

SIMULATION BASED PERFORMANCE COMPARISON OF AODV, DSR, FSR ROUTING PROTOCOL WITH WORMHOLE ATTACK

R.Sherine Jenny

Assistant Professor, Department of ECE
Dr.Mahalingam College of Engineering &
Technology, Coimbatore, India.
sherinejenny@drmcet.ac.in

N.Sugirtham

Assistant Professor, Department of ECE
Dr.Mahalingam College of Engineering &
Technology, Coimbatore, India
nsugirtham@drmcet.ac.in

Abstract-An ADHOC Network is a cluster of nodes where individual nodes help in forwarding the packets even beyond the wireless transmission range. This network does not rely on routers in wired network or access points in Wireless network, hence it's named ADHOC. In this paper we have introduced the worm hole attack to one network and analysed the impact of this attack on various protocols such as AODV, DSR and Fisheye. This is a severe and challenging attack and can attack any network which is considered to be more secure. Here we have collated the performance of the above protocols in terms of throughput, packet delivery, jitter and end to end delay in mobile and immobile ADHOC Networks when attacked by wormhole. It's found that DSR performs better in terms of packet delivery ratio and throughput but end to end delay is very large when compared to other two protocols in a wormhole attacked network.

Keywords - ADHOC Network, Wormhole attack, Throughput, Jitter, Packet Delivery Ratio, End-to-End delay.

I. INTRODUCTION

Ad hoc networks are famous because it's a network without infrastructure and performs an extreme adaptive self organized communication. It does not have a base station for communication, here each node will act as a router and are helpful in forwarding the packets even beyond the transmission range. Performance and reliability of mobile Ad hoc networks can be achieved by using efficient routing protocols. Security issue in wireless network is more critical than in wired network. Network functions like packet forwarding and routing requires a secured network but the nodes of an Ad hoc network cannot be relied upon for proper functioning. As air is used as the medium for broadcasting a sophisticated attacker can easily intrude into the network though the network is highly secured [8]. The intruders target is to spy, disrupt the network. One such attack is wormhole that degrades the performance of wireless network. This paper deals with the degradation on the performance of routing protocols due to malicious wormhole attack further it presents a qualitative analysis of the protocols that offer better resistance to wormhole attack. The rest of this paper is organized as follows: Section II describes briefly about the routing protocols that are used for analysis. Performance of the network under wormhole attack is described in section III. Section IV presents the

actual simulation results and analysis graphs. The last section concludes the work of this paper.

II. ADHOC ROUTING PROTOCOLS

Mobility implies that links make and break often and in a deterministic fashion. Extensive research work has been carried out with the routing protocols for an Ad hoc Network. Different routing protocols were simulated with different simulators like NS2, Glomosim and Qualnet. Here we have compared the behaviour of very commonly used protocols of an Ad hoc network with the Wormhole Attack using Qualnet 5.0.1. The sample scenario created is analysed with and without mobility.

The Ad-hoc On-demand Distance Vector (AODV) routing protocol [1][10] is used for dynamic wireless network where the nodes can enter and leave the network at anytime. A route to a particular destination is found by sending RREQ to its immediate neighbours. A neighbour will reply with RREP message when it has a route to the destination. Otherwise the neighbour nodes will rebroadcast the RREQ, this continues until a path is found to the destination. AODV uses destination sequence numbers to all routers and ensures that they are loop free and contain recent router information.

FSR is a hierarchical routing protocol that works on the principle that it uses the property of fisheye [7][9] that can capture pixel information with greater accuracy near its eyes focal point. It maintains the topology of the network at every node but does not flood the entire network with information as is done in LSR. Instead of flooding, node exchanges topology information only with its neighbours. Recent topology changes are identified using sequence numbers.

Two major phases in DSR are route discovery and route maintenance [7]. To send a packet to some destination mobile node consults route cache to determine whether it already has a route to the destination. If unexpired route exists it will use this route to send the packet else initiates route request packet. DSR is designed particularly for mobile Ad hoc network and it can perform well with more than hundred nodes. It is designed such that it operates well in a network with high rate of mobility.

