BAŞKENT UNIVERSITY
INSTITUTE OF SCIENCE AND ENGINEERING

IMPROVEMENT OF PERFORMANCE AND CAPACITIES OF WIRELESS AD HOC NETWORKS

HANDE BAKİLER

MSc. THESIS
2014

IMPROVEMENT OF PERFORMANCE AND CAPACITIES OF WIRELESS AD HOC NETWORKS

TELSİZ AD HOC AĞLARIN BAŞARIM VE KAPASİTELERİNİN ARTTIRILMASI

HANDE BAKİLER

Thesis Submitted
in Partial Fulfillment of the Requirements
For the Degree of Master of Science
in Department of Electrical and Electronics Engineering
at Başkent University

2014

This thesis, titled: “Improvement of Performance and Capacities of Wireless Ad Hoc Networks”, has been approved in partial fulfillment of the requirements for the degree of MASTER OF SCIENCE IN ELECTRICAL AND ELECTRONICS ENGINEERING, by our jury, on 25/12/2014.

Chairman :

(Assoc. Prof. Dr. Hasan OĞUL)

Member (Supervisor) :

(Asst. Prof. Dr. Aysel ŞAFAK)

Member :

(Assoc. Prof. Dr. Sıtkı Çağdaş İNAM)

APPROVAL

..../12/2014

Prof. Dr. Emin AKATA

Institute of Science and Engineering

ACKNOWLEDGEMENTS

I would like to express my gratitude and appreciation to my supervisor Asst. Prof. Dr. Aysel Şafak for her valuable guidance, support, advice and encouragements during all the stages of my thesis.

I am also very grateful to my family for their endless love and support they have shown throughout all my life.

Hande BAKİLER

December 2014

ABSTRACT

IMPROVEMENT OF PERFORMANCE AND CAPACITIES OF WIRELESS AD HOC NETWORKS

Hande BAKİLER
Başkent University Institute of Science & Engineering
The Department of Electrical and Electronics Engineering

Mobile Ad Hoc Networks 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 these networks. This thesis describes the effects of Pulse Jammer attack, Misbehavior Nodes attack and Byzantine attacks on the network performance under different traffic loads using Position-based Routing Protocol such as 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 mobile ad hoc network performance is evaluated by investigating which attack is more harmful to the network. Additionally, mentioned security routing protocols are surveyed for mobile ad hoc networks and the performance of these routing protocols are compared under Pulse Jammer attack, under Misbehavior Node attack and under Byzantine attack. Simulation results using OPNET simulator show that the efficient utilization of the network reduces considerably in the presence of the mentioned attacks.

KEYWORDS: Ad hoc networks, network security, routing protocols, OPNET
Advisor: Asst. Prof. Dr. Aysel ŞAFAK, Başkent University, Department of Electrical and Electronics Engineering

ÖZ

TELSİZ AD HOC AĞLARIN BAŞARIM VE KAPASİTELERİNİN ARTTIRILMASI

Hande BAKİLER
Başkent Üniversitesi Fen Bilimleri Enstitüsü
Elektrik-Elektronik Mühendisliği Anabilim Dalı

Gezgin ad hoc ağlar, ortam koşullarına kendi kendini uyarlayabilen, sabit bir alt yapı gerektirmeyen, ağın denetimi, yönetimi için herhangi bir merkezi otoriteye gerek duymayarak iletişimi sağlayan dinamik varlıklardır. Güvenlik, gezgin ad hoc ağların savunmasız doğası nedeniyle önemli bir konudur. Bu çalışma, Darbe Parazit saldırısı, Haşarı Düğüm saldırısı ve Bizans ağ saldırısının farklı trafik yüklerine göre ağ performansı üzerindeki etkilerini, Konum tabanlı yol atama protokollerinden olan Coğrafi Yönlendirme Protokolü (GRP), Tabloya dayalı yol atama protokollerinden olan İyileştirilmiş Bağ Durumu Yönlendirme (OLSR) protokolü ve İsteğe bağlı yol atama protokollerinden olan Ad Hoc İsteğe Bağlı Uzaklık Vektör (AODV) ve Dinamik Kaynak Yönlendirme (DSR) protokollerini kullanarak açıklamaktadır. Gezgin ad hoc ağlar üzerindeki ağ saldırılarının etkileri araştırılarak değerlendirilmektedir. Ayrıca, gezgin ad hoc ağlar için sözedilen güvenlik yönlendirme protokolleri de incelenmektedir ve bu protokollerin performansları da Darbe Parazit, Haşarı Düğüm ve Bizans ağ saldırıları altında karşılaştırılmaktadır. OPNET simülatörü kullanılarak elde edilen simülasyon sonuçları, ağın etkin kullanımının söz konusu saldırıların varlığında önemli ölçüde azaldığını göstermektedir.

ANAHTAR SÖZCÜKLER: Ad hoc ağlar, ağ güvenliği, yönlendirme protokolleri, OPNET

Danışman: Yrd.Doç.Dr. Aysel ŞAFAK, Başkent Üniversitesi, Elektrik-Elektronik Mühendisliği Bölümü

TABLE OF CONTENTS

Page

ABSTRACT i
ÖZ ii
TABLE OF CONTENTS iii
LIST OF FIGURES viii
LIST OF TABLES xi
LIST OF ABBREVIATIONS xii
1 INTRODUCTION 1
2 AD HOC NETWORKS 4
2.1 Characteristics of Mobile Ad Hoc Networks 5
2.1.1 Wireless medium 6
2.1.2 Dynamic network topology 6
2.1.3 Autonomous and infrastructureless 6
2.1.4 Limited energy resources 6
2.2 Standards using in Ad Hoc Networks 7
2.3 Quality of Service (QoS) in IEEE 802.11 8
2.3.1 Quality of service metrics 9
2.3.1.1 Delay 9
2.3.1.2 Bandwith 10
2.3.1.3 Throughput 10
2.3.1.4 Jitter 11
2.3.1.5 Packet loss 11
2.3.1.6 SINR 11
2.3.2 Security in quality of service 12
2.4 Wireless Channel Characteristics 12
2.4.1 Attenuation 12
2.4.2 Path loss 13
2.4.3 Signal to noise ratio 13
2.4.4 Multipath propagation 14
3 ROUTING PROTOCOLS 16
3.1 The Dynamic Source Routing (DSR) Protocol 18

3.2 The Ad Hoc on Demand Distance Vector (AODV) Routing Protocol.....20
3.2.1 The differences between DSR and AODV.....25
3.3 Optimized Link State Routing (OLSR) Protocol.....26
3.4 Geographic Routing Protocol (GRP).....28
4 SECURITY ATTACKS IN MOBILE AD HOC NETWORKS.....31
4.1 Attack Characteristics.....31
4.1.1 Active and passive attacks.....32
4.1.2 External and internal attacks.....32
4.1.3 Mobile and wired attacks.....33
4.1.4 Single and multiple attacks.....34
4.2 Security Attack Types In Ad Hoc Networks.....34
4.2.1 Physical layer attacks.....34
4.2.1.1 Eavesdropping.....35
4.2.1.2 Jamming.....36
4.2.1.3 Interference.....36
4.2.2 Data link layer attacks.....36
4.2.2.1 Traffic analysis.....37
4.2.2.2 Attacks in IEEE 802.11 MAC.....37
4.2.2.3 IEEE 802.11 WEP weakness.....37
4.2.3 Network layer attacks.....38
4.2.3.1 Black hole attack.....38
4.2.3.2 Wormhole attack.....39
4.2.3.3 Byzantine attack.....40
4.2.3.4 Rushing attack.....41
4.2.3.5 Flooding attack.....41
4.2.3.6 Resource consumption attack.....41
4.2.3.7 Location disclosure attack.....42
4.2.4 Transport layer attacks.....42
4.2.4.1 Session hijacking.....42
4.2.4.2 SYN flooding.....43
4.2.5 Application layer attacks.....43
4.2.5.1 Repudiation attacks.....43
4.2.5.2 Malicious code attacks.....43

4.2.6 Multilayer attacks 44
4.2.6.1 Denial of service (DoS) attacks 44
4.2.6.2 Impersonation 44
4.3 Security Services 45
4.3.1 Availability 45
4.3.2 Confidentiality 45
4.3.3 Integrity 45
4.3.4 Authentication 46
4.3.5 Nonrepudiation 46
5 MOBILE AD HOC COMMUNICATION SYSTEM 47
5.1 Simulation Tool 48
5.2 Performance Metrics 49
5.2.1 Throughput (bits/sec) 49
5.2.2 Network load (bits/sec) 49
5.2.3 Delay (sec) 49
5.2.4 Data dropped (bits/sec) 49
5.2.5 Traffic Received (bytes/sec) 49
5.3 Network Attacks Used in the Mobile Ad Hoc Networks 49
5.3.1 Pulse Jammer attack 50
5.3.2 Byzantine attack 50
5.3.3 Misbehavior Nodes attack 50
5.4 Application Configuration Setting 51
5.5 Profile Configuration Setting 52
5.6 Mobility Configuration Setting 52
5.7 Traffic Model Setting for Wireless Stations 53
5.8 Intelligent Pulse Jammer Node Model 55
5.9 Misbehavior Node Model 55
5.10 Byzantine Node Model 57
6 SIMULATION RESULTS AND ANALYSIS 59
6.1 Performance of DSR under Pulse Jammer Attack, under Misbehavior Node Attack and under Byzantine Attack for the Network 59
6.1.1 Data dropped statistics of DSR protocol for the network 59
6.1.2 Delay statistics of DSR protocol for the network 60

6.1.3 Network load statistics of DSR protocol for the network 62
6.1.4 Throughput statistics of DSR protocol for the network 63
6.2 Performance of AODV under Pulse Jammer Attack, under Misbehavior Node Attack and under Byzantine Attack for the Network 64
6.2.1 Data dropped statistics of AODV routing protocol for the network 65
6.2.2 Delay statistics of AODV routing protocol for the network.....66
6.2.3 Network load statistics of AODV routing protocol for the network.....67
6.2.4 Throughput statistics of AODV routing protocol for the network 68
6.3 Performance of OLSR under Pulse Jammer Attack, under Misbehavior Node Attack and under Byzantine Attack for the Network 69
6.3.1 Data dropped statistics of OLSR protocol for the network 70
6.3.2 Delay statistics of OLSR protocol for the network.....71
6.3.3 Network load statistics of OLSR protocol for the network 72
6.3.4 Throughput statistics of OLSR protocol for the network.....73
6.4 Performance of GRP under Pulse Jammer Attack, under Misbehavior Node Attack and under Byzantine Attack for the Network 74
6.4.1 Data dropped statistics of GRP for the network 75
6.4.2 Delay statistics of GRP for the network.....76
6.4.3 Network load statistics of GRP for the network.....77
6.4.4 Throughput statistics of GRP for the network 78
6.5 Performance of Routing Protocols under Pulse Jammer Attack, under Misbehavior Node Attack and under Byzantine Attack for Voice Application in respect of Packet End-to-End Delay Statistics 79
6.5.1 Packet end-to-end delay statistics of DSR protocol for voice application.....80
6.5.2 Packet end-to-end delay statistics of AODV routing protocol for voice application.....81
6.5.3 Packet end-to-end delay statistics of OLSR protocol for voice application.....82
6.5.4 Packet end-to-end delay statistics of GRP for voice application 84
6.6 Performance of Routing Protocols under Pulse Jammer Attack, under Misbehavior Node Attack and under Byzantine Attack for Voice Application in respect of Jitter Statistics.....85
6.6.1 Jitter statistics of DSR protocol for voice application.....86
6.6.2 Jitter statistics of AODV routing protocol for voice application 87
6.6.3 Jitter statistics of OLSR protocol for voice application 88

6.6.4 Jitter statistics of GRP for voice application 90
6.7 Performance of Routing Protocols under Pulse Jammer Attack, under Misbehavior Node Attack and under Byzantine Attack for Email Application in respect of Traffic Received Statistics.....91
6.7.1 Traffic received statistics of DSR protocol for email application.....91
6.7.2 Traffic received statistics of AODV routing protocol for email application 93
6.7.3 Traffic received statistics of OLSR protocol for email application 94
6.7.4 Traffic received statistics of GRP for email application 95
6.8 Performance of Routing Protocols under Pulse Jammer Attack, under Misbehavior Node Attack and under Byzantine Attack for Video Conferencing Application in respect of Traffic Received Statistics 96
6.8.1 Traffic received statistics of DSR protocol for video conferencing application.....97
6.8.2 Traffic received statistics of AODV routing protocol for video conferencing application.....98
6.8.3 Traffic received statistics of OLSR protocol for video conferencing application.....100
6.8.4 Traffic received statistics of GRP for video conferencing application101
6.9 Simulation Results 102
7 CONCLUSION AND FUTURE WORK.....106
REFERENCES.....108

LIST OF FIGURES

Page

Figure 2.1 Communication in a MANET 4
Figure 2.2 Vehicular ad hoc network architecture 5
Figure 2.3 Illustration of multipath effects in wireless communication 14
Figure 3.1 Classification of MANET routing protocols 17
Figure 3.2 Source node's broadcast....19
Figure 3.3 Destination node's reply 20
Figure 3.4 Example of AODV RREQ messages....22
Figure 3.5 Example of AODV RREP messages 23
Figure 3.6 Example of AODV RERR messages....24
Figure 3.7 Flooding packets using MPR....27
Figure 3.8 OLSR symmetric link formation (Hello Message Exchange) 28
Figure 3.9 Greedy forwarding example. *y* is *x*'s closest neighbor to *D* 29
Figure 3.10 Example of position-based routing protocol 30
Figure 4.1 Classifications of passive and active attacks....31
Figure 4.2 Active and passive attacks in MANETs 32
Figure 4.3 External and internal attacks in ad hoc networks 33
Figure 4.4 An attack on communication between source and destination....35
Figure 4.5 Routing attack by malicious node....38
Figure 4.6 Blackhole attack 39
Figure 4.7 Wormhole attack 40
Figure 4.8 Session hijacking 42
Figure 4.9 SYN flooding attack....43
Figure 5.1 The normal network model....47
Figure 5.2 Application configuration setting....51
Figure 5.3 Profile configuration setting 52
Figure 5.4 Mobile configuration setting....53
Figure 5.5 Traffic model and wireless attributes of a station node 54
Figure 5.6 Intelligent Pulse Jammer node model attributes....55
Figure 5.7 Misbehavior node model attributes for the networks with manet_station and wlan_wkstn mobile nodes 56
Figure 5.8 Byzantine node model attributes for AODV and DSR 57

Figure 5.9 Byzantine node model attributes for GRP and OLSR.....58
Figure 6.1 Data dropped results of the normal network with and without network attacks for DSR protocol.....60
Figure 6.2 Delay results of the normal network with and without network attacks for DSR protocol 61
Figure 6.3 Network load results of the normal network with and without network attacks for DSR protocol.....62
Figure 6.4 Throughput results of the normal network with and without network attacks for DSR protocol.....64
Figure 6.5 Data dropped results of the normal network with and without network attacks for AODV routing protocol 65
Figure 6.6 Delay results of the normal network with and without network attacks for AODV routing protocol.....66
Figure 6.7 Network load results of the normal network with and without network attacks for AODV routing protocol 67
Figure 6.8 Throughput results of the normal network with and without network attacks for AODV routing protocol 69
Figure 6.9 Data dropped results of the normal network with and without network attacks for OLSR protocol.....70
Figure 6.10 Delay results of the normal network with and without network attacks for OLSR protocol 71
Figure 6.11 Network load results of the normal network with and without network attacks for OLSR protocol.....72
Figure 6.12 Throughput results of the normal network with and without network attacks for OLSR protocol.....74
Figure 6.13 Data dropped results of the normal network with and without network attacks for GRP 75
Figure 6.14 Delay results of the normal network with and without network attacks for GRP.....76
Figure 6.15 Network load results of the normal network with and without network attacks for GRP 78
Figure 6.16 Throughput results of the normal network with and without network attacks for GRP 79
Figure 6.17 Packet end-to-end delay results of the normal network's voice application with and without network attacks for DSR protocol 80
Figure 6.18 Packet end-to-end delay results of the normal network's voice application with and without network attacks for AODV routing protocol 81

Figure 6.19 Packet end-to-end delay results of the normal network's voice application with and without network attacks for OLSR protocol 83
Figure 6.20 Packet end-to-end delay results of the normal network's voice application with and without network attacks for GRP 84
Figure 6.21 Jitter results of the normal network's voice application with and without network attacks for DSR protocol 86
Figure 6.22 Jitter results of the normal network's voice application with and without network attacks for AODV routing protocol 87
Figure 6.23 Jitter results of the normal network's voice application with and without network attacks for OLSR protocol 89
Figure 6.24 Jitter results of the normal network's voice application with and without network attacks for GRP 90
Figure 6.25 Traffic received results of the normal network's email application with and without network attacks for DSR protocol 92
Figure 6.26 Traffic received results of the normal network's email application with and without network attacks for AODV routing protocol 93
Figure 6.27 Traffic received results of the normal network's email application with and without network attacks for OLSR protocol 95
Figure 6.28 Traffic received results of the normal network's email application with and without network attacks for GRP 96
Figure 6.29 Traffic received results of the normal network's video conferencing application with and without network attacks for DSR protocol 98
Figure 6.30 Traffic received results of the normal network's video conferencing application with and without network attacks for AODV routing protocol 99
Figure 6.31 Traffic received results of the normal network's video conferencing application with and without network attacks for OLSR protocol 100
Figure 6.32 Traffic received results of the normal network's video conferencing application with and without network attacks for GRP 101

LIST OF TABLES

Page

Table 2.1 Comparison of 80.11a/b/g and 802.16 standards 7
Table 3.1 Comparison of routing protocols in MANETs 18
Table 5.1 Simulation parameter 48

LIST OF ABBREVIATIONS

ACK	Acknowledgement
AODV	Ad Hoc on Demand Distance Vector Routing
CSMA/CA	Carrier Sense Multiple Access With Collision Avoidance
DCF	Distributed Coordination Function
DoS	Denial of Service
DSR	Dynamic Source Routing
FTP	File Transfer Protocol
GRP	Geographic Routing Protocol
HCF	Hybrid Coordination Function
HTTP	Hyper-Text Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineering
IP	Internet Protocol
MAC	Media Access Control
MANET	Mobile Ad Hoc Networks
MID	Multiple Interface Declaration
MPRs	Multi Point Relays
OLSR	Optimized Link State Routing Protocol
PCM	Pulse-Code Modulation
PREQ	Propagation of Request
QoS	Quality of Service
RERR	Route Error
RF	Radio Frequency
RREP	Route Reply
RREQ	Route Request
SINR	Signal to Interference and Noise Ratio
SMTP	Simple Mail Transfer Protocol
SNR	Signal to Noise Ratio
TC	Topology Control
TCP	Transport Control Protocol
TORA	Temporally Ordered Routing Algorithm
TTL	Time-To-Live

VANET	Vehicular ad hoc networks
WEP	Wired Equivalent Privacy
WIMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
ZRP	Zone Routing Protocol

1 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.

Various protocol aware jamming attacks that can be launched in an access point based 802.11b network are studied in [3]. 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.

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 [4], 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.

The performance analysis of misbehavior node attack in WiMAX system are investigated in [5]. In the first case study, the results with and without misbehavior node attack are compared in WiMAX Network. It is observed that due to misbehaving node, the performance of entire network is degraded by increasing delay in the network and the unwanted throughput in the network increases. In the second case study, an algorithm to detect misbehavior node attack is proposed as they can protect the unwanted communication from misbehavior node attack.

The problem of selective jamming in wireless networks is addressed in [6]. The effectiveness of selective jamming attacks are illustrated by implementing such attacks against the TCP protocol. The feasibility of selective jamming attacks are illustrated by performing realtime packet classification.

In this paper, the effects of Pulse Jammer Attack, Misbehavior Node attack and Byzantine security attacks on MANET network topology are studied using DSR, AODV, OLSR and GRP routing protocols. The purpose of this work is analysing the 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 and the results are compared.

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, performance metrics are provided for different network applications in addition to the whole network performance using different routing protocols.

The paper is organized as follows: in Chapter 2, characteristics of ad hoc wireless networks, IEEE 802.11 wireless communication standards are described. Quality

of Service (QoS) in IEEE 802.11, security in QoS and wireless channel characteristics are presented and some related equations are given in this chapter.

In Chapter 3, an overview of the AODV, DSR, OLSR, and GRP routing protocols are provided.

In Chapter 4, security attacks in mobile ad hoc networks, attack characteristics, security services, the layer-wise security attacks that are mainly based on physical layer, network layer, link layer, transport layer and application layer are presented.

In Chapter 5, mobile ad hoc wireless network design is introduced by using OPNET simulator. Simulation tool, performance metrics and network attacks which are used in the simulations are presented and described. In addition, application configuration, profile configuration, mobility configuration settings, etc. are described.

Simulation results and analysis are given in Chapter 6, the normal networks are 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 and followed by the conclusion and future work in Chapter 7.

2 AD HOC NETWORKS

A mobile ad hoc network [7-10] is a set of wireless mobile nodes forming a dynamic autonomous network and it is also called infrastructure less networking. Mobile ad hoc network is the new advancement on field telecommunication technology which changes the entire concept of communication. This technology is formed as a collaboration of self organized node which formed few hundred to thousand of nodes. Nodes communicate with each other without the intervention of access points or base stations. This technology is efficient, effective, quick, and easy to deploy. Such a network may be connected to the larger internet. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those far apart rely on other nodes to relay messages as routers. For example, nodes A and C are able to communicate via node B despite being separated by more than the transmission range as represented in Figure 2.1.

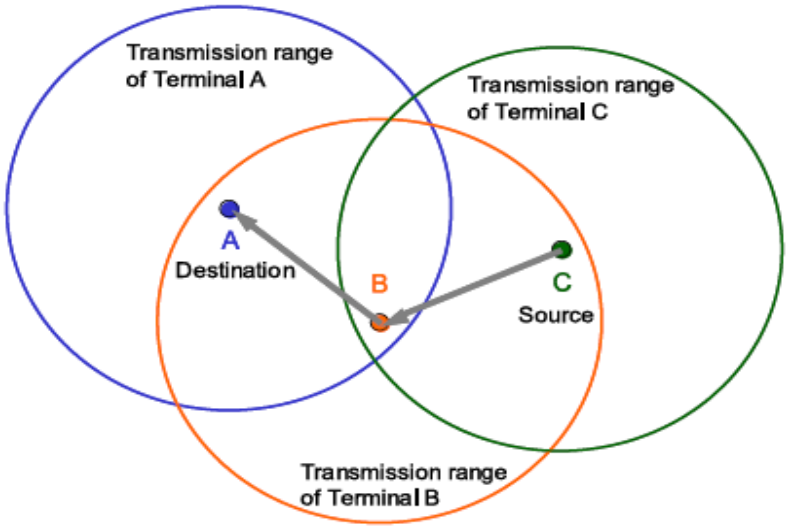


Figure 2.1 Communication in a MANET

Mobile ad hoc networks (MANETs) has no fixed infrastructure and depends on nodes to perform routing of data packets. Vehicular ad hoc networks (VANET) [11; 12] are a form of MANET, wherein, moving vehicles form the nodes of the mobile network. VANET uses the participating vehicle as wireless router or node, allowing vehicles to connect and create a network with wide range. VANETs differ

from typical MANETs, due to their characteristics like high mobility of nodes, timevarying density of nodes, frequent disconnections, highly partitioned network and dynamically changing topology, which makes them more challenging.

VANET is an emerging technology, which enables a wide range of applications, including road safety, passenger convenience, infotainment and intelligent transportation. They help to create safer roads by disseminating information regarding the road conditions and traffic scenario among the participating vehicles in a timely manner. Figure 2.2 represents an example of vehicular ad hoc network architecture.

In this research, mobile ad hoc networks are used for investigating their behavior in respect of security. MANETs are simulated with and without security attacks and an analyzing of these attacks and their impact on the routing mechanism are examined.

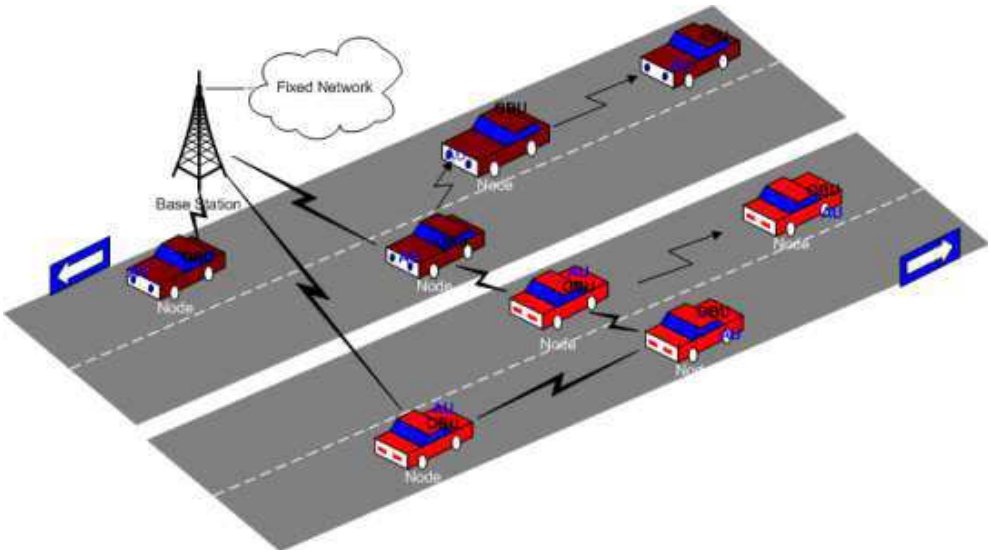


Figure 2.2 Vehicular ad hoc network architecture

2.1 Characteristics of Mobile Ad Hoc Networks

Mobile ad hoc networks eliminate the constraint of infrastructure set up and enable devices to create and join networks on the fly, any where, any time and virtually for

any application. Some of the characteristics which differentiate ad hoc wireless networks from other networks are discussed in below.

2.1.1 Wireless medium

In mobile ad hoc networks, nodes communicate wirelessly and share the same media. Wireless medium is less reliable than wired media and the channel is unprotected from outside signals.

2.1.2 Dynamic network topology

In mobile ad hoc networks, nodes can leave or join the network arbitrarily. They have temporary network topologies and they dynamically self-organize in arbitrary. Therefore, the network topology which is typically multi-hop, can change frequently and unpredictably. It causes route changes, frequent network partitions, and possibly packet losses.

2.1.3 Autonomous and infrastructureless

In mobile ad hoc networks, nodes can directly communicate with all the other nodes within their radio ranges. Mobile ad hoc networks does not depend on any established infrastructure or centralized administration. People and vehicles can be internetworked in areas without a preexisting communication infrastructure. Each node acts as an independent router and generates independent data. Network management is distributed across different nodes, which brings added difficulty in fault detection and management.

2.1.4 Limited energy resources

The MANETs consists of different set of devices such as laptops, computers, mobile phones etc. All of such devices have different computational power. In mobile ad hoc networks, there is a limited time they can operate without changing energy resources. Each mobile node which are battery power have limited power supply. Processing power is limited and that limits services and applications that can be supported.

2.2 Standards using in Ad Hoc Networks

The IEEE802.11 wireless local area network (WLAN) is a shared-medium communication network that transmits information over wireless links for all IEEE802.11 stations in its transmission range to receive.

