# Security Threats in Mobile Ad Hoc Networks

Hande Bakiler, Aysel Şafak
Department of Electrical & Electronics Engineering
Baskent University
Ankara, Turkey
21020013@baskent.edu.tr, asafak@baskent.edu.tr

Ilgın Şafak
Progress R&D Center
Provus Information Technologies
Sisli, Istanbul, Turkey
ilgin.safak@provus.com.tr

***Abstract*—Mobile Ad Hoc Networks (MANET) are continuously self-organizing wireless networks with no fixed infrastructure, where network communication is established without a centralized administration. Security is an important issue for mobile ad hoc networks, due to the vulnerable nature of MANETs. This paper describes the effects of Pulse Jammer attack, Misbehavior Node attack and Byzantine attacks on the network performance under different traffic loads using Geographic Routing Protocol (GRP), Proactive Routing Protocol such as Optimized Link State Routing (OLSR) Protocol and Reactive Routing Protocols such as Ad Hoc On Demand Distance Vector (AODV) Routing Protocol and Dynamic Source Routing (DSR) Protocol. The impact of security attacks on MANET performance is evaluated by investigating which attack is more harmful to the network. IEEE 802.11b and 802.11g standards are compared with respect to the Pulse Jammer attack, Misbehavior Node attack and Byzantine attack for AODV Routing Protocol. Simulation results using OPNET simulator show that the efficient utilization of the network reduces considerably in the presence of the mentioned attacks.**

***Keywords- mobile ad hoc networks (MANETs); routing attacks; network security; OPNET***

## I. INTRODUCTION

Next generation wireless communication systems will require a rapid deployment of independent mobile users. An emerging wireless technology, mobile ad hoc networks (MANETs), are efficient, effective, quick, and easy to deploy in networks with changing topologies. Each mobile node acts as a host, and also acts as a router. Nodes communicate with each other without the intervention of access points or base stations [1]. Ad-hoc networks are suitable for applications where it is not possible to set up a fixed infrastructure and have a dynamic topology so that nodes can easily join or leave the network at any time. Possible MANET scenarios include communications in military and rescue missions in connecting soldiers on the battlefield or establishing new networks where a network has collapsed after a disaster like an earthquake [2]. Nodes cooperate by forwarding data packets to other nodes in the network to find a path to the destination node using routing protocols. However, due to security vulnerabilities of the routing protocols, wireless ad-hoc networks are unprotected to attacks of the malicious nodes. These nodes destroy the network, thereby degrading the network performance.

The effects of Pulse Jammer attack and Misbehavior nodes using Optimized Link State Routing Protocol (OLSR), Reactive routing protocol, Ad Hoc On Demand Distance Vector (AODV) and Geographical are studied in [3], where the impact of attack on MANET performance is evaluated in finding out which protocol is more vulnerable to these attacks. No single protocol that was studied had an overall better performance under Pulse Jammer attack and Misbehavior nodes security threats.

Various protocol aware jamming attacks that can be launched in an access point based 802.11b network are studied in [4]. It is shown that misbehaving nodes that do not adhere to the underlying MAC protocol significantly degrade the network throughput. Several hybrid attacks that increase the effectiveness of the attack or the decrease the probability of detection of the attack are also presented in the paper.

In this paper, the effects of Pulse Jammer Attack, Misbehavior Node attack and Byzantine security attacks on MANET network topology are studied using different routing protocols. The purpose of this work is access security attacks on MANETs that lead to a reduced network performance, reliability and availability. Additionally, several security routing protocols are investigated for MANET. For each scenario, normal network traffic is compared to the network traffic with five disruptive nodes that are placed in the network separately.

The main contribution of this work is providing insight about network security challenges and potential harmful attacks in MANET security under different traffic loads using various routing protocols. In this work, wlan_wkstn (Wireless LAN Workstation) mobile nodes are used, so the network traffic loads, i.e., http, ftp, email, voice and video conferencing can be enabled on these mobile nodes in the network. Performance metrics are provided for different network applications in addition to the whole network performance using different routing protocols. The IEEE 802.11b and 802.11g standards are compared for the normal network with and without network attackers.

