Performance Analysis of AODV using HTTP traffic under Black Hole Attack in MANET

Ekta Barkhodia[1], Parulpreet Singh[2], Gurleen Kaur Walia[3]

Lovely Professional University, Phagwara, India
ektab0@gmail.com, parulpreet89@gmail.com

ABSTRACT

Mobile Ad-hoc Network (MANET) is a collection of wireless mobile nodes dynamically forming a temporary network without the aid of any established infrastructure or centralized administration. The mobility of nodes in MANETs changes frequently which results in changing network topology, due to changing network topology routing in MANETs a challenging task. MANETs are weak against many types of attack, one of the attacks is the black hole attack. In this attack, a malicious node advertises itself as having freshest or shortest path to specific node to absorb packets itself. The effect of black hole attack on ad hoc network using AODV as a routing protocol with Http traffic load will be examined in this research. The performance analysis of AODV reactive protocol is evaluated with respect to throughput and end-to-end delay using OPNET modeller.

KEYWORDS

MANET, AODV, HTTP, OPNET.

1. INTRODUCTION

Mobile Ad-hoc Network (MANET) is a set of wireless mobile nodes. These networks are decentralised system. Here nodes communicate with each other without any centralized access points or base stations. In this type of network, each node acts both as a router and as a host at the same time. Due to the limited transmission range, multiple hops are needed for the data exchange in the network.

Mobile Ad hoc Network is the rapid growing technology from the past 20 years. The gain in their popularity is because of the ease of deployment, infrastructure less and their dynamic nature. MANETs created a new set of demands to be implemented and to provide efficient better end to end communication. MANETs works on TCP/IP structure in order to provide the communication between the work stations. Work stations are mobile, that is why the traditional TCP/IP model needs to be modified, in order to compensate the MANETs mobility to provide efficient functionality of the network. That is why the key research area is Routing. Routing protocols in MANETs is a challenging task, researchers are giving their attention to this area [1].

2. AODV ROUTING PROTOCOL

AODV: AODV is a reactive routing protocol, used to find a route between source and destination. AODV uses three type of messages, route request (RREQ), route reply (RREP) and

DOI : 10.5121/cseij.2012.2308

route error (RERR). In MANET each node has a routing table contains the information about the route to the specific destination.

Route discovery mechanism in AODV- It is used to find the route between the nodes. We can understand this mechanism with the help of an example. When a node "E" wants to start transmission with another node "P", then it will generate a route request message (RREQ). This message is propagated to other nodes. This control message is firstly forward to the neighbours, and that neighbour node forwards the control message to their neighbours' nodes. This process is goes on and on until destination node is located. Once the destination node is located, they generate a control message route reply message (RREP) to the source node. When RREP reaches the source node, a route is established between the source node "E" and destination node "P". Once the route is establish node "E" and "P" can communicate with each other [1].

Route error in AODV- When there is an error occur between the nodes, then the RERR message is sent to the source node. We can understand this mechanism by an example. When RREQ message is broadcasted for finding destination node i.e. from node "E" to the neighbours nodes, at node "G" the link is broken between "G" and "P", so a route error RERR message is generated at node "E" and transmitted to the source node informing the source node that there is a route error [1].

HTTP- In the simulation environment of HTTP traffic effect evaluation, scenarios have been implemented separately on HTTP heavy traffic load. HTTP traffic has been selected because of its importance in the Internet applications. It has been used with Web to provide secure communication. The simulation attempts to show the effect of HTTP traffic load on the routing protocols. It is assumed that the network includes 40 nodes with speed of 10 m/s. For each investigated scenarios, the performance parameters throughput and delay have been computed and tabulated as shown in Table.

3. BLACK HOLE ATTACK

Black hole attack is one of the possible attacks in MANET. In black hole attack, a malicious node sends the route reply message to the source node in order to advertise itself for having the shortest path to the destination node. The malicious node reply will be received by the requesting node before the reception of the any other node in the network. When this route is created, malicious node receives the data packet now it's up to the malicious node whether to drop all the data or forward it to the unknown locations [3]. Black hole attack in AODV can be describe into two types-

3.1. Internal Black Hole Attack

As its name implies that it's present in the network internally. Here the internal malicious node fits in between the routes of source and destination. As its present internally so this node make itself an active data route element. At this stage it is now capable of conducting attack with the start of data transmission. This is called an internal attack because here node itself belongs to the network internally. Internal attack is more severe to attack because here malicious node present inside the network actively.