Table 2.1 Comparison of 80.11a/b/g and 802.16 standards

Feature	**Wi-Fi (802.11b)**	**Wi-Fi (802.11a/g)**	**WIMAX (802.16)**
Primary Application	Wireless LAN	Wireless LAN	Broadband Wireless Access
Frequency Band	2.4 GHz	2.4GHz, 802.11g 5GHz, 802.11a	2 GHz to 11 GHz NLOS 10 GHz to 66 GHz NLOS
Channel Bandwidth	25 MHz	20 Hz	20 MHz
Max Data Rate	11 Mbit/s	54 Mbit/s	72 Mbit/s
MIMO streams	1	1	2x2
Half/Full Duplex	Half	Half	Full
Radio Technology	Direct Sequence Spread Spectrum	OFDM (64-channels)	OFDM (256-channels)
Bandwidth Efficiency	<=0.44 bps/Hz	<=2.7 bps/Hz	<=5 bps/Hz
Modulation	QPSK	BPSK,QPSK, 16QAM, 64QAM	BPSK, QPSK, 16QAM,64QAM, 256QAM
Forward Error Correction	None	Convolutional Code	Convolutional Code, Reed-Solomon
Outdoor Range	140 meters	120 meters for 802.11a, 140 meters for 802.11g	50 km
Access Protocol	CSMA/CA	CSMA/CA	Request/Grant

It is one of the most deployed wireless networks in the world and is highly likely to play a major role in multimedia home networks and next-generation wireless communications. The main characteristic of the IEEE 802.11 WLAN is its simplicity, scalability, and robustness against failures due to its distributed nature. IEEE 802.11 wireless networks can be configured into two different modes: ad hoc and infrastructure. In ad hoc mode, all wireless stations within the communication range can communicate directly with each other, whereas in infrastructure mode, an access point (AP) is needed to connect all stations to a distribution system (DS), and each station can communicate with others through the AP. Today, IEEE 802.11 wireless networks are widely installed in homes, corporate buildings, and hot spots. As shown in Table 2.1, WLAN and WIMAX are compared with each other.

2.3 Quality of Service (QoS) in IEEE 802.11

Quality of Services [13-15] is based on the application, a set of service performance and the effect of determining the degree of user satisfaction in how to provide their service according to European Telecommunications Standards Institute. QoS parameters are including bandwidth, delay, jitter (delay variation), packet loss for delivery of network services such as voice, video conferencing and other application which can control by network administrators to provide users consent.

With the increase in quality of service (QoS) needs in evolving applications, it is also desirable to support these services in MANETs. The resource limitations and variability further add to the need for QoS provisioning in such networks. However, the characteristics of these networks make QoS support a very complex process.

Many researchers have shown much interest in developing new medium access schemes to support QoS. Accordingly, the IEEE 802.11 working group is currently working on a new standard called 802.11e to enhance the original 802.11 medium access control (MAC) sublayer to support QoS. The original 802.11 WLAN MAC

sublayer employs a distributed coordination function (DCF) based on carrier sense multiple access with collision avoidance (CSMA/CA) for medium access, and is best known for its asynchronous best effort data transfer. In order to support QoS in 802.11 WLAN, the upcoming IEEE802.11e standard adds a new function called a hybrid coordination function (HCF) that includes both controlled contention-free and contention-based channel access methods in a single channel access protocol. The HCF uses a contention-based channel access method called enhanced DCF (EDCF) that operates concurrently with a controlled channel access mechanism based on a central polling mechanism. HCF supports both prioritized and parameterized medium access.

2.3.1 Quality of service metrics

QoS is usually defined as a set of service requirements that needs to be met by the network while transporting a packet stream from a source to its destination. The network is expected to guarantee a set of measurable prespecified service attributes to users in terms of end-to-end performance, such as delay, bandwidth, probability of packet loss, and delay variance (jitter) [15].

2.3.1.1 Delay

The 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. The flow delay per hop traffic is defined as in the following Equation 2.1 and 2.2 [16]:

$$D_{(i,k)} = D_k + D_{q(i,k)} \tag{2.1}$$

$$D_k = d_{proc} + d_{prop} + d_{trans} \tag{2.2}$$

where D_k : constant delay at single hop (k) due to processing delay (d_{proc}), propagation delay (d_{prop}) and transmission delay (d_{trans}).

$D_{q(i,k)}$: represent the queue delay of the (i) packet at (k) hop.

2.3.1.2 Bandwith

Bandwidth is concave in the sense that end-to-end bandwidth is the minimum of all the links along the path [15]. *B* in Equation represents the channel bandwidth specifically used for transmission of information in an OFDMA system. In OFDM systems, each user is allocated all subcarriers and hence resource management is limited to which time slots should be allocated to each user. This can be determined by the following Equation 2.3.

$$B = \frac{F_s N_{used}}{N_{FFT}} \tag{2.3}$$

Where B : effective channel bandwidth (Hz),

N_f: noise Figure (dB),

N_o: thermal noise level (dBm).

2.3.1.3 Throughput

Throughput is the ratio of total number of packets received successfully by the destination nodes to the number of packets sent by the source nodes. It is an important metric as it describes the loss rate. Thus, network throughput in turn reflects the maximum throughput that the network can support [17]. The cell throughput can be derived as following Equation 2.4 [18].

$$U_{i,j} = \frac{N_{used}}{T_s \sum_{k=1}^{n} W_k} n \tag{2.4}$$

Where $U_{i,j}$: cell or sector throughput of the sector j of the BS i and in the case of omni antenna,

N_{used}: number of data subcarriers,

T_s: symbol duration, n : number of SSs in the cell,

W_k: sum of weights of the more efficient transmission path from SS k to the BS: $\min (w^r+w^s, w^b)$.

2.3.1.4 Jitter

Jitter [19] is the ratio of transmission delay of the current packet and the transmission delay of the previous packet. Jitter can be calculated only if at least two packets have been received.

2.3.1.5 Packet loss

Packet loss 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 other devices.

Additionaly percentage of packets dropped that passed through malicious nodes indicates the percentage of total packets dropped that traverse malicious nodes when using each routing protocol, in the presence of different percentages of malicious nodes. Assuming that all the packets that pass through a malicious or compromised node were altered, this metric can be calculated as Equation 2.5 [7]:

$$\%\ of\ Packets\ Dropped\ that\ passed\ through\ Malicious\ Nodes = \left(\frac{No.\ of\ packets\ dropped\ by\ the\ benign\ nodes\ that\ are\ previously\ generated\ by\ or\ passed\ through\ any\ malicious\ node\ in\ the\ network}{Total\ number\ of\ packets\ communicated} \right) X\ 100 \quad (2.5)$$

The metric evaluates the degree to which the communication is secure, as packets passing through malicious nodes may possibly disrupt secure communication.

2.3.1.6 SINR

SINR is Signal to Interference plus Noise ratio can be determined following Equation 2.6 [20]:

$$SINR_r\left[dB\right] = 10\log\left(\frac{P(t,r)}{BN_fN_o + \sum_{t'\neq t} P(t',t)}\right) \quad (2.6)$$

Where t : parent node of the receiver r,

t' : different potential concurrent transmitters in the DL

2.3.2 Security in quality of service

Security can be considered a QoS attribute. Without adequate security, unauthorized access and usage may violate QoS negotiations. The nature of broadcasts in wireless networks potentially results in more security exposure. The physical medium of communication is inherently insecure, so we need to design security-aware routing algorithms for MANETs [15].

2.4 Wireless Channel Characteristics

The characteristics of the wireless communication channel between transmitter and receiver controls the performance of the overall system. In this section, the mobile radio environment which will be used in this thesis is introduced.

2.4.1 Attenuation

Strength of signal falls off with distance over transmission medium. Attenuation is greater at higher frequencies. Received signal must be enough to be detected and must be sufficiently higher than noise to be received without error. Attenuation can be determined following Equation 2.7:

Attenuation = P_r / P_t (2.7)

Where P_t : transmitted signal power,

P_r : received signal power,

2.4.2 Path loss

In a wireless environment, communication channel is very diverse between transmitter and receiver. Path loss is proportional to the square of the distance between the transmitter and receiver. Free-space path loss is the loss in signal strength of an electromagnetic wave.

Free space path loss is calculated for gain of antennas using Equation 2.8:

$$\frac{P_t}{P_r} = \frac{(4\pi d)^2}{\lambda^2} = \frac{(4\pi f d)^2}{c^2} \tag{2.8}$$

Where P_t : transmitted signal power,

P_r : received signal power,

λ = carrier wavelength,

d : propagation distance,

c : speed of light ($\approx 3 \times 10^8$ m/s),

where d and λ are in the same units (e.g., meters)

Free space loss is calculated for gain of antennas using Equation 2.9:

$$\frac{P_t}{P_r} = \frac{(4\pi)^2 (d)^2}{G_r G_t \lambda^2} = \frac{(\lambda d)^2}{A_r A_t} = \frac{(cd)^2}{f^2 A_r A_t} \tag{2.9}$$

Where G_t : transmitted gain,

G_r : received gain,

A_t : transmitted effective area,

A_r : received effective area.

2.4.3 Signal to noise ratio

Signal to Noise Ratio (SNR) is the difference between the received power and the channel noise.

Ratio of signal energy per bit to noise power density per Hertz is calculated using Equation 2.10:

$$\frac{E_b}{N_0} = \frac{S/R}{N_0} = \frac{S}{kTR} \tag{2.10}$$

Where E_b : signal energy associated with each user data bit,

N_0 : noise spectral density,

S: signal power,

R: user bit rate,

k: Boltzmann's constant

T_R : receiver noise temperature in degrees Kelvin.

Boltzmann's constant equala 1.38E-23 Joules/^{0}K.

2.4.4 Multipath propagation

Multipath describes the multiple paths a radio wave may follow between transmitter and receiver. Multipath obstacles reflect signals so that multiple copies with varying delays are received.

Fading, shadowing, reflection, and scattering are mechanisms in multipath propagation. Figure 2.3 shows an examole of multipath effects in wireless communication.

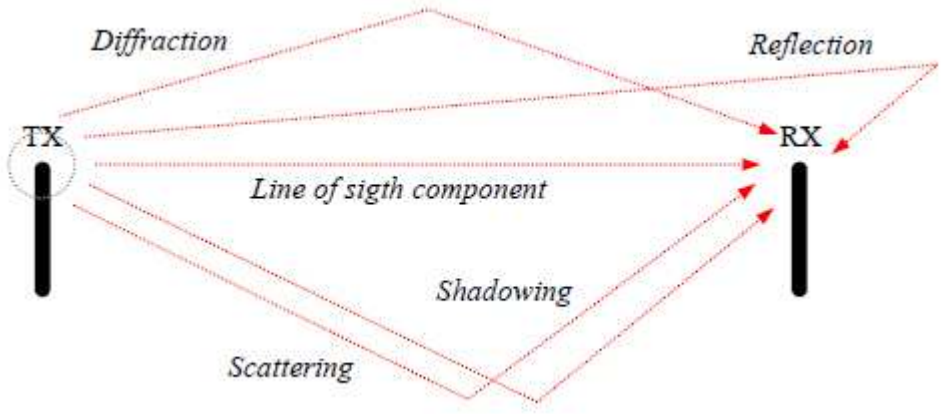


Figure 2.3 Illustration of multipath effects in wireless communication

Reflection occurs when signal encounters a surface that is large relative to the wavelength of the signal. Diffraction occurs at the edge of an impenetrable body that is large compared to wavelength of radio wave. Scattering occurs when incoming signal hits an object whose size is in the order of the wavelength of the signal or less.

Propagation losses are also an issue in wireless channels. These are of two basic types: diffusive losses and shadow fading. Diffusive losses arise because of the open nature of wireless channels. For example, the energy radiated by a simple point source in free space will spread over an ever-expanding spherical surface as the energy propagates away from the source. Shadow fading is typically modeled by attenuation (i.e., a multiplicative factor) in signal amplitude that follows a log-normal distribution. The variation in this fading is specified by the standard deviation of the logarithm of this attenuation [21].

There are two types of fading effects called as large-scale fading and small-scale fading that characterize mobile communications (Rappaport 1996). Large-scale fading represents the average signal power attenuation or path-loss due to the motion over large areas. In this type of fading the receiver is shadowed by obstacles between the tranmitterreceiver pair. Small-scale fading is used to describe the rapid fluctuations of the amplitude of a radio signal over a short period of time or travel distance [22].

Multi-path propagation is calculated using Equation 2.11 :

$$\mathrm{Pr} = Pt * \frac{\left[1+\eta^2+2*\eta\cos\left(\frac{4*\pi*h^2}{d*\lambda}\right)\right]}{4*\pi^2*\left(\frac{d}{\lambda}\right)^{\gamma}} \qquad (2.11)$$

Where η : reflection coefficent of the road,

λ : wavelength, h: antenna height, γ : path-loss coefficient,

d : distance between transmitter and receiver.

3 ROUTING PROTOCOLS

The routing protocols of MANETs are classified into two main categories, topology-based and position-based. Topology-based routing protocols [23] use the information about the links that exist in the network to perform packet forwarding. They can be further divided into proactive, reactive, and hybrid approaches.

A proactive routing protocol [24; 25] is also called "table driven" routing protocol. Using a proactive routing protocol, nodes in a mobile ad hoc network continuously evaluate routes to all reachable nodes and attempt to maintain consistent, up-to-date routing information. Therefore, a source node can get a routing path immediately if it needs one. Table-driven routing protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and they respond to changes in network topology by propagating updates throughout the network in order to maintain a consistent network view. Example of Proactive Routing Protocol is Optimized Link State Routing Protocol (OLSR).

A reactive routing protocol [1; 26] is often known as on- demand routing or source-initiated routing protocol. In a reactive routing protocol, a route discovery operation invokes a route-determination procedure. The discovery procedure terminates either when a route has been found or no route available after examination for all route permutations. On-Demand Routing Protocols are not maintained periodically. Here route tables are created when required. When the source node wants to connect to the destination node, it broad casts the route request (RREQ) packet to its neighbours. Just as neighbours of the source node receive the broadcasted request packet, they forward the packet to their neighbours and this action is happen until the destination is found. Afterward, the destination node sends acknowledgement to source node in the shortest path. The route remains in the route tables of the nodes through shortest path until the route is no longer needed. Examples of Reactive Routing Protocols are the Dynamic Source Routing (DSR), Ad Hoc on Demand Distance Vector Routing (AODV).

Hybrid ad hoc routing protocols [1; 19] combine local proactive routing and global reactive routing and overcome their shortcomings in order to achieve a higher level of efficiency and scalability. Normally, hybrid routing protocols for mobile ad hoc networks exploit hierarchical network architectures. Proper proactive routing approach and reactive routing approach are exploited in different hierarchical levels, respectively. Hybrid ad hoc routing protocol is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. Some of the existing hybrid protocols are Zone Routing Protocol (ZRP) [27; 28] and Temporally Ordered Routing Algorithm (TORA) [25; 27]. Figure 3.1 shows the prominent way of classifying MANET routing protocols.

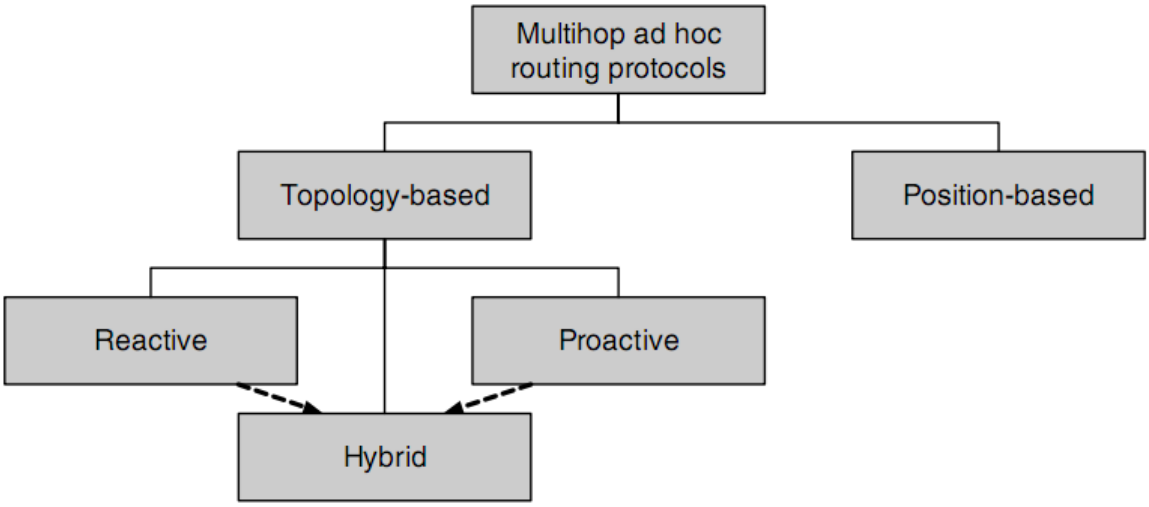


Figure 3.1 Classification of MANET routing protocols

In position based routing protocols [23; 24], the routing decisions are made on the basis of the current position of the source and the destination nodes, instead of using routing tables and network addresses and each node determines its own position through the use of GPS or some other type of positioning service [29; 30]. A location service is used by the sender of a packet to determine the position of the destination and to include it in the packet's destination address. The routing decision at each node is then based on the destination's position contained in the packet and the position of the forwarding node's neighbors. Position-based routing

thus does not require the establishment or maintenance of routes. The nodes have neither to store routing tables nor to transmit messages to keep routing tables up to date. As a further advantage, position-based routing supports the delivery of packets to all nodes in a given geographic region in a natural way. Table 3.1 represents the comparison of routing protocols in MANETs.

Table 3.1 Comparison of routing protocols in MANETs

Characteristics	DSR	AODV	OLSR	GRP	TORA
Routing Philosophy	Reactive	Reactive	Proactive	Position-based	Hybrid
Type of Routing	Source Routing	Hop by hop routing	Hop by hop routing	Hop by hop routing	Hop by hop routing
Frequency of Updates	As needed	As needed	Periodically	Based on mode of operation	Periodically
Multiple routes	Yes	No	No	No	No

3.1 The Dynamic Source Routing (DSR) Protocol

DSR [1; 25; 31; 32] is a reactive unicast routing protocol that utilizes source routing algorithm. It is similar to AODV in that it establishes a route on-demand when a transmitting mobile node requests one. However, it uses source routing instead of relying on the routing table at each intermediate device. In source routing algorithm, each data packet contains complete routing information to reach its dissemination. Additionally, in DSR each node uses caching technology to maintain route information that it has learnt.

The sender knows the complete hop-by-hop route to the destination, where the routes are stored in a route cache. This protocol is particularly designed for use in multi hop wireless ad hoc networks of mobile nodes. Basically, DSR protocol does not need any existing network infrastructure or administration and this allows the network to be completely self-organizing and self-configuring.

When a node in a mobile 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. This route request contains the address of the destination, along with the source node's address and a unique identification number. The sender will be waiting till the route is discovered. During waiting time, the sender can perform other tasks such as sending/forwarding other packets. As the route request packet arrives to any of the nodes, each node receiving the packet checks whether it knows of a route to the destination. If it does not, it adds its own address to the route record of the packet and then forwards the packet along its outgoing links. To limit the number of route requests propagated on the outgoing links of a node, a mobile only forwards the route request if the request has not yet been seen by the mobile and if the mobile's address does not already appear in the route record.

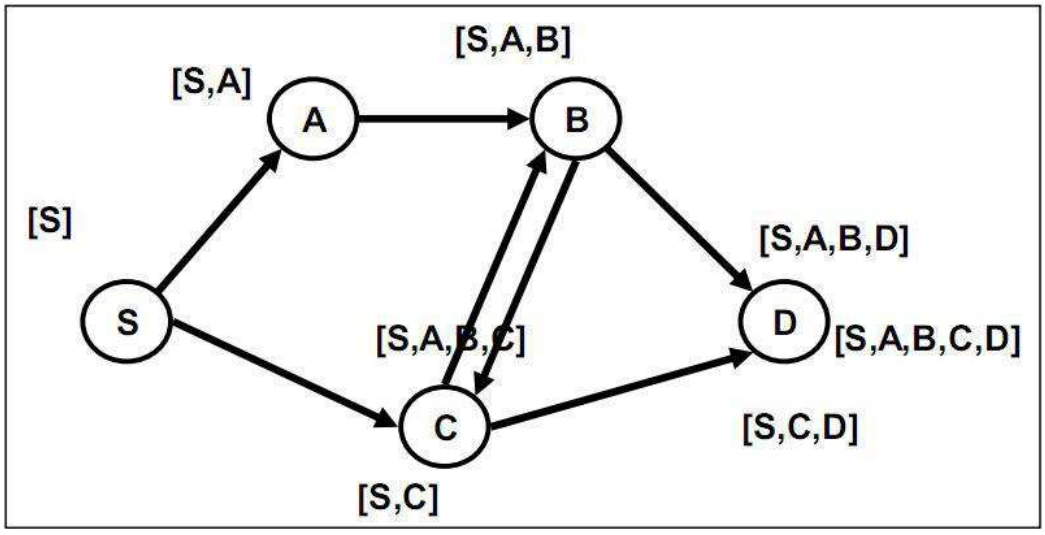


Figure 3.2 Source node's broadcast

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. RREQ and RREP packets are also source routed. The RREQ builds up the path traversed across the network. The RREP routes itself back to the source by traversing this path backward. The route carried back by the RREP packet is cached at the source for future use. By the time the packet reaches the destination or an intermediate node, it contains a route record yielding the sequence of hops taken.

In DSR, when the data link layer detects a link disconnection, a ROUTE_ERROR packet is sent backward to the source. After receiving the ROUTE_ERROR packet, the source node initiates another route discovery operation. Additionally, all routes containing the broken link should be removed from the route caches of the immediate nodes when the ROUTE_ERROR packet is transmitted to the source. Figure 3.2 and Figure 3.3 represents the propagation of request (PREQ) packet and the route reply with route record in DSR, respectively.

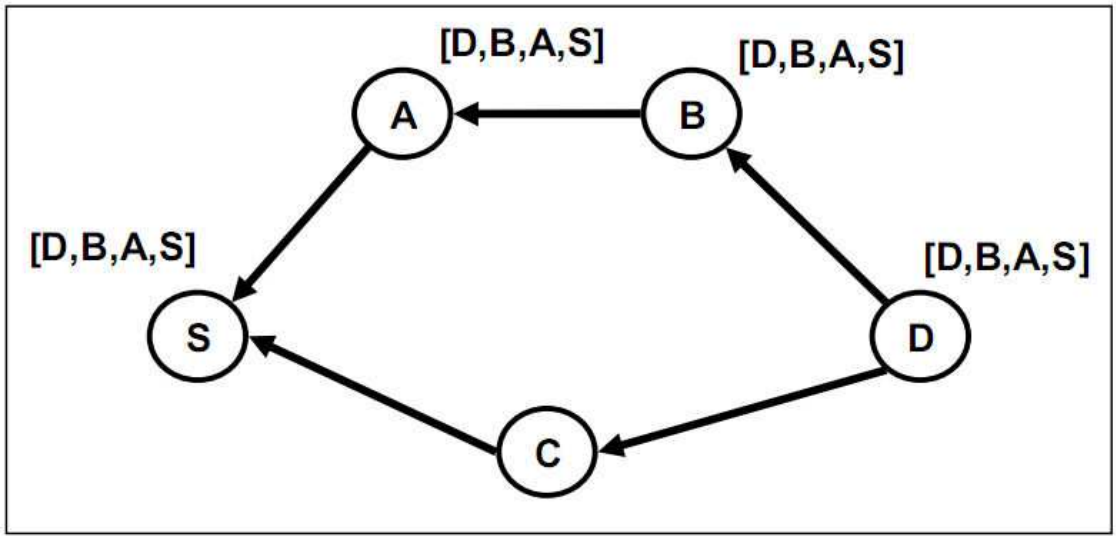


Figure 3.3 Destination node's reply

3.2 The Ad Hoc on Demand Distance Vector (AODV) Routing Protocol

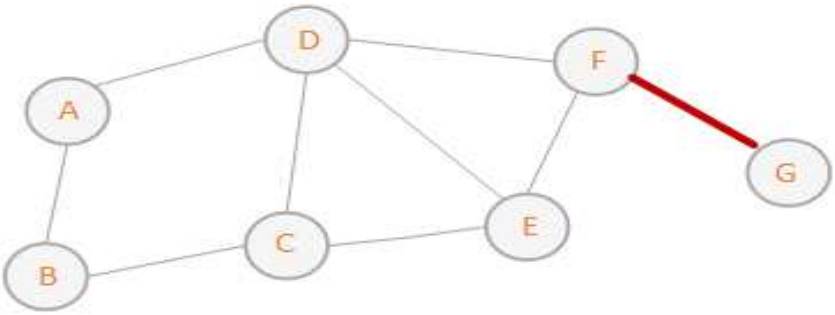
AODV routing protocol [1; 25; 31; 33] is a reactive unicast routing protocol for mobile ad hoc networks which only needs to maintain the routing information

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.

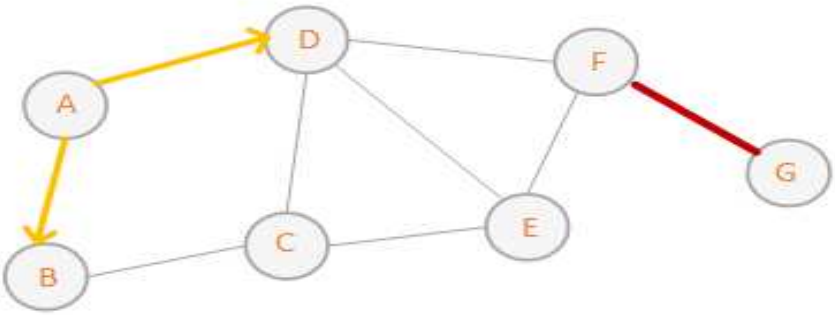
In AODV, when a source node wants to send a data packet to a destination node and does not have a route to the destination node, it initiates route discovery by broadcasting a route request (RREQ) to its neighbors. A RREQ includes addresses of the source and the destination, the broadcast ID, which is used as its identifier, the last seen sequence number of the destination as well as the source node's sequence number. Sequence numbers are important to ensure loop-free and up-to-date routes. The immediate neighbors who receive this RREQ rebroadcast the same RREQ to their neighbors. This process is repeated until the RREQ reaches the destination node.

Upon receiving the first arrived RREQ, the destination node sends a route reply (RREP) to the source node through the reverse path where the RREQ arrived. The same RREQ that arrives later will be ignored by the destination node. To reduce the flooding overhead, a node discards RREQs that it has seen before and the expanding ring search algorithm is used in route discovery operation. In addition, AODV enables intermediate nodes that have sufficiently fresh routes (with destination sequence number equal or greater than the one in the RREQ) to generate and send an RREP to the source node.