 ISBN: 978-1-61208-373-5 

The paper is organized as follows: in Section II, an overview of the OLSR, GRP, DSR and AODV routing protocols are provided. In Section III, Pulse Jammer attack is described. In Section IV, Misbehavior Node attack is described and in Section V, Byzantine attack is described. Performance metrics which are used in the simulations are presented and described in Section VI. Simulation results are given in Section VII, followed by the conclusion in Section VIII.

## II. Overview of Current Routing Protocols

In this section, various existing routing protocols are described.

### A. The Dynamic Source Routing (DSR) Protocol

DSR [5] is a reactive unicast routing protocol that utilizes source routing algorithm. The sender knows the complete hop-by-hop route to the destination, where the routes are stored in a route cache. When a node in the ad hoc network attempts to send a data packet to a destination for which it does not know the route, it uses a route discovery process to dynamically determine one. Route discovery works by flooding the network with route request (RREQ) packets. A route reply is generated when the route request reaches either the destination itself, or an intermediate node which contains in its route cache an unexpired route to the destination. By the time the packet reaches the destination or an intermediate node, it contains a route record yielding the sequence of hops taken.

### B. The Ad Hoc On-demand Distance Vector (AODV) Routing Protocol

AODV routing protocol [1] is a reactive unicast routing protocol for mobile ad hoc networks which only needs to maintain the routing information about the active paths. In AODV, routing information is maintained in routing tables at nodes. Every mobile node keeps a next-hop routing table, which contains the destinations to which it currently has a route to. A routing table entry expires if it has not been used or reactivated for a pre-specified expiration time.

### C. Optimized Link State Routing (OLSR) Protocol

OLSR protocol, as defined in [6], is a proactive routing protocol based on the periodic exchange of topology information. Generally, three types of control messages are used in the OLSR protocol, namely, a HELLO message, a TC (Topology Control) message and a MID (Multiple Interface Declaration) message. The HELLO message is transmitted for sensing neighbors and for Multi-Point Distribution Relays (MPRs) calculation. Topology control is link state signaling that is performed by OLSR. MPRs are used to optimize the messaging process. MID messages contains the list of all IP addresses used by any node in the network. OLSR exchanges the topology information always with other nodes. Nodes maintain information of neighbors and MPRs by sending and receiving HELLO messages from its neighbors.

### D. Geographic Routing Protocol (GRP)

GRP [7][8] is a well researched approach for ad hoc routing where nodes are aware of their own geographic locations and also of its immediate neighbors and source node are aware of the destination's position. The data packets are routed through the network using the geographic location of the destination and not the network address. GRP operates without routing tables and routing to destination depends upon the information each node has about its neighbors. Geographic routing is simple and efficient.

## III. Pulse Jammer Attack

The most trivial way of disrupting a wireless network is by generating a continuous high power noise across the entire bandwidth near the transmitting and/or receiving nodes. The device that generates such a noise is called a jammer and the process is called jamming [4]. The reason to call jammer as intelligent is because its pulse off time and pulse on time are the main parameters which act on jammer to behave on and off at certain time as define to generate the transmission [3].

## IV. Misbehavior Nodes Attack

The purpose of misbehaving nodes [9] is not to function properly in the network and they achieve their goal by acting maliciously. They stop forwarding packets to the other nodes by simply start dropping the packets, or consume the bandwidth of the network by broadcasting route when it is not necessary. The misbehavior nodes stop performing the basic task; as a result, the network becomes congested and the traffic on the network leads to delay of data and degrade the performances of the network.

## V. Byzantine Attack

In Byzantine attacks, a compromised intermediate node or a set of compromised intermediate nodes collectively carries out attacks such as creating routing loops, routing packets on non-optimal paths and selectively dropping packets [10]. Byzantine attack drops, modifies and misroutes the forwarding packets in an attempt to disrupt the routing service [11].

## VI. Performance Metrics

The performance of the whole network under different routing protocols is analyzed by four metrics: throughput, network load, delay and data dropped.

### A. Throughput (bits/sec)

The average rate at which the data packet is delivered successfully from one node to another over a communication network is known as throughput.

 ISBN: 978-1-61208-373-5 

### B. *Network Load (bits/sec)*

Network load is the total packet sent and received across the whole network at a particular time.

### C. *Delay (sec)*

The packet end to end delay is the average time of the packet passing through inside the network.

### D. *Data Dropped (bits/sec)*

Data dropped shows that how many packets are successfully sent and received across the whole network.

