International Journal of
Applied Mathematics,
Electronics and Computers

Advanced Technology and Science

ISSN: 2147-8228 www.atscience.org/IJAMEC **Original Research Paper**

Analysis of Current Routing Attacks in Mobile Ad Hoc Networks

Hande BAKİLER*[1], Aysel ŞAFAK [2]

Accepted 15th August 2014

Abstract: Mobile ad hoc networks (MANET) has no fixed infrastructure and depends on nodes to perform routing of data packets. MANET nodes are highly self-organized even with a collection of few mobile nodes. Security is an important issue for mobile ad hoc networks. Even though mobile ad hoc networks have many advantages over the traditional wired network, when it comes to security it poses an immense set of threats. The scope of this project is to study about Misbehavior Node attack, Byzantine attack and Pulse Jammer attack on Reactive Routing Protocol i.e. Ad Hoc On Demand Distance Vector (AODV) on MANET simulation environment. To perform the simulations we used OPNET modeller 14.5 as the network simulator for our proposed work. The results showed that MANET posed a high security risk attack either from internal or from external attack.

Keywords: *MANET, AODV, Misbehaving Node Attack, Byzantine Attack, Pulse Jammer Attack, OPNET.*

1. Introduction

A mobile ad hoc network [1, 2] is the new advancement in the field of telecommunication technology which changes the entire concept of communication. The speciality of this technology is that it could be managed even in lack of fixed infrastructure. This technology is efficient, effective, quick, and easy to deploy. MANET consists of independent mobile nodes connected by wireless medium. Each mobile node acts as a host, operates as an end system and also acts as a router for all nodes in the network.

2. AODV (Ad-Hoc On Demand Distance Vector)

This is an on demand routing protocol for wireless ad hoc mobile networks. It works by constructing routes between nodes on demand by source nodes and are kept until they are not needed. Requests for routes have a time to live which stop's flooding of route requests and there is a time limit of double the TTL before it can be re-requested [3].

3. Misbehavior Nodes Attack Scenario

First attack is misbehaving node attack [4, 5]. Misbehaving node attack is implemented on a normal network with 30 nodes, where the numbers of misbehaving nodes are kept as 5 nodes.
The purpose of misbehaving node is to drop the packets and stop forwarding the packets for the other nodes in the network. Dropping packet occurs for many reasons. Misbehaving node might want to reserve the battery power of its own. It consuming a lot of bandwidth and it is not collaborating with other nodes in the network.

4. Byzantine Attack Scenario

Second scenario is Byzantine attack [6, 7]. Five attackers are placed in the same network.In this attack, a compromised intermediate node or a set of compromised intermediate nodes works in collusion and carries out attacks such as creating routing loops, forwarding packets on non-optimal paths and selectively dropping the packets which results in disruption or degradation of the routing services.

5. Pulse Jammer Attack Scenario

Third attack is jammer attack [8]. Pulse jammer attack is implemented on a normal network. Five pulse jamming nodes are placed in the network with 30 nodes at different locations. As jammer attack generates noise on the wireless radio frequency medium to stop the communication in order to the trigger network, it causes packet lost or corrupt of packet.

6. Simulation Tool

Table 1. Simulation parameters

Simulation Parameter	Value
Simulator	OPNET 14.5
Area	800x800 (m)
Network Size	30 Nodes
Mobility Model	Random Waypoint
Traffic Type	FTP, Email
Simulation Time	600sec.
Data Rate of Each Node	11 Mbps
Packet Reception Power Threshold	-95 dBm

7. Performance Metrics

Performance metrics are well organized with respect to security attack against MANET network. Performance metrics make network's behaviour more comprehensible.

7.1. Throughput

The throughput of each scenario for each attack which will help understanding the results are used for analysing the network. The average rate at which the data packet is delivered successfully from

[1-2] Electrical & Electronics Engineering Department, Institute of Science and Engineering, Başkent University, Ankara/Turkey
* *Corresponding Author: Email: 21020013@baskent.edu.tr*

Note: This paper has been presented at the International Conference on Advanced Technology&Sciences (ICAT'14) held in Antalya (Turkey), August 12-15, 2014.

