Performance Evaluation of MANET Using AODV Routing Algorithm

Devottam Kumar, Ruhy Khanam

***Abstract*— A mobile Ad Hoc Network (MANET) is a collection of wireless mobile nodes forming temporary network without using any existing infrastructures and it frequently changes network topology for efficient dynamic routing protocols. This paper presents the performance comparison of AODV with and without malicious node in the MANET with respect to the packet lost, packet received, packet delay, packet throughput. The entire activities were simulated on NS-2.35 (Network Simulator Version 2.35) which works on MAC 802.11 model and wireless transmission channel model. The overall 25 mobile nodes are used to get the simulated results and helps to determine the performance with and without malicious node.**

***Index Terms*— MANET, Routing Protocols, Packet Lost, Packet Received, Packet Delay, Packet Throughput**

I. INTRODUCTION

MANET often interacts among them using multiple hops wireless links. They do not have any fixed framework networks and base-station. Classrooms, meetings, conferences, battle-fields, disaster relief activities are a few situations where MANET can be used effectively. In this paper, we emphasized on the evaluation of AODV protocols with and without the use of malicious nodes .The routing protocol able to keep up with the high degree of node mobility that often changes the network topology drastically and unpredictably. Routing protocol for MANET can be categorized into three which are as follows:

1. Proactive Routing Protocols
2. Reactive Routing Protocols
3. Hybrid Routing Protocols

Proactive Routing Protocols:-Every nodes in the network has one or more routes to any possible destination in its routing table at any given time.

Reactive Routing Protocols:-Every node in the network obtains a route to a destination on a demand fashion. Reactive protocol does not maintain up-to date routes to any destination in the network and do not generally exchange any periodic control messages. Hybrid Routing Protocols:-Every nodes acts re-actively in the regions close to its proximity and proactively outside of that region or zone.

Manuscript received October 17, 2014.
Devottam Kumar, CSE Department, M.Tech Scholar, CSVTU, Bhilai/ RCET College.
Ruhy Khanam, CSE Department, Assistant Professor, CSVTU, Bhilai / RCET College.

Ad Hoc On-Demand Distance Vector Routing (AODV): It uses a traditional routing table i.e. one entry per destination. From the names it reveals that it is an on demand protocol and reactive in nature for finding routes only when sender wants to send data. AODV spread sequence number to control packets flooding in the network. When the source wants to communicate with destination node whose route is unknown for sender, its broadcasts a RREQ (Route Request) packets to all it neighbors node. Each RREQ packet contains request-id, source and destination node IP addresses and sequence number along with the hop count and flags fields in its packet format. When the RREQ packet arrived at the destination node a RREP (Route Reply) the packet is generated and sends back to the source. RREP packet contains the destination node, IP - addresses, sequence number, route life time of a hop count and flags. Intermediate nodes that receive the RREP packet, increment the hop count field and it establishes a forward route to the source of the packet and transmit the packet on the reverse route. When a link failure is detected for a network, RERR (Route Error) message is sent to its active neighbors that were using a route to send packets.

Destination Sequenced Distance Vector (DSDV):- DSDV is a proactive and table driven routing protocol for MANET. In DSDV network, every node maintains its own routing table and share by the neighbor node. The routing table contains nodes IP address, sequence number and hop count to reach the next node along with the address of neighbor destination node and the time-stamp of the last update received for that node. Each node of ad hoc networks updates the three fields in the routing table i.e. destination address, sequence number and hop count. These updating is made by periodic and trigger updates. DSDV routing a table is updated periodically when new information is available which help in maintaining consistency of the dynamically changing of the routing table. The other updating a trigger where source need to communicate with the destination. Then a trigger is applied where fixed route neighbor nodes are updated the route table to send the packet of the destination.

Dynamic Source Routing (DSR):- DSR use the concept of a source routing, where each packet carries the list of the nodes through which the packet is routed. The purpose of using DSR is that intermediate nodes do not need to maintain to update routing information in order to forward the packets through the fixed route. DSR protocol consists of two mechanisms that are Route Discovery and Route Maintenance.