III. WORMHOLE ATTACK

There are two categories of attack [6], passive and active attack. A passive attack tries to get the information from the system but does not damage the system resources. An active attack tries to alter and damage the system resources. Active attack can be further classified according to the layer attacked as network layer attack, application layer attack, transport layer attack and multi layer attack. Attack considered here for analysis is wormhole attack which is a network layer attack.

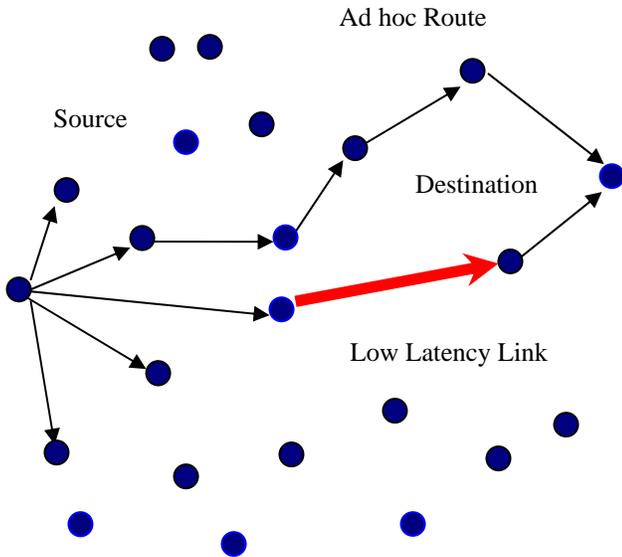


Figure. 1 Wormhole Attack with low latency link

Wormhole attack is a very serious attack [2][9] which disrupts the routing protocol and hence breakdowns the whole network. Ad hoc networks are more vulnerable to this kind of attack. This may be due to lack of protection, poor infrastructure and no centralised management system. Existing Ad hoc routing protocols, without any defending mechanism against this attack finds very difficult to route their packet. Here in wormhole attack the adversary creates a link which is of very low latency, which is said to be the wormhole links[5] as shown in Fig.1. This link can be created using an ethernet cable, an optical Link or a long range wireless link. In our Scenario we have created five networks wherein one network is wormhole attacked as shown in Fig.2 .This network creates a low latency link hence any packet that is transferred from one network to other network which is not wormhole attacked tends to find the route through the wormhole attacked network. If the source node chooses this fake low latency link route, malicious nodes have the option of delivering the packets or dropping them.

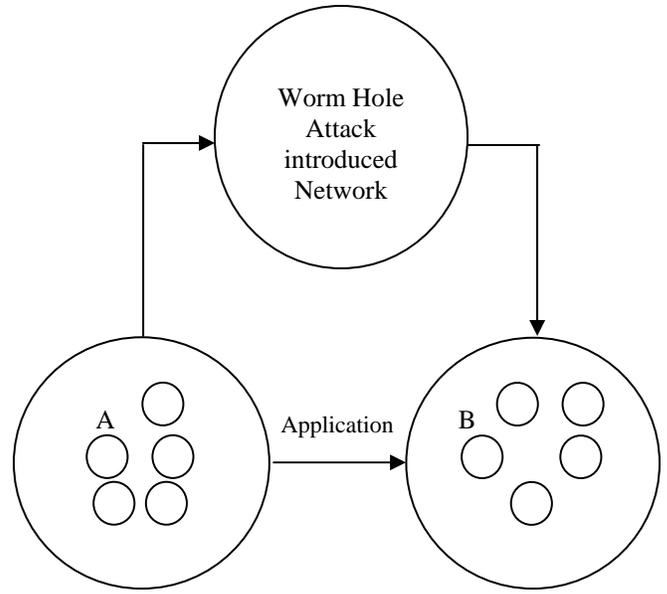


Figure. 2 ADHOC Network with Wormhole Attack introduced

IV. RELATED WORK

The performance of AODV, DSR and Fisheye protocols were evaluated with respect to parameters such as packet delivery ratio, throughput, average jitter and end-to-end delay[8] with a mobile and immobile network with wormhole Attack using Qualnet 5.0

A. Performance Metrics

Throughput: The overall capacity of any system to process its inputs and generate the required output is called the system's Throughput. Throughput is the average number of information bits transmitted in one second, and is calculated as

$$\text{Throughput} = \frac{\text{Number of information bits transferred}}{\text{Time taken to transfer the bits}}$$

Packet delivery ratio: It is the ratio that illustrates the total amount of packets delivered to the destination

$$\text{Packet Delivery Ratio} = \frac{\sum \text{Number of packets received}}{\sum \text{Number of packets sent}}$$

Greater the value of packet delivery, better the performance of the Protocol

End-to-end delay: It is the average time taken for the data packet to arrive at the destination. It also includes the delay that is caused to the route discovery process and queue. Packets that are delivered to the destination are only accountable. Lower the value of end-to-end delay, better the performance.