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 characterized as in equation.

Throughput=Number of delivered packet*Packet size*8/Total duration of simulation

7.2. Data Dropped

Data dropped shows that how many packets are successfully sent and received across the whole network. It also explains the number of data dropped during the transmission due to interference from the other devices.

7.3. Delay

The packet end to end delay is the average time of the packet passing through the network. It includes all over the delay of the network like transmission time delay which occurs due to routing broadcastings and buffer queues. It also includes the time of generating packet from source to destination and express in seconds.

7.4. Network Load

Network load represents the total data traffic (in bits/sec) received by the entire wlan from higher layers of the MACs that is accepted and queued for transmission.

8. Simulation Result and Analysis

In this section, we briefly explain throughput, packet dropped, delay and load metric parameters. The results are compared with their normal network scenarios where no malicious activities take place.

8.1. Scenario 1: Performance of AODV Routing Protocol under Misbehavior Nodes Attack

Five misbehaving nodes are placed on the network to adversely affect the network traffic. The misbehaving nodes drop the packets and stop forwarding them to the other nodes.

8.1.1. Delay

Figure 1 shows the network delay on the normal network traffic with the average value of 15.884 seconds and later with misbehaving nodes in the network, it shows the network delay with the average value of 19.587 seconds.

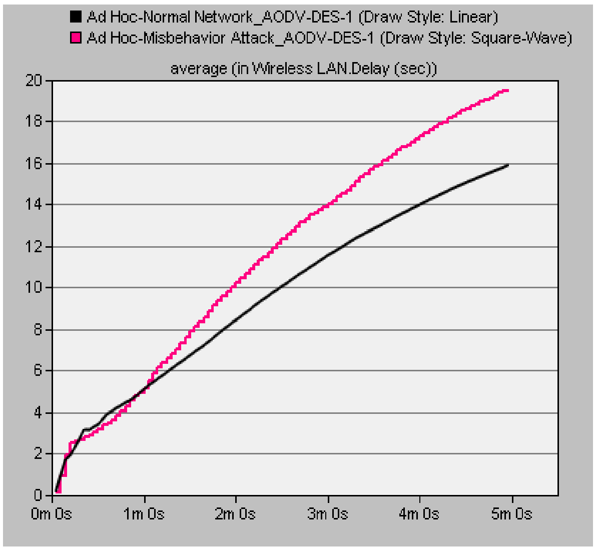

Figure 1. Delay of the normal network and with misbehaving nodes in the network

The delay increases in presence of the misbehaving nodes in the network when it is compared to the normal network. It starts to increase at the beginning of the simulation in the misbehaving nodes scenario.

We can say that due to the abnormal activities and due to the misbehaving nodes, the network becomes more vulnerable which reflect the need of confidently, availability and authentication on the network.

8.1.2. Network Load

Figure 2 shows that the normal network load is recorded as 2,113,504 bits/sec. On the other hand, with misbehaving nodes in the network the network load is noted as 1,931,240 bits/sec.

It is clearly seen in the network result that the network load with misbehaving nodes decreases when it is compared to the normal network. The misbehaving nodes act maliciously to drop the packets and to stop forwarding the packets to the other nodes and they consume a lot of bandwidth.

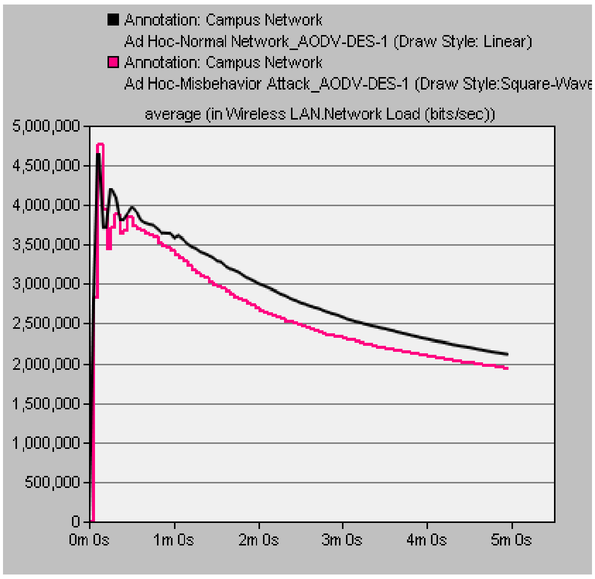

Figure 2. Network load of the normal network and with misbehaving nodes in the network

