole attack under different scenarios in terms of the performance metrics such as packet delivery ratio and end to end delay. The evaluation is done with network simulator NS-2. Simulation results indicate that both the protocols suffer a significant reduction in packet delivery ratio in the presence of black hole attackers but the impact is more in MAODV when compared to ODMRP due to the presence of alternate data delivery paths in ODMRP.

Keywords: MANET, Black hole, MAODV, ODMRP, Packet Delivery Ratio, End to End Delay.

1. INTRODUCTION

Security in wireless ad-hoc networks is a complex issue. This complexity is due to various factors like insecure wireless communication links, absence of a fixed infrastructure, node mobility and resource constraints [1]. Nodes are more vulnerable to security attacks in mobile ad-hoc networks than in traditional networks with a fixed infrastructure. The security issues of Mobile Ad-hoc Networks (MANETs) are more challenging in a multicasting environment with multiple senders and receivers. There are different kinds of attacks by malicious nodes that can harm a network and make it unreliable for communication. These attacks can be classified as active and passive attacks [2]. A passive attack is one in which the information is snooped by an intruder without disrupting the network activity. An active attack disrupts the normal operation of a network by modifying the packets in the network. Active attacks can be further classified as internal and external attacks. External attacks are carried out by nodes that do not form part of the network. Internal attacks are from compromised nodes that were once legitimate part of the network.

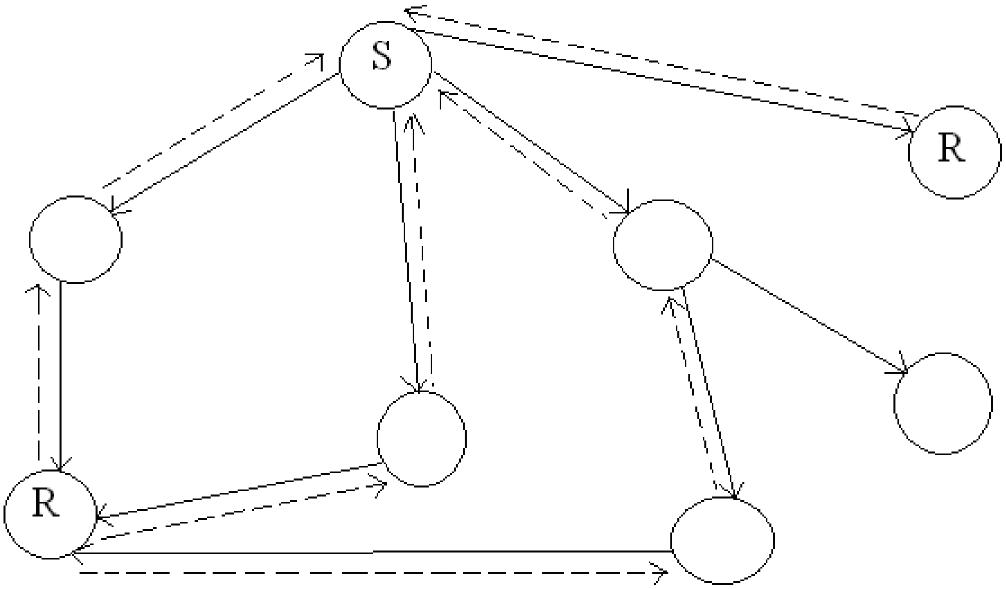
A black hole attack is one in which a malicious node advertises itself as having the shortest path to a destination in a network. This can cause Denial of Service (DoS) by dropping the received packets.

The rest of the paper is organized as follows. The next section gives an overview of MAODV and ODMRP. Section III discusses about black hole attack. In section IV the results of simulation experiments that show the impact of black hole attack on the performance of MAODV and ODMRP under different scenarios are discussed. Finally section V summarizes the conclusion

2. OVERVIEW OF ROUTING PROTOCOLS

2.1 Overview of MAODV

MAODV is a multicast routing protocol for ad-hoc networks. It is an extension of AODV. As nodes join the group, a tree is created. This tree connects the group members and many routers which are not group members but exist in the tree to connect the group members.