Route Discovery:-Source node wants to communicate with Destination node by sending packets. For sending packets route are discovered in DSR network. The source node will flood the route request packet in the network. The intermediate node in the network is responses from the route reply packet to the source node that the intermediate node

knows the route to the destinations. Each intermediate node maintains a cache of source routes which help to reduce the cost of route discovery and limit the propagation of route request.

Route Maintenance:-When route is discovered to send the packet from source to destination. If the network gets to break down then the neighbor node must send the error packet to the source node in aspect to notify that there is no existence of route to the destination which already in the cache or can invoke route discovery again to find a new route.

II. Related Work

The main aim is to evaluate the performance of the particular protocol i .e AODV with and without the malicious node. The simulator will behave the simple transmission of packets from Source to Destination through the intermediate nodes, which exist in the route. In the second steps the Simulator will try to transmit the packets from Sender to Receiver through the malicious node which exist in the route. In both cases the simulator will calculate the overall Throughput, End to End Delay, Packet Cost as well as comparison of Packet Lost with Packet received in the packet transmission.

Table 1 represents parameters used in the network simulation activity.

Simulator Used	NS-2.35
Number of Nodes	25
Malicious Nodes	3
Simulation Area	1186*584
Routing Protocol	AODV
Traffic Protocol	UDP
Application	CBR
Packet Size At UDP	1500
Packet Size At CBR	1000
Simulation Time	28 min

Table1. Parameters used in the simulation

NAM (Network Animator Visualization):-The NAM consists 25 nodes, where 21, 24 nodes are the Sources and 18, 16 nodes are the Destinations. The node no 0, 4, 9 are the hackers. At zero second node 0 are hacked and it continued till the end of the simulator. The node 9 get to hack at 4 seconds and in 6 second the node move from its fixed position. At one second the source1 and source2 starts delivery the packets to the Destination1 and Destination2 through the intermediate nodes which are shown in figure1.

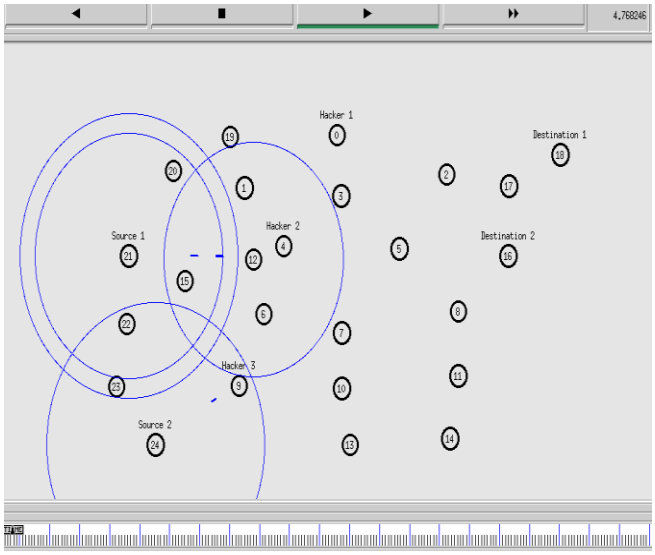

Figure1. Packet moving towards the destination.

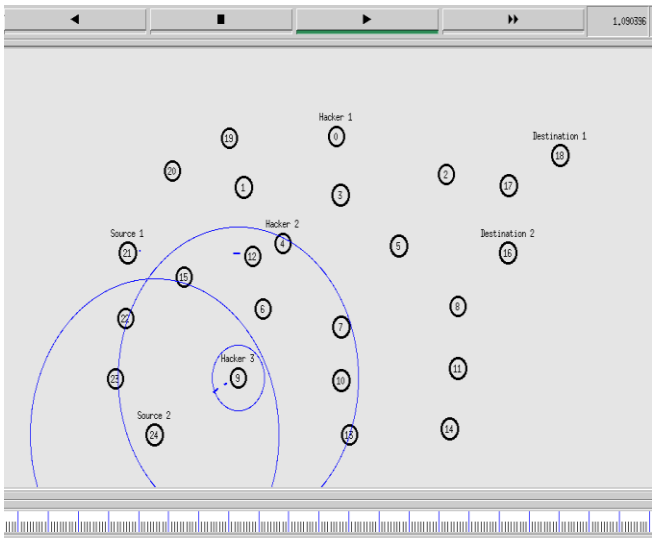

Figure2. Packets are blocked by the hacker from reaching to the destination.