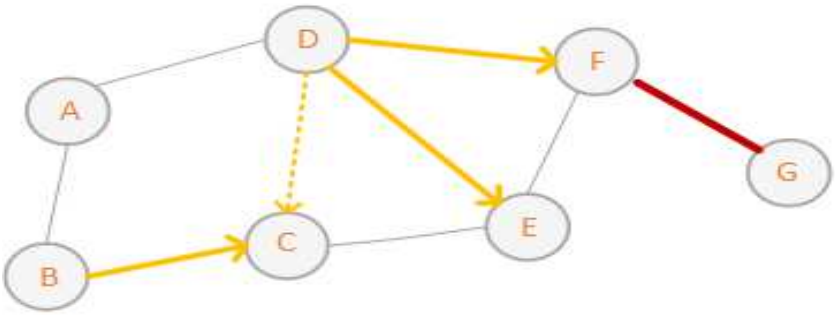
AODV uses only symmetric links and a RREP follows the reverse path of the respective RREP. Upon receiving the RREP packet, each intermediate node along the route updates its next-hop table entries with respect to the destination node. The redundant RREP packets or RREP packets with lower destination sequence number will be dropped. Figure 3.4 represents an example of RREQ messages in action where node A wants to send data packets to node G, Figure 3.5 shows an example of RREP messages in respect of AODV routing protocol, and Figure 3.6 represents an example of RERR messages in respect of AODV routing protocol.



- Node A needs to send a data packet to Node G
- Assume Node F knows a current route to Node G
- Assume that no other route information exists in the network (related to Node G)

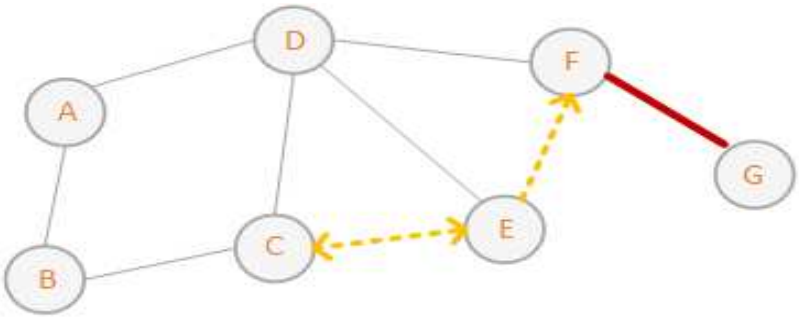


- Node A sends a RREQ packet to its neighbors
- source_addr = A
- dest_addr = G
- broadcast_id = broadcast_id + 1
- source_sequence_# = source_sequence_# + 1
- dest_sequence_# = last dest_sequence_# for Node G

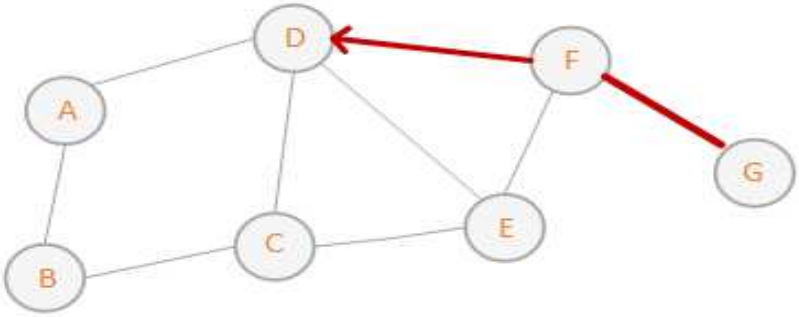


- Nodes B and D verify that this is a new RREQ and that the source_sequence_# is not stale with respect to the reverse route to Node A
- Nodes B and D forward the RREQ
  -Update source_sequence_# for Node A
  -Increment hop_cnt in the RREQ packet

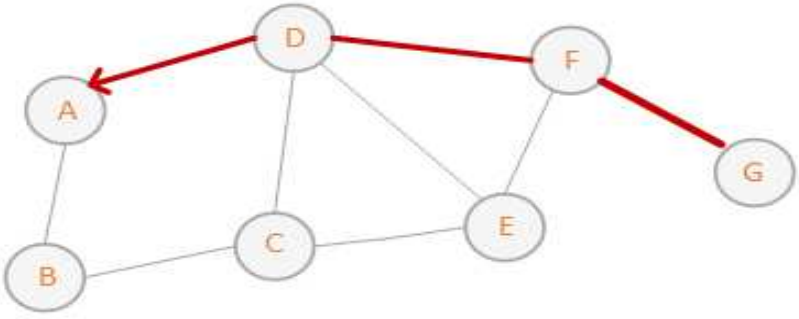
Figure 3.4 Example of AODV RREQ messages



- RREQ reaches Node F, which knows a route to G
  -Node F must verify that the destination sequence number is less than or equal to the destination sequence number it has recorded for Node G
- Nodes C and E will forward the RREQ packet, but the receivers recognize the packets as duplicates

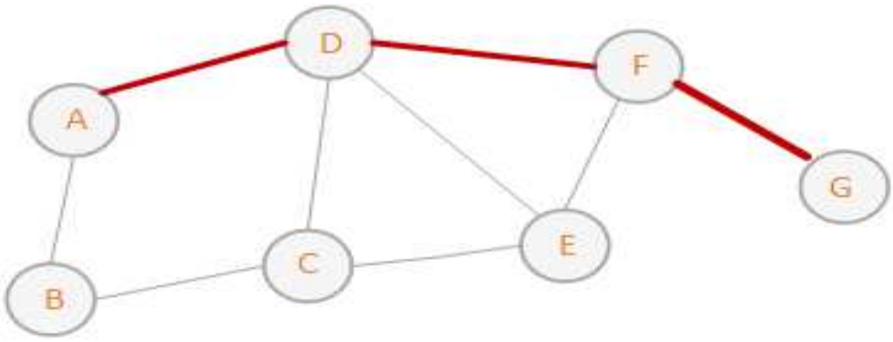


- Node F knows a route to Node G and sends an RREP to Node D
  -source_addr = A
  -dest_addr = G
  -dest_sequence_# = max(own sequence number, dest_sequence_# in RREQ)
  -hop_cnt = 1



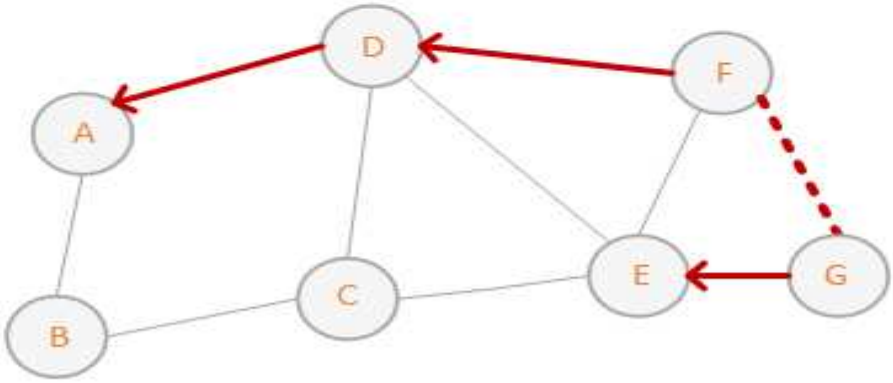
- Node D verifies that this is a new route reply (the case here) or one that has a lower hop count and, if so, propagates the RREP packet to Node A
  -Increments hop_cnt in the RREP packet

Figure 3.5 Example of AODV RREP messages



- Node A now has a route to Node G in three hops and can use it immediately to send data packets
- Note that the first data packet that prompted path discovery has been delayed until the first RREP was returned

- Route changes can be detected by...
  - -Failure of periodic HELLO packets
  - -Failure or disconnect indication from the link level
  - -Failure of transmission of a packet to the next hop (can detect by listening for the retransmission if it is not the final destination)
- The upstream (toward the source) node detecting a failure propagates an route error (RERR) packet with a new destination sequence number and a hop count of infinity (unreachable)
- The source (or another node on the path) can rebuild a path by sending a RREQ packet



- Assume that Node G moves and link F-G breaks
- Node G issues an RERR packet indicating the broken path
- The RERR propagates back to Node A
- Node A can discover a new route

Figure 3.6 Example of AODV RERR message

An important feature of AODV is the maintenance of timer-based states in each node, regarding utilization of individual routing table entries. A routing table entry is expired if not used recently. A node uses hello messages to notify its existence to its neighbors. Therefore, the link status to the next hop in an active route can be monitored. A set of predecessor nodes is maintained for each routing table entry, indicating the set of neighboring nodes which use that entry to route data packets. When a node discovers a link disconnection, it broadcasts a route error (RERR) packet to its neighbors, which in turn propagates the RERR packet towards nodes whose routes may be affected by the disconnected link. Then, the affected source can re-initiate a route discovery operation if the route is still needed. In contrast to DSR, RERR packets in AODV are intended to inform all sources using a link when a failure occurs.

3.2.1 The differences between DSR and AODV

DSR has access to a significantly greater amount of routing information than AODV. For example, in DSR, using a single request-reply cycle, the source can learn routes to each intermediate node on the route in addition to the intended destination. Each intermediate node can also learn routes to every other node on the route. Promiscuous listening of data packet transmissions can also give DSR access to a significant amount of routing information. In particular, it can learn routes to every node on the source route of that data packet. In the absence of source routing and promiscuous listening, AODV can gather only a very limited amount of routing information. In particular, route learning is limited only to the source of any routing packets being forwarded. This usually causes AODV to rely on a route discovery flood more often, which may carry significant network overhead. The current specification of DSR does not contain any explicit mechanism to expire stale routes in the cache, or prefer “fresher” routes when faced with multiple choices.

In contrast, AODV has a much more conservative approach than DSR. When faced with two choices for routes, the fresher route (based on destination

sequence numbers) is always chosen. Also, if a routing table entry is not used recently, the entry is expired.

The route deletion activity using RERR is also conservative in AODV. By way of a predecessor list, the error packets reach all nodes using a failed link on its route to any destination. In DSR, however, a route error simply backtracks the data packet that meets a failed link. Nodes that are not on the upstream route of this data packet but use the failed link are not notified promptly [31].

In AODV, there is no need for system-wide broadcasts due to local changes, in contrast to DSR. AODV has multicasting and uncasting routing protocol property within a uniform framework. Source node, destination node and next hops are addressed using IP addressing. AODV builds routes using a route request / route reply cycle.

3.3 Optimized Link State Routing (OLSR) Protocol

OLSR Protocol, as defined in [7; 19; 25; 34], is a proactive routing protocol where the routes are always immediately available when needed. It is often called table-driven protocol as it maintains and updates its routing table frequently.

In OLSR, each node intermittently broadcasts its routing table, allowing each node to build an inclusive view of the network topology. The nature of this protocol creates a large amount of overhead and in order to reduce overhead, it limits the number of mobile nodes that can forward network wide traffic and for this purpose it use Multi Point Relays (MPRs), which are responsible for forwarding routing messages and optimization for flooding operation. In OLSR, each node selects its own MPR from its neighbors, such that, it may reach each two hop neighbor via at least one MPR, then it can forward packets, if control traffic received from a previous hop has selected the current node as a MPR. Each MPR node maintains the list of nodes that were selected as an MPR; this list is called an MPR selector list. Only nodes selected as MPR nodes are responsible for advertising, as well as forwarding an MPR selector list advertised by other MPRs.

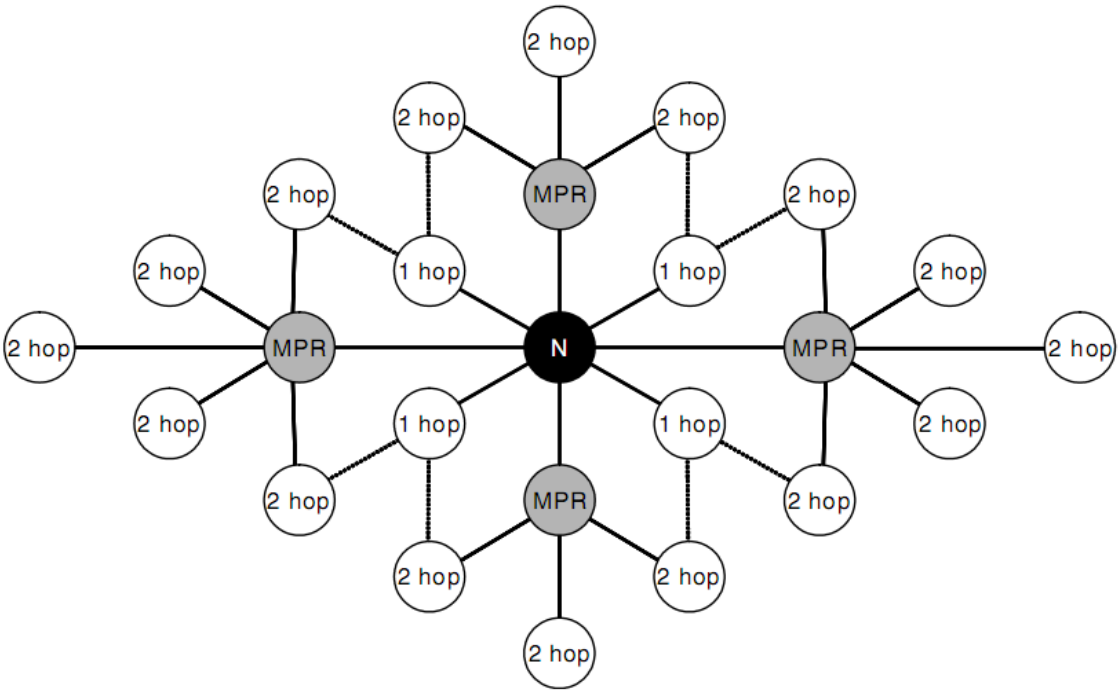


Figure 3.7 Flooding packets using MPR

Generally, OLSR has also three types of control messages such that HELLO message, Topology Control (TC) message and Multiple Interface Declaration (MID) mesage. The Hello message is transmitted for sensing the neighbor and for Multi-Point Distribution Relays (MPR) 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.

In OLSR, each node generates a HELLO message periodically. A node's HELLO message contains its own address and the list of its one-hop neighbors. By exchanging HELLO messages, each node can learn a complete topology up to two hops. HELLO messages are exchanged locally by neighbor nodes and are not forwarded further to other nodes. Nodes maintain information of neighbors and MPRs by sending and receiving HELLO messages from its neighbors.

A TC message is the message that is used for route calculation. Mobility causes, route change and topology changes very frequently and TC messages are

broadcasted throughout the network. In OLSR, each MPR node advertises TC messages periodically. A TC message contains the list of the sender's MPR selector. In OLSR, only MPR nodes are responsible for forwarding TC messages. Upon receiving TC messages from all of the MPR nodes, all mobile nodes maintain the routing table that contains routes to all reachable destination nodes. Figure 3.7 represents the flooding packets in OLSR.

Associated with each neighbour is an attribute including the directionality of the link to that neighbour. The node is labeled symmetric if the link to the neighbour is bidirectional, or asymmetric if a Hello has been received from that node but the link has not been confirmed as bidirectional. When a node receives this Hello message from each of its neighbours, it obtains complete knowledge of its two-hop neighbour set at that point in time. Further, if its own address is listed in the Hello message, it knows the link with that neighbour is bidirectional. It can then update the status of that neighbour to be symmetric. Figure 3.8 represents the symmetric link formation for OLSR protocol.

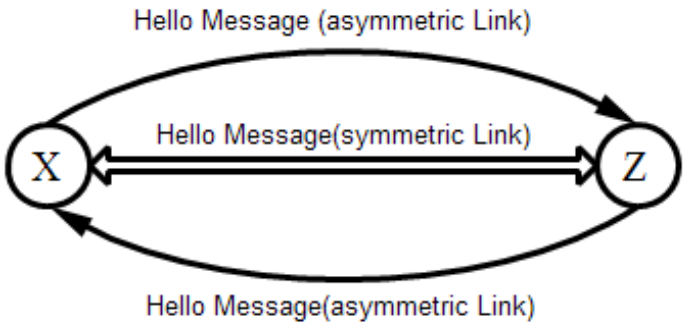


Figure 3.8 OLSR symmetric link formation (Hello Message Exchange)

3.4 Geographic Routing Protocol (GRP)

GRP [11; 24; 35] also known as position-based routing, 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. Under the assumption of bidirectional connectivity, geographic routing can be efficiently implemented on a planar sub-graph of the one-hop connectivity graph.

The most commonly used geographic routing algorithms are greedy routing and face routing. In greedy forwarding, the data packet is brought closer to the destination in each step by the nodes forwarding it to the most suitable neighbor. The suitable neighbor is the one which reduces the distance to the destination in each step. In face routing, the regions are considered to be separated by the edges of a planar graph. The algorithm takes a way around the face; it returns to the point closest to the destination and explores the next face closer to the destination.

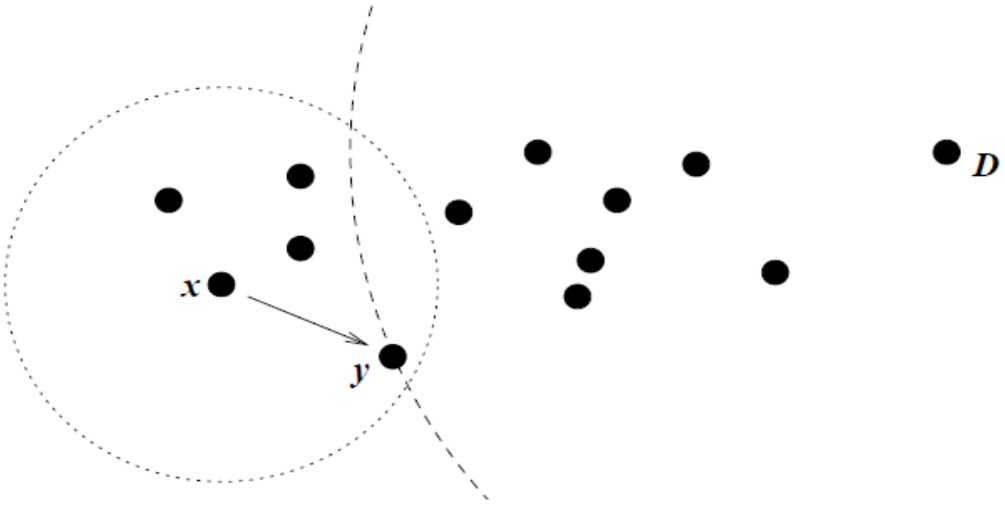


Figure 3.9 Greedy forwarding example. *y* is *x*'s closest neighbor to *D*.

In Figure 3.9, x receives a packet for destination D. Radio range of x is denoted by the dotted circle about x, and the arc with radius equal to the distance between y and D is shown as the dashed arc about D. x forwards the packet to y, as the

distance between y and D is less than that between D and any of x's other neighbors. This greedy forwarding process repeats until the packet reaches D [36].

Face routing always finds a path to the destination. Greedy forwarding fails if there is no next hop among the neighbors which is closer to the destination. When no neighbor provides progress towards the destination, perimeter routing must be used where the next-hop is selected to traverse the perimeter of the region where greedy forwarding fails. Traditional perimeter routing requires the sender to know all its neighbors so that it can construct a planar subgraph. Perimeter mode forwarding continues as long as there is no better greedy next hop neighbor. The state required at each node depends only on the node density. Figure 3.10 represents an example of position-based routing protocol.

In position-based routing, route breakups will frequently occur. It is induced by nodal mobility or nodal and link failures as well as by fluctuations in the communications transport quality experienced across the networks communications links. In addition to that, it is caused by signal interferences, fading and multi-path phenomena, producing environmental noise and signal interference processes. On the other hand, route breakups lead the frequent operation of rebuilding routes that consume lots of the network resources and the energy of the nodes.

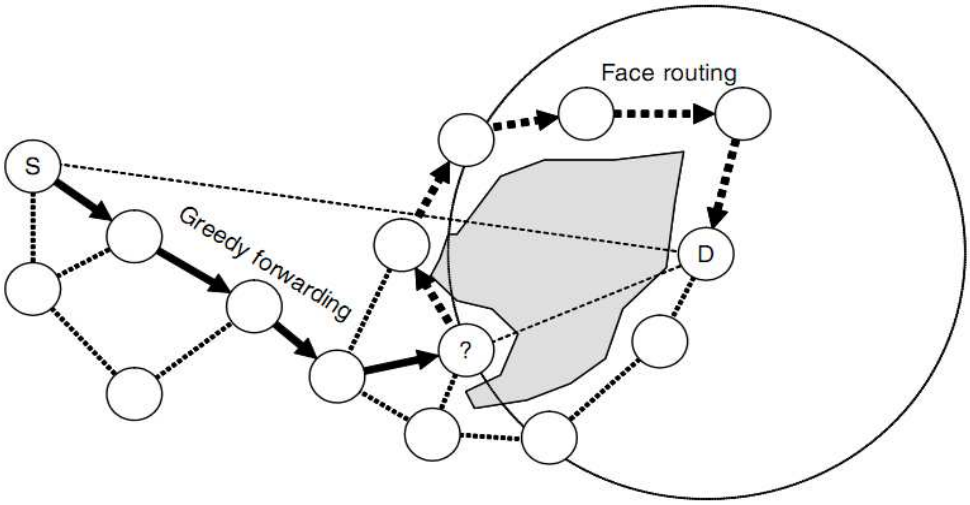


Figure 3.10 Example of position-based routing protocol

4 SECURITY ATTACKS IN MOBILE AD HOC NETWORKS

Ad hoc networks are more vulnerable than the traditional wired networks. Security is much more difficult to maintain and malicious attackers can easily disrupt network operations by violating protocol specifications in ad hoc networks. In the following subsections, possible attacks on routing protocols and layer-wise security attacks against ad hoc networks are discussed in detail.

4.1 Attack Characteristics

Open medium, lack of central monitoring, dynamic topology, no clear defense mechanism, distributed operation and resource constraints are some of the unique characteristics that exist in the ad hoc networks. They increase the vulnerability of such networks. Examples include looking at the behaviour of network attacks, i.e., passive and active which are represented in Figure 4.1, the source of the attacks, i.e., external and internal, the processing capability of the attackers, i.e., mobile and wired and the number of the attackers, i.e., single and multiple.

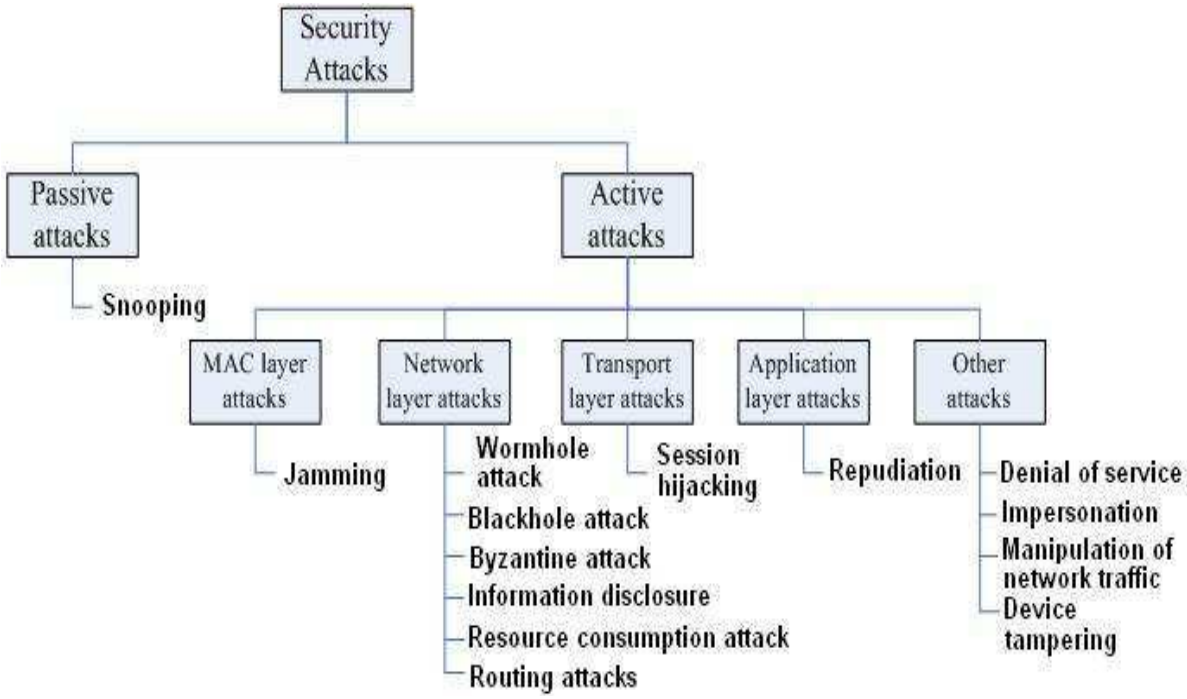


Figure 4.1 Classifications of passive and active attacks

4.1.1 Active and passive attacks

In active attack [8; 37], the attacker disrupts the performance of the network, steal important information and try to destroy the data during the exchange in the network. Active attacks can be an internal or an external attack. The active attacks destroy the performance of the network, in such case they act as an internal node in the network and it is easy for the attacker to exploit any internal node. Active attacks actively alter the data with the intention to obstruct the operation of the targeted networks. Examples of active attacks comprise actions such as message modifications, message replays, message fabrications and the denial of service attacks.

Passive attacks [8; 37] do not disrupt the normal operations of the network. Before the attacker launch an attack against the network, the attacker has enough information about the network that it can easily hijack and inject attack in the network. Examples of passive attacks in mobile ad hoc networks are eavesdropping attacks and traffic analysis attacks. Figure 4.2 represents the active and passive attacks for ad hoc networks.

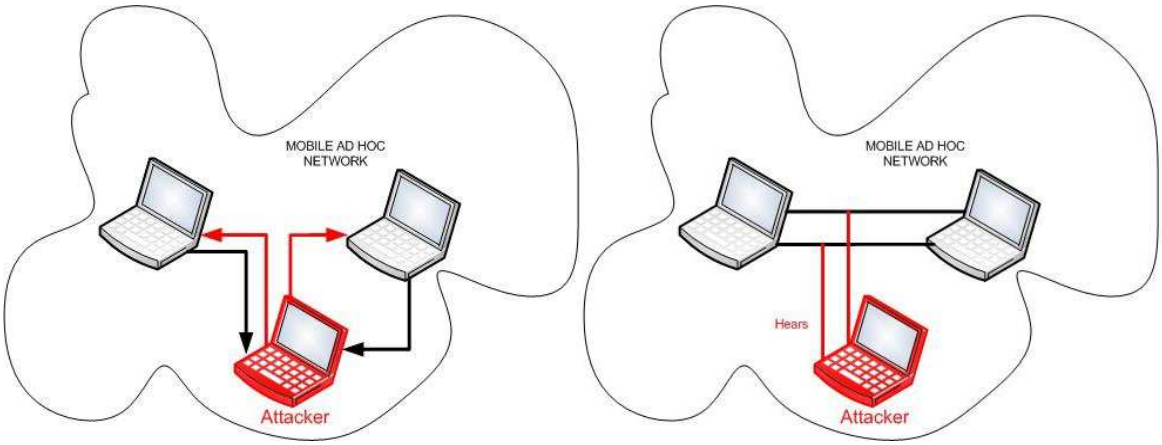


Figure 4.2 Active and passive attacks in MANETs

4.1.2 External and internal attacks

External attacks [8; 37] are typically active attacks that are targeted e.g. to cause congestion, propagate incorrect routing information, prevent services from working

properly or shut down them completely. External attacks can typically be prevented by using standard security mechanisms such as firewalls where the access of unauthorized person to the network can be mitigated, encryption and so on.

Internal attacks [8; 37] are typically more severe attacks, since the adversaries are already part of the mobile ad hoc network as authorized nodes. Internal attacks are much more severe attacks then external attacks and difficult to detect when compared to external attacks. Internal nodes are identified as compromised nodes if the external attackers hijacked the authorized internal nodes and are then using them to launch attacks against the mobile ad hoc networks. Security requirements such as authentication, confidentiality and integrity are severely vulnerable in the mobile ad hoc networks with the compromised internal nodes. Figure 4.3 shows the external and internal attacks in the ad hoc wireless networks.