Throughput

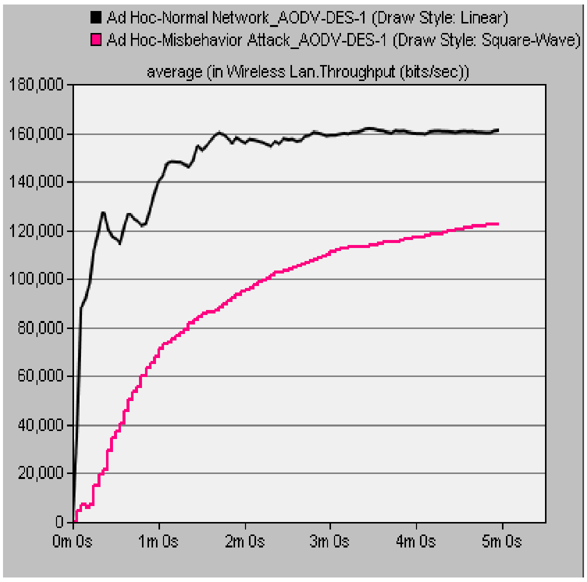

Figure 3. Throughput of the network nodes with normal traffic and with misbehaving nodes in the network

The throughput result is more clearly seen through the graph of the nodes in the network.

The throughput result shows that in the presence of the misbehaving nodes, the transmission degrades as misbehaving nodes drop the data and they are not coloration in the network.

Figure 3 represents the throughput on the network nodes with normal traffic and with misbehaving nodes.

The throughput of the network nodes with normal traffic is noted as 161,036 bits/sec and later with misbehaving nodes in the network it is noted as 122,378 bits/sec at the duration time of simulation 300 seconds.

As the throughput shows that the misbehaving nodes start dropping the packets when the simulation start compare to the normal network. If the misbehaving nodes start to act maliciously and prevent forwarding the packets on time to the other nodes, the network performance degrades.

8.1.3. Data Dropped (Retry Threshold Exceeded)

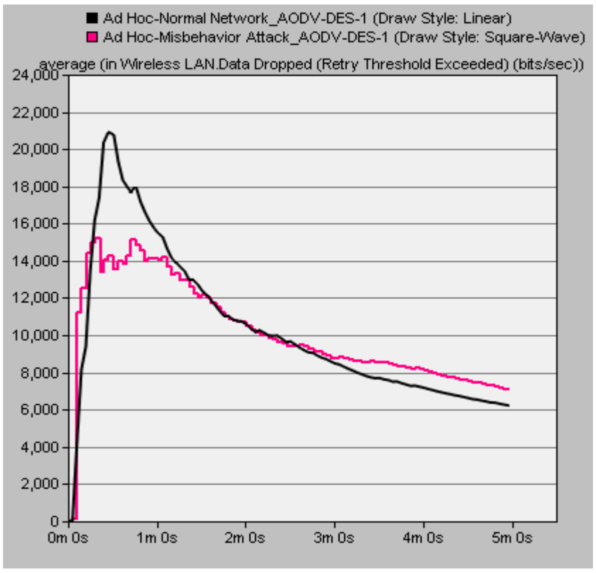

Figure 4. Data dropped of the normal network and with misbehaving nodes in the network

Figure 4 shows that data dropped average value is 6,228 bits/sec for the normal network traffic. On the other hand, with misbehaving nodes in the network the data dropped recorded as 7,089 bits/sec average value.

As misbehaving nodes do not forward packet to the other nodes and drop packet increased, the network lead to deadlock in terms of performance. These activities lead network to congestion and decrease it performance.

8.1.4. Retransmission Attempts

In Figure 5, we analyse the retransmission attempts of the entire network with and without misbehaving nodes.