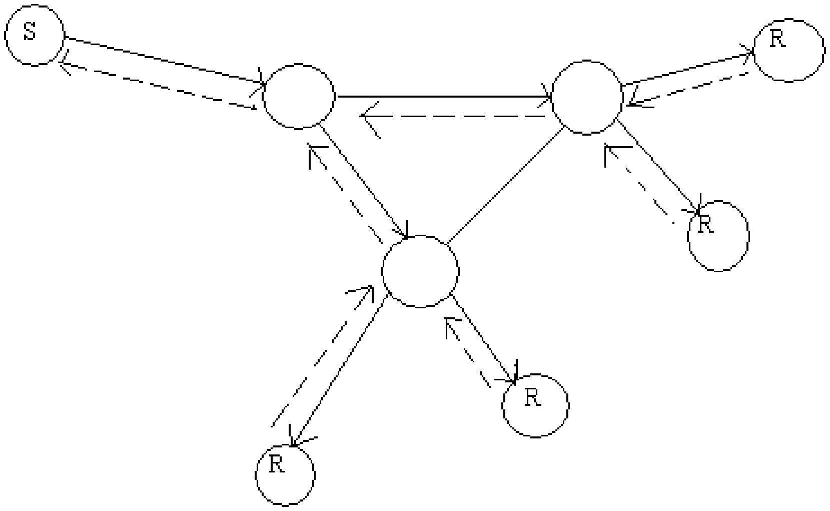
R – Multicast Receiver ________RREQ _ _ _ _ _ RREP

FIGURE 1: Route Request procedure of MAODV

Multicast group membership is dynamic. The group members and routers are all members of the tree. Every multicast group is identified by a unique address and group sequence number for tracing the freshness of the group condition [3]. When a node wants to find a route to a group or join a group it broadcasts a RREQ message. Any node with a fresh enough route to the multicast group may respond to this request message with a RREP message. If a node wants to become a member of the group that does not exist, then this node becomes the leader of that group and is responsible for maintaining the group. Group Hello messages are broadcasted periodically to check for connectivity of tree structure [4]. This results in increased overhead in maintaining route

2.2 Overview of ODMRP

ODMRP is a mesh based multicast routing protocol that uses the concept of forwarding group. Only a subset of nodes forwards the multicast packets on shortest paths between member pairs to build a forwarding mesh for each multicast group [5].



O – Mobile node S – Multicast Source R – Multicast Receiver

______ JREQ _ _ _ _ _ JREP

FIGURE 2: On demand route and mesh creation

In ODMRP, group membership and multicast routes are established and updated by the source on demand. When a multicast source has packets to send, it initiates a route discovery process. A JOIN REQUEST packet is periodically broadcast to the entire network. Any intermediate node that receives a non- duplicate JREQ packet stores the upstream node ID and rebroadcasts the packet. Finally when this packet reaches the destination, the receiver creates a JOIN REPLY and broadcasts it to its neighbors. Every node receiving the JREP checks to see if the next node id in JREP matches its own. If there is a match, it is a part of the forwarding group, sets its FG_FLAG and broadcasts its JREP built upon matched entries. This JREP is thus propagated by each forwarding group member until it reaches the source via a shortest path. Thus routes from sources to receivers build a mesh of nodes called forwarding group.

The forwarding group is a set of nodes that forward the multicast packets. It supports shortest paths between any member pairs. All nodes inside the bubble (multicast members and forwarding group nodes) forward multicast data packets [6]. A multicast receiver can also be a forwarding group node if it is on the path between a multicast source and another receiver. The mesh provides richer connectivity among multicast members compared to trees.
After the route establishment and route construction process, a multicast source can transmit packets to receivers via selected routes and forwarding groups. A data packet is forwarded by a node only if it is not a duplicate one and the setting of the FG_Flag for the multicast group has not expired. This procedure minimizes traffic overhead and prevents sending packets through stale routes.