At four seconds the node 9 get activate and packets are blocked to reach the destination2, which is send by source2. Mean time source1 finds the next route to send the packets of the destination1. This whole scenario will represent in the graph of Packet Lost and Packet Received, End to End Delay in packet delivery, Overall Throughput in packet delivery at last Overall Packet Loss.

III. RESULTS

The figure3 represents the overall packet lost and packet received in the two routes. The first route starts at 1 sec, where the green graph represents the packet received to the destination1 having the steady peak of packets send by the source1 are continuously received by the destination1 without any destruction make by the intrusion.

The yellow graph represents the second route which raise up but form the constant flow along with the y-axis because the route is affected by the hacker which remain till the end of the simulator time.

The red and blue graph represents the overall packet lost in the respective route. The packet lost in both the route is quite negligible.

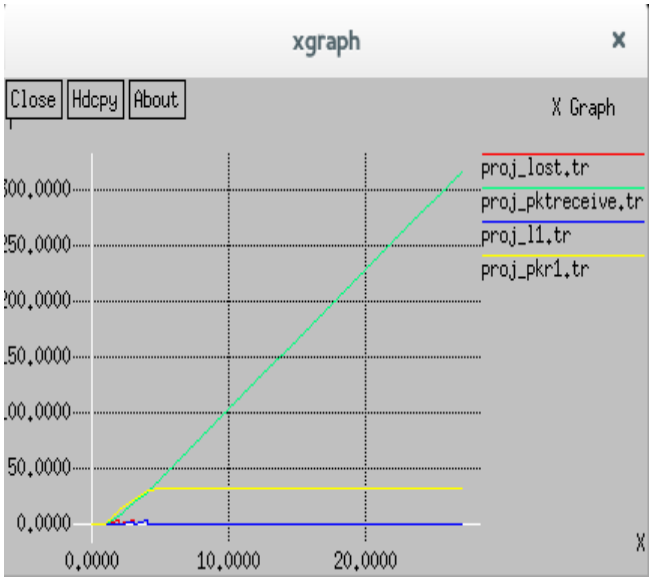

Figure3. The graph represents the packet lost and received in the respective routes.

X-Axis represents the simulator time.
Y-Axis represents the numbers of packets.

The figure4 represents the throughput of the two routes respectively. The red graphs having regular throughput till the end time without affecting by the intrusion. The next route which is represented by the green graph, is affected by the hacker, having the good throughput at initial time but keeps on decreasing at five second it remain constant along x-axis till the end of the simulator.

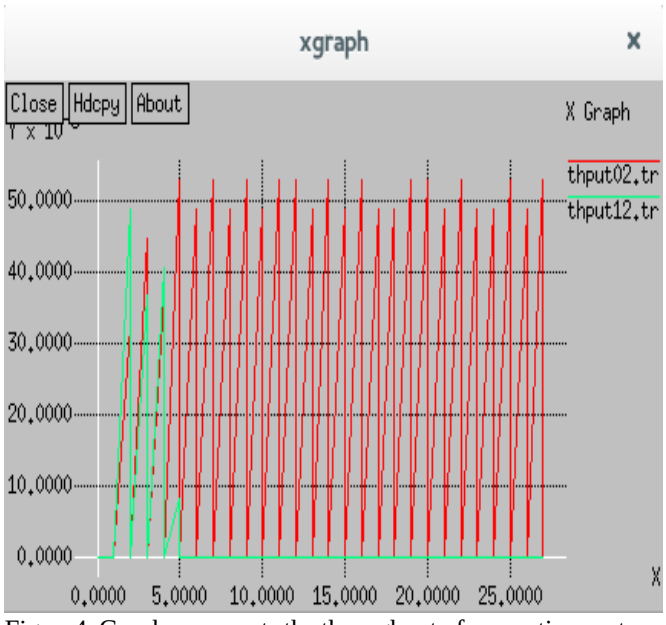

Figure4. Graph represents the throughput of respective routes.