The normal network retransmission attempts result is recorded with the average value of 0.7838 packets and later with misbehaving nodes in the network, the retransmission attempts result is noted as 0.8266 packets.

Retransmission attempts occurred in the network when delivery of the packets is dropped or lost without reaching the destination nodes. Total number of retransmission attempts by all WLAN MACs in the network until either packet is succesfully transmitted or it is discarded as a result of reaching short or long retry limit. Retransmission attempts increases in the presence of the misbehaving nodes shown in Figure 5.

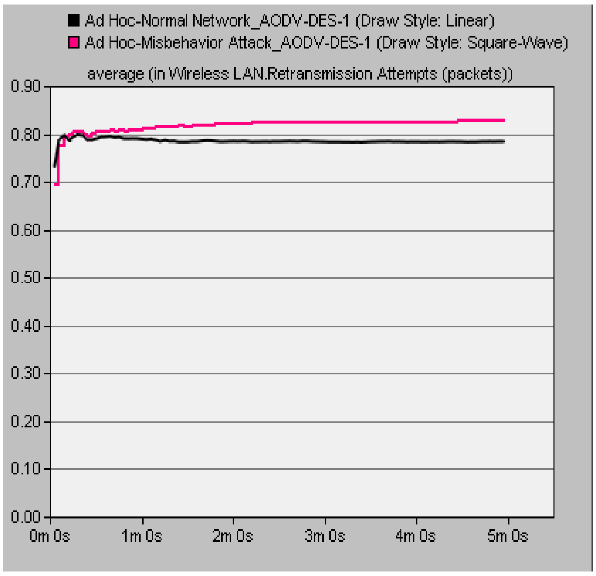

Figure 5. Retransmission attempts result of normal network and with misbehaving nodes in the network

8.2. Scenario 2: Performance of AODV Routing Protocol under Byzantine Attack

Five Byzantine nodes are deployed in the network. These nodes work as cooperation to launched the attack against the target network. Byzantine attacks are hard to detect.

8.2.1. Delay

Figure 6 shows the normal network delay with the average value of 15.884 seconds and later with Byzantine nodes in the network it shows the network delay with the average value of 20.775 seconds.

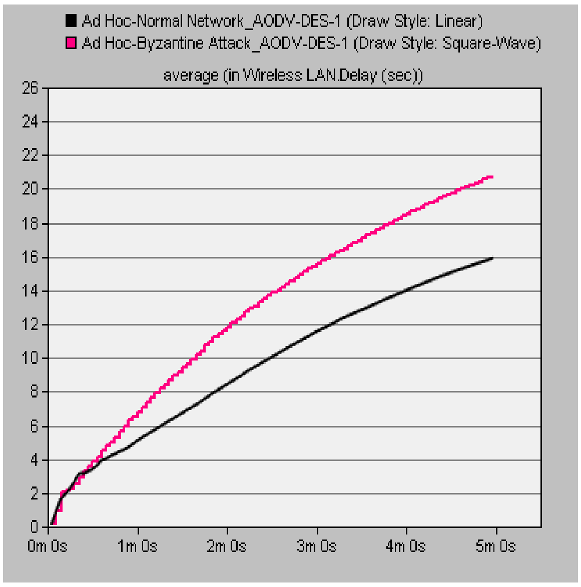

Figure 6. Delay of the normal network and with Byzantine nodes in the network

It shows that the increase in delay will affect the reliability of the network and takes the network in to the congestion deadlock. The delay increases systematically to higher level by placing the Byzantine nodes in the network. The reason for this situation is because even though all nodes using the same routing protocol, the Byzantine nodes drop the packets in the network and these kind of malicious activities degrade the network routing services.