3.2. External Black Hole Attack

As its name implies that this type of attack present externally outside the network. External attacks don't access to the network traffic or create trafficking in the network. External attack can be the internal attack once it gets control of the internal malicious node and then control it to attack other nodes in MANET.

4. RELATED WORK

To protect against the Black Hole Attack, five methods have been proposed. In [4], the method requires the intermediate node to send a RREP packet with next hop information. When a source node receives the RREP packet from an intermediate node, it sends a Further Request to the next hop to verify that it has a route to the intermediate node who sends back the RREP packet, and that it has a route to the destination. When the next hop receives Further Request, it sends Further Reply which includes check result to source node. Based on information in Further Reply, the source node judges the validity of the route. In [6], here in this method requires the intermediate node to send Route Confirmation Request (CREQ) to the next node. Then, next hop node receives CREQ, and look up its cache for a route the destination. If it has one, it sends Route Confirmation Reply (CREP) to source node with its route information. The source judges whether the path in RREP is valid by comparing the information with CREP. In these methods, the operation is added to routing protocol. This operation can increase the routing overhead resulting in performance degradation of MANET which is bandwidth-constrained.

A malicious or corrupted node has to increase the destination sequence number in order to convince the source node that the route provided is sufficient. Based on this analysis, the authors propose a statistical based anomaly detection approach to detect the black hole attack, based on differences between the destination sequence numbers of the received RREPs. Importance of this approach is that it can detect the attack at the least price without any extra routing traffic, and it doesn't require any modification in the existing protocol. However, false positives are the main drawback due to anomaly detection [7].From the characteristics of the Black Hole Attack, we need to take a destination sequence number into account. In [8], feature related to the destination sequence number has not been taken into account as the feature to define the normal state.

5. SIMULATION TOOL

This research is conducted using discrete event simulation software known as OPNET Modeler, which is just one of several tools provided from the OPNET Technologies suite. In order to undertake the experimental evaluation, the most recently available version, namely the OPNET Modeler 14.5 has been adopted in our study [5]. OPNET is one of the most extensively used commercial simulators based on Microsoft Windows platform, which incorporates most of the MANET routing parameters compared to other commercial simulators available.

The network entities used during the design of the network model are wireless server, application configuration, profile configuration, mobility configuration and workstations (nodes). The parameters that have been used in the following experiments are summarized in Table I.

Table 1. Simulation Parameter

Simulation parameter	value
Simulator	OPNET 14.5
Area	1000m x1000m
Network Size	40 nodes
Mobility Model	Random way point
Traffic type	HTTP (heavy browsing)
Simulation Time	600 sec
Address mode	IPv4
Packet Reception power threshold	-95

6. PERFORMANCE METRICS

End-to-End Delay: - The end-to-end delay is the time needed to traverse from the source node to the destination node in a network. End-to-end delay assesses the ability of the routing protocols in terms of use- efficiency of the network resources.

Throughput: - The average rate at which the data packet is delivered successfully from one node to another over a communication network is known as throughput. The throughput is usually measured in bits per second (bits/sec). A throughput with a higher value is more often an absolute choice in every network. Mathematically, throughput can be defined by the following formula.

Throughput= (number of delivered packet * packet size)/total duration of simulation

7. SIMULATION RESULTS AND ANALYSIS

A network size of 40 nodes and the file size of 50,000 bytes (for HTTP) in a (1000×1000) square meter area.

This paper represent the scenarios of 40 nodes which are simulated by taking Reactive routing protocols AODV and showing graphically their delay, throughput. The simulation period is 600 seconds in all the cases.