In ODMRP, no explicit control packets need to be sent to join or leave the group. A multicast source can leave the group by just stop sending JREQ packets when it does not have any data to be sent to the group. If a receiver no longer wants to receive data from a particular group, it removes the corresponding entries from its member table and does not transmit the JOINTABLE for that group.

3. BLACK HOLE ATTACK

Routing protocols are exposed to a variety of attacks. Black hole attack is one such attack in which a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept [7]. This attack aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. During the route discovery process, the source node sends route discovery packets to the intermediate nodes to find fresh path to the intended destination. Malicious nodes respond immediately to the source node as these nodes do not refer the routing table.

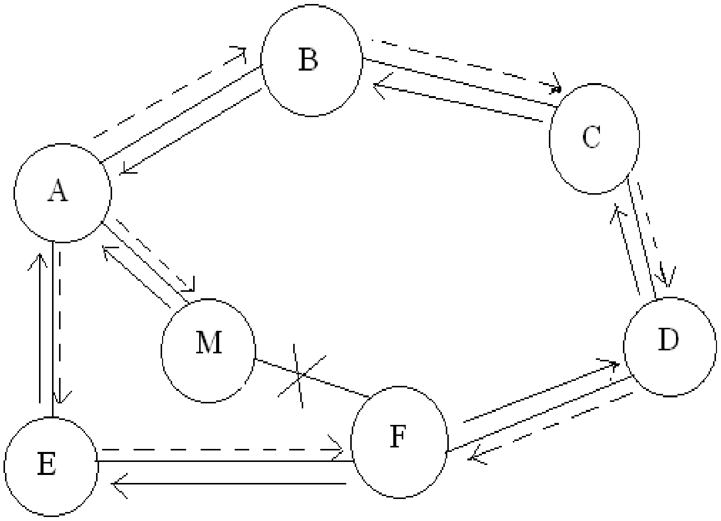
The source node assumes that the route discovery process is complete, ignores other route reply messages from other nodes and selects the path through the malicious node to route the data packets. The malicious node does this by assigning a high sequence number to the reply packet [8]. The attacker now drops the received messages instead of relaying them as the protocol requires.

3.1 Security in MAODV and ODMRP

ODMRP and MAODV are important on demand multicasting routing protocols that create routes only when desired by the source node. These protocols do not include any provisions for security and hence they are susceptible to attacks .When a node requires a route to a destination it initiates a route discovery process within the network. Any malicious node can interrupt this route discovery process by claiming to have the shortest route to the destination thereby attracting more traffic towards it [9].

For example, source A wants to send packets to destination D, in figure 3; source A initiates the route discovery process. Let M be the malicious node which has no fresh route to destination D. M claims to have the route to destination and sends route reply/join reply (RREP/JREP) packet to S. The reply from the malicious node reaches the source node earlier than the reply from the legitimate node, as the malicious node does not have to check its routing table like the other legitimate nodes [14].

The source chooses the path provided by the malicious node and the data packets are dropped [10].The malicious node forms a black hole in the network and this problem is called black hole problem.



A-Source node D-Destination node M-Malicious node

- - - -RREQ/JREQ ____ RREP/JREP

FIGURE 3: Black hole attack

4. SIMULATION

In this section, the simulation environment and the simulation results are discussed. Simulation is done using the network simulator NS-2.

4.1 Simulation Metrics

The metrics used in evaluating the performance are:

4.1.1 Packet Delivery Ratio: It is the ratio of the number of data packets delivered to the destinations to the number of data packets generated by the sources. This evaluates the ability of the protocol to deliver data packets to the destination in the presence of malicious nodes [11].

4.1.2 Average End-to-End Delay: This is the average delay between the sending of packets by the source and its receipt by the receiver [12]. This includes all possible delays caused during data acquisition, route discovery, queuing, processing at intermediate nodes, retransmission delays, propagation time, etc. It is measured in milliseconds.