8.2.2. Network Load

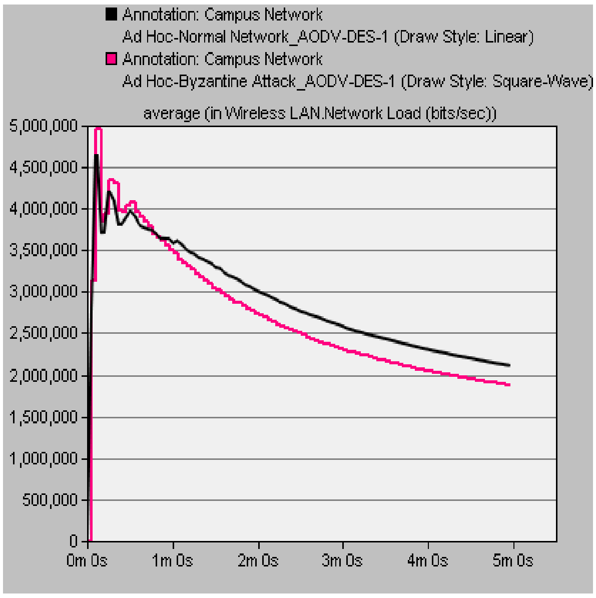

Figure 7. Network load of the normal network and with Byzantine nodes in the network

Figure 7 shows that the network load of the normal network is noted as 2,113,504 bits/sec and with the Byzantine nodes in the network it is noted as 1,878,898 bits/sec. The Byzantine nodes drop the packets and not forwarding the packets for the other nodes. When malicious nodes activate themselves, the Byzantine attack spoil the transmission and the network traffic suffer badly.

8.2.3. Throughput

The throughput result is examined through the graph of the nodes in the network. Comparison of the nodes throughput with the normal network and with the Byzantine nodes attack is shown in the diagram.

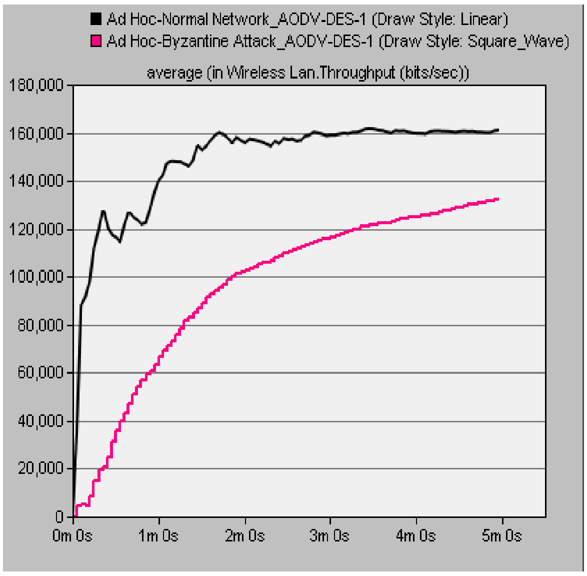

Figure 8. Throughput of the network nodes with normal traffic and with Byzantine nodes in the network

Analysis on Figure 8 shows that the throughput of the normal network nodes average value is 161,036 bits/sec. On the other hand, the network with the Byzantine nodes shows that the network nodes throughput average value is 132,491 bits/sec. The graph represents that the network performance reduces because of the malicious attack.

8.2.4. Data Dropped (Buffer Overflow)

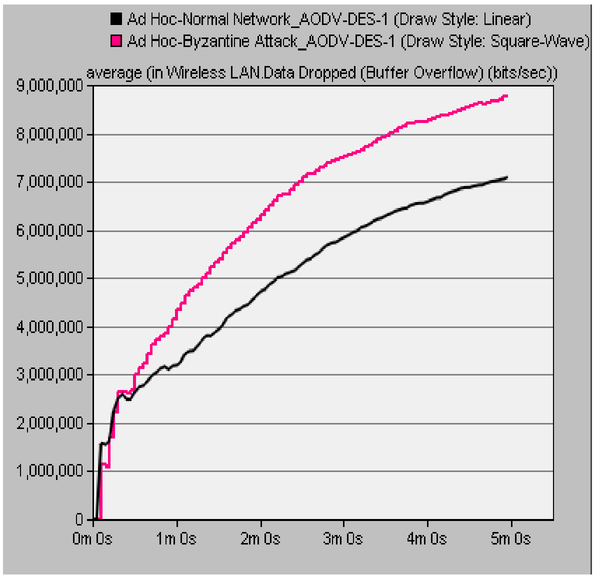

Figure 9. Data dropped of the normal network and with Byzantine nodes in the network

The data dropped is shown in Figure 9 of the normal network traffic and with Byzantine nodes in the network. The data dropped of the normal network is noted as 7,084,170 bits/sec and with the Byzantine nodes in the network it is noted as 8,778,950 bits/sec. This clearly shows that malicious nodes are the Byzantine nodes which were placed in the network. They are not performing their duties, they are missing the packets and not forwarding the require packets to the other nodes in the network.