X-Axis represents the simulator time.
Y-Axis represents the overall throughput of the route.

The figure5 represents the packet lost in the respective routes. The green graph remain constant along x-axis due to intrusion into the route but at the initial period graph raised with respect to y-axis because a source take time to find the path to the destination.

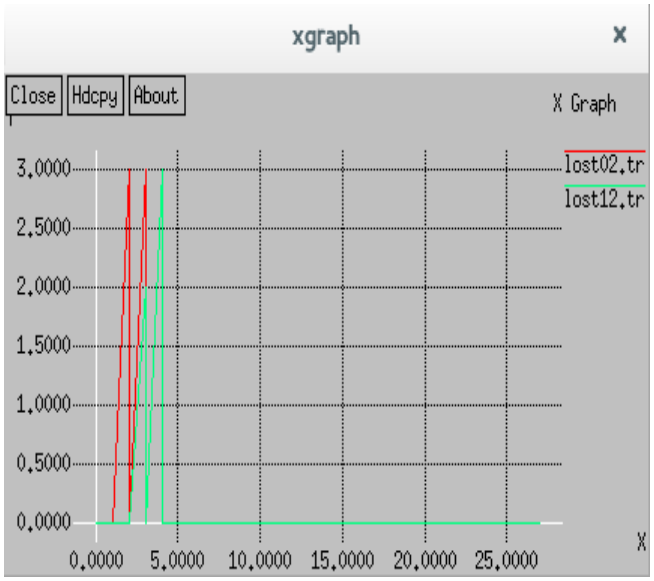

Figure5. The graph represents the packet lost in the route.

X-Axis represents the simulator time.
Y-Axis represents the packet lost in time.

The figure6 represents the packets delay between the two routes. The red graph represents the first route which starts at 1 second. At the initial period the graph raised to the peak at the y-axis, but as the time proceeds there is less and steady fluctuation in graph, this is due to packets are travelling through the intermediate nodes to reached the destination. The green graph raises up and remains constant through-out the simulator time because the second route is interrupted by hackers.

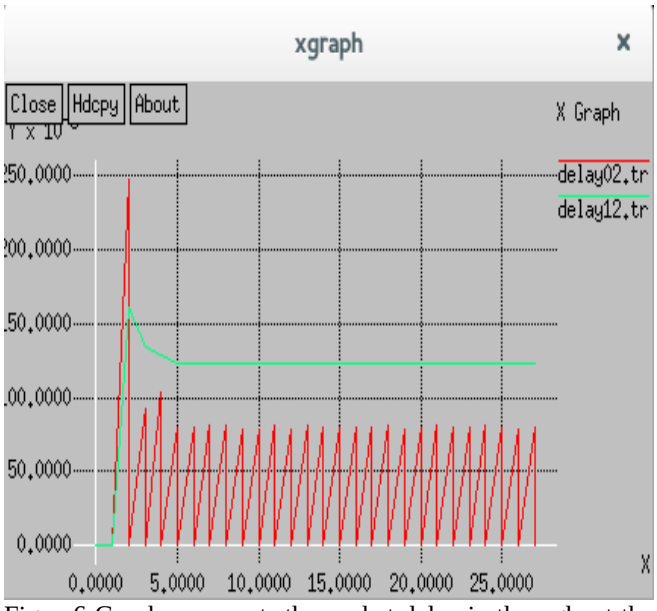

Figure6 Graph represents the packet delay in throughout the route.

X-Axis represents the simulator time.
Y-Axis represents the overall packets delay.

IV. CONCLUSION AND FUTURE WORK

This paper has presented the evaluation of AODV with and without malicious nodes along with the graph. The graph

concludes that there is very less efficiency in packet throughput and packet received when the route is being hacked by the intruder. The path which is free from intrusion having high efficiency of packets received, packet throughput. The packet delay and packet lost is less with respect to the route which hacked by hacker.