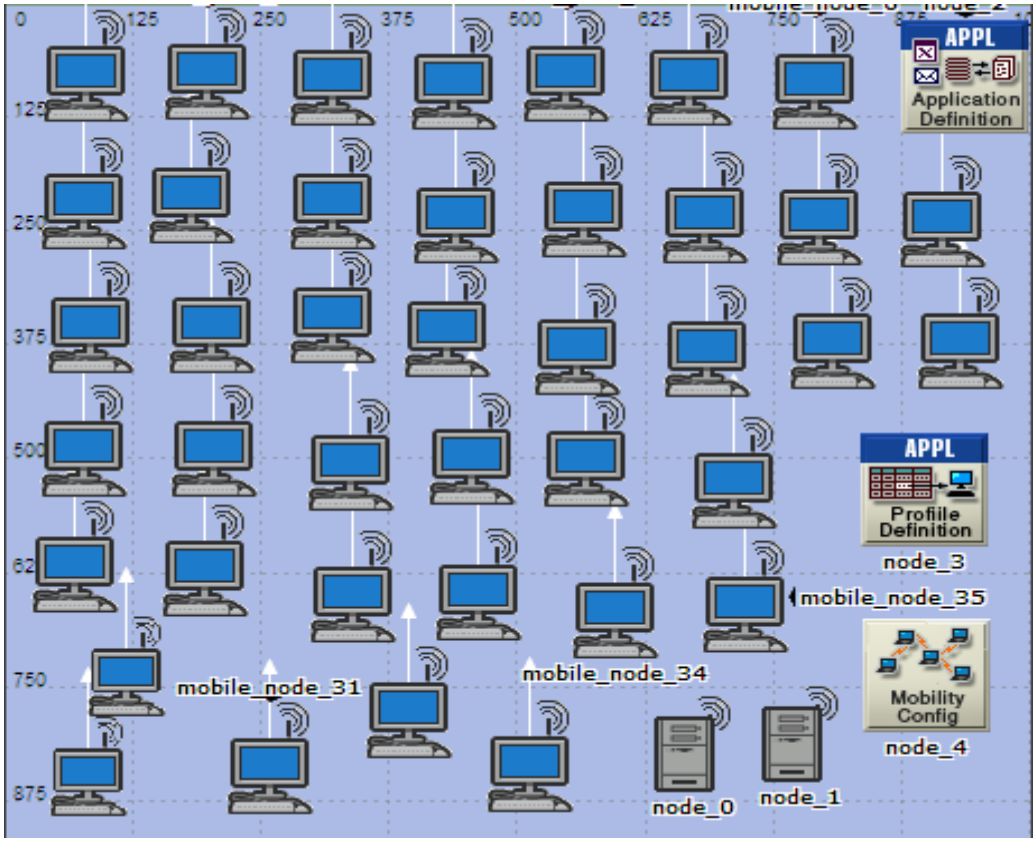

Figure 1. Simulation scenario having 40 nodes

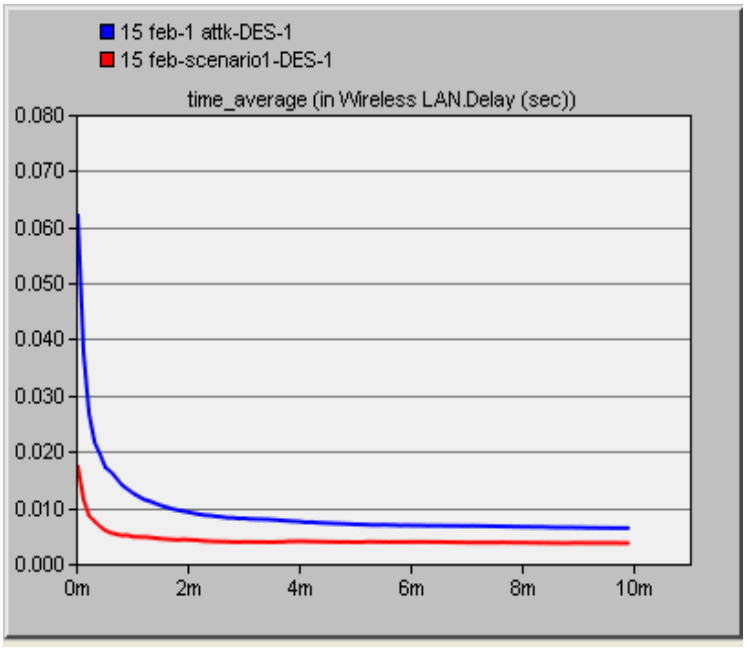

Figure 2. Comparison of Average end to end delay of normal AODV with 1 attacker node

In the above figure comparison of end to end delay of normal AODV with 1 attacker node is shown which gives that in case of normal AODV the delay is much less than that of 1 attacker node.