## VII. SIMULATION RESULT AND ANALYSIS

The simulation is performed in analyzing the effects of Pulse Jammer attack, Misbehavior Node attack and Byzantine attack on the network performance under different traffic loads. Simulation parameters used are depicted in Table 1.

TABLE I. SIMULATION PARAMETER

| Simulation Parameter | Value |
|---|---|
| Simulator | OPNET 14.5 |
| Area | 800x800 (m) |
| Number of Nodes | 30 Nodes |
| Operation Mode | 802.11b, 802.11g |
| Data Rate of Each Node | 11 Mbps, 54 Mbps |
| Routing Protocols | DSR, AODV, OLSR, GRP |
| Mobility Model | Random Waypoint |
| Traffic Type | HTTP, FTP, Email, Voice, Video Conferencing |
| Simulation Time | 300 sec. |
| Packet Reception Power Threshold | -95 dBm |

### A. *Performance of DSR under Pulse Jammer Attack, under Misbehavior Node Attack and under Byzantine Attack for Voice Application*

In the simulation enviroment, five jamming nodes, five misbehaving nodes and five Byzantine nodes were placed separately in the normal network with different scenarios. Then, packet end-to-end delay statistics are represented for voice application in the same graph.

Figure 1 represents the packet end-to-end delay statistics for voice application on the normal network traffic with the average value of 7.667 seconds. It shows the “packet end-to-end delay” with jamming nodes in the network as 10.864 seconds, with misbehaving nodes as 9.748 seconds and with Byzantine nodes in the network as 9.235 seconds with respect to the DSR.

The delay increases in presence of the network attacks on the network when it is compared to the normal network.

Jamming nodes deny the network transmission services to authorized users by generating noise on the wireless medium in order to block the access for authorized nodes. Misbehaving nodes consume a lot of bandwidth and do not collaborate with the other nodes in the network. Byzantine nodes drop the packets in the network which degrades the network routing services.

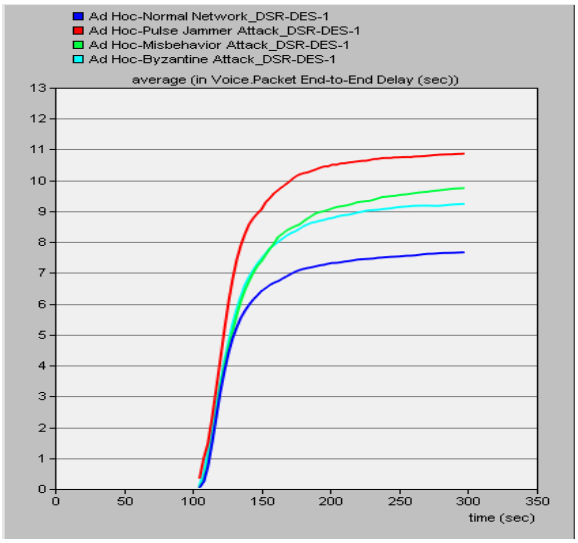


Figure 1. Packet end-to-end delay results of the normal network’s voice application with and without network attacks for DSR

### B. *Performance of AODV under Pulse Jammer Attack, under Misbehavior Node Attack and under Byzantine Attack for Voice Application*

In this section, the performance of AODV routing protocol under jamming nodes, misbehaving nodes and Byzantine nodes are compared. First, normal traffic is generated under AODV, and then the scenario was duplicated with a jitter parameter for different attacks. For each network attack scenario, five malicious nodes are placed in the normal network. Jitter [12] is the ratio of transmission delay of the current packet and the transmission delay of the previous packet.

In Figure 2, jitter statistics are represented for voice application in the same graph.