In the future work can be evaluating with other routing protocol i.e. DSR, DSDV, TORA etc with and without malicious node.

REFERENCES

[1] Ravinder Ahuja, Alisha Banga Ahuja and Pawan Ahuja "Performance Evaluation and Comparison of AODV and DSR Routing Protocols in Manets under Wormhole Attack" 2013 IEEE Second International Conference on 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013).

[2] Samir R.Das and Mahesh K.Marina "Performance Comparison of Two on-Demand Routing Protocols for Ad Hoc Networks"2001 IEEE Personal Communication.

[3] Mehdi Barati, Kayvan Atefi, Farshad Khosravi, and Yashar Azar Daftari "Performance Evaluation of Energy Consumption for AODV and DSR Routing Protocols in Manet" 2012 IEEE International Conference on Computer and Information Science (ICCIS).

[4] Ibrahim K.Tabash, Nesar Ahmad and Salim Beg et.al "Performance Evaluation of TCP Reno and Vegas over Different Routing Protocols for Manets" 2010 IEEE 4thInternational Symposium on Advanced Network and Telecommunication Systems.

[5] Pragya Gupta ,Sudha Gupta et.al "Performance Evaluation of Mobility Models on Manet Routing Protocols" 2013 IEEE 3rd International Conference on Advanced Computing and Communication Technologies.

[6] Bhabani Shankar Gouda, Chandan Kumar Behera and Ranjit kumar Behera "A Scenario Based Simulation Analysis and Performance Evaluation of Energy Efficiency Enhancement Routing Protocols in Manets" 2013 IEEE.

[7] Dilli Ravilla, Murali Nath R.S and M.L Ravi Chandra; Dr Chandra Shekar Reddy Putta and Dr K Bhanu Prasad et.al "Performance of Ad Hoc Routing Protocols in IEEE 802.11" 2010 IEEE International Conference on Computer and Communication Technologies (ICCCT-10).

[8] Hui Xu "A Unified Analysis of Routing Protocols in Manets" IEEE Transcation on Communication, Vol. 58, No. 3, March 2010.

[9] Laxmi Shrivastava, Sarita S.Bhadauria and G.S Tomar "Performance Evaluation of Routing Protocols in Manets with different traffic loads" 2011 IEEE International Conference on Communication Systems And Network Technologies.

[10] Vasudha Arora and C.Rama Krishna "Performance Evaluation of Routing Protocols in Manets under Different Traffic Loads" 2010 IEEE.

[11] Bello Lawal and Dr. Panos Bakalis et.al "Performance Evaluation of CBR and TCP Traffic Models on Manets Using DSR Routing Protocol" 2010 IEEE IEEE International Conference on Communication and Mobile Computing.

[12] Josh Broch and David A. Maltz "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols"1998 ACM/IEEE InternationalConference on Mobile Computing and Networking (MobiCom).

[13] Narayan Sadagopan "A Framework to systematically Analyze the Impact of Mobility on Performance of Routing protocols for Ad hoc Networks" 2003 IEEE INFOCOM.

[14] Sesha Bhargavi Velagaleti, M. Seetha and S. Viswanadha Raju "A Simulation and Analysis Of Secured AODV Protocol in Mobile Ad Hoc Networks" 2013 IJRET.

[15] Morli Pandya "Improvising Performance with Security Of AODV Routing Protocol for Manets" 2013 IJCA.

[16] Darshana Patel and Vandana Verma "Security Enhacement of AODV Protocol for Mobile Ad hoc Network" 2013 IJAIEM.

[17] Abdul Shabbir and Anasuri Sunil Kumar "An Efficient Authentication Protocol for Security In Mobile Ad Hoc Networks" IJCCT, ISSN (ONLINE): 2231-0371, ISSN (PRINT): 0975-7449, Volume-3.

Devottam Kumar MCA, M.TECH (pursuing) in Computer Science from Rungta College of Engineering & Technology, Bhilai, India.

Prof. Ruhy Khanam CSE Department, Assistant Professor, in Rungta College of Engineering & Technology, Bhilai, India. /