Average Jitter : Jitter is the variation in the time of packet arrival. This is caused due to many factors like timing drift, congestion and route change. Normally Jitter is expected to be low.

B. Simulation Methodology

In this Paper Qualnet Version 5.0.1 is used as simulation Software. QualNet is a tool used for modelling wired and wireless networks. The behaviour and performance of networks are predicted using simulation[4][7] and emulation so that one can improve their design, operation and management.

The simulation parameters chosen for the analysis are as follows: simulation time is 300seconds, simulation area 1500m*5000m, radio type 802.11b, MAC protocol is wormhole, number of nodes chosen is 30,routing protocol used for analysis is AODV,DSR,FSR, traffic pattern followed is CBR, Item size is 512bytes and packet interval is 1second as shown in Table. I.

TABLE. I .SIMULATION PARAMETERS

S No	Simulation Parameters	Values
1	Simulation Time	300 Seconds
2	Simulation Area	1500mX1500m
3	Radio Type	802.11b
4	MAC Protocol	Wormhole
5	Number of Nodes	30
6	Routing Protocol	DSR,AODV,Fisheye
7	Traffic Pattern	CBR
8	Item Size	512 Bytes
9	Packet Interval	1 Second

V. SIMULATED RESULTS AND CONCLUSION

Analysis is done using qualnet 5.0.1network simulator and the CBR is the application between two nodes in two different networks. It generates packet at a constant bit rate and it's a well known traffic pattern for mobile Ad hoc network. Qualnet simulator can be configured more accurately to model different scenarios with increasing the number of nodes with and without mobility. In this section the simulation efforts are used to evaluate and to compare the performance of the protocols that are described in the previous section II. MAC Protocol is set to Wormhole. The simulated output as shown in figure 3 and figure 4 are for the FSR protocol and the nodes are immobile and mobile respectively.

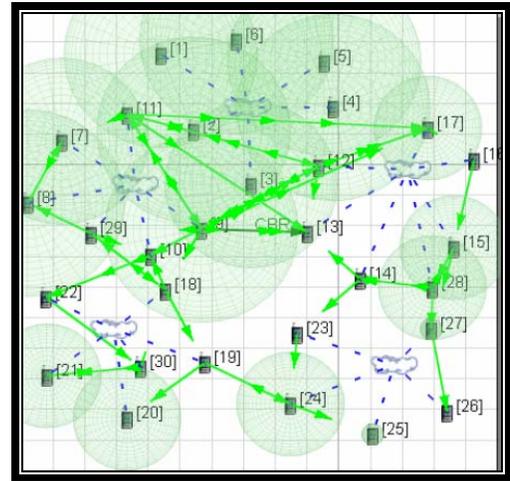


Figure. 3 Simulated output for a wormhole attacked immobile network

In order to investigate the performance of different routing protocols with and without mobility under wormhole attack scenarios were designed and simulated.