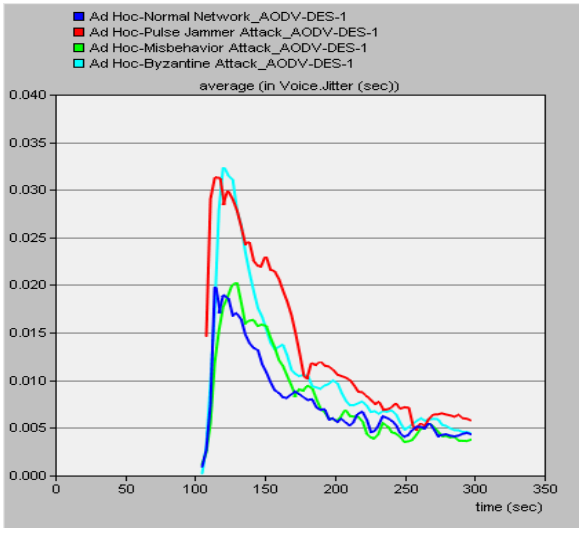


Figure 2. Jitter results of the normal network’s voice application with and without network attacks for AODV routing protocol

In the graph above, it is clearly seen that jitter increases in the beginning of the simulation up to a certain point and from that point onwards it degrades rapidly. This is due to the fact that the utilization of the network reaches a steady state after some time.

Figure 2 shows that the average value of the normal network traffic jitter in voice applications is 0.0043 seconds. On the other hand, the network with jammer nodes shows the jitter with the average value of 0.0057 seconds; with Byzantine nodes the value it is noted as 0.0044 seconds and with misbehaving nodes it is recorded as 0.004 seconds with respect to the AODV routing protocol.

The results show significant changes in jitter for voice application, especially for the network with jamming nodes and with Byzantine nodes. Due to malicious activities of the jamming nodes and Byzantine nodes, the jitter increment is more than the normal network for AODV routing protocol. Also for the network with misbehaving nodes, the jitter increment is more than the normal network in general. However, it reduces at some certain points. The reason of this reduction could be that misbehaving nodes start dropping the packets and do not forward the packets to the other nodes on the network, then the misbehaving nodes start sending the packets and forwarding packets faster than the normal nodes. As a result, normal nodes are not able to process the packets.

### C. *Performance of OLSR under Pulse Jammer Attack, under Misbehavior Node Attack and under Byzantine Attack for Email Application*

In this section, the performance of OLSR protocol under jamming nodes, misbehaving nodes and Byzantine nodes are compared. For each network attack scenario, five malicious nodes are placed in the normal network.

In Figure 3, the traffic received statistics for email application on the normal network traffic with and without malicious nodes are analyzed. The normal network's traffic received statistics is recorded as 153.9 bytes/sec. Then, it is noted as 140.5 bytes/sec with jammer nodes in the network. The traffic received statistics average value is 127.1 bytes/sec with misbehaving nodes and with Byzantine nodes in the network its value is noted as 100.32 bytes/sec with respect to the OLSR.

When placing the malicious nodes in the network, the MANET traffic received is recorded lower than the normal network traffic. There is significant traffic destruction of the packets transmission on the network when applying network attacks.

### D. *Performance of GRP under Pulse Jammer Attack, under Misbehavior Node Attack and under Byzantine Attack for Video Conferencing Application*

To implement the network attacks on MANET nodes network, five jamming nodes, five misbehaving nodes and five Byzantine nodes are deployed separately in the network for GRP with different scenarios.

The packet end-to-end delay statistics for voice application of the normal network is noted as 0.269 seconds at the duration time of simulation 300 seconds in Figure 4. After implementing the five jamming nodes, it increases to 0.928 seconds. The reason for this is because pulse jammer nodes generate a noise on radio frequency in pulse time which increases the packet end-to-end delay statistics on the network for GRP. The graph represents the packet end-to-end delay statistics of voice application as 0.40 seconds for the network with misbehaving nodes. Due to the misbehaving nodes, the network becomes congested.

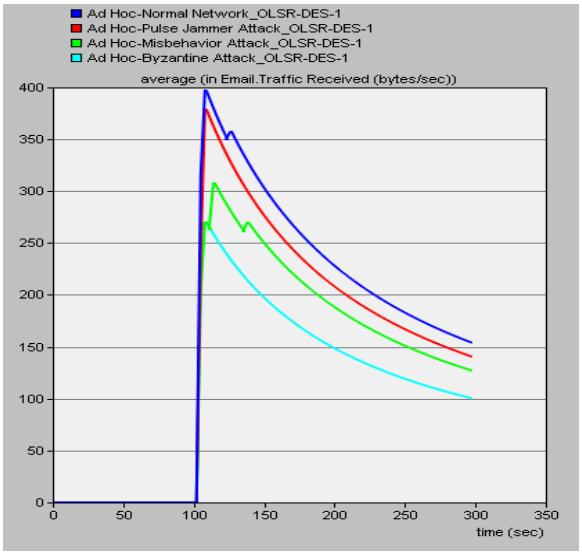


Figure 3. Traffic received results of the normal network's email application with and without network attacks for OLSR protocol