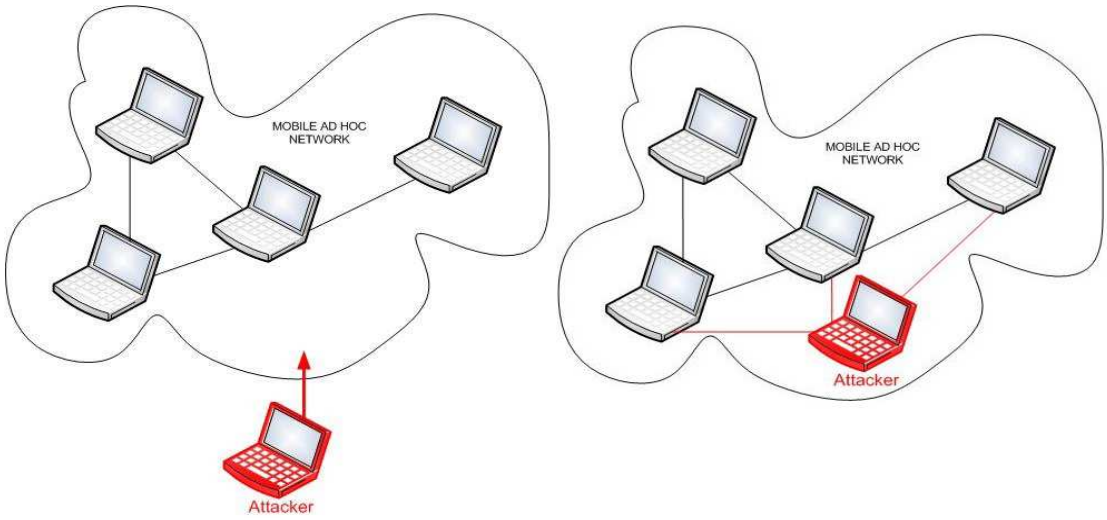


Figure 4.3 External and internal attacks in ad hoc networks

4.1.3 Mobile and wired attacks

Mobile attackers have the same capabilities as the other nodes in the ad hoc networks. Since they have the same resources limitations, their capabilities to harm the networks operations are also limited. They are not capable to launch the network jamming attacks to disrupt the whole networks operations.

Wired attackers are capable of gaining access to the external resources such as the electricity. Existence of the wired attackers in the mobile ad hoc networks is always possible. Since they have more resources, they could launch more severe attacks in the networks, such as jamming the whole networks or breaking expensive cryptography algorithms [8].

4.1.4 Single and multiple attackers

Attackers might choose to launch attacks against the ad hoc networks independently or by colluding with the other attackers. One man action or single attackers usually generate a moderate traffic load as long as they are not capable to reach any wired facilities. Since they also have similar abilities to the other nodes in the networks, their limited resources become the weak points to them.

However, if several attackers are colluding to launch attacks, defending the ad hoc networks against them will be much harder. Colluding attackers could easily shut down any single node in the network and be capable to degrading the effectiveness of network's distributed operations including the security mechanisms [8; 38].

4.2 Security Attack Types In Ad Hoc Networks

The fundamental characteristics of ad hoc networks make them susceptible to many network attacks. There are many types of attacks in different layers. The intruder nodes attack ad hoc networks using different ways. The layer-wise security attacks are mainly based on physical layer, network layer, link layer, transport layer and application layer.

4.2.1 Physical layer attacks

The physical layer [8; 39; 40] transmits the data packets through physical medium. The signal of radio waves are highly vulnerable on physical layer in ad hoc networks. The common radio wireless communication is easy to jam, because of

its nature of using open medium. Any attacker can overhear and disrupt the transmission of wireless network physically.

Physical layer security is important for ad hoc network security, because many attacks can take place in this layer. An attacker with sufficient transmission power and knowledge of the physical and medium access control layer mechanisms can gain access to the wireless medium. Such attacks could be made less useful by encrypting the communication signal, employing spread-spectrum communication technology, and using a tamper-resistant hardware. These attacks are simple to execute as compared to the other attacks. They do not require the complete knowledge of the technology. Some of the attacks identified at physical layer include eavesdropping, interference, and jamming etc.

4.2.1.1 Eavesdropping

Eavesdropping [38; 39; 40] can be defined as interception and reading of messages and conversations by unintended receivers. It includes the tracking and taping the information traversing on the network. The nodes in ad hoc networks share a wireless medium and the wireless communication use the RF spectrum and transmission by nature which can be easily captured with receivers tuned to the proper frequency. The main aim of such attacks is to obtain the confidential information that should be kept secret during the communication. As a result conveyed message can be eavesdropped as well as fake message can be injected into the network**.**

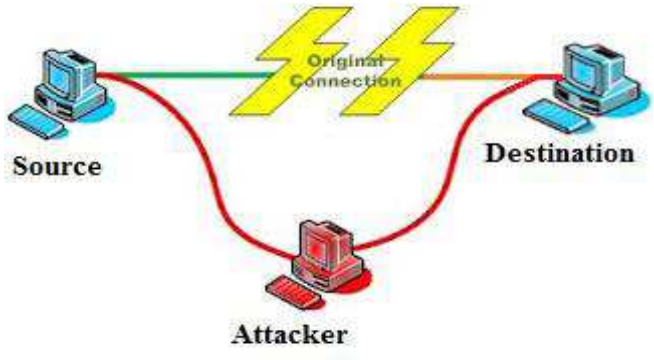


Figure 4.4 An attack on communication between source and destination

4.2.1.2 Jamming

Jamming [4; 39] is a special class of DoS attacks which are initiated by malicious node after determining the frequency of communication. Jammer attack is commonly used to wipe out the transmission on the target wireless networks. In this type of attack, the jammer transmits signals along with security threats. Jammer attack prevents sending and receiving data packets on ad hoc networks and causes message to be lost or corrupt.

4.2.1.3 Interference

In interference of radio signals [38; 39; 41], a powerful transmitter can generate signal that will be strong enough to overwhelm the target signal and can disrupt communications. The effects of such attacks depend on the routing protocol in use. Attacker can change the order of messages or attempt to replay old messages. Old messages may be replayed to reintroduce out of date information. Interference can happen with radio waves of MANETs, because WLAN use abandoned radio frequencies. Other electromagnetic devices operating in the infrared can overlap over the traffic.

4.2.2 Data link layer attacks

Data link layer is commonly known as link layer. It ensures the reliable communication link between neighbour nodes. Data link layer defines different networks and protocol characteristics. Many attacks can be launched in link layer by disrupting the cooperation of the protocols of this layer. In data link layer, adversaries might jam the communication links by sending huge data to the networks, or by replaying unnecessary packets to exhaust the networks' resources. Expensive cryptography algorithms and more sophisticated security measures could be very useful at this layer to protect the networks and to distinguish between valid and invalid packets traversed in the networks [8].

4.2.2.1 Traffic analysis

The attacks of traffic analysis [38; 39] identifies the characteristics of communication on radio wireless transmission. Data on who is connecting with whom, how often, how much, and when is simply available to any listener within range of the wireless network. Traffic analysis can also be conducted as active attack by destroying nodes, which stimulates self organization in the network, and valuable data about the topology can be gathered. These attacks are not considerable for ad hoc networks but they are fall into other WLAN attacks.

4.2.2.2 Attacks in IEEE 802.11 MAC

Many attacks can be thrown in link layer by unsettling the teamwork of the protocols of this layer. MAC protocols have to coordinate the transmission of the nodes on the shared communication or transmission medium. The IEEE 802.11 MAC is susceptible for DoS attacks. To launch the DoS attack, the attacker may exploit the binary exponential backoff scheme. For example, the attacker may corrupt frames easily by adding some bits or ignoring the ongoing transmission. Among the contending nodes, the binary exponential scheme favors the last winner which leads to capture effect. Capture effect means that nodes which are heavily loaded tend to capture the channel by sending data continuously, thereby resulting lightly loaded neighbors to backoff endlessly. Malicious nodes may take the advantage of this capture effect vulnerability. Moreover, it can cause a chain reaction in the upper level protocols using backoff scheme, like TCP window management [41].

4.2.2.3 IEEE 802.11 WEP weakness

The Wired Equivalent Privacy (WEP) [38; 40] was designed for pointing at giving some layer of security to wireless networks. It is well known that WEP is vulnerable to message privacy and message integrity attacks and probabilistic cipher key recovery attacks. Various security standards such as IEEE 802.11i, WPA, and IEEE 802.1 X were recommended to enhance the security issues in

802.11. In spite of their efficiency, these standards do not provide any strength to the security approach for monitoring of the verification in a disseminated architecture.

4.2.3 Network layer attacks

In network layer [4; 39], the attackers disturbs the network traffic by attacking on network layer, inject themselves in the path between source and destination, and get control of the network traffic flow. When the network is hijack, the attackers can create routing loops to form severe congestion.

As shown in Figure 4.5, the malicious node “X” can absorb important data by placing itself between source “A” and destination “D”. “X” can also divert the data packets exchanged between “A” and “D”, which results in significant end to end delay between “A” and “D”. This example shows that there is no route security between nodes, therefore any intruder node disturb the traffic on an ad hoc network.

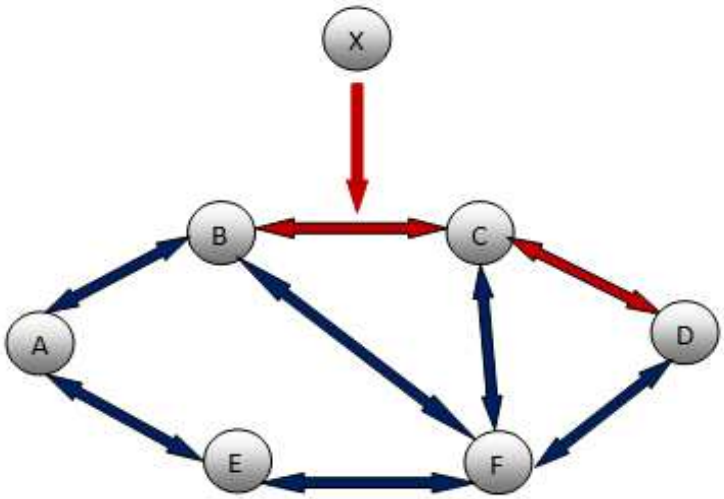


Figure 4.5 Routing attack by malicious node

4.2.3.1 Black hole attack

In black hole attack [38; 39], a malicious nodes trick all their adjoining nodes to attract all the routing packets to them. It exploits the routing protocol to promote

itself as having a good and valid path to a endpoint node. It tries to become an element of an active route. On receiving the request the malicious node sends a fake reply with extremely short route. In Figure 4.6, malicious node “4” advertises itself in such a way that it has a shortest route to the destination. When source node “S” wants to send data to destination node “D”, it initiates the route discovery process. The malicious node “4” when receives the route request, it immediately sends response to source. If reply from node “4” reaches first to the source than the source node “S” ignores all other reply messages and begin to send packet via route node “2”. As a result, all data packets are consumed or lost at malicious node.

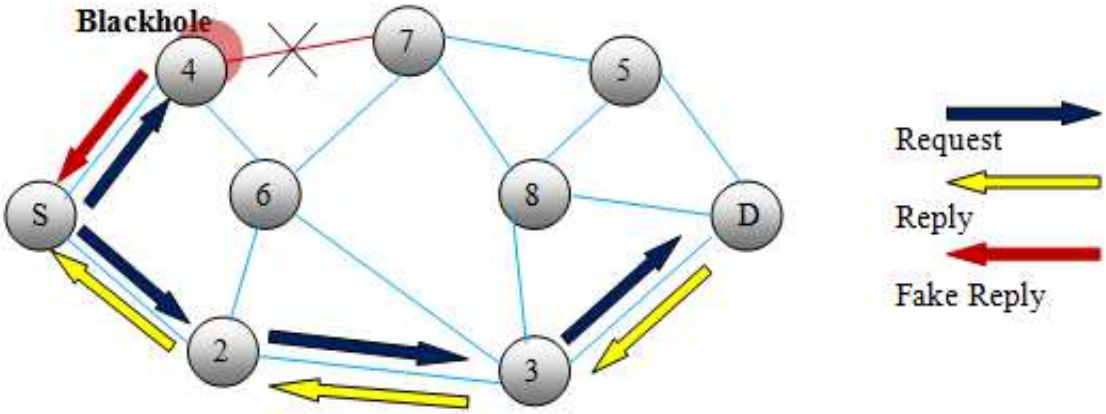


Figure 4.6 Blackhole attack

4.2.3.2 Wormhole attack

Wormhole attack [39; 41] takes place when two geographically separated adversaries create a tunnel called wormhole tunnel and uses encapsulation and decapsulation to make a false route between two malicious nodes. The tunnel is created either using a wired link or by having a long range high bandwidth wireless link operating at a different frequency band.

Wormhole attack is similar to black hole attack. Both attacks share the similar phenomena, but wormhole atttacks work with a collision with other nodes.

The goal of wormhole attack is to affect the routing protocols of ad hoc networks such as AODV and DSR protocols. In this attack, a pair of conniving attackers record packets at one location and replay them at another location using a private network.

Figure 4.7 represents the wormhole attack. It is also possible for the attacker to forward each bit by the wormhole directly, without waiting for a whole packet to be received before start to tunnel the bits of the packet, in order to lessen delay introduced by the wormhole.

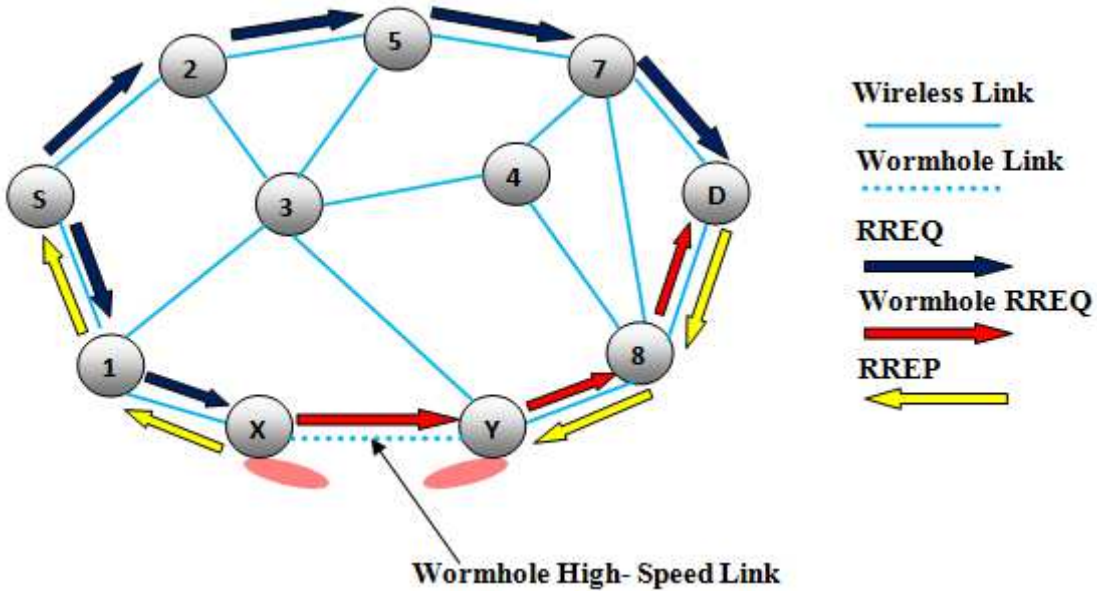


Figure 4.7 Wormhole attack

4.2.3.3 Byzantine attack

In Byzantine attacks [42; 43], 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. Byzantine attack drops, modifies and misroutes the forwarding packets in an attempt to disrupt the routing service. This kind of failures is not easy for identification, since the network seems to be operating very normally in the view of the user.

4.2.3.4 Rushing attack

In rushing attack [4; 26], the authorized node in on-demand routing protocol require a RREQ packet to find a path to destination. When a malicious node receives a RREQ packet from a source node, it rapidly broadcast it throughout the network topology before the other nodes on the network topology receives RREQ packets. When nodes on the network receive this original packet, data packets will be duplicate. Because, they already have received that data packet form the malicious node. Therefore, the original packet is discarded. On-demand routing protocols such as AODV and DSR routing protocols are more vulnerable to this attack, because whenever source node floods the route request packet in the network, an adversary node receives the route request packet and sends without any hop count update and delay into the network.

4.2.3.5 Flooding attack

In flooding attack [26; 38], attacker consumes the network resources such as bandwidth and consumes a node resources such as battery power. In RREQ flooding attack, the attacker broadcasts many RREQ packets time-to-time to the IP address which does not exist in the network. On demand routing protocols uses the route discovery process to obtain the route between the two nodes. In route discovery, the source node broadcast the RREQ packets in the network. Since the priority of the RREQ control packet is higher than the packet, RREQ packets are transmitted.

4.2.3.6 Resource consumption attack

Resource consumption attack [9; 44] is also known as the sleep deprivation attack. In MANETs, the battery-powered devices try to save energy by transmitting only when absolutely needed. The target of resource consumption attack is to send request of excessive route detection or needless packets to the victim node in order to consume the battery life. An attacker thus can upset the normal functionalities of the MANET.

4.2.3.7 Location disclosure attack

Location dislosure attack [39; 40] is a part of the information expose attack. The malicious node leaks information regarding the location or the structure of the network and uses the information for further attack. It gathers the node location information such as a route map and knows which nodes are situated on the target route.

4.2.4 Transport layer attacks

In transport layer, messages are exchanged on the end-to-end basis using secured routes established in the network layer. The security issues related to transport layer are authentication, securing end-to-end communications through data encryption, handling delays, packet loss and so on. The nodes in a MANET are vulnerable to the SYN flooding and session hijacking attacks [8; 40].

4.2.4.1 Session hijacking

In session hijacking [4; 38; 39; 40] an intruder node behaves as an authentic system. In this attack, the attacker spoofs the victim node's IP address, finds the correct sequence number, i.e., expected by the target and then launches various DoS attacks. The malicious node tries to collect secure data such as passwords, secret keys, logon names and other information from nodes. Figure 4.8 represents an example of session hijacking.

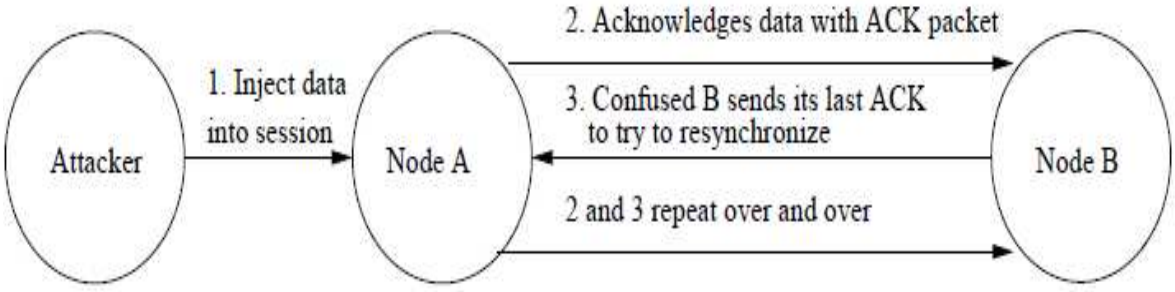


Figure 4.8 Session hijacking

4.2.4.2 SYN flooding

The SYN flooding attack is also Denial of Service (DoS) attack which is completed by generating a large number of half-opened TCP connections with a victim node. Due to nature of this attack malicious node never open the full connection to handshake. Figure 4.9 represents an example of SYN flooding attack.

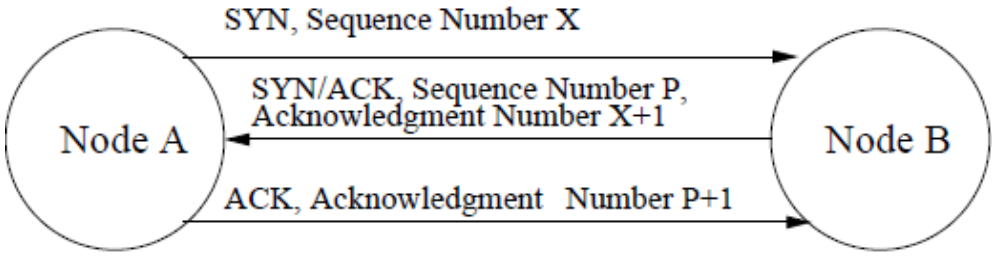


Figure 4.9 SYN flooding attack

4.2.5 Application layer attacks

Applications need to be designed to handle frequent disconnection and reconnection with peer applications as well as widely varying delay and packet loss characteristics. Application layer protocols are vulnerable to many DoS attacks. The application layer contains user data. It supports protocols such as HTTP, SMTP, TELNET and FTP, which provides many vulnerabilities and access points for attackers. The main attacks in application layer are repudiation attacks and malicious code attacks [39; 40].

4.2.5.1 Repudiation attacks

In Repudiation attacks [40] the solution that taken to solve authentication or non-repudiation attacks in network layer or in transport layer is not enough. Because, repudiation refers to a denial of participation in the communication.

4.2.5.2 Malicious code attacks

Various malicious codes such as virus, worm, spywares and Trojan horse attack both operating systems and user applications that cause the computer system and

network to slow down or even damaged. An attacker can produce this type of attacks in WLAN and can seek their desire information [41].

4.2.6 Multilayer attacks

In the following, the main multilyer attack types that emerge in the mobile ad hoc networks are discussed.

4.2.6.1 Denial of service (DoS) attacks

Denial of service attacks [45; 46], aim at the complete disruption of the routing function and therefore the whole operation of the ad-hoc network.In the practice, the attackers exactly use the radio jamming and battery exhaustion methods to conduct DoS attacks to the mobile ad hoc networks, which well correspond to the two vulnerabilities.

The denial of service attack has many forms. Distributed denial of service attack is a more severe threat: if the attackers have enough computing power and bandwidth to operate with, smaller ad hoc networks can be crashed or congested rather easily.

There are however more serious threats to ad hoc networks. Compromised nodes may be able to reconfigure the routing protocol or any part of it so that they send routing information very frequently, thus causing congestion or very rarely, thus preventing nodes to gain new information about the changed topology of the network. In the worst case the adversary is able to change routing protocol to operate arbitrarily. If the compromised nodes and the changes to the routing protocol are not detected, the consequences are severe, as from the viewpoint of the nodes the network may seem to operate normally.

4.2.6.2 Impersonation

The impersonation attack [47] is a severe threat to the security of mobile ad hoc network. These attacks, also called the spoofing attacks, are attacks where malicious node assumes the identity of another node in the networks. By

impersonating another node, attackers are able to receive routing messages that are directed to the nodes they faked.

As we can see, if there is not such a proper authentication mechanism among the nodes, the adversary can capture some nodes in the network and make them look like benign nodes. In this way, the compromised nodes can join the network as the normal nodes and begin to conduct the malicious behaviors such as propagate fake routing information and gain inappropriate priority to access some confidential information.

4.3 Security Services

The ultimate goals of the security solutions [25; 40; 45; 48] for ad hoc networks is to provide security services, such as authentication, confidentiality, integrity, authentication, nonrepudiation, anonymity and availability to mobile users. There is no single mechanism that will provide all the security services in ad hoc networks.

4.3.1 Availability

Availability means that a node should maintain its ability to provide all services regardless of the security state of it. Services are available whenever required.

4.3.2 Confidentiality

Confidential information is need to keep secret from all entities, so they don’t have the privilege to access them. Disclosure of information should only be accessible to the authorized individuals. Confidentiality protects data or a field in message.

4.3.3 Integrity

Integrity guarantees that a message being transmitted is never corrupted or altered. A message could be corrupted, because of being failures, or because of malicious attacks on the network.

4.3.4 Authentication

Authentication ensures that the access and supply of data is done only by the authorized parties. Authorization is generally used to assign different access rights to different level of users. For instance, we need to ensure that network management function is only accessible by the network administrator. Without authentication malicious nodes get access on the network and data can be modify without any prior notice to authorized nodes.

4.3.5 Nonrepudiation

It is the assurance that in a network communication both parties cannot later deny their participation. It should be verifiable for a secure network that the sender and the receiver in a transmission are really the parties who conducted to do the transmission. This is useful especially when we need to discriminate if a node with some abnormal behavior is compromised or not: if a node recognizes that the message it has received is erroneous, it can then use the incorrect message as an evidence to notify other nodes that the node sending out the improper message should have been compromised.

5 MOBILE AD HOC COMMUNICATION SYSTEM

In this section, mobile ad hoc system based on IEEE 802.11b standard is introduced. Firstly, manet_station (Wireless LAN Workstation) mobile nodes are used in the network and the results focuse on the whole network performance. For each network scenario, five jamming nodes, five misbehaving nodes and Byzantine nodes are placed in the network. The results are compared in the same graph with and without security attacks.

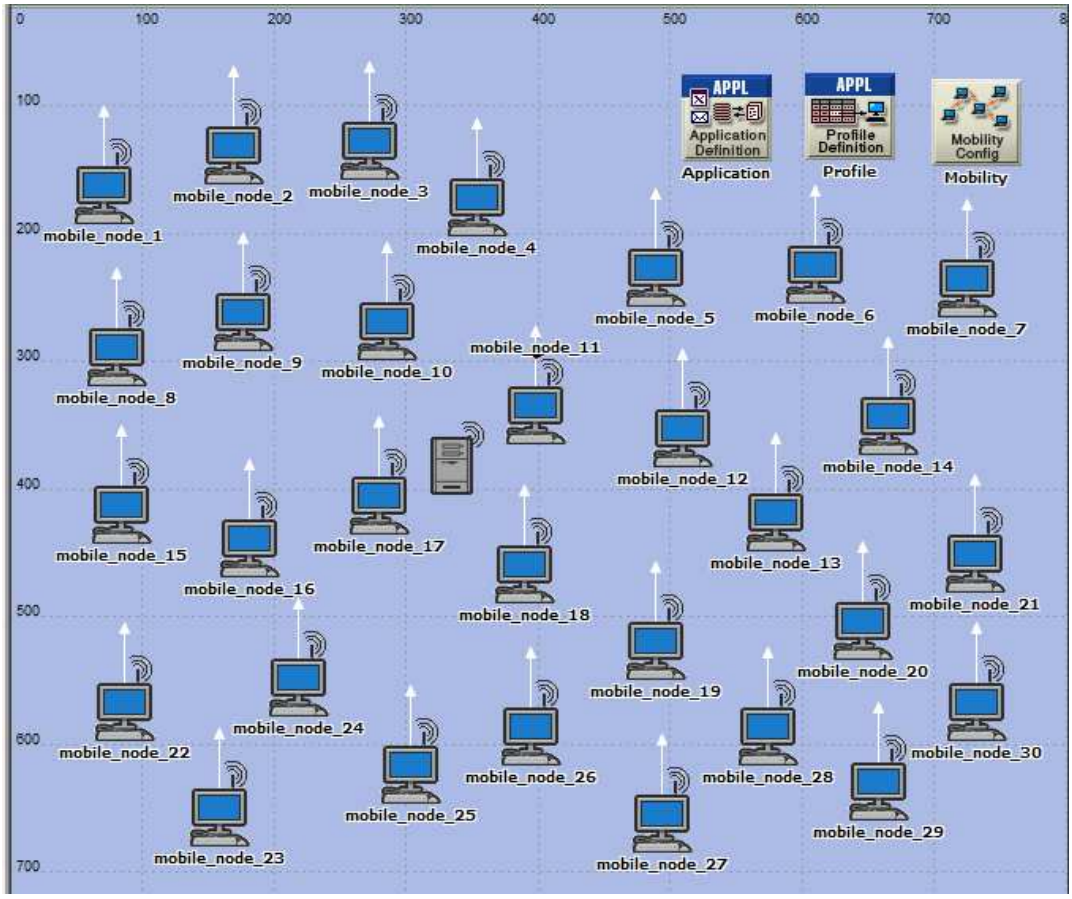


Figure 5.1 The normal network model

Subsequently, wlan_wkstn (Wireless LAN Workstation) mobile nodes are used, they have different attributes than manet_station nodes, so the network traffic loads, i.e., http, ftp, email, voice and video conferencing can be enabled on the wlan_wkstn mobile nodes which are placed in the network. Thus, the performance metrics can be examined in the figures for different network applications in the

addition to the whole network performance using different routing protocols. The security attacks are examined in the same figures and the results are compared. For each network model, the campus network scenario 800x800 (m) is created, 30 mobile ad nodes are deployed on OPNET Modeler 14.5 simulator. IEEE 802.11b network standard is used for mobile ad hoc nodes. The simulation run time is set at 300 sec. for each network simulation. Application configuration, profile configuration, and mobility configuration settings are configured to run the network as expected. Figure 5.1 represents the normal network model.