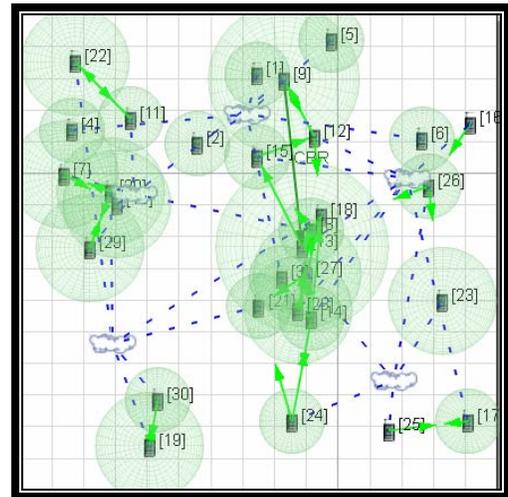


Figure.4 Simulated output for a wormhole attacked mobile network

It is observed in the analysis that DSR Protocol performance better in terms of packet reception. Considering the packet delivery ratio which is the ratio of total number of packets received at the destination successfully to the total number of packets sent at the source node, its found that the packet delivery ratio for DSR protocol on a Wormhole attacked scenario is about 11% for a mobile network whereas its around 28% for immobile network. From Fig 5, under wormhole attack with the protocols AODV and FSR the delivery ratio are very less compared to DSR.

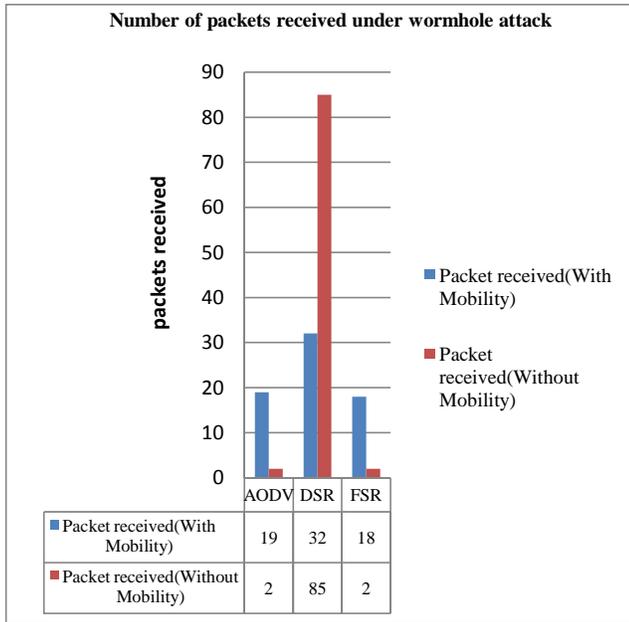


Figure.5 Total number of packets received under different protocols

According to our analysis it is inferred that the wormhole attacked network with DSR protocol provides a superior throughput. The throughput for the network with and without mobility under wormhole attack is shown in Fig 6.

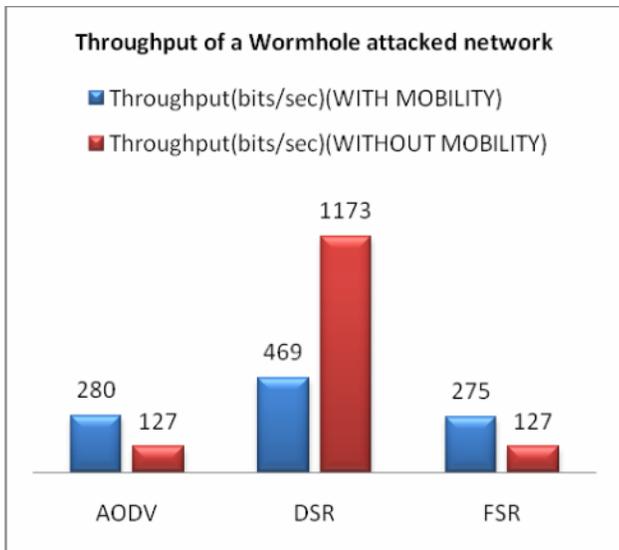


Figure.6 Throughput of a Wormhole attacked network

The analytical values for throughput with and without mobility for AODV,DSR and FSR are tabulated as in Table II . The throughput and packet delivery ratio under DSR protocol is better than AODV and FSR protocol.

TABLE III .THROUGHPUT OBSERVED UNDER SIMULATION

Protocol	Throughput (Bits/Sec)with mobility	Throughput (Bits/Sec)without mobility
AODV	280	127
DSR	469	1173
FSR	275	127

Though End-End Delay[8] as shown in Fig 7 and the fluctuation in end-end Delay which is called as Jitter depicted in Fig 8 both clearly reveals that it is more in the network with DSR protocol, the packets dropped due to wormhole attack in the network with other two protocols is more when compared to DSR.