8.2.5. Total Packets Dropped in AODV Routing Protocol

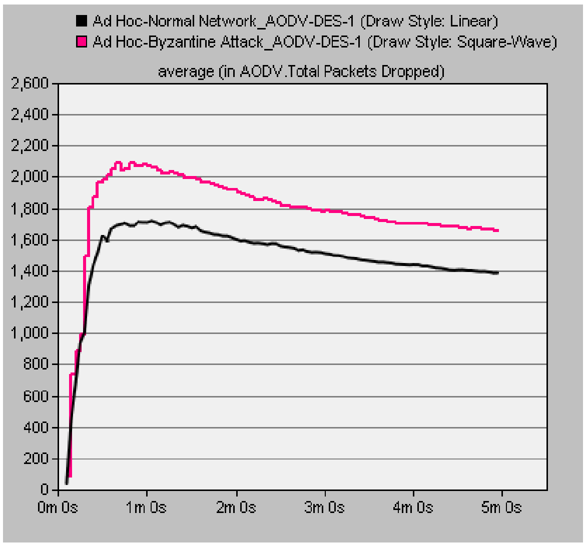

Figure 10. AODV routing total packets dropped of the normal network and with Byzantine nodes in the network

In Figure10, the total packets dropped in AODV routing for the normal network is noted as 1,383 packets and with the Byzantine node on the network it is noted as 1,651 packets.

Because of the malicious activities of the Byzantine nodes, in AODV routing total packets dropped average value for the network with Byzantine nodes is more than the average value of the normal network. When no route is found to the destination, the node drops the packets queued to the destination. This statistic represents the total number of application packets discarded by all nodes in the network.

8.3. Performance of AODV Routing Protocol under Pulse Jammer Attack

Trajectory of the pulse jammer is configured as "vector". Altitude is changed to 12 instead of 0, because on 0 altitude the surface of the earth curves on it and it affects the pulse jammer to transmit signals. Jammer band base frequency is set to 2,402, jammer bandwidth is set to 100,000 and transmitter power is set to 0.001. We compare the results under a number of parameters.

8.3.1. Delay

Figure 11 shows the normal network traffic delay with the average value of 15.884 seconds and later with the jamming nodes in the network it shows the network delay with average value of 20.856 seconds.

The delay increases systematically to higher level by placing the jamming nodes in the network. We can say that jamming nodes generates noise on the wireless radio frequency medium to stop the communication, make the network more vulnerable and prevent the MANET nodes to continue the transmission on the network.

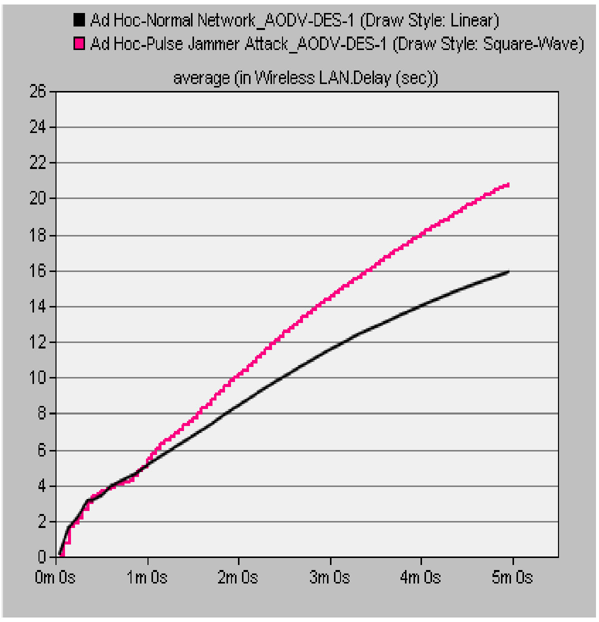

Figure 11. Delay of the normal network and with jamming nodes in the network

8.3.2. Network Load

The function of jammer is to deny the network transmission services to authorized users by generating noise on the wireless medium in order to block the access for authorized nodes.