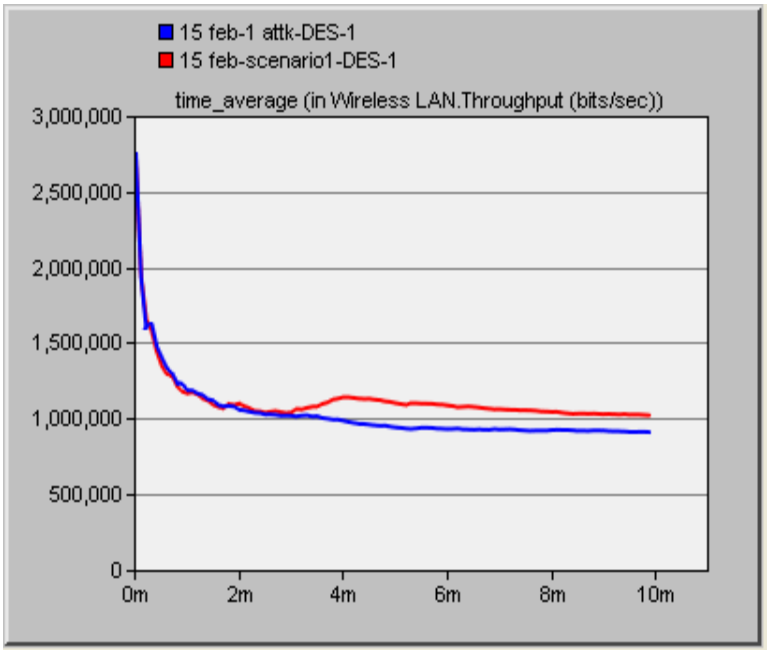

Figure 3.Comparison of Throughputs of normal AODV with 1 attacker node

In the above figure comparison of throughput of normal AODV with 1 attacker nodes is shown which gives that the throughput of 1 attacker node is higher than the normal AODV.

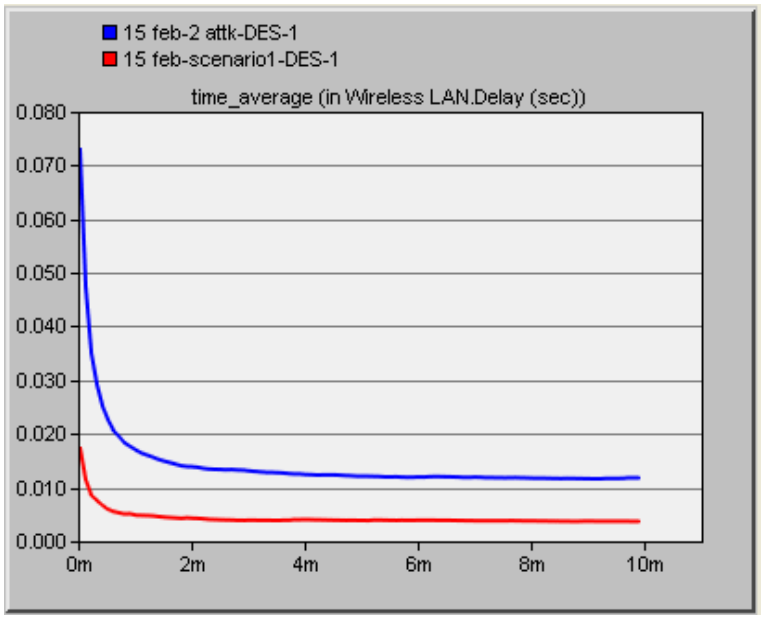

Figure 4. Comparison of Average end to end delay of normal AODV with 2 attacker node

In the above figure comparison of end to end delay of normal AODV with 2 attacker nodes is shown which gives that the end to end delay of 2 attacker nodes is more than the normal AODV.