4.2 Simulation Profile

The simulation settings are as follows. The network consists of 50 nodes placed randomly within an area of 1000m x 1000 m. Each node moves randomly and has a transmission range of 250m. The random way point model is used as the mobility model. In this model, a node selects a random destination and moves towards that destination at a speed between the pre-defined maximum and minimum speed. The minimum speed for the simulations is 0 m/s while the maximum speed is 50 m/s. The channel capacity is set to 2Mbps and the packet size is 512 bytes. The CBR traffic is generated with a rate of 4 packets per second. The simulation time is 900 seconds. The simulations were carried out with 0, 2 and 5 attackers for different number of receivers. The malicious nodes were selected randomly.

4.3 Discussion of results

Figure 4 shows the variation of packet delivery ratio (PDR) with mobility when the multicast group consists of 1 sender and 20 receivers with no attackers.

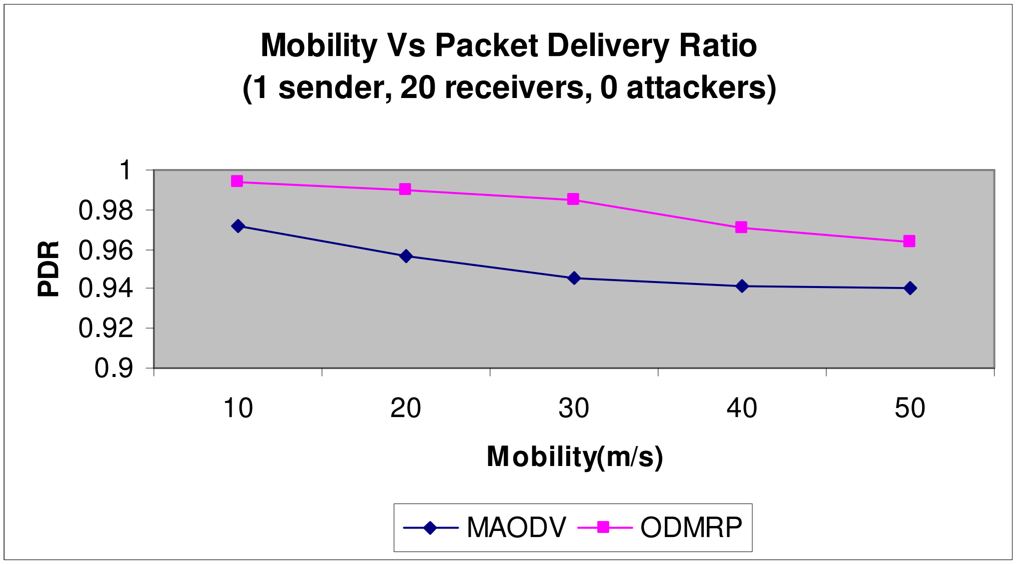


FIGURE 4: Variation of PDR with mobility in the absence of attackers

It is seen that the PDR decreases with increased mobility. Also the PDR of MAODV is less than the PDR of ODMRP by around 2 to 10%. This may be attributed to the fact that more alternate routing paths are available in ODMRP. The mesh structure in ODMRP provides multiple paths spanning all multicast group members and these paths become available in case of any failure in the primary path.