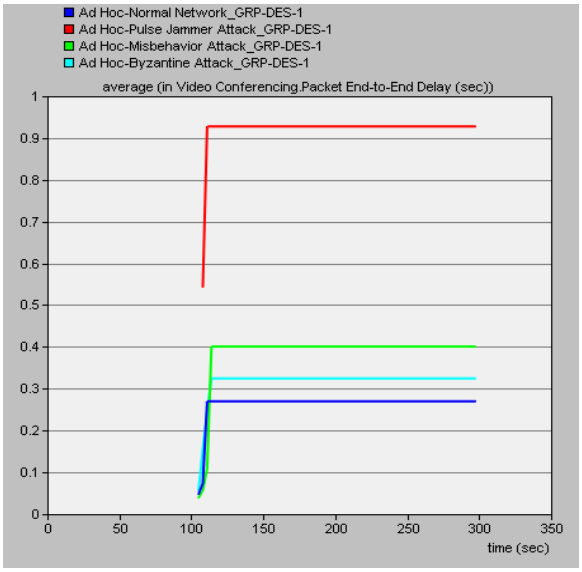


Figure 4. Packet end-to-end delay results of the normal network's video conferencing with and without network attacks for GRP

 ISBN: 978-1-61208-373-5 

Figure 4 shows the packet end-to-end delay with Byzantine nodes in the network as 0.325 seconds with respect to the GRP. The Byzantine attack has a negative impact on the transmission and network traffic.

### *E. Performance of DSR under Pulse Jammer Attack, under Misbehavior Node Attack and under Byzantine Attack for the Network with respect to "Throughput" Statistics*

In this section, five jamming nodes, five misbehaving nodes and five Byzantine nodes were placed separately in the normal network with different scenarios. The throughput statistics are represented for the whole network in the same graph in Figure 5.

The throughput of the network nodes with normal traffic is noted as 741,085 bits/sec, whereas the throughput with jamming nodes is noted as 544,661 bits/sec, both for a simulation of 300 seconds duration. As seen in Figure 5, the throughput of the network with Byzantine nodes is recorded as 699,863 bits/sec and with misbehaving nodes as 715,089 bits/sec. The largest reduction of the network throughput statistic is represented for the network with jamming nodes and the least reduction is indicated for the network with misbehaving nodes with respect to the DSR protocol.

### *F. Performance of AODV under Pulse Jammer Attack, under Misbehavior Node Attack and under Byzantine Attack for the Network with respect to "Network Load" Statistics*

In this section, different network attack scenarios were designed separately to examine the AODV routing protocol under five Byzantine nodes, five misbehaving nodes and five jamming nodes.

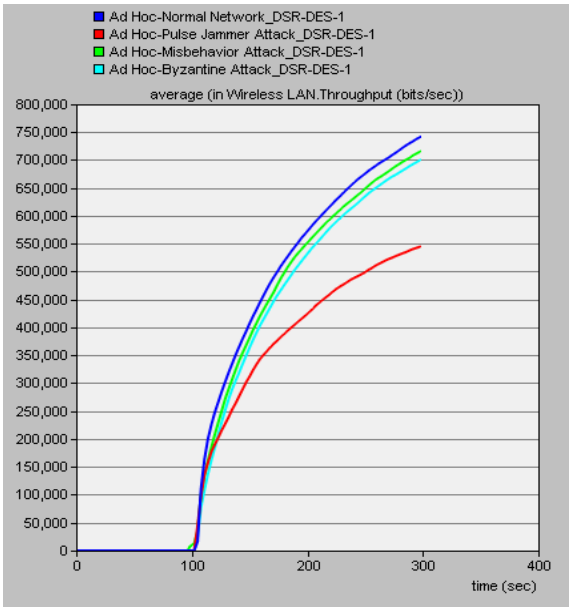


Figure 5. Throughput results of the normal network with and without network attacks for DSR protocol