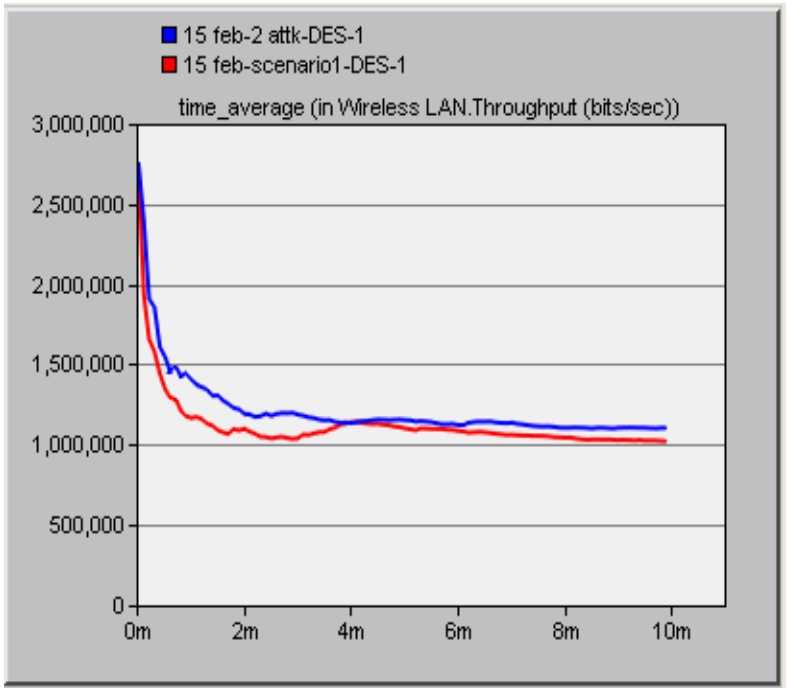

Figure 5. Comparison of Throughputs of normal AODV with 2 attacker node

In the above figure comparison of throughput of normal AODV with 2 attacker nodes is shown which gives that the throughput of 2 attacker nodes is higher than the normal AODV as shown in case of 1 attacker node.

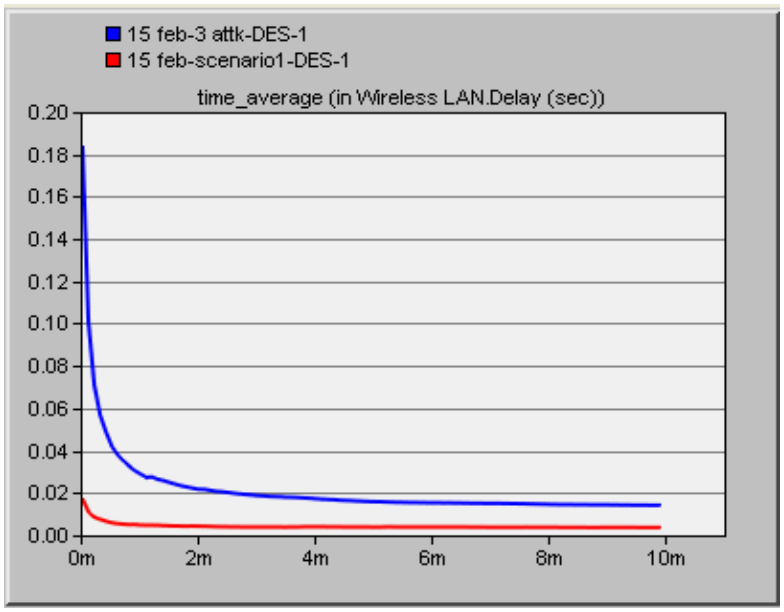

Figure 6. Comparison of Average end to end delay of normal AODV with 3 attacker nodes

In the above figure comparison of end to end delay of normal AODV with 3 attacker nodes is shown which gives that the end to end delay of 3 attacker nodes is much more than as compare to the normal AODV.