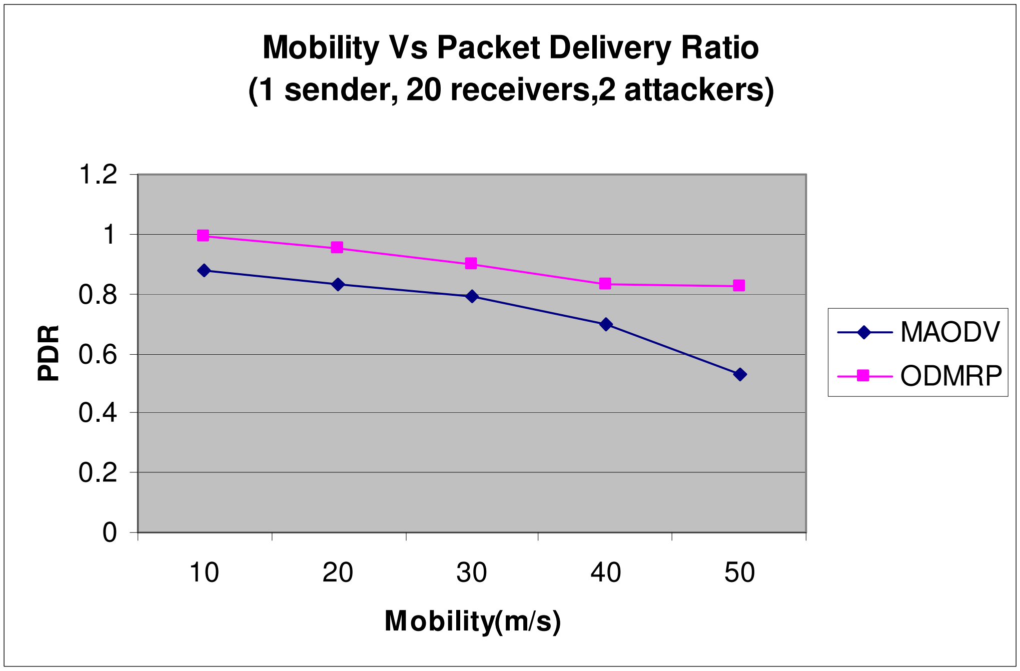


FIGURE 5: Variation of PDR with mobility in the presence of 2 attackers

When there are 2 numbers of attackers, the PDR reduces to about 1 to 4% for ODMRP and the reduction is around 5% to 20% in MAODV as shown in figure 5. This loss is partially due to black hole nodes dropping the packets and partially due to congestion in the network over the paths towards the black hole nodes.

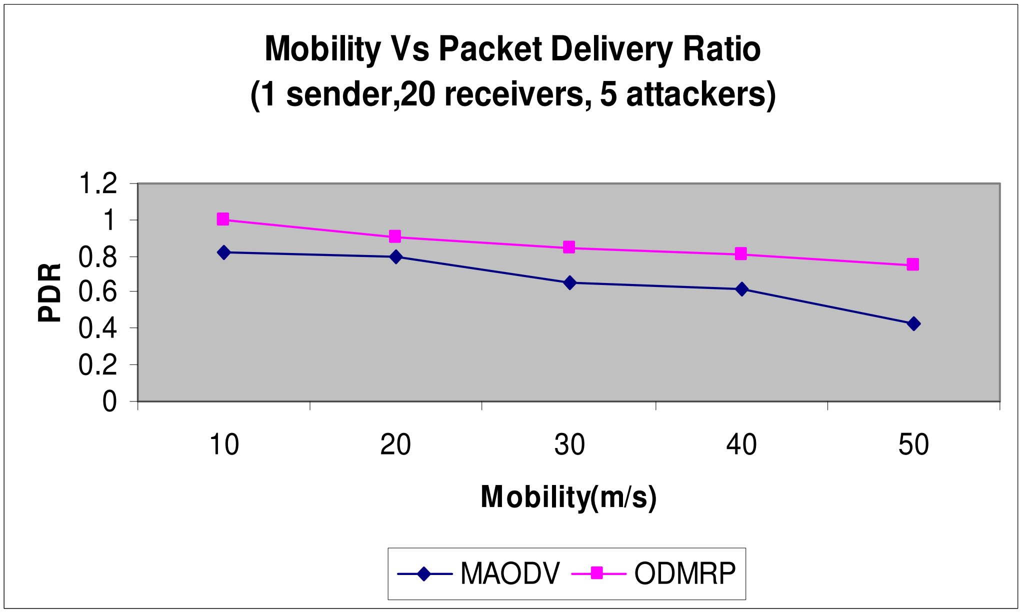


FIGURE 6: Variation of PDR with mobility in the presence of 5 attackers

When the number of attackers is increased to 5, the PDR further drops by around 5 for ODMRP and 20% for MAODV. Higher the number of attackers, higher the reduction in PDR. This is shown in figure 6.