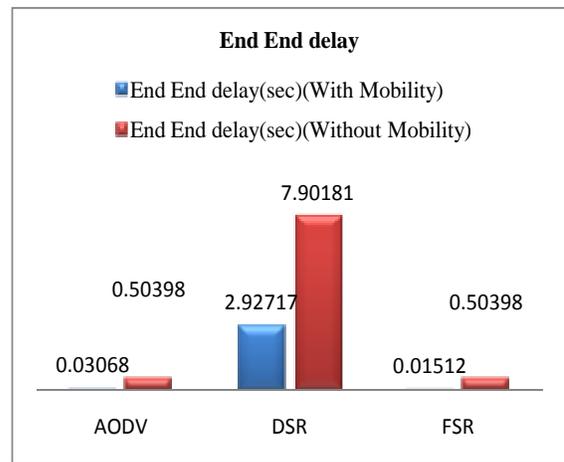


Figure.7 End-End Delay of a Wormhole attacked network

In our network we have considered the threshold to be 145 bytes. In this case, wormhole drops all the packets which are above 145 bytes in size.

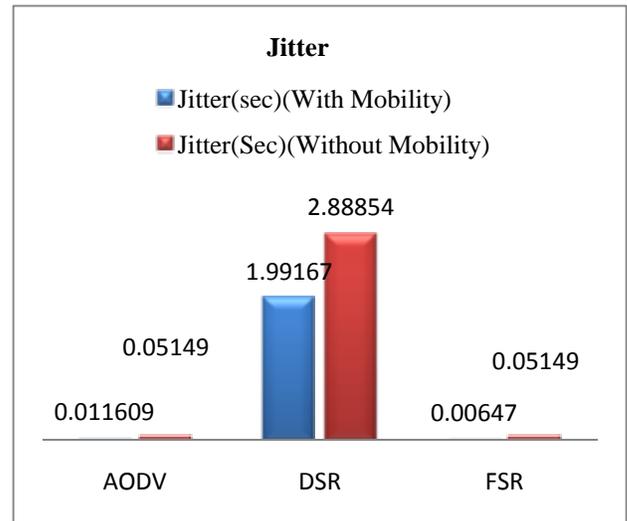


Figure.8 Jitter of a Wormhole attacked network

The simulation has been conducted using network simulator Qualnet 5.0.2 for the performance comparison of AODV, DSR and Fisheye protocols with wormhole attack and under mobile and immobile network scenarios. Qualnet network simulator was used to generate the graph shown below in Fig 9 that illustrates the frames dropped due to wormhole attack with various routing protocols.

- [4] Suresh Kumar, Jogendra Kumar, "Simulation Based Comparative Performance Study of AODV, DSR and ZRP in Mobile Ad hoc Networks (MANETs) Using Qualnet 5.0.2" IOSR Journal of Engineering, Vol. 2(4), pp: 568- 572, Apr. 2012.
- [5] Susheel Kumar, Vishal Pahal , Sachin Garg, "Wormhole attack in Mobile Ad Hoc Networks: A Review" Departm-