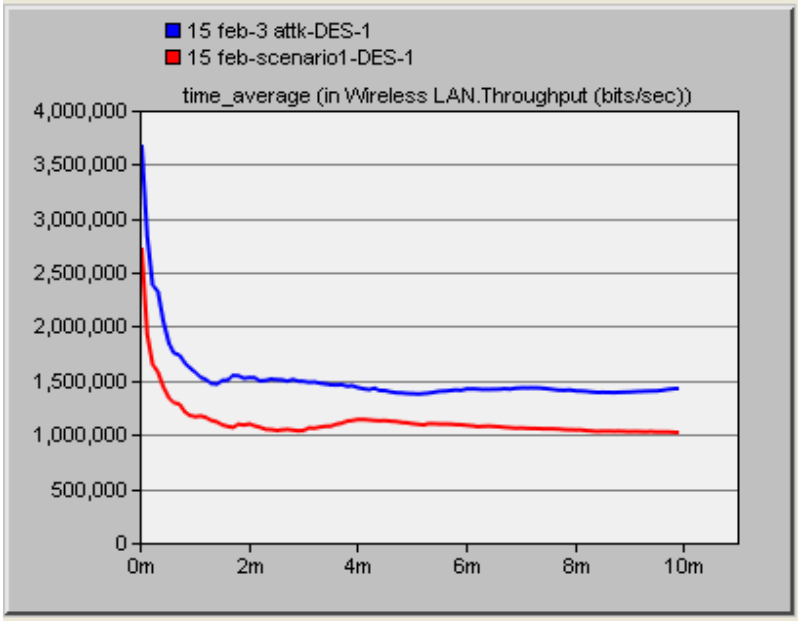

Figure 7. Comparison of Throughputs of normal AODV with 3 attacker nodes

In the above figure comparison of throughput of normal AODV with 3 attacker nodes is shown which gives that the throughput of 3 attacker nodes is much higher than the normal AODV as shown in case of 2 attacker nodes.

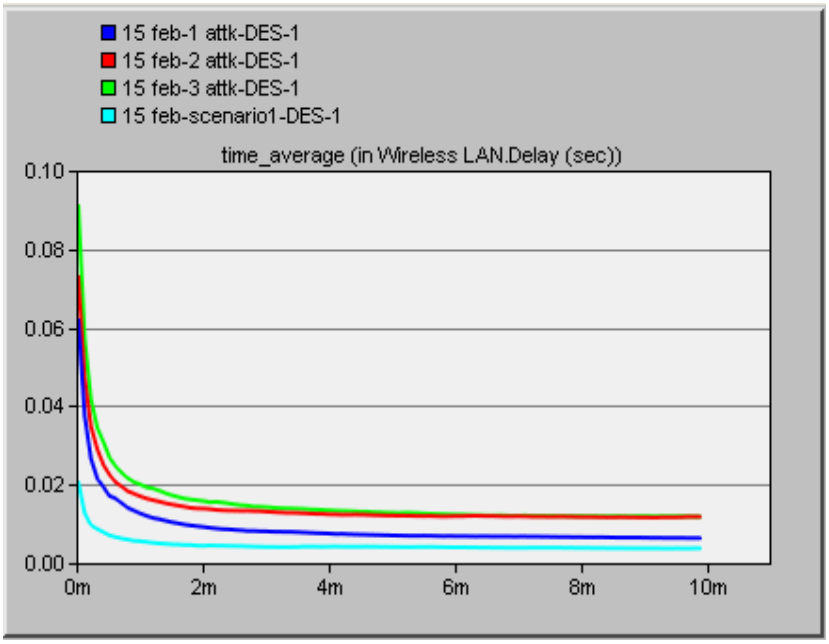

Figure 8. Comparison of Average end to end delay of normal AODV with 1, 2, 3 attacker nodes

As shown in the above figure delay of 3rd attacker node is highest while lowest in case of normal AODV.