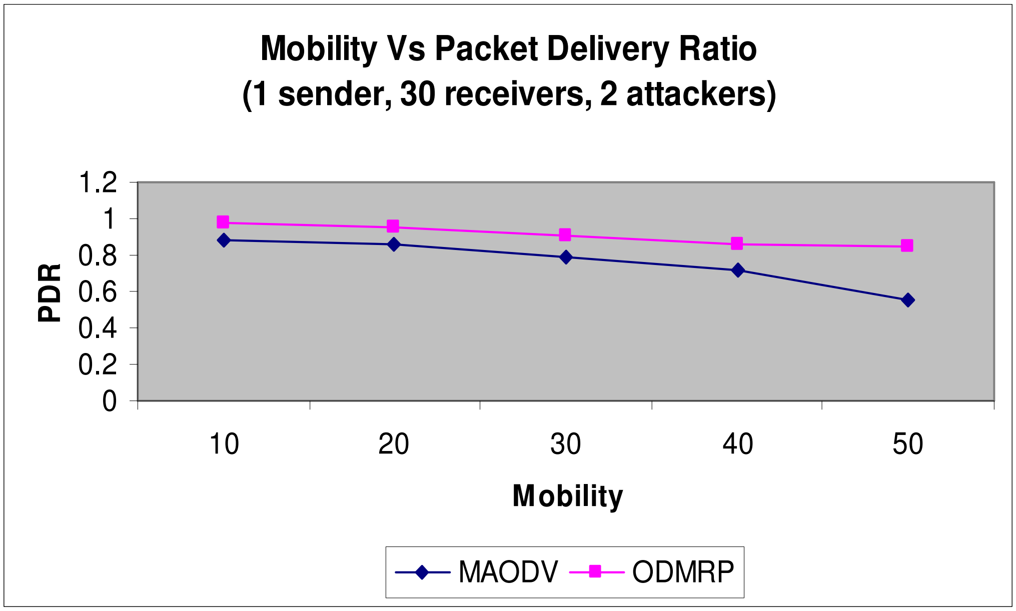


FIGURE 7: Variation of PDR with mobility in the presence of 30 receivers and 2 attackers

Figure 7 shows the variation of PDR with mobility with an increased group size of 30 receivers. It is seen that though the PDR reduces in the presence of attackers, a large group is able to withstand the attack to a reasonable extent when compared to a smaller group which is easily susceptible to attacks.