In Figure 12, we analyse the network load of the entire network with and without intelligent pulse jammer. The normal traffic network load is recorded as 2,113,504 bits/sec and later with jamming nodes in the network, the network load is noted as 1,613,227 seconds. There is a difference between the normal network and with the jamming nodes in the network. Jamming nodes clearly reflects the availability and reliability of MANET nodes in terms of security.

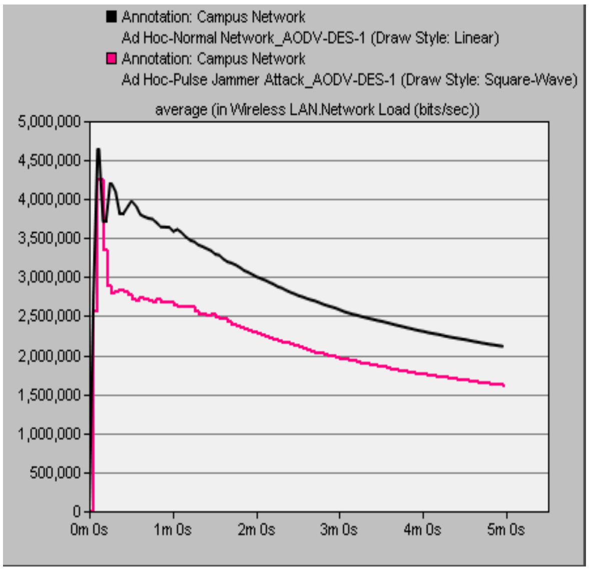

Figure 12. Network load of the normal network and with jamming nodes in the network

8.3.3. Throughput

The throughput of the jammer attack reduces the traffic on the network when it is compared to the normal network traffic. There is significant traffic destruction of the packets transmission on the network when applying a pulse jammer attack.

Figure 13 shows that the normal network throughput average value is 5,086,809 bits/sec and later with jamming nodes in the network, it shows that the network throughput average value is 3,880,674 bits/sec. Therefore we can say that pulse jammer attacks use the wireless medium and decrease the network traffic throughput.

The experiment of the pulse jammer attack shows that the jammer attack is harmful for the network as jammer can easily break down the communication in the network nodes.

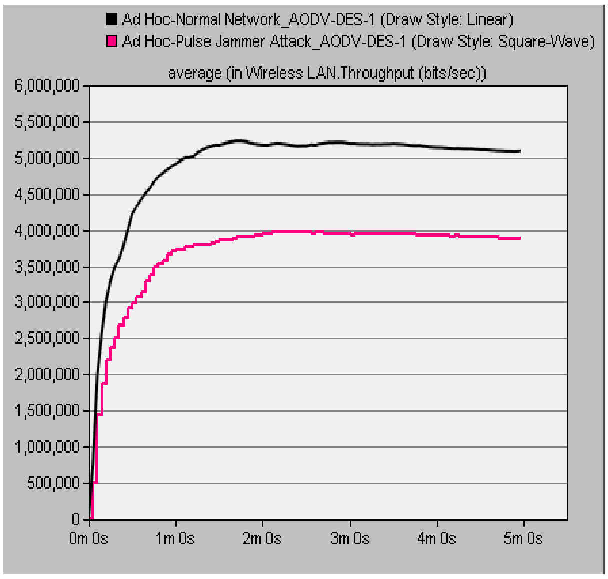

Figure 13. Throughput result of the jamming attack on the network

8.3.4. Data Dropped (Retry Threshold Exceeded)

As shown in Figure 14 for the normal network and the network with jamming nodes, the data dropped of the normal network is recorded as 6,228 bits/sec, whereas it is recorded as 18,599 bits/sec for the network with jamming nodes.