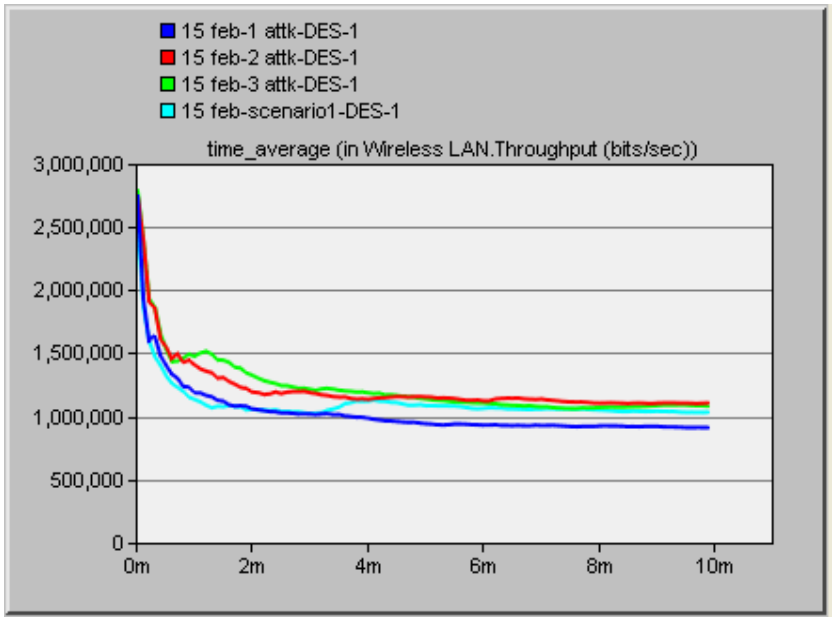

Figure 9. Comparison of Throughputs of normal AODV with 1, 2, 3 attacker nodes

As shown in the above figure the throughput of 3rd attacker node is highest while lowest in case of normal AODV routing protocol.

8. CONCLUSION

The key observations of the research are as follows.

In this paper the performance is made under the presence of malicious node. As the number of malicious nodes increases the average end to end delay is also increases while throughput can be varied as the number of malicious nodes increases. As the number of malicious nodes increases throughput will be increases. In the presence of 3rd attacker node the value of throughput will be highest.

Table 2- Resultant value

	Delay (sec)	**Throughput (bits/sec)**
Normal AODV	0.018	2,500,000
1 attacker	0.062	2,750,000
2 attacker	0.073	2,750,000
3 attacker	0.18	3,700,000

Acknowledgement

The authors would like to thank OPNET for modelling tool support through their OPNET University Program.

REFERENCES

[1] I.U. Shoaib Rehmaan, "Analysis of Black hole Attack on MANET using different MANET routing protocols". Thesis no: MEE-2010-2698 June, 2010.
[2] K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007
[3] G. A. Pegueno and J. R. Rivera, "Extension to MAC 802.11 for performance Improvement in MANET", Karlstads University, Sweden, December 2006
[4] H. Deng, W. Li, and D. P. Agrawal, "Routing se curity in ad hoc networks," IEEE Communications Magazine, vol. 40, no. 10, pp. 70-75, Oct. 2002.
[5] Opnet Technologies, Inc. "Opnet Simulator," Internet: www.opnet.com, date last viewed: 2010-05-05
[6] S. Lee, B. Han, and M. Shin, "Robust routing in wireless ad hoc networks," in ICPP Workshops, pp.73, 2002.
[7] Kurosawa, S., Nakayama, H., et al., "Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method," Proc. Int'l. J. Network Sec., 2006.
[8] Y. A. Huang, W. Fan, W. Lee, and P. S. Yu, "Crossfeature analysis for detecting ad-hoc routing anomalies," in The 23rd International Conference on Di tributed Computing Systems (ICDCS'03), pp. 478-487, May 2003.

Authors

Ekta Barkhodia received her Bachelor's degree in Electronics from BRCM College of engineering and technology, Haryana, India. Now, she is pursuing her M.Tech degree in Electronics and communication from Lovel y Professional University, Phagwara, India. Her areas of interest are MANET and Wireless Network.

Parulpreet Singh received his Bachelor's degree in Electronics from CEM, Kapurthala, Punjab, India. Now, he is pursuing his M.Tech degree in Electronics and communication from Lovely Professional University, Phagwara, India. His areas of interest are MANET and Wireless Network.