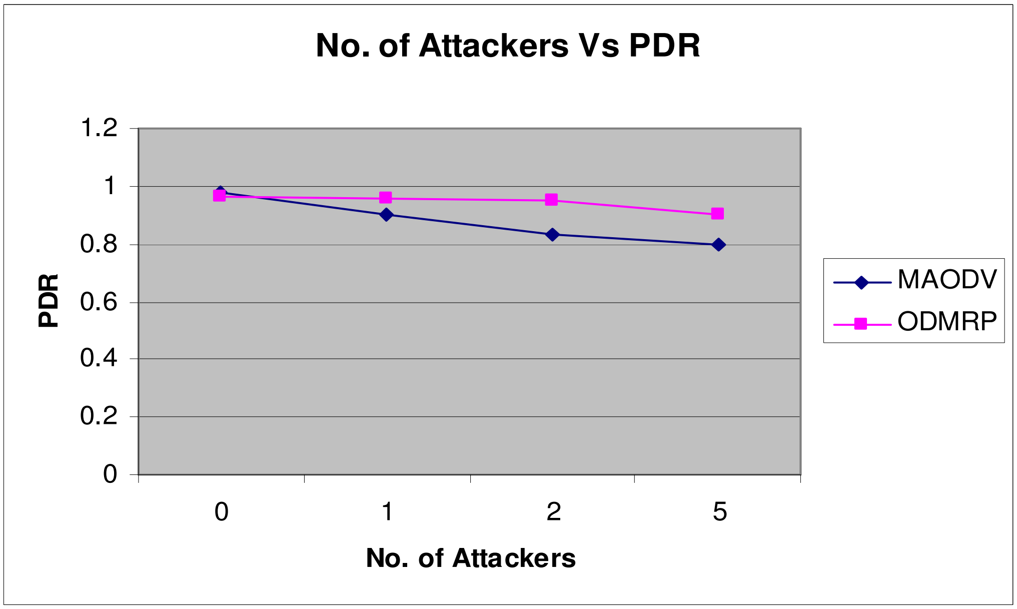


FIGURE 8: Variation of PDR with attackers

Figure 8 shows the variation of PDR for different number of attackers. It is seen that the packet delivery ratio reduces in the presence of attackers and the effect of the attack is more in MAODV when compared to ODMRP. This is due to the presence of alternate paths available in ODMRP. Since the mesh becomes denser with the growth if the members, more redundant routes are formed thereby improving the performance. So even if a packet gets dropped in one path due to the presence of black hole nodes, there is a chance for the duplicate copy of the packet to reach the destination through alternate paths free from malicious nodes [13].

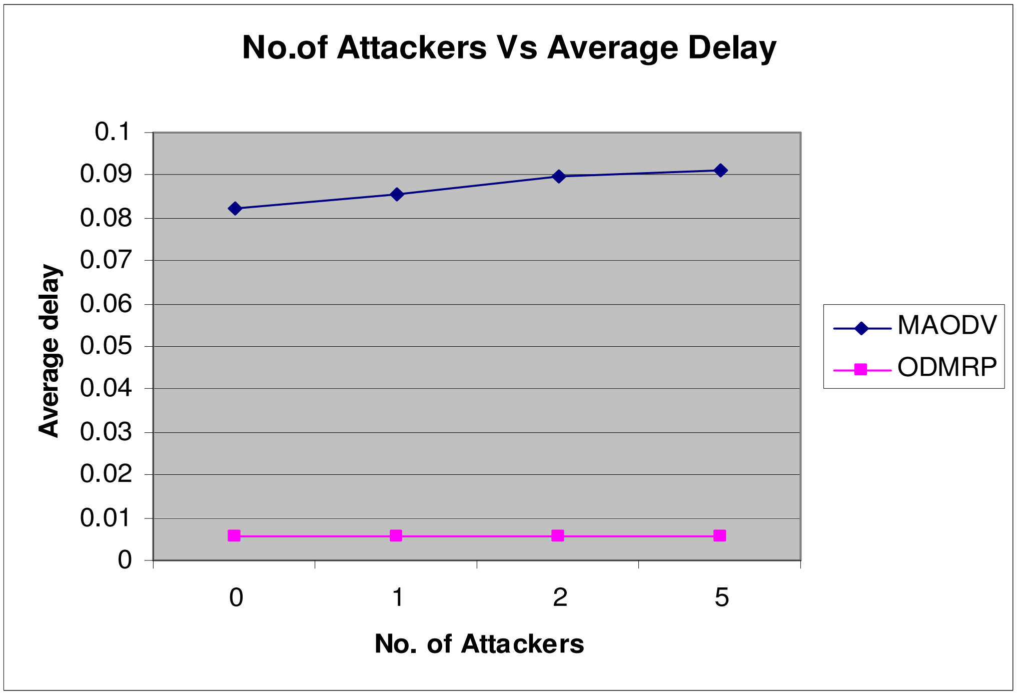


FIGURE 9: Variation of Average Delay with attackers

Figure 9 shows the variation of end to end delay for different numbers. There seems to be an increase in the delay in the presence of attackers. Also the delay is more in MAODV than in ODMRP. This is due to the fact that non shortest paths containing black hole nodes are selected for routing the packets.

5. CONCLUSION

Security is one of the major issues in MANETs. In this paper the effect of black hole attack on MAODV and ODMRP are analysed and compared under different scenarios.The performance of a multicast routing protocol under black hole attack depends on factors such as number of multicast senders, number of multicast receivers and number of black hole nodes

From the simulation results it is observed that, the packet delivery ratio reduces with increased mobility of the nodes and also with increased number of black hole nodes and affect the performance of the network. Also the packet delivery ratio is higher for large number of receivers for the same number of attackers. That is, the effect of the attack is more in a small group than in a large group. A large group is able to withstand the attack to a reasonable extent when compared to a smaller group which is easily susceptible to attacks. This can be attributed to the existence of alternate paths for routing the data packets.