5.1 Simulation Tool

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 5.1.

Table 5.1 Simulation parameter

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

5.2 Performance Metrics

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

5.2.1 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.

5.2.2 Network load (bits/sec)

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

5.2.3 Delay (sec)

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

5.2.4 Data dropped (bits/sec)

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

5.2.5 Traffic received (bytes/sec)

Average number of bytes per second forwarded to all applications by the transport layers in the network.

5.3 Network Attacks Used in the Mobile Ad Hoc Networks

In this section, the security attacks such as Pulse Jammer attack, Misbehavior Node attack and Byzantine attack are explained. These attacks are implemented to the normal networks and the results are compared under different traffic loads in terms of performance metrics that is mentioned in Section 5.2.

5.3.1 Pulse Jammer attack

Jammer attack [3; 4; 38; 39; 40] generates noise on the wireless radio frequency medium to stop the communication in order to trigger the network. 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. Jammer frequency device of the targeted networks transmits radio signals with generating a continuous high radio frequency (RF) which is powerful signal that overwhelmed within the range of network transmission. Subsequently, jamming nodes causes corruption of the packets or they causes packet lost. The device that generates such a noise is called a jammer and the process is called jamming.

5.3.2 Byzantine attack

Byzantine attack [40] can be launched by a single malicious node or a group of nodes that work in cooperation. A compromised intermediate node works alone or set of compromised intermediate nodes works in collusion to form attacks. The compromised nodes may create routing loops, forwarding packets in a long route instead of optimal one, even may drop packets. This attack reduces the routing performance and also disrupts the routing services. Byzantine attacks are hard to detect.

5.3.3 Misbehavior Nodes attack

The purpose of misbehaving nodes [43; 49; 50; 51] 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. Dropping the packets occurs for many reasons. Misbehaving nodes might want to reserve the battery power of their own. They use a lot of bandwidth and they don’t collaborate with the other nodes in the network. 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.

5.4 Application Configuration Setting

Application configuration describe the types of traffic in the simulation model. The applications that is used in the network which contains manet_station nodes are FTP, E-Mail (medium load) and low Database traffic analyzing. For the network which contains wlan_wkstn nodes, the applications are FTP, Email (High Load), HTTP (Heavy Browsing), Voice (PCM Quality Speech), Video Conferencing (Low Resolution Video). Figure 5.2 represents the attributes of the application configuration setting

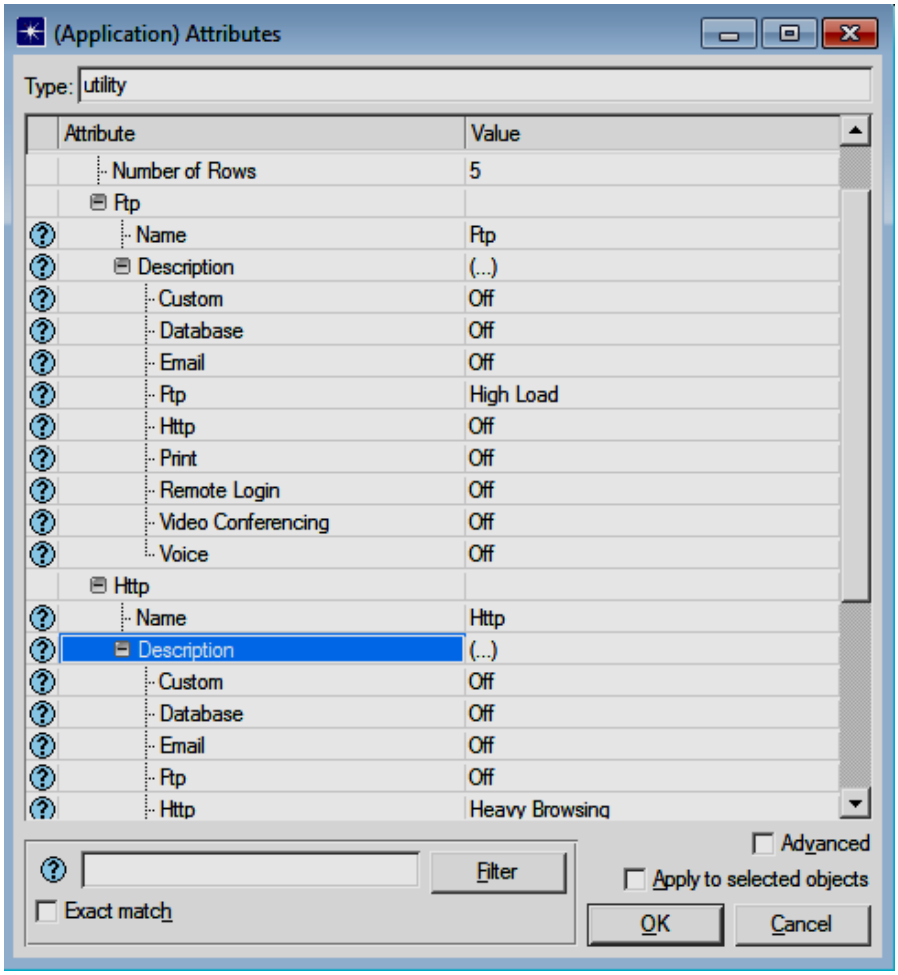


Figure 5.2 Application configuration setting

5.5 Profile Configuration Setting

The attributes, i.e., implementation period, number of repetition and duration of time, etc. of the traffic types defined in the applications are determined during the simulation. Profile configuration also specific the operation mode as serial (Ordered), serial (Random) and simultaneous. Figure 5.3 represents the attributes of the profile configuration setting.

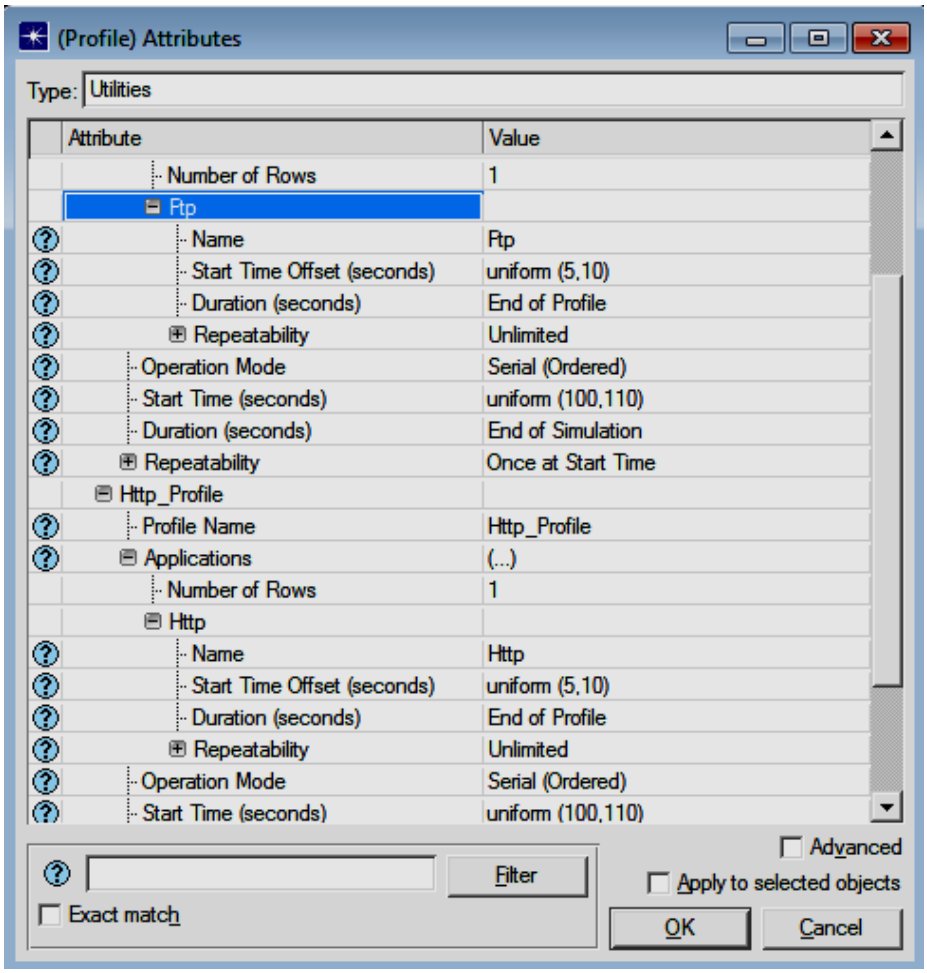


Figure 5.3 Profile configuration setting

5.6 Mobility Configuration Setting

The mobile ad hoc nodes move around in random directions with mobility configuration, thus the links between nodes can break and the new links establish by discovering new routing tables. Figure 5.4 represents the attributes of the

mobility configuration setting. Speed is set as “uniform_int (0,10)”, pause time is set as “constant (50)”, start time is set as “constant (10)” and stop time is left as default “end of simulation”.

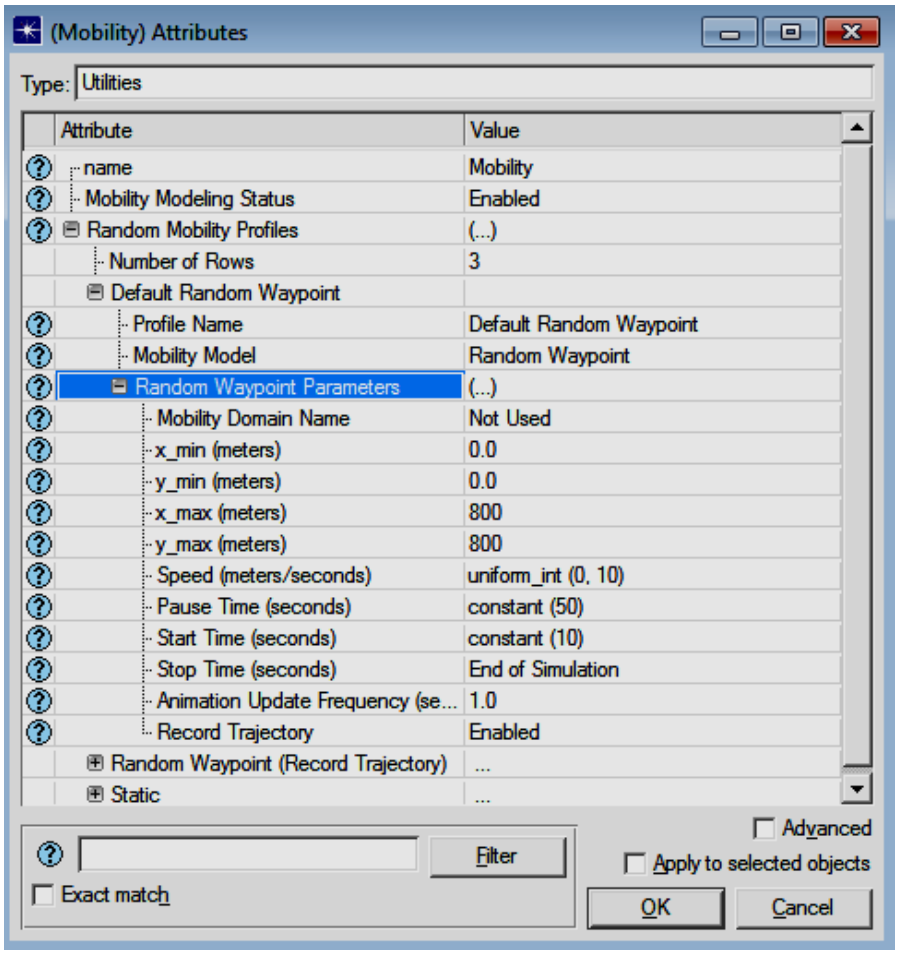


Figure 5.4 Mobile configuration setting

5.7 Traffic Model Setting for Wireless Stations

IEEE 802.11b standard is used for mobile ad hoc nodes with data rate 11Mbps. The packet interarrival time is set as “exponential (.03)” for all the nodes unless otherwise specified. The packet size distribution is exponential with a mean of 2000 bits. The maximum packet size transmitted in a 802.11b network is 2304 bytes and packets over this size are discarded at the source. All the wireless station nodes use “Direct Sequence Spread Spectrum” at the physical layer. The wireless attributes of a station node are represented in Figure 5.5.

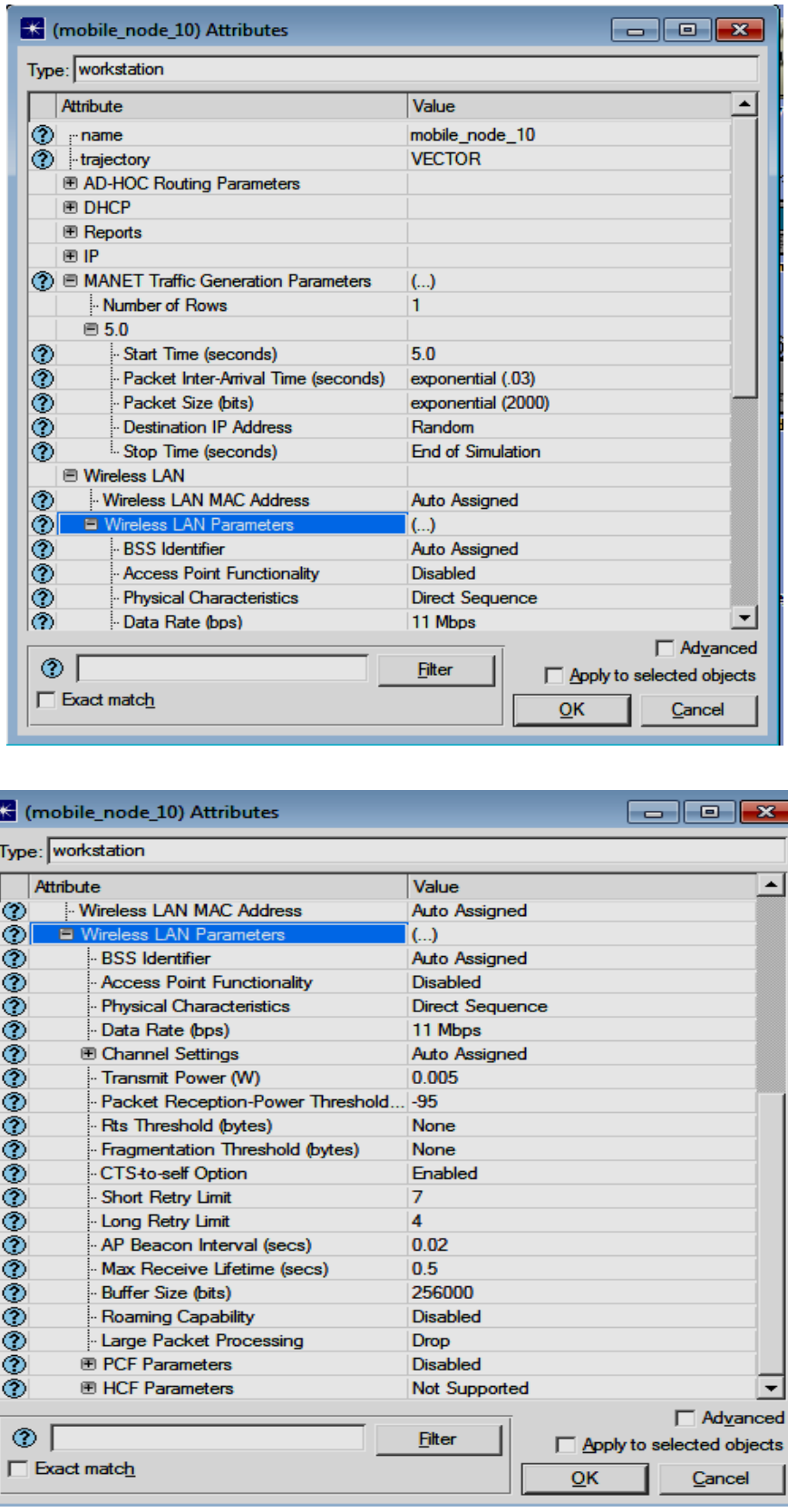


Figure 5.5 Traffic model and wireless attributes of a station node

5.8 Intelligent Pulse Jammer Node Model

Pulse jammer node has different structure than MANET node, it has radio transmitter that continuously generate the noise on wireless medium. Jammer bandwidth specifies the bandwidth (in kHz) of the transmitting channel. Jammer band base frequency specifies the base frequency (in MHz) of the transmitting channel. Jammer transmitter power specifies the transmission power (in Watts) allocated to packets transmitted through the channel. Finally, the jammer has a pulse width which specifies the length of time (in seconds) a pulse is transmitted and a silence width specifies the interval (in seconds) between pulses [3]. In Figure 5.6, the jammer node model attributes are represented.

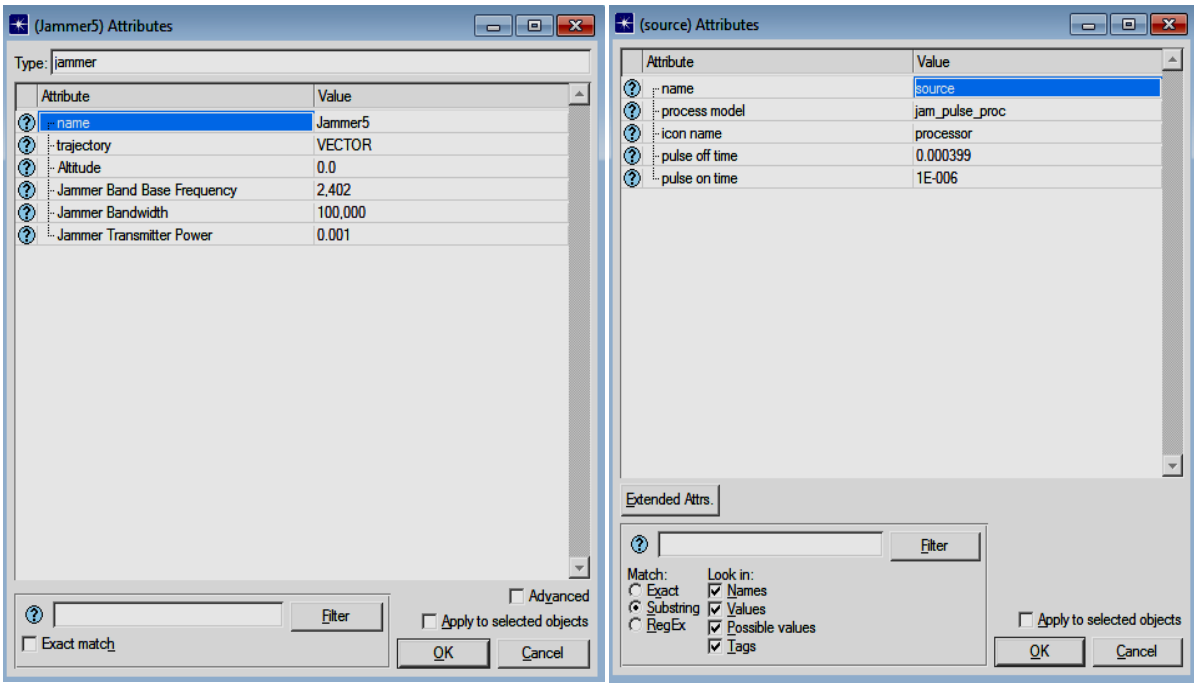
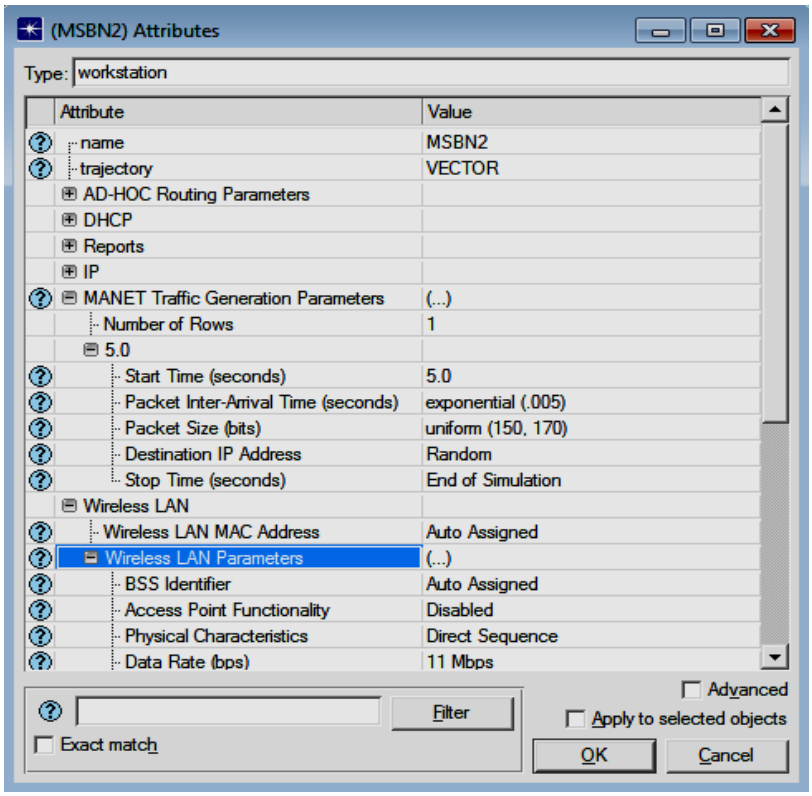


Figure 5.6 Intelligent Pulse Jammer node model attributes

5.9 Misbehavior Node Model

Misbehaving nodes act different on the network, by applying the different packet setting. As shown in Figure 5.7, the packet size and packet inter-arrival time are changed for misbehaving nodes.



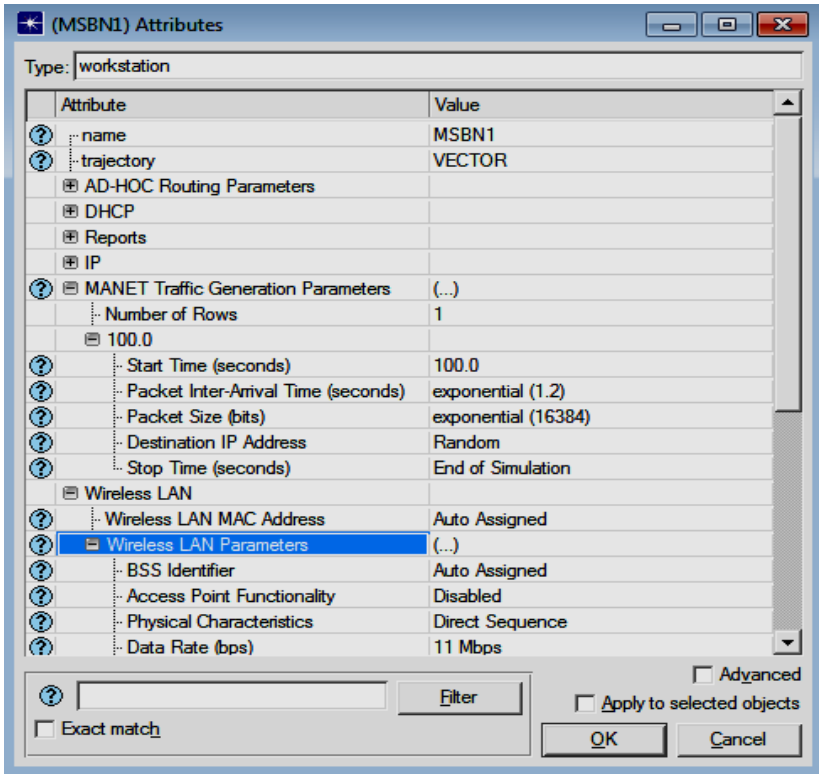


Figure 5.7 Misbehavior node model attributes for the networks with manet_station and wlan_wkstn mobile nodes

5.10 Byzantine Node Model

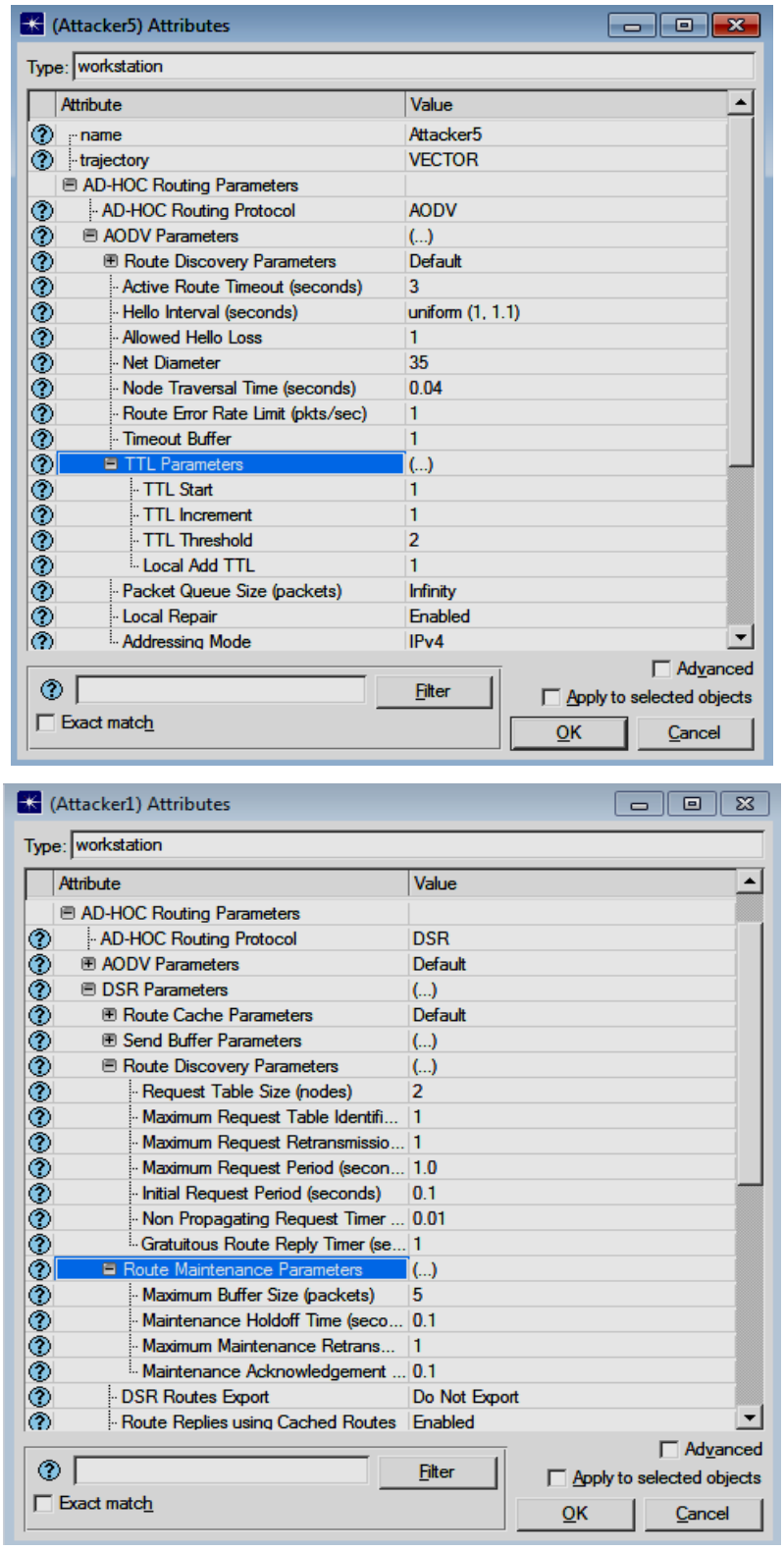


Figure 5.8 Byzantine node model attributes for AODV and DSR

Byzantine nodes attributes are changed for dropping routing packets. AODV, DSR, GRP and OLSR parameters are changed for making the nodes malicious as shown in Figure 5.8 and 5.9.