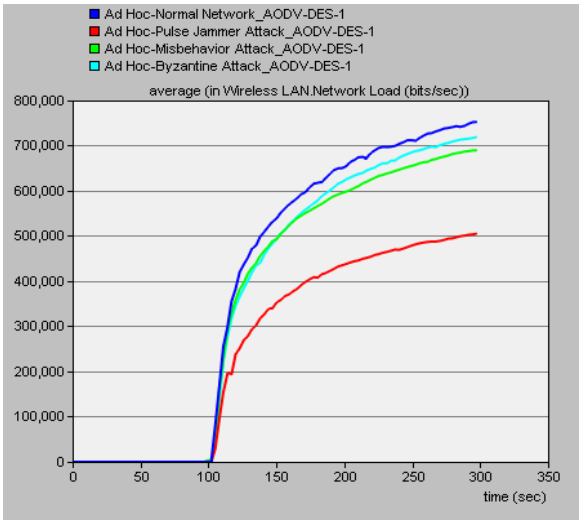


Figure 6. Network load results of the normal network with and without network attacks for AODV routing protocol

The network scenarios for different attacks are depicted in Figure 6. The network load of the normal network has the average value of 752,620 bits/sec and with the jamming nodes in the network it is noted as 505,130 bits/sec. For the network with misbehaving nodes, its average value is 690,004 bits/sec and the network load statistics according to the network with Byzantine nodes is recorded as 718,929 bits/sec. The largest reduction of the network load statistic is represented for the network with jamming nodes and the least reduction is represented for the network with Byzantine nodes with respect to AODV routing protocol.

According to Figure 6, AODV routing protocol is more vulnerable to jamming nodes. Jamming nodes deny service by generating noise and causes protocol packets lost. Jamming nodes block the access for authorized users.

As a result, the network traffic effected negatively when malicious nodes are placed in the normal network and they start dropping the forwarding packets to the other the nodes on the network.

### *G. Performance of GRP under Pulse Jammer Attack, under Misbehavior Node Attack and under Byzantine Attack for the Network with respect to "Delay" Statistics*

Five jamming nodes, five misbehaving nodes and five Byzantine nodes were placed separately in the normal network with different scenarios.

Different network scenarios for the mentioned network attacks are represented in Figure 7 according to GRP protocol.

Figure 7 represents that the normal network traffic delay average value is 3.27 seconds. On the other hand, the network with jammer nodes shows the delay with the average value of 4.42 seconds, with Byzantine nodes the value it is recorded as 3.92 seconds and with misbehaving nodes it is noted as 3.51 seconds with respect to the GRP.

 ISBN: 978-1-61208-373-5 

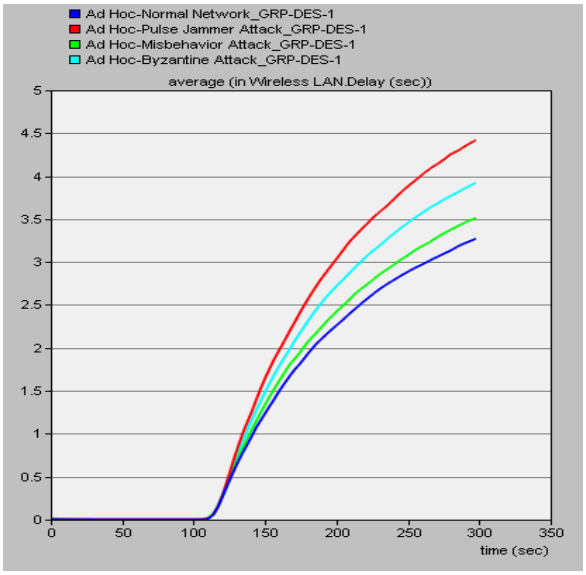


Figure 7. Delay results of the normal network with and without network attacks for GRP

The largest increment of the delay statistic is depicted for the network with jamming nodes and the least increment is represented for the network with misbehaving nodes with respect to GRP. The jamming node attack on GRP shows a significant result. The jamming nodes stop performing the basic task of the network; as a result, the network becomes congested and the traffic on the network leads to delay of the data and degrading of the performances of the network.

### *H. Performance of OLSR under Pulse Jammer Attack, under Misbehavior Node Attack and under Byzantine Attack for the Network with respect to "Data Dropped" Statistics*

In this section, five jamming nodes, five misbehaving nodes and five Byzantine nodes are placed in the network separately for OLSR protocol with different scenarios in implementing the network attacks on MANET nodes network. The data dropped statistics are shown for the whole network in the same graph.