The results also depict that the delay increases with increase in group size and increase in number of attackers. This is because of the fact that non shortest paths containing black hole nodes are selected for routing the packets.

When comparing the performances of MAODV and ODMRP under black hole attack, a general conclusion is that, given the same number of attacker nodes, a mesh based protocol like ODMRP outperforms a tree based protocol like MAODV. This is because to the fact that redundant routes in the mesh of ODMRP provide alternate paths for data delivery.

The simulation results and analysis may pave way for researchers to propose solutions to counter the effect of black hole attacks thereby improving the network performance. Given the constrained resources and the rapidly varying conditions in which the nodes operate, any authentication mechanism that can prevent malicious nodes from participating in the routing process and identify secure routes may provide a proper solution to tackle black hole attack.

6. REFERENCES

1. D. Djenouri, L. Khelladi and N. Badache, A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks, IEEE Communication Surveys & Tutorials, Vol. 7, No. 4, 4th Quarter 2005.
2. L. Zhou and Z. J. Haas, Securing Ad Hoc Networks, IEEE Network Magazine, Vol. 13, No. 6, Nov./Dec. 1999, pp. 24–30.
3. P. Papadimitratos and Z. J. Haas, Secure Routing for Mobile Ad hoc Networks, Proceedings of Communication Networks and Distributed Systems, Modeling and Simulation Conference (CNDS'02), San Antonio, Texas, Jan. 2002, pp. 27–31.
4. E. A. Mary Anita and V. Vasudevan, Performance Evaluation of Mesh based Multicast Reactive Routing Protocol under Black Hole Attack, IJCSIS, Vol. 3, No.1, 2009.
5. S.Lee, M.Gerla and C.Chain, On Demand Multicast Routing protocol-(ODMRP), Proc. of the IEEE Wireless Communication and Networking Conference (WCNC), September 1999
6. A. Vasiliou and A. A. Economides, Evaluation of Multicasting Algorithms in Manets, PWASET, vol. 5, April 2005, pp. 94-97.
7. H. Deng, W. Li, and Dharma P. Agrawal, Routing Security in Ad Hoc Networks, IEEE Communications Magazine, Special Topics on Security in Telecommunication Networks, Vol. 40, No. 10, October 2002, pp. 70-75.
8. Al-Shurman, M. Yoo, S. Park, Black hole attack in Mobile Ad Hoc Networks, ACM Southeast Regional Conference, 2004, pp. 96-97.
9. Sanzgiri K., Dahill B., Levine B. N., Shields, C., and Belding-Royer, E. M., Authenticated routing for ad hoc networks, IEEE Journals on Selected Areas in Communications, 23(3), 2005, 598- 610.
10. B. Sun, Y. Guan, J. Chen and U. Pooch, Detecting black hole attack in mobile ad hoc networks, Personal Mobile Communications Conference. 2003.5th European (Conf. Publ. No. 492), pp. 490 – 495, April 2003.
11. Pankaj Kumar Sehgal & Rajender Nath, A Encryption Based Dynamic and Secure Routing Protocol for Mobile Ad Hoc Network, International Journal of Computer Science and Security (IJCSS), Volume (3) : Issue (1) 16
12. A.Patcha and A.Mishra, Collaborative security architecture for black hole attack prevention in mobile ad hoc networks, Radio and Wireless Conference, 2003. RAWCON '03, Proceedings, pp. 75-78, 10-13 Aug. 2003.
13. E. A. Mary Anita and V. Vasudevan, Black Hole Attack on Multicast Routing Protocols, Journal of Convergence Information Technology, Vol.4, No.2, pp.64–68, 2009.
14. C. Siva Ram Murthy and B. S. Manoj, Ad hoc Wireless Networks- Architectures and Protocols, Pearson Education, 2007

.