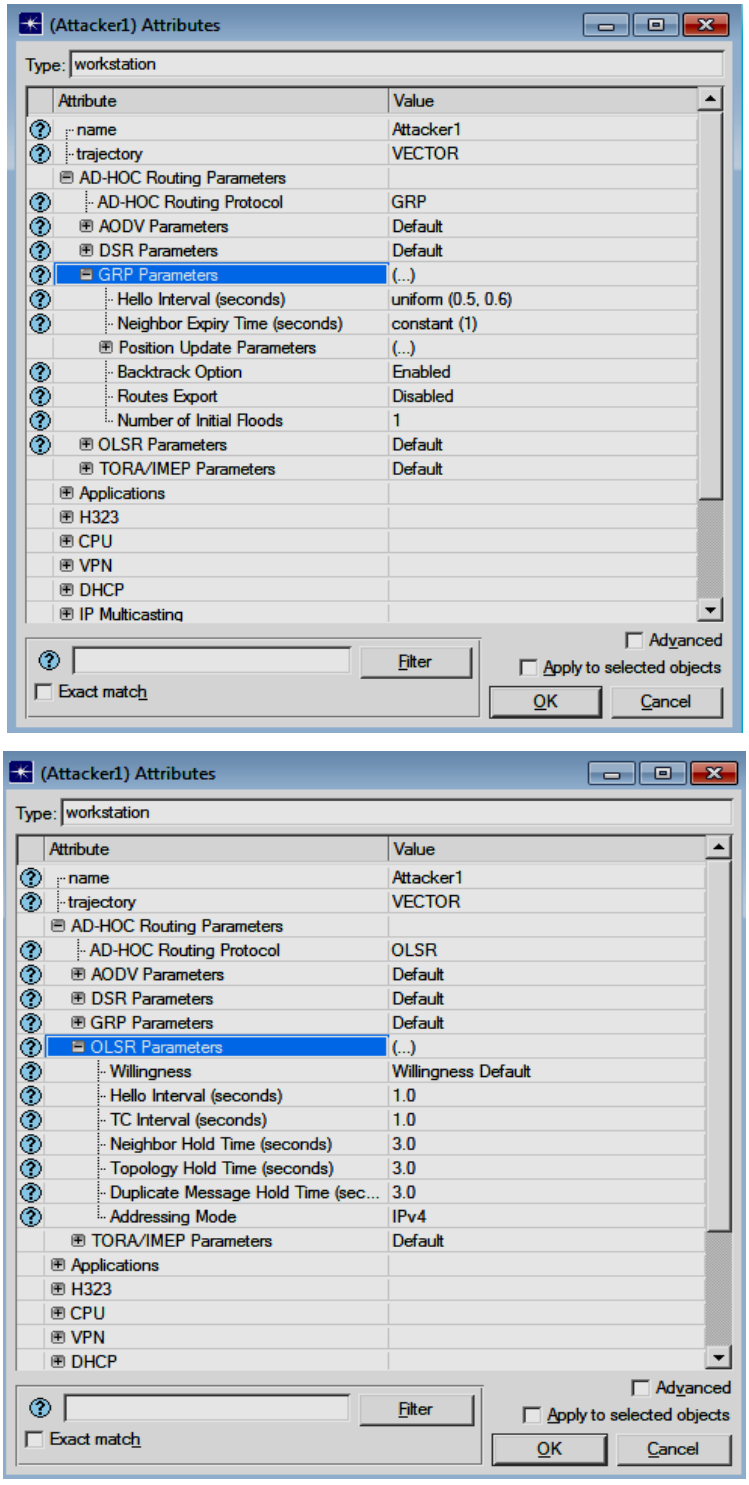


Figure 5.9 Byzantine node model attributes for GRP and OLSR

6 SIMULATION RESULTS AND ANALYSIS

The simulation is done to analyze the effects of Pulse Jammer attack, Misbehavior Node attack and Byzantine attack on the network performance under different traffic loads. In this thesis, analysis of performances and capacities of mobile ad hoc networks is based on the OPNET simulation tool [52] which provides a good model of the IEEE 802.11b standard. 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.

6.1 Performance of DSR under Pulse Jammer Attack, under Misbehavior Node Attack and under Byzantine Attack for the Network

In this section, the performance of DSR protocol was compared under jamming nodes, misbehaving nodes and Byzantine nodes. Application configuration, profile configuration and mobility configuration were defined. Firstly, a normal network traffic was generated under DSR protocol, later the scenario was duplicated with Pulse Jammer attack, with Misbehavior Node attack, and with Byzantine attack respectively. Intruder nodes were placed in the network which contains 30 nodes in different locations. DSR protocol was studied in IEEE 802.11b networks and the simulation run time was set as 300 seconds.

6.1.1 Data dropped statistics of DSR protocol for the network

Different network attack scenarios are designed separately to examine the DSR protocol under five Byzantine nodes, five misbehaving nodes and five jamming nodes. The results are compared in terms of “data dropped” parameter.

Figure 6.1 represents the “data dropped” statistics on the normal network traffic with the average value of 3,842,385 bits/sec. It shows the “data dropped” with Byzantine nodes in the network as 4,501,331 bits/sec, with misbehaving nodes as 4,384,450 bits/sec and with jamming nodes in the network as 3,894,932 bits/sec with respect to the DSR protocol.

The “data dropped” increases in the 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.

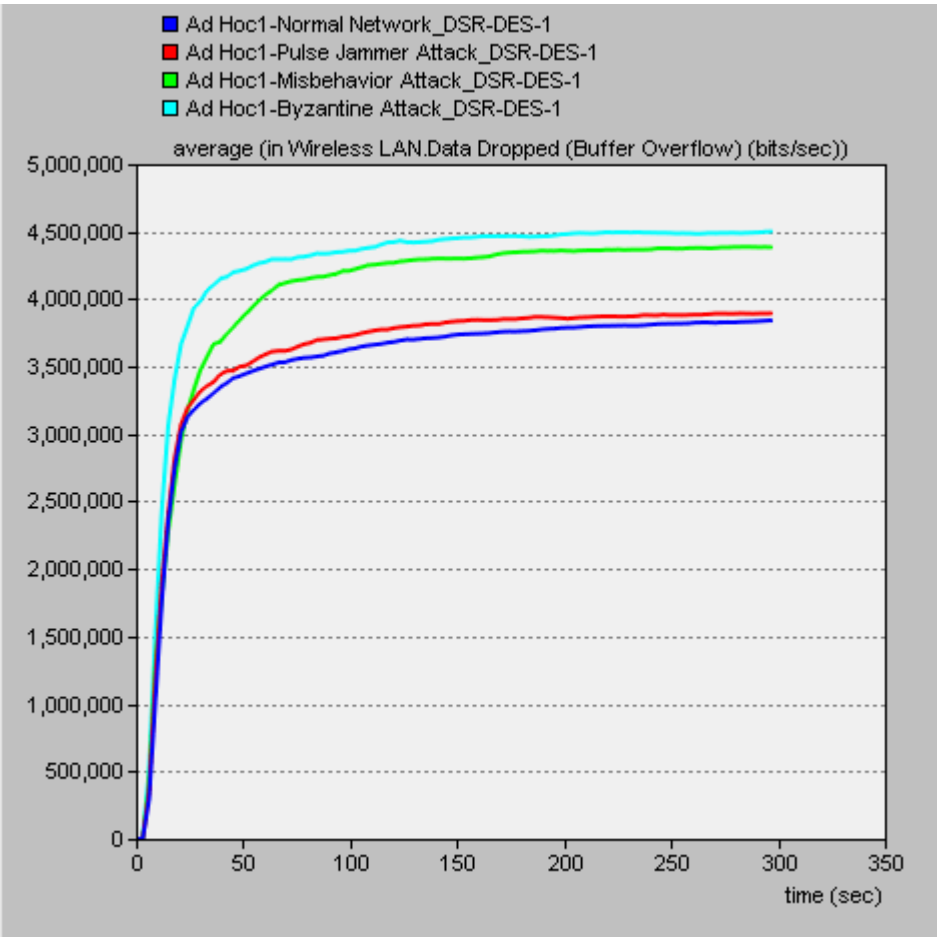


Figure 6.1 Data dropped results of the normal network with and without network attacks for DSR protocol

6.1.2 Delay statistics of DSR protocol for the network

In this section, five jamming nodes, five misbehaving nodes and five Byzantine nodes are placed separately in the normal network with different scenarios. The

“delay” statistics are represented for the whole network in the same graph in Figure 6.2.

As seen in Figure 6.2, the delay of the network nodes with normal traffic is noted as 9.285 seconds, whereas the delay with jamming nodes is noted as 13.936 seconds, both for a simulation of 300 seconds duration. The delay of the network with misbehaving nodes is recorded as 12.295 seconds and with Byzantine nodes as 11.496 seconds.

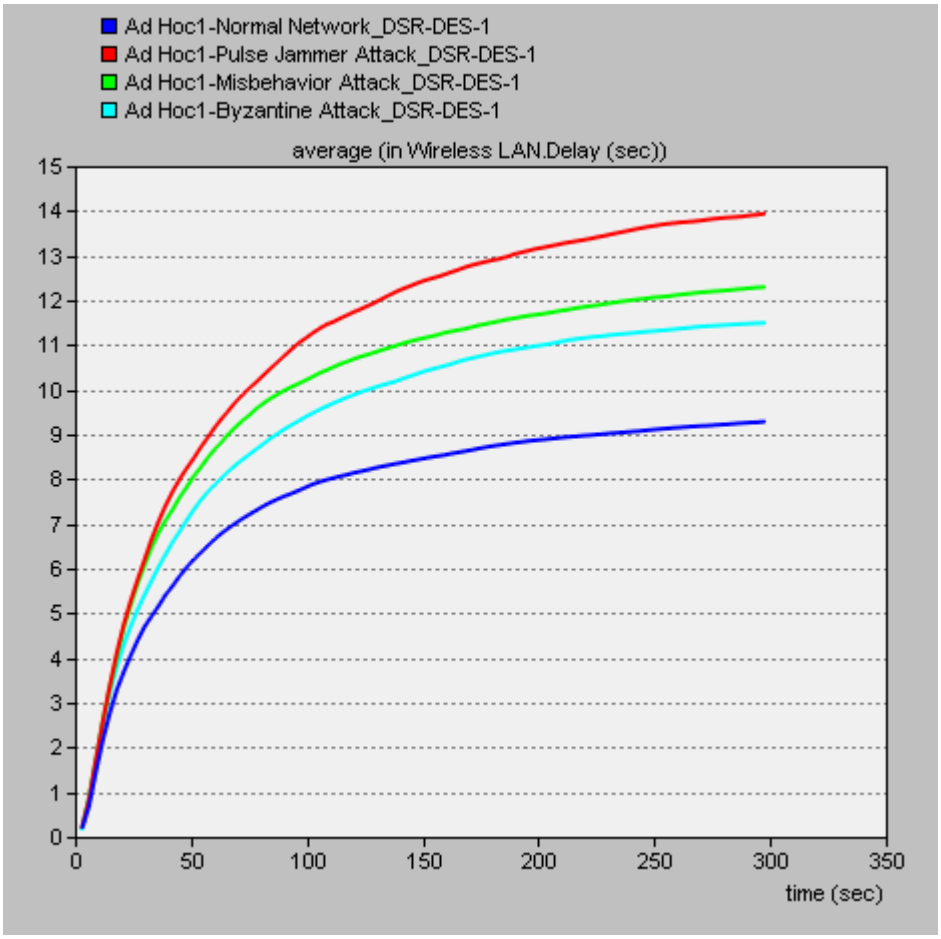


Figure 6.2 Delay results of the normal network with and without network attacks for DSR protocol

Security attacks on DSR shows a significant result. It is clearly seen in the network result that the delay of the whole network with intruder nodes increases when it is compared to the normal network. The largest increment of the network “delay”

statistic is represented for the network with jamming nodes and the least increment is indicated for the network with Byzantine nodes with respect to the DSR protocol.

6.1.3 Network load statistics of DSR protocol for the network

To implement the network attacks on mobile ad hoc nodes network, five jamming nodes, five misbehaving nodes and five Byzantine nodes are deployed separately in the network for DSR with different scenarios.

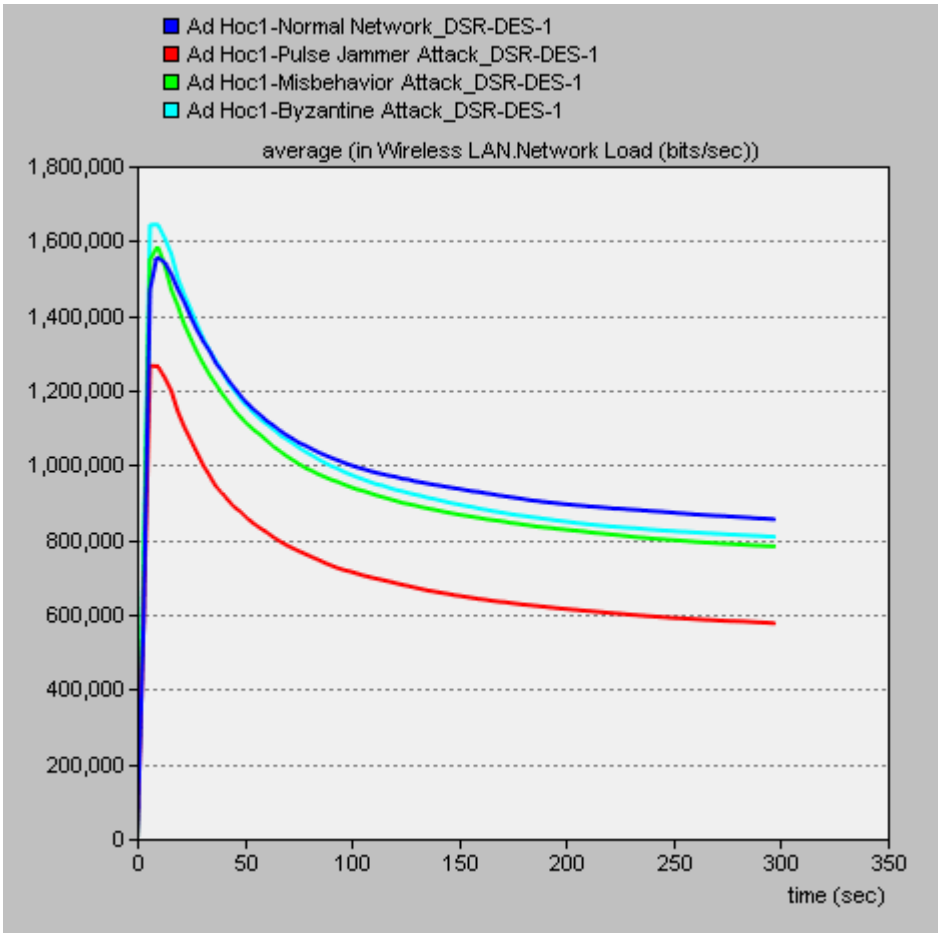


Figure 6.3 Network load results of the normal network with and without network attacks for DSR protocol

The network scenarios for different attacks are represented in Figure 6.3. The “network load” of the normal network has the average value of 854,878 bits/sec

and with the jamming nodes in the network it is noted as 576,976 bits/sec. For the network with misbehaving nodes, its average value is 782,385 bits/sec and the “network load” statistics according to the network with Byzantine nodes is recorded as 808,432 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 the DSR protocol. The jamming node attack on DSR shows a significant result. The pulse jammer attack use the wireless medium and decrease the network load. It can be seen that the “network load” slightly reduce when the malicious nodes start generating raw packet on the network.

6.1.4 Throughput statistics of DSR protocol for the network

In this section, five jamming nodes, five misbehaving nodes and five Byzantine nodes are placed separately in the normal network with different scenarios. The “throughput” statistics are represented for the whole network in the same graph in Figure 6.4.

The “throughput” of the network nodes with normal traffic is noted as 876,445 bits/sec and later with jamming nodes in the network it is noted as 594,755 bits/sec at the time of simulation 300 seconds. As seen in Figure 6.4, the “throughput” of the network with misbehaving nodes is recorded as 816,574 bits/sec and with Byzantine nodes it is noted as 862,088 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. This shows the packet sent to its destination or forwarding the packets to the other nodes is successfully executed before deploying malicious nodes in the network. They reduce the performance of the network by all means.

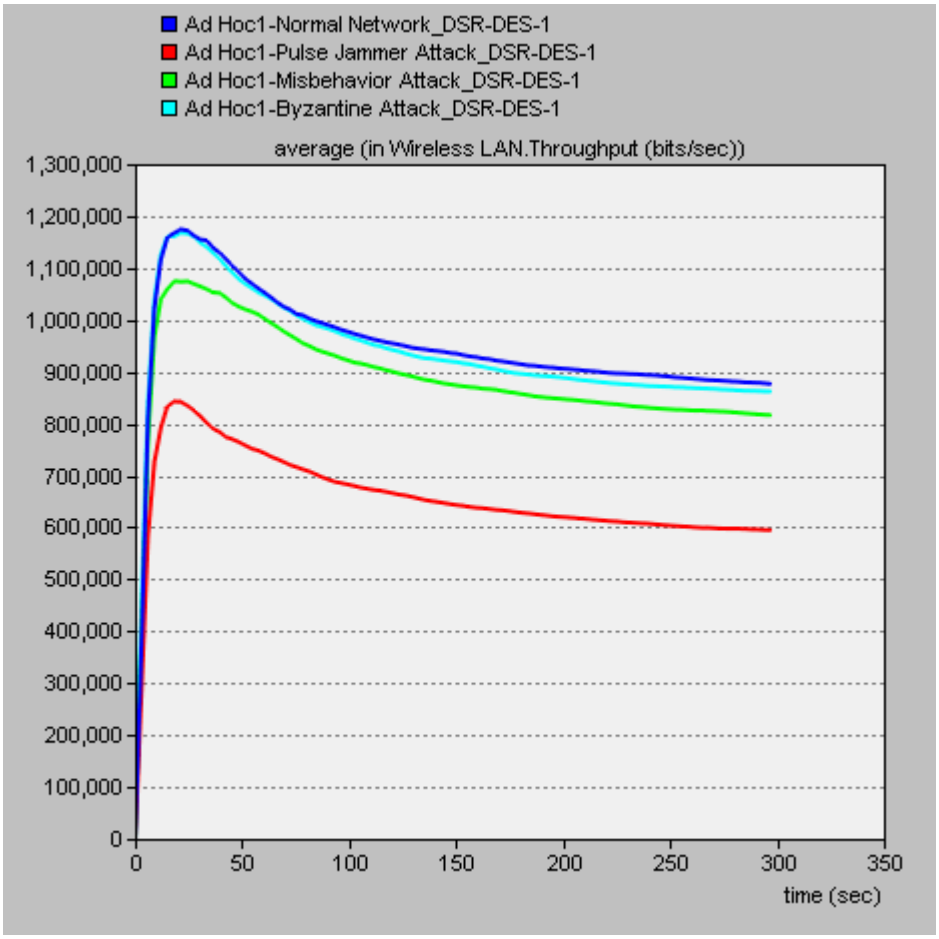


Figure 6.4 Throughput results of the normal network with and without network attacks for DSR protocol

6.2 Performance of AODV under Pulse Jammer Attack, under Misbehavior Node Attack and under Byzantine Attack for the Network

In this section, Pulse Jammer attack, Misbehavior Node attack and Byzantine attack were implemented on AODV routing protocol. 30 mobile ad hoc nodes were used for the network without attackers; until then, for each network attack scenario, five malicious nodes were placed at different positions in the normal network. Thus, when the traffic was generated among the nodes, attackers started dropping the packets and stopped forwarding the packets to the other nodes. All results were captured and they were compared against the normal network in terms of data dropped, delay, network load and throughput.

6.2.1 Data dropped statistics of AODV routing protocol for the network

The “data dropped” statistics of each security attack scenarios are shown for the whole network in the same graph.

Figure 6.5 shows the normal network “data dropped” statistic’s average value as 914,061 bits/sec, with jamming nodes its average value is recorded as 1,007,433 bits/sec, with misbehaving nodes the “data dropped” statistic is represented as 1,149,641 bits/sec and with Byzantine nodes its value is recorded as 1,304,230 bits/sec.

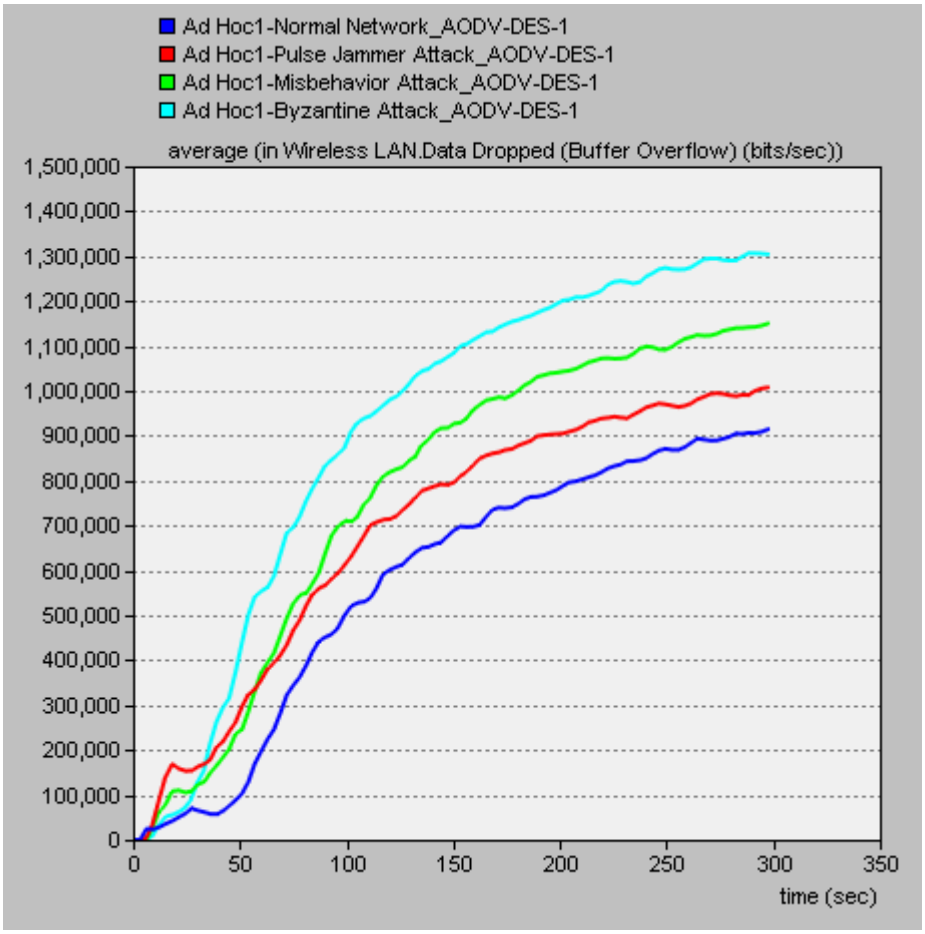


Figure 6.5 Data dropped results of the normal network with and without network attacks for AODV routing protocol

By analyzing the results, the largest increment of the “data dropped” statistic is represented for the network with Byzantine nodes and the least increment is

represented for the network with jamming nodes with respect to the AODV routing protocol. That means, AODV routing protocol is more vulnerable to the network with Byzantine nodes for “data dropped” statistics.

6.2.2 Delay statistics of AODV routing protocol for the network

The “delay” results of the normal network and the networks with intruder nodes are compared in Figure 6.6 for AODV routing protocol.

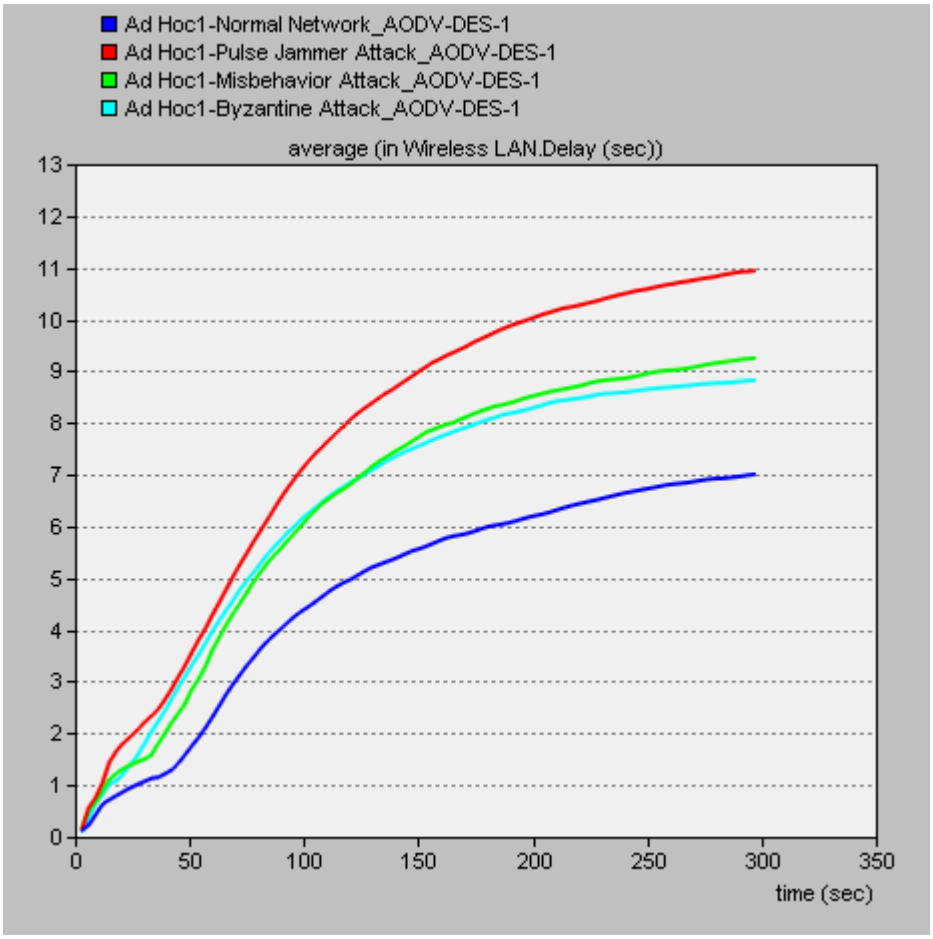


Figure 6.6 Delay results of the normal network with and without network attacks for AODV routing protocol

As seen in Figure 6.6, the “delay” performance of the network nodes with normal traffic is 7.007 seconds and with jamming nodes in the network it is represented as

10.943 seconds. The delay of the network with misbehaving nodes is noted as 9.252 seconds and with Byzantine nodes it is recorded as 8.825 seconds.