Figure 8 shows the normal network data dropped statistics average value as 22,577 bits/sec. For the network with jamming nodes, the average data dropped value is recorded as 23.074 bits/sec; with misbehaving nodes the data dropped statistics is 24,437 bits/sec and with Byzantine nodes its value is 28,353 bits/sec.

It is seen that the largest increment of the data dropped statistic is represented for the network with misbehaving nodes and the least increment is represented for the network with jamming nodes with respect to the OLSR protocol. That means that the OLSR protocol is more vulnerable to the network with misbehaving nodes.

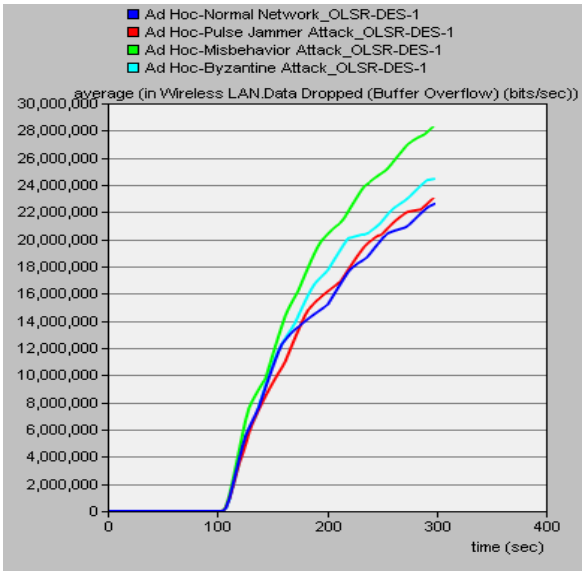


Figure 8. Data dropped results of the normal network with and without network attacks for OLSR

### *I. Performance of AODV under Pulse Jammer Attack, under Misbehavior Node Attack and under Byzantine Attack for IEEE 802.11g Standard with respect to "Network Load" Statistics*

In this section, different network attack scenarios were designed for the AODV routing separately under Byzantine nodes, misbehaving nodes and jamming nodes in order to examine the IEEE 802.11g standard. For each network attack scenario, five malicious nodes are placed in the normal network.

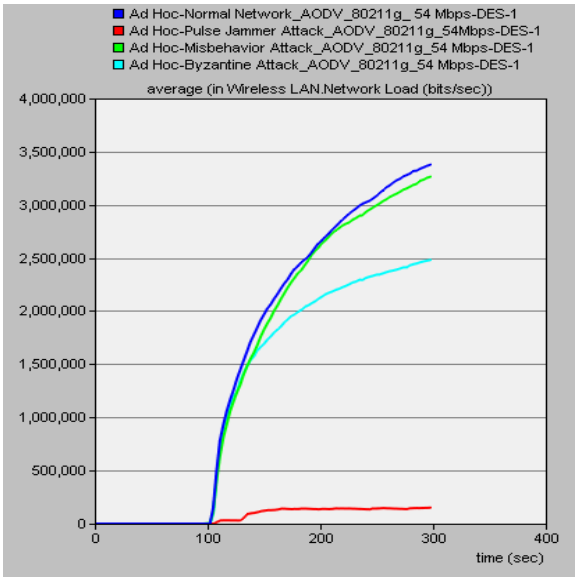


Figure 9. Network load results of the normal network with and without network attacks for AODV with respect to the IEEE 802.11g standard

As seen in Figure 9, the network load performance of the network nodes with normal traffic is 3,376,409 bits/sec and with misbehaving nodes in the network it is represented as 3,262,975 bits/sec. The network load of the network with Byzantine nodes is noted as 2,480,452 bits/sec and with jamming nodes it is recorded as 150,486 bits/sec.

The largest reduction of the network load statistic is represented for the network with jamming nodes and the least reduction is represented for the network with misbehaving nodes with respect to the IEEE 802.11g standard for AODV routing protocol. Hence, networks using 802.11b standard are more vulnerable to jamming nodes in the network.

Compared to the networks using IEEE 802.11b and 802.11g standards, networks using IEEE 802.11b standard are more vulnerable to networks with jamming nodes. On the other hand, networks using IEEE 802.11g standard are the least affected from the network with jamming nodes for AODV routing protocol.