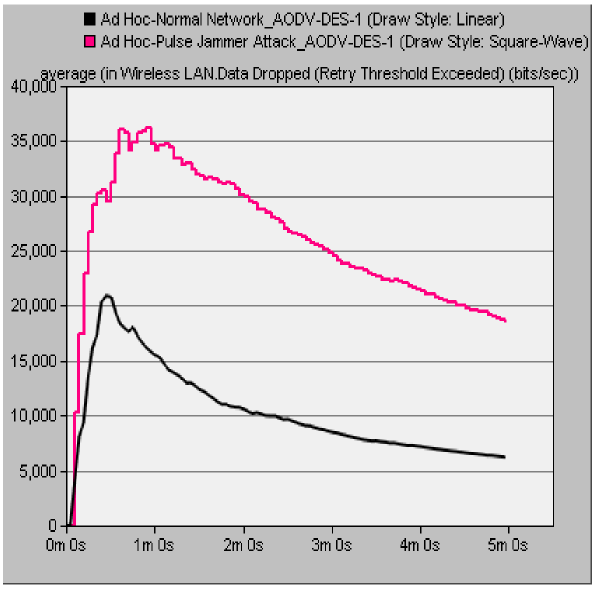

Figure 14. Data dropped of the normal network and with jamming nodes in the network

Total higher layer data traffic dropped by all the wlan MACs in the network as a result of consistently failing retransmissions.
The graph shows that AODV routing protocol with jammer attack had a severe effect on the network data dropped. The intelligent pulse jammer attack on AODV routing shows a significant result. The pulse jamming nodes increases the data dropped of the entire network by generating noise in the wireless medium and reduce the reliability of the network.

9. Conclusion

In this research, the simulation study focuses on three attack scenarios, which are Misbehavior Node attack, Byzantine attack and Pulse Jammer attack. The aim is to look at the network performance under these three attacks. The normal network is compared with the networks which contain misbehaving nodes, jamming nodes and Byzantine nodes in terms of performance metrics, i.e., delay, network load, throughput, data dropped and retransmission attempts by using AODV routing protocol. Jammer attack generates noise on the wireless radio frequency medium and cause corruption of the packets. Misbehaving nodes attack stops performing the basic task. And Byzantine attack drops and mis-routes the forwarding packets to disrupt the routing service. Several security breaches are represented under these three attack models using OPNET. They give significant results for the network security. Based on the research and analysis of the simulation results, the conclusion is drawn that AODV routing protocol is more vulnerable to the networks with jamming nodes. In addition, placing the intruder nodes in the network reduces the reliability, availability and the performance of the network.

References

[1] Hongmei Deng, Wei Li, and Dharma P. Agrawal, “Routing Security in Wireless Ad Hoc Networks,” IEEE Communications Magazine, pp. 70-75, October 2002.

[2] Ekta Nehra and Er. Jasvir Singh, “Performance Comparison of AODV, TODV,OLSR and ABR using OPNET,” International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, pp. 984-990, May 2013.

[3] Changling Liu and Jörg Kaiser, “A Survey of Mobile Ad Hoc Network Routing Protocols,” The University of Magdeburg, October 2005.

[4] Rakesh Kumar Jha, Idris Z. Bholebawa, Upena D. Dalal, and A. Vishal Wankhede, "Detection and Fortification Analysis of WiMAX Network: With Misbehavior Node Attack," International Journal on Communications, Network and System Sciences, vol. 5, pp. 353-367, June 2012.

[5] Yu Zhang, Loukas Lazos, and William Jr. Kozma, “AMD: Audit-based Misbehavior Detection in Wireless Ad Hoc Networks,” IEEE Transactions on Mobile Computing, pp. 1-14.

[6] Niroj Kumar Pani, “A Secure Zone-Based Routing Protocol for Mobile Ad Hoc Networks,” Department of Computer Science and Engineering, National Institute of Technology, May 2009.

[7] A. Rajaram and Dr. S. Palaniswami, “The Trust-Based MAC-Layer Security Protocol for Mobile Ad hoc Networks,” International Journal of Computer Science and Engineering, Vol. 2, No. 2, pp 400-408, 2010.

[8] David J. Thuente and Mithun Acharya, “Intelligent Jamming in Wireless Networks with Applications to 802.11b and Other Networks,” North Carolina State University