When the normal network results are compared with the networks including malicious nodes, it seems that AODV routing protocol is more vulnerable to the network with jamming nodes. On the other hand, it is least affected from the network with Byzantine nodes for “delay” statistics.

6.2.3 Network load statistics of AODV routing protocol for the network

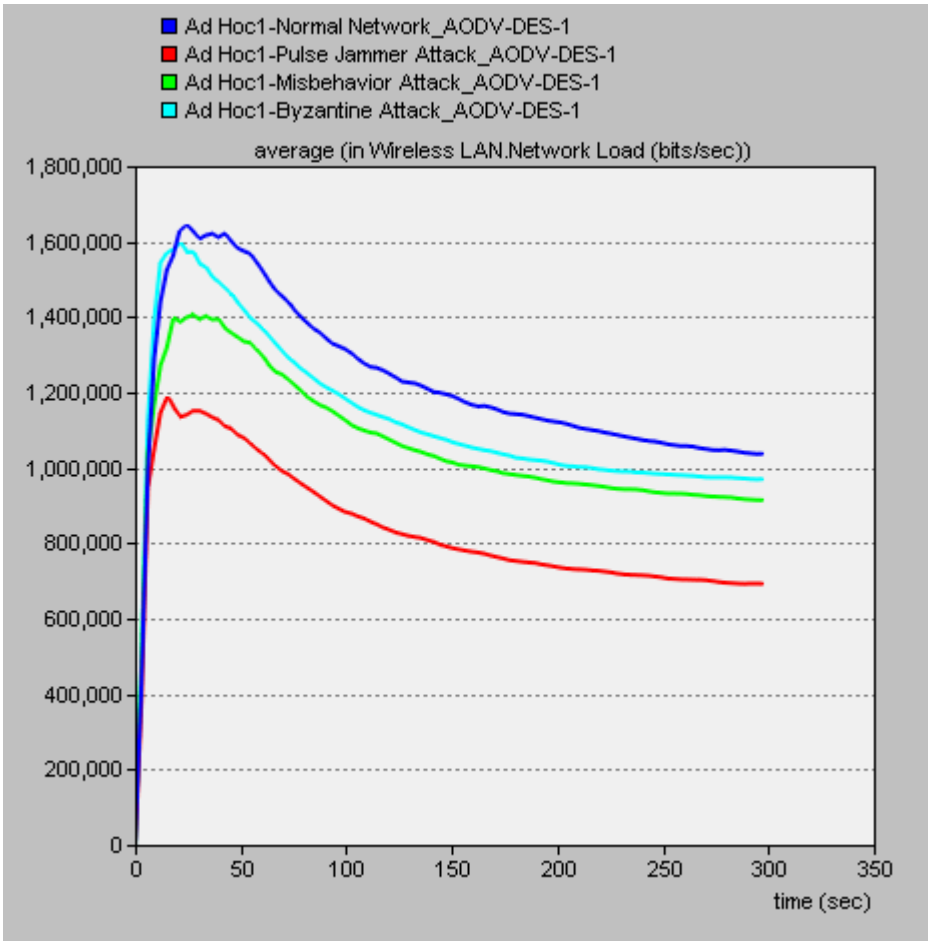


Figure 6.7 Network load results of the normal network with and without network attacks for AODV routing protocol

The network scenarios for different attacks are depicted in Figure 6.7. The “network load” of the normal network has the average value of 1,037,157 bits/sec

and with the jamming nodes in the network it is noted as 692,594 bits/sec. For the network with misbehaving nodes, its average value is 914,203 bits/sec and the “network load” statistic according to the network with Byzantine nodes is recorded as 970,141 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 6.7, AODV routing protocol is more vulnerable to the network with 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 badly when malicious nodes are placed in the normal network and they start dropping the forwarding packets to the other nodes on the network.

6.2.4 Throughput statistics of AODV routing protocol for the network

The “throughput” results of AODV normal network and AODV with intruder nodes are shown in Figure 6.8. It shows that the network throughput reduces by placing the attackers.

Figure 6.8 shows the normal network “throughput” statistic’s average value as 4,900,837 bits/sec, with jamming nodes its average value is recorded as 3,414,509 bits/sec, with misbehaving nodes the “throughput” statistic is represented as 4,275,057 bits/sec and with Byzantine nodes its value is recorded as 4,461,919 bits/sec.

When the graph is analyzed, it is clearly seen that the largest reduction of the “throughput” statistic is represented for the network with jamming nodes and the least reduction is represented for the network with Byzantine nodes with respect to the AODV routing protocol. That means, AODV routing protocol is more vulnerable to the network with jamming nodes. Due to the abnormal activities of the jamming

nodes on the network, the network becomes more vulnerable and it influences the need of reliability, availability and the performance of the network.

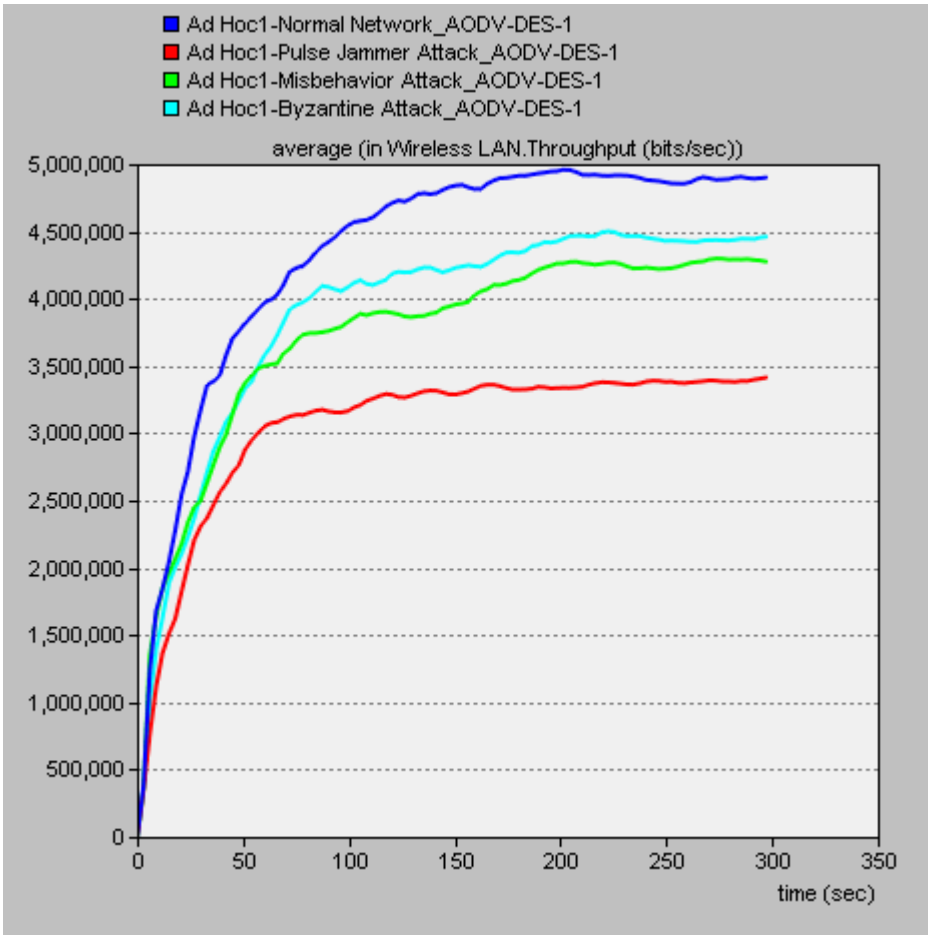


Figure 6.8 Throughput results of the normal network with and without network attacks for AODV routing protocol

6.3 Performance of OLSR under Pulse Jammer Attack, under Misbehavior Node Attack and under Byzantine Attack for the Network

In this section, the performance of OLSR protocol was compared under jamming nodes, misbehaving nodes and Byzantine nodes. As previously described, application configuration, profile configuration and mobility configuration were defined. The MANET nodes were configured to use OLSR protocol in OPNET. Then, for the first, a normal traffic was generated using OLSR protocol, later the scenario was duplicated with different security attacks. For each network attack

scenario, five malicious nodes were placed in the normal network respectively. After simulating both the normal network and the network with malicious nodes, the results of each network scenario were compared in terms of data dropped, delay, network load and throughput results.

6.3.1 Data dropped statistics of OLSR protocol for the network

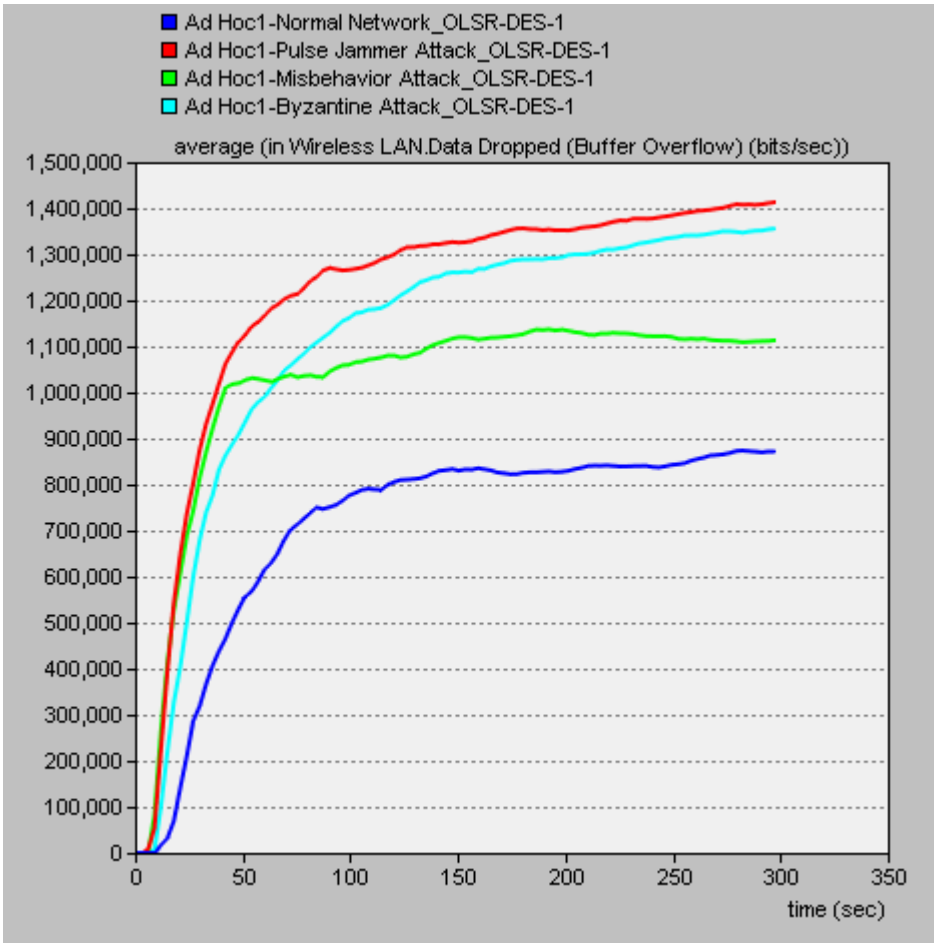


Figure 6.9 Data dropped results of the normal network with and without network attacks for OLSR protocol

The “data dropped” statistics are shown for the whole network in the same graph with respect to the OLSR protocol with different network attacks.

Figure 6.9 shows the normal network “data dropped” statistic’s average value as 871,638 bits/sec. For the network with jamming nodes, the average data dropped

value is recorded as 1,413,018 bits/sec; with Byzantine nodes its value is 1,355,869 bits/sec and with misbehaving nodes the “data dropped” statistic is 1,113,137 bits/sec. It is seen that the largest increment of the “data dropped” statistic is represented for the network with jamming nodes and the least increment is represented for the network with misbehaving nodes with respect to the OLSR protocol.

6.3.2 Delay statistics of OLSR protocol for the network

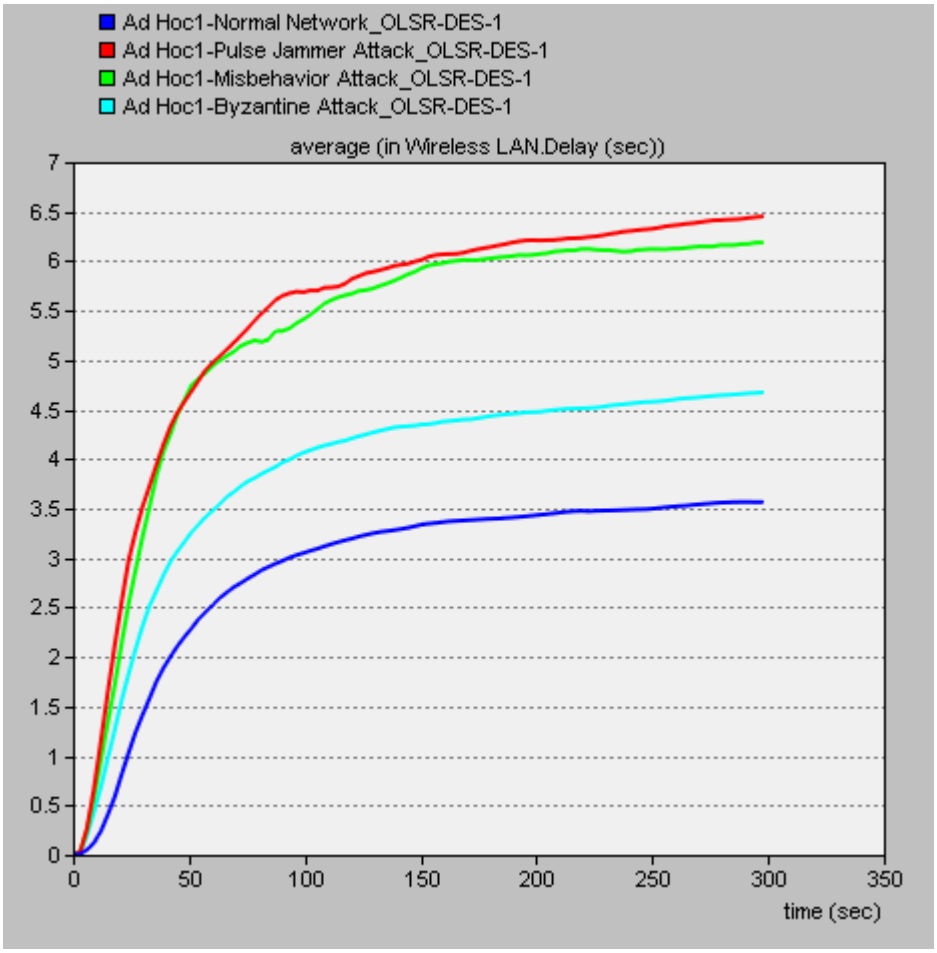


Figure 6.10 Delay results of the normal network with and without network attacks for OLSR protocol

The OLSR protocol is observed by implementing the network attacks on the network.

Figure 6.10 represents that the normal network traffic “delay” average value is 3.565 seconds. On the other hand, the network with jamming nodes shows the “delay” with the average value of 6.451 seconds, with misbehaving nodes the value is recorded as 6.188 seconds and with Byzantine nodes it is noted as 4.672 seconds with respect to the OLSR protocol. The largest increment of the network “delay” statistic is represented for the network with jamming nodes and the least increment is indicated for the network with Byzantine nodes with respect to the OLSR protocol. That means, OLSR protocol is more vulnerable to the network with jamming nodes for “delay” statistics.

6.3.3 Network load statistics of OLSR protocol for the network

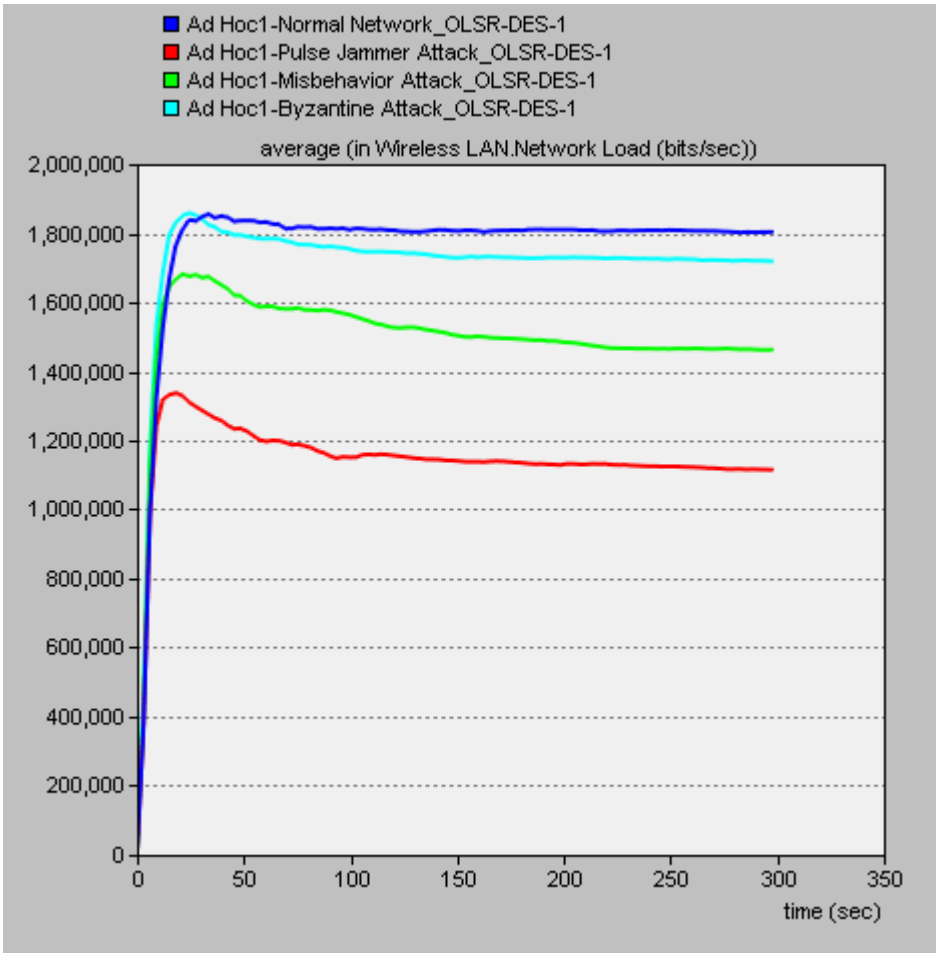


Figure 6.11 Network load results of the normal network with and without network attacks for OLSR protocol

Figure 6.11 shows that the OLSR protocol with network attacks has a significant impact on network load. The normal network load statistic is recorded as 1,803,619 bits/sec. Then, it is noted as 1,115,144 bits/sec with jamming nodes in the network. The network load statistic average value is 1,462,642 bits/sec with misbehaving nodes and with Byzantine nodes in the network its value is noted as 1,719,109 bits/sec for OLSR protocol.

It is clearly showed that the decrease in network load affects the reliability of the network. 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 the OLSR protocol.

6.3.4 Throughput statistics of OLSR protocol for the network

The normal network throughput is compared with Pulse Jammer attack, with Misbehavior Node attack and with Byzantine attack for OLSR protocol in Figure 6.12. As we notice the differences of security attacks, they cause network congestion and decrease the network performance.

The “throughput” results on the normal network traffic with and without intruder nodes are analyzed. The normal network’s throughput is recorded as 2,127,076 bits/sec. Then, it is noted as 1,333,900 bits/sec with jamming nodes in the network. The “throughput” statistic’s average value is 1,860,430 bits/sec with misbehaving nodes and with Byzantine nodes in the network its value is noted as 2,112,589 bits/sec with respect to the OLSR.

The throughput decreases in the presence of the intruder nodes in the network when it is compared to the normal network. The largest reduction of the “throughput” statistic is represented for the network with jamming nodes and the least reduction is represented for the network with Byzantine nodes for OLSR protocol. As the throughput shows that the jamming nodes start dropping the packets when the simulation start working. If the jamming nodes start to act

maliciously and prevent forwarding the packets on time to the other nodes, the network performance degrades.

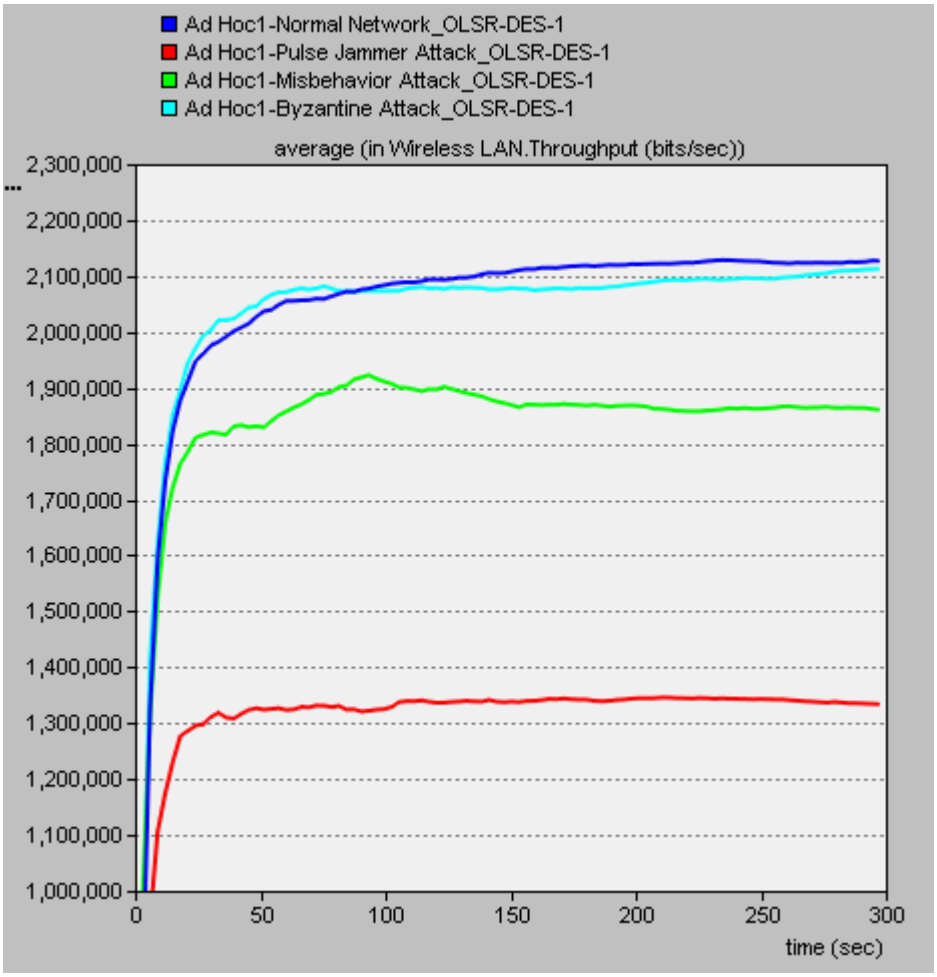


Figure 6.12 Throughput results of the normal network with and without network attacks for OLSR protocol

6.4 Performance of GRP under Pulse Jammer Attack, under Misbehavior Node Attack and under Byzantine Attack for the Network

In this section, GRP was used as the routing protocol. GRP network was generated with 30 mobile ad hoc nodes. The normal network traffic results were collected, then five jamming nodes, five misbehaving nodes and five Byzantine nodes were placed in the network respectively and the captured results were compared in respect of data dropped, delay, network load and throughput.

6.4.1 Data dropped statistics of GRP for the network

“Data dropped” results of the whole network is shown in Figure 6.12. When the normal network and the networks with attacker nodes are compared, it can be observed that the intruder nodes decrease the network performance. As the packets sent from the mobile ad hoc nodes to the other nodes on the network, they lost due to the attackers. This clearly reflects the availability and reliability of mobile ad hoc nodes in terms of network security.

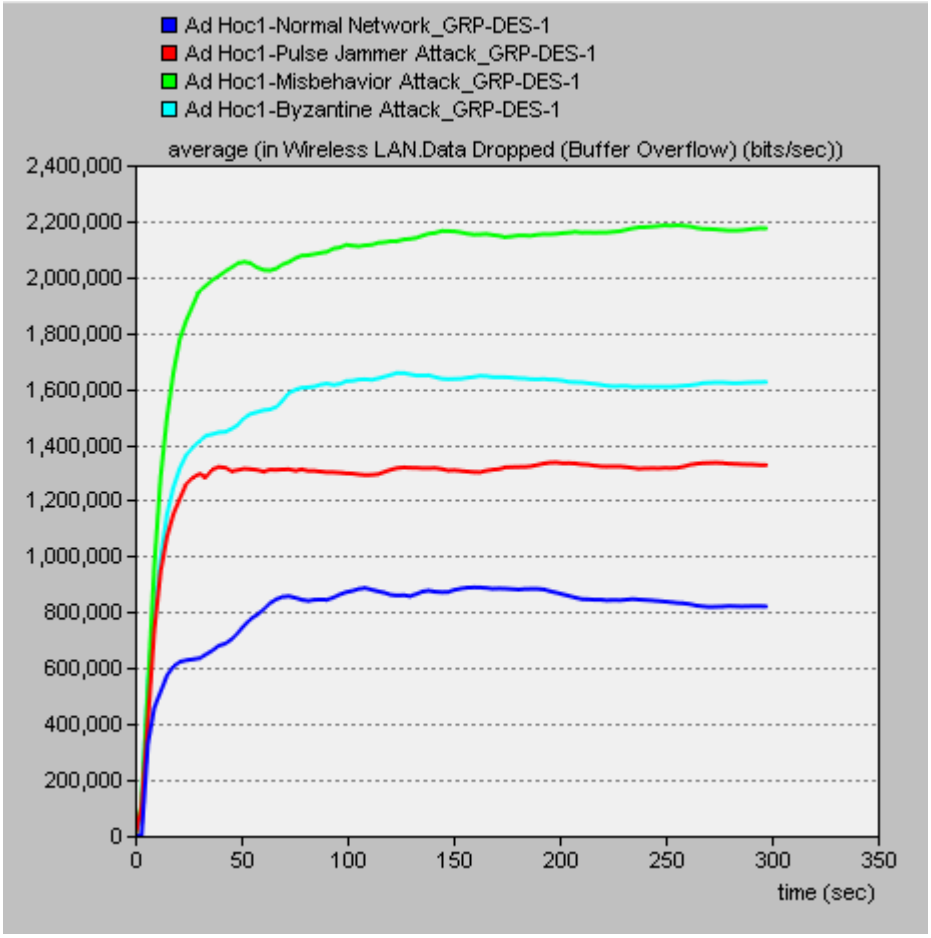


Figure 6.13 Data dropped results of the normal network with and without network attacks for GRP

Analysis on Figure 6.13, it shows that the data dropped of the normal network’s average value is 821,149 bits/sec. On the other hand, the network with misbehaving nodes shows the network data dropped with the average value of

2,173,947 bits/sec, with Byzantine nodes the value is noted as 1,624,040 bits/sec and with jamming nodes it is recorded as 1,326,377 bits/sec with respect to the GRP. 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 according to the GRP.