## VIII. CONCLUSION AND FUTURE WORK

In this work, the routing protocols GRP, Proactive Routing Protocol (OLSR), and Reactive Routing Protocols (AODV and DSR) are studied in IEEE 802.11b networks. The network performance under Pulse Jammer attack, Misbehavior Node attack and Byzantine attack is investigated. The network contains http (heavy browsing), ftp (high load), email (high load), voice (PCM Quality Spech) and video conferencing (low resolution video) applications. The normal network is compared with the networks which contain jamming nodes, misbehaving nodes and Byzantine nodes in terms of performance metrics, i.e., delay, network load, throughput, data dropped, jitter and traffic received by using different routing protocols. Then, the IEEE 802.11b and 802.11g standards, which share the same propagation characteristics, are compared for networks with and without security attacks using the AODV routing protocol. Results show that routing protocols are more vulnerable to networks with jamming nodes, and placing the intruder nodes in the network reduces the reliability, availability and the performance of the network. Networks using the IEEE 802.11b standard are more vulnerable in networks with jamming nodes for the AODV routing protocol. Jammer attack generates noise on the wireless radio frequency medium to stop the communication in order to trigger the network. Jamming nodes cause corruption of the packets or they cause packet lost. Misbehavior Node attack stops forwarding packets to the other nodes and drop the packets, it stop performing the basic task and the network performance degrades. Also, Byzantine attack drops the routing forwarding table or drops the forwarding packets to the other nodes. Several security breaches are represented under these three attack models using OPNET. They provide useful insight in understanding MANET in terms of the network security.

Future work encompasses extending results to other security attacks and wireless protocols, and adding detection and defense mechanisms that can protect the network from the intruders.

## ACKNOWLEDGMENT

This work was supported by ITEA2 ADAX Project No. 10030 and TUBITAK TEYDEB Project No. 9130016.

## REFERENCES

[1] C. Liu and J. Kaiser, “A Survey of Mobile Ad Hoc Network Routing Protocols,” The University of Magdeburg, October 2005.

[2] S. Vrutik, D. N. Modi, and P. Ashwin, "AODVGAP-An Acknowledgement Based Approach to Mitigate Selective Forwarding Attacks in MANET," International Journal of Computer Engineering and Technology (IJCET), vol. 3, no. 2, July-September 2012, pp. 458-469.

[3] S. Salim, "Mobile Ad hoc Network Security Issues," M.Sc. Thesis, University of Central Lancashire, 2010, pp. 1-81.

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

[5] C. E. Perkins, E. M. Royer, S. R. Das, and M. K. Marina, "Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks," IEEE Personal Communications, February 2001, pp. 16-28.

[6] S. Ehrampoosh and A. K. Mahani, "Secure Routing Protocols: Affections on MANETs Performance," First International Conference on Communications Engineering, 22-24 December 2010, pp. 77-82.

[7] A. Tamizhselvi and Dr. R. S. D. W. Banu, "Performance Evaluation of Geographical Routing Protocol under Different Traffic Scenario," International Journal of Computer Science and Telecommunications, vol. 3, no. 3, March 2012, pp. 64-67.

[8] J. A. Sanchez, P. M. Ruiz, and R. Marin-Perez, "Beacon-Less Geographic Routing Made Practical: Challenges, Design Guidelines, and Protocols," IEEE Communications Magazine, August 2009, pp. 85-91.

[9] R. K. Jha, I. Z. Bholebawa, U. D. Dalal, and A. V. Wankhede, "Detection and Fortification Analysis of WiMAX Network: With Misbehavior Node Attack," International Journal on Communications, Network and System Sciences, vol. 5, April 2012, pp. 353-367.

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

[11] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An On-demand Secure Routing Protocol Resilient to Byzantine Failures," Proceedings of the ACM Workshop on Wireless Security (WiSe), September 2002, pp. 21-30.

[12] H. Paul and P. Sarkar, "A Study and Comparison of OLSR, AODV and ZRP Routing Protocols in Ad Hoc Networks," International Journal of Research in Engineering and Technology (IJRET), vol. 2, no.8, August 2013, pp. 370-374.

 ISBN: 978-1-61208-373-5 