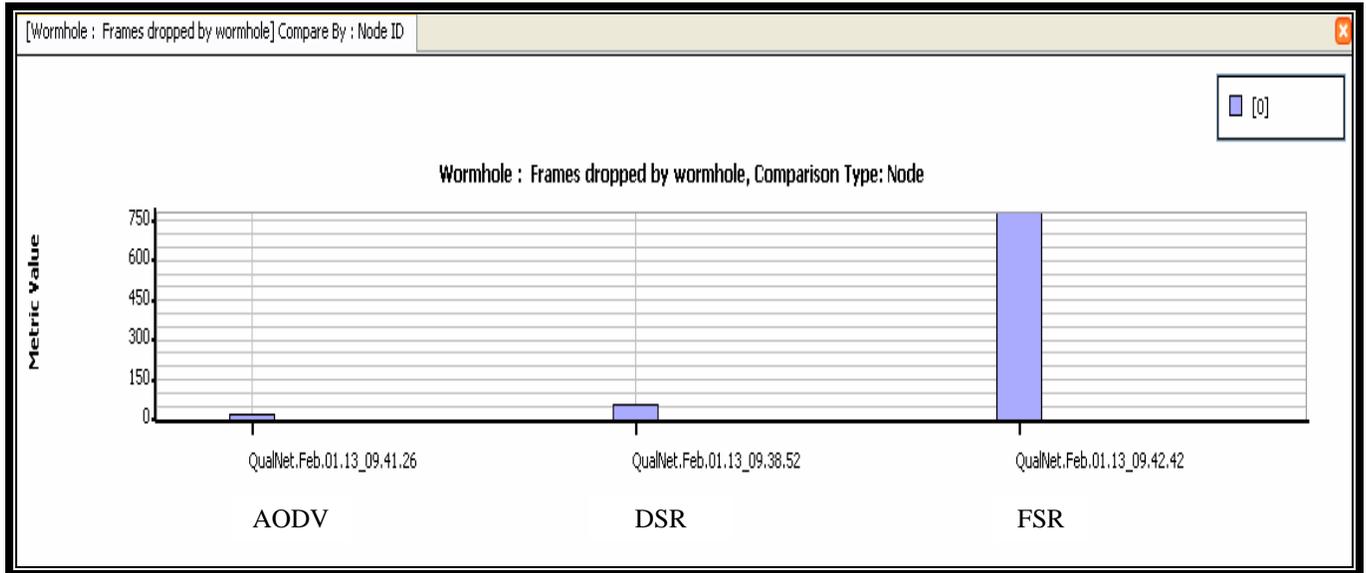


Figure 9 Frames dropped by wormhole

Based on the scenario considered for analysis we observed that DSR protocol performs better in mobile and immobile network under wormhole attack but when it comes to Jitter and end-end delay AODV performs better. Network parameters like end-to-end delay, jitter, throughput and packets dropped varies as the number of nodes increases or decreases. It is essential to note that results are specific to particular scenario with change in routing protocols.

REFERENCES

- [1] Alok Kumar Jagadev, Binod Kumar Pattanayak, Manoj Kumar, Mishra Manojranjan Nayak, "Power and Delay Aware On-Demand Routing for Ad Hoc Networks" International Journal on Computer Science and Engineering, Vol.02, No. 04, 917-923, 2010.
- [2] N.S.Raote, K.N.Hande, "Approaches towards Mitigating Wormhole Attack in Wireless Ad-hoc Network "International journal of advanced engineering sciences and technologies vol no. 2, issue no. 2, pp-172-175.
- [3] Sumaiya Thaseen, K. Santhi, "Performance Analysis of FSR, LAR and ZRP Routing Protocols in MANET" Int. J. Computer Applications, 4, Vol 41, March 2012.
- [4] Suresh Kumar, Jogendra Kumar, "Simulation Based Comparative Performance Study of AODV, DSR and ZRP in Mobile Ad hoc Networks (MANETs) Using Qualnet 5.0.2" IOSR Journal of Engineering, Vol. 2(4), pp: 568- 572, Apr. 2012.
- [5] Susheel Kumar, Vishal Pahal , Sachin Garg, "Wormhole attack in Mobile Ad Hoc Networks: A Review" Department of Computer Science and Engineering IRACST – Engineering Science and Technology: An International Journal (ESTIJ), ISSN: 2250-3498, Vol.2, No. 2, April 2012
- [6] Tsu-Wei chen and Mario Gerla, "Global State Routing: A New Routing Scheme for Ad-Hoc Wireless Networks" proc IEEE ICC'98.
- [7] R. Vinodkumar, R. S. D. Wahidabanu, "Performance Comparison of Wireless Mobile Ad-Hoc Networks European Journal of Scientific Research ISSN 1450-216X Vol.61 No.2 (2011), pp. 299-304
- [8] Yahya Ghanbarzadeh, Ahmad Heidari, Jaber Karimpour, "Wormhole Attack in Wireless Ad-Hoc Networks" International Journal of Computer Theory and Engineering Vol. 4, No. 2, pp-229-233, April 2012.
- [9] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Wormhole Attacks in Wireless Networks" IEEE Journal on Selected Areas In Communications, Vol. 24, No. 2, pp370-380, Feb 2006.
- [10] Siva Ram murthy and B.S.Manoj [2011], "Ad hoc wireless networks architectures and protocols".