6.4.2 Delay statistics of GRP for the network

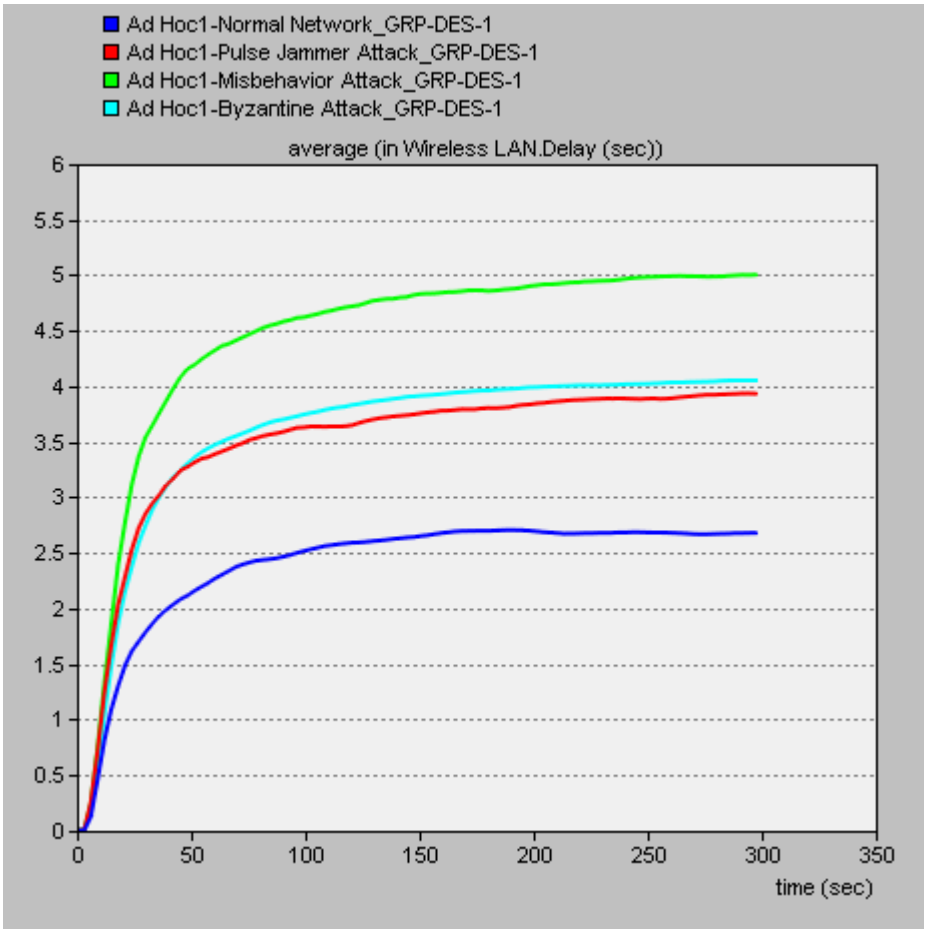


Figure 6.14 Delay results of the normal network with and without network attacks for GRP

In Figure 6.14, the “delay” statistic of the entire network with and without intruder nodes is analyzed. By observing the graph, it can be seen that there is a difference between normal network and the networks with malicious nodes. The delay increases, when the network attacks implemented to normal network. It

starts increasing at the beginning of the simulation and continues to increase until the end of of the simulation.

Figure 6.14 represents the “delay” statistics on the normal network traffic with the average value of 2.681 seconds. It shows the delay with misbehaving nodes in the network as 5.004 seconds, with Byzantine nodes as 4.054 seconds and with jamming nodes in the network as 3.934 seconds with respect to the GRP.

According to the graph, GRP is more vulnerable to the network with misbehaving nodes for the “delay” statistics. Misbehaving nodes act as maliciously, for that reason some intermediates nodes in the network follows the selected nodes to forwarding the packets and the delay of packet transmission increases.

6.4.3 Network load statistics of GRP for the network

In Figure 6.15, different network scenarios for the metioned network attacks are represented with respect to the GRP.

The average value of the normal “network load” is 2,162,370 bits/sec. Moreover, the network with jamming nodes shows the network load with the average value of 1,611,132 bits/sec, with misbehaving nodes the value is recorded as 1,876,978 bits/sec and with Byzantine nodes it is noted as 2,031,115 bits/sec according to the GRP.

It represents the network load decreased by placing the intruder nodes on the network, they prevent the mobile ad hoc nodes to continue the transmission on the network and the packets lost because of the network attacks.

The largest reduction of the “network load” statistic is represented for the network with jamming nodes and the least increment is represented for the network with Byzantine nodes according to the GRP. MANETs deal with a lot of network attacks and each security attack has its own specification to damage or to destroy the mobile ad hoc node infrastructure.

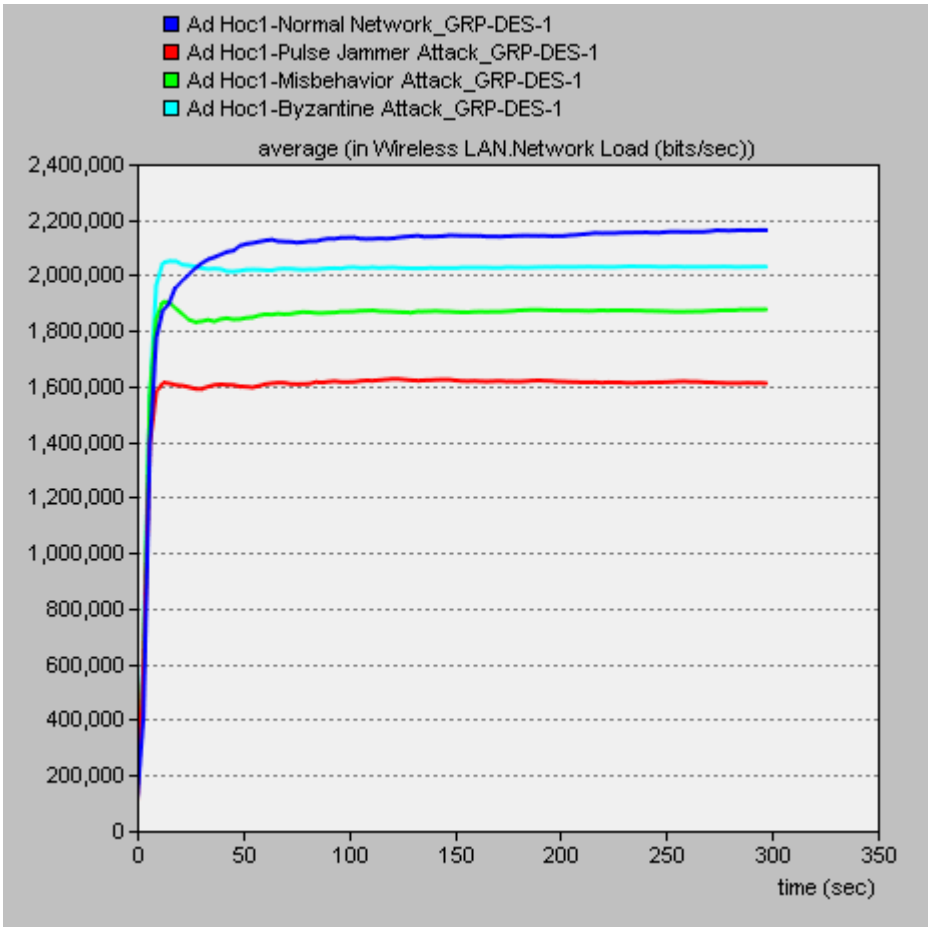


Figure 6.15 Network load results of the normal network with and without network attacks for GRP

6.4.4 Throughput statistics of GRP for the network

The throughput of the security attacks reduces the traffic on the network when it is compared to the normal network traffic as shown shown in Figure 6.16. There is a significant traffic destruction of the packets transmission on the network when employing the network attacks. Figure 6.16 represents the “throughput” statistics on the normal network traffic with the average value of 2,208,482 bits/sec. It shows the throughput with jamming nodes in the network as 1,650,695 bits/sec, with misbehaving nodes as 2,003,187 bits/sec and with Byzantine nodes in the network as 2,176,862 bits/sec according to the GRP. The largest reduction of the “throughput” statistic is represented for the network with jamming nodes and the least increment is represented for the network with Byzantine nodes for GRP.

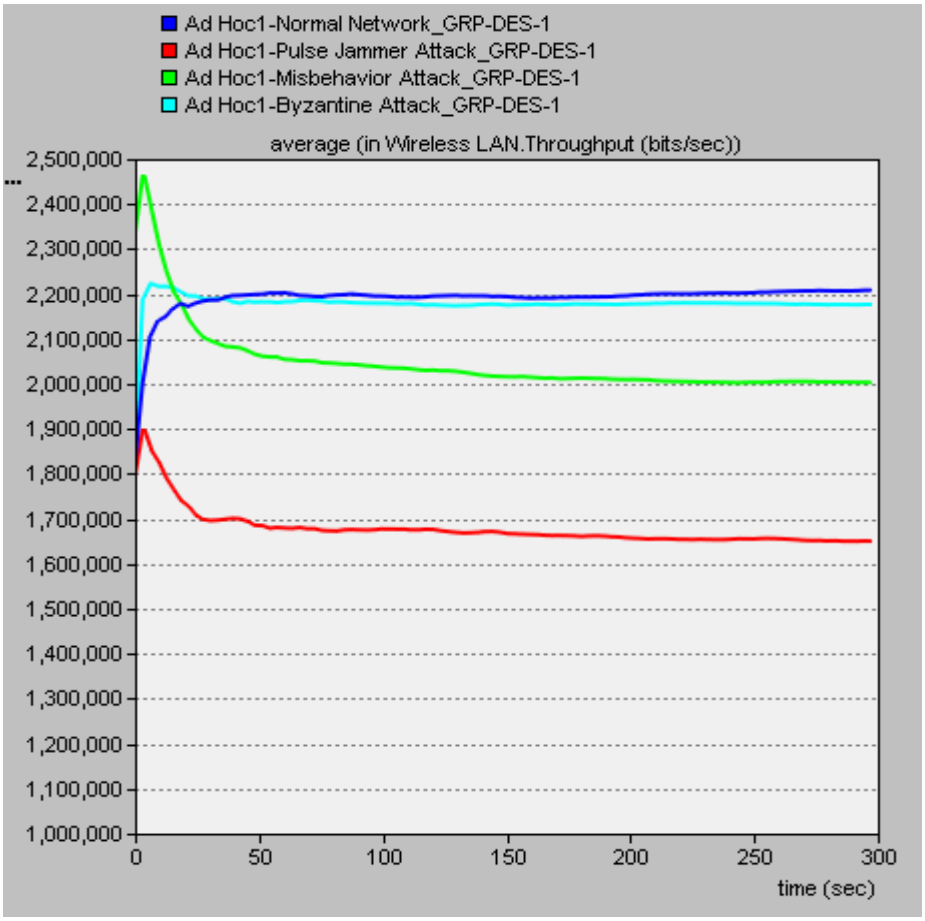


Figure 6.16 Throughput results of the normal network with and without network attacks for GRP

6.5 Performance of Routing Protocols under Pulse Jammer Attack, under Misbehavior Node Attack and under Byzantine Attack for Voice Application in respect of Packet End-to-End Delay Statistics

In this section, intelligent pulse jammer attack, misbehavior node attack and Byzantine attack were created and implemented on DSR, AODV, OLSR, GRP protocols and all these routing protocols were implemented on each single network scenario. Firstly, application configuration, profile configuration and mobility configuration were defined and a normal network traffic was generated with 30 nodes, later five intruder nodes for each single network scenario were implemented to the network and the results were compared for voice application in respect of “packet end-to-end delay“ statistics.

6.5.1 Packet end-to-end delay statistics of DSR protocol for voice application

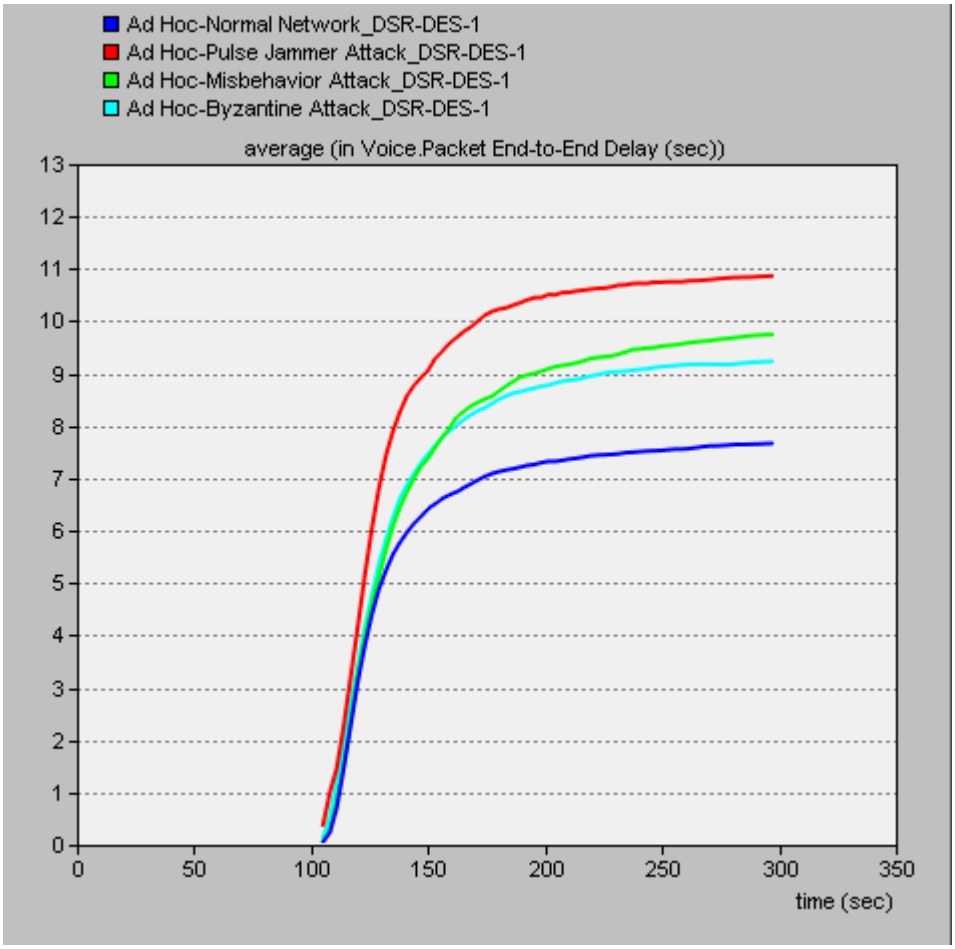


Figure 6.17 Packet end-to-end delay results of the normal network's voice application with and without network attacks for DSR protocol

The graph provides details of the results and evaluation of the normal network's voice application with and without network attacks for DSR protocol. Figure 6.17 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 of the network's voice application increases in the presence of the network attacks when it is compared to the normal network's voice traffic. Secure communication involves the secure transmission on the wireless medium and the communication mechanisms among nodes. Each security attack has its own specification to damage or to destroy the mobile ad hoc nodes infrastructure.

6.5.2 Packet end-to-end delay statistics of AODV routing protocol for voice application

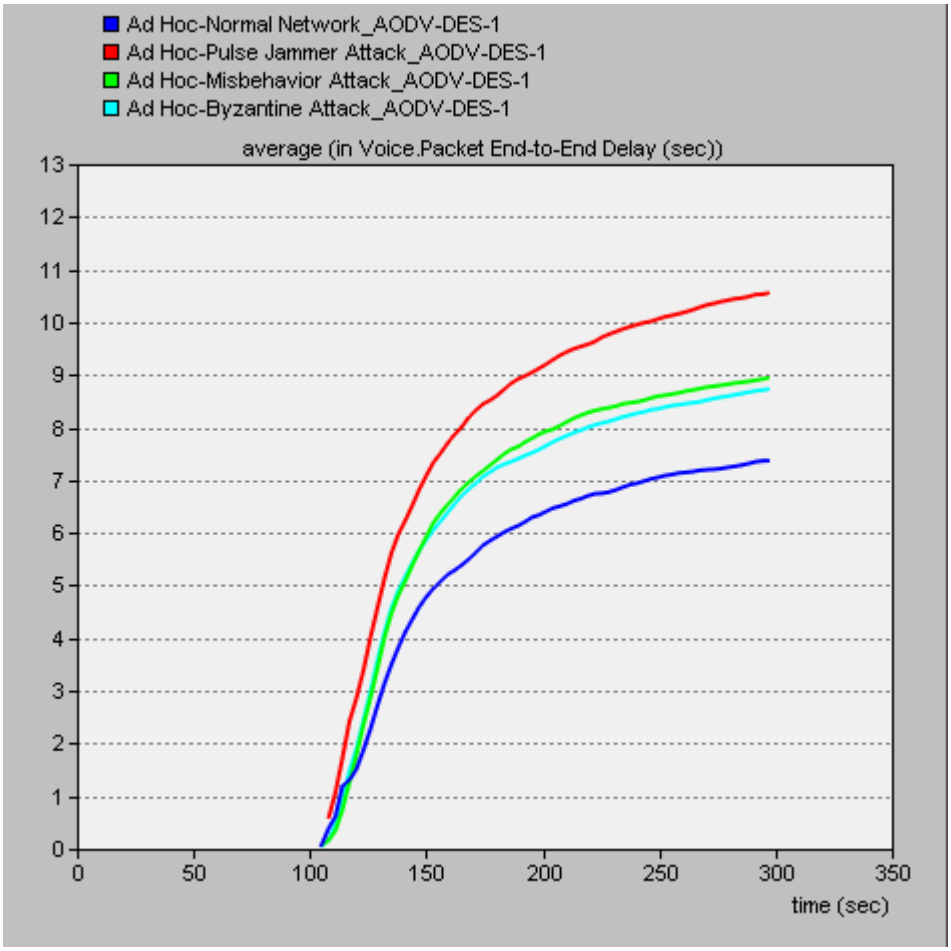


Figure 6.18 Packet end-to-end delay results of the normal network's voice application with and without network attacks for AODV routing protocol

Figure 6.18 shows the jamming nodes, misbehaving nodes and Byzantine nodes activities on the network for voice application in respect of "packet end-to-end

delay” parameters using the AODV protocol. The delay increases systematically to higher levels by placing of the intruder nodes in the network.

The packet end-to-end delay for voice application has the average value of 7.372 seconds and with the jamming nodes in the network it is noted as 10.556 seconds. For the network with misbehaving nodes, its average value is 8.945 seconds and the “packet end-to-end delay” statistics according to the network with Byzantine nodes is recorded as 8.731 seconds.

The largest reduction of the “packet end-to-end delay” statistic for voice traffic 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.

By observation the graph, it can be clearly seen that the packet end-to-end delay of the networks with intruder nodes for voice traffic starts almost at the same time together with the delay of the normal nerwork’s voice traffic. It shows that the increase in delay affects the reliability and the avaliability of the network and takes the network in to the congestion.

6.5.3 Packet end-to-end delay statistics of OLSR protocol for voice application

The Figure 6.19 shows the “packet end-to-end delay” statistics of OLSR protocol for voice application on the networks with and without jamming nodes, misbehaving nodes and Byzantine nodes in the network.

As seen in Figure 6.19, the delay of the network’s voice application with normal network traffic is recorded as 5.134 seconds, whereas the voice traffic’s delay with jamming nodes is noted as 8.250 seconds, both for the simulation of 300 seconds duration. The delay of the network’s voice application with Byzantine nodes is recorded as 5.904 seconds and with misbehaving nodes as 5.446 seconds.

The packet end-to-end delay increases when it is compared with the normal network's voice traffic. The reason for the increase in delay is that the intruder nodes act as maliciously, they don't cooperate with the other nodes on the network and the data packets aren't transmited from the source node to the destination node on time. The intruder nodes forward the packets only when they want too.

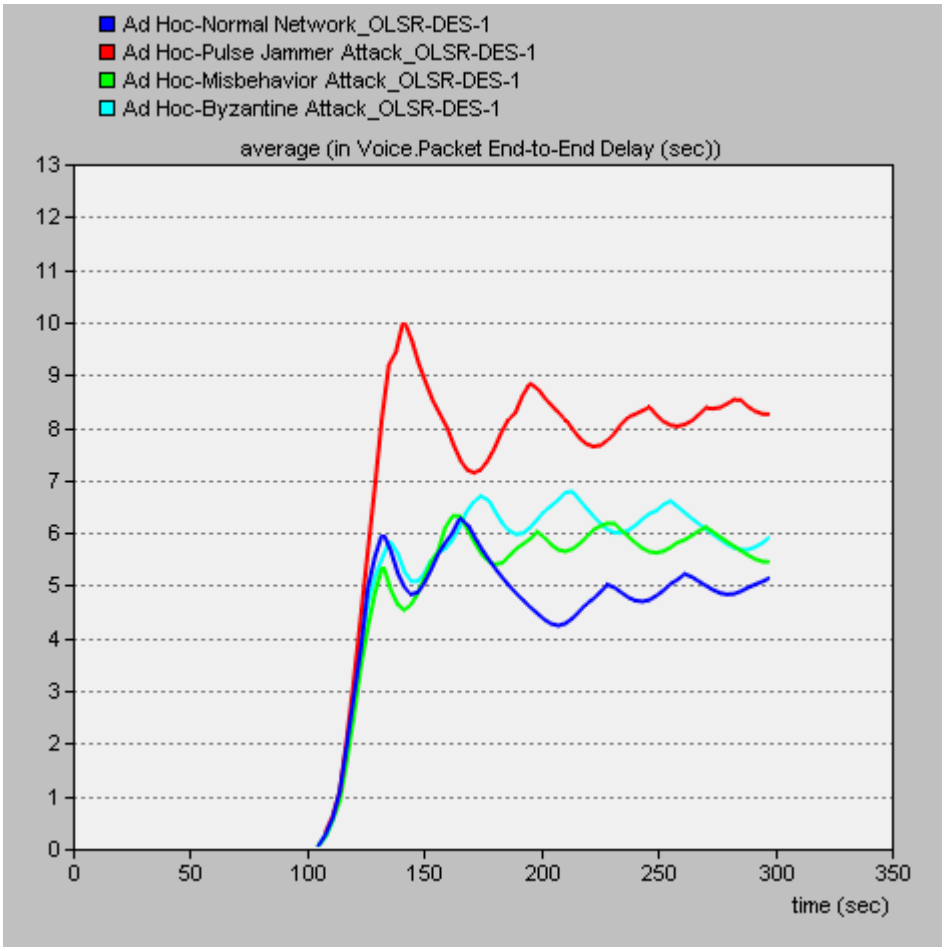


Figure 6.19 Packet end-to-end delay results of the normal network's voice application with and without network attacks for OLSR protocol

The up and down voice delay of OLSR protocol under the network with and without network attacks is unbalanced. The possible reason for this up and down rate of the voice traffic delay could be that the network nodes start to exchange the routing discovery, route request and routing table among each other in respect of

the OLSR protocol. When the malicious nodes are placed in the network, the voice traffic delay is recorded higher than the normal network's voice traffic delay.

6.5.4 Packet end-to-end delay statistics of GRP for voice application

The packet end-to-end delay of the network's voice application with normal nodes and with intruder nodes is simulated and the results are captured in Figure 20. The results show that there is significant changes on the delay of the network's voice traffic with implementation of the security attacks to the network.

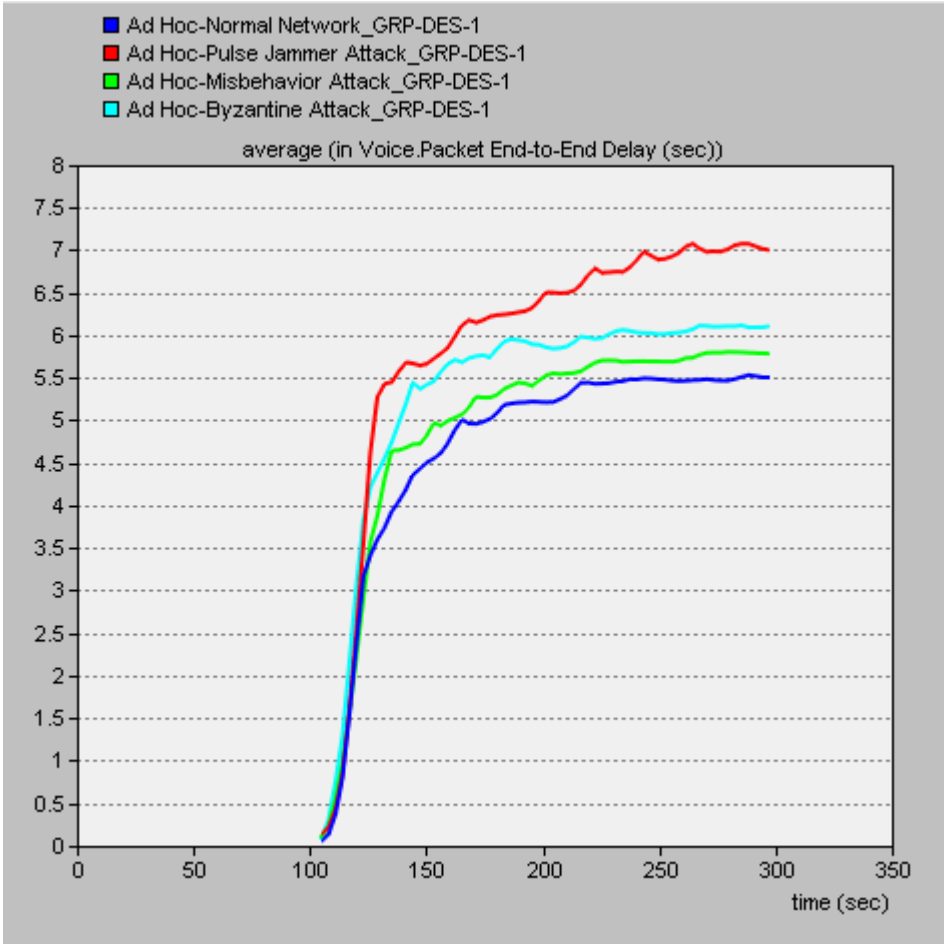


Figure 6.20 Packet end-to-end delay results of the normal network's voice application with and without network attacks for GRP

In Figure 6.20, the "packet end-to-end delay" statistics are analyzed for voice application on the normal network traffic with and without malicious nodes. The

normal network's "packet end-to-end delay" statistic is recorded as 5.506 seconds. Then, it is noted as 7.004 seconds with jamming nodes in the network. The delay statistics average value is 6.107 seconds with Byzantine nodes and with misbehaving nodes in the network its value is noted as 5.785 seconds with respect to the GRP.

According to the graph, GRP is more vulnerable to the network with jamming nodes. Pulse jammer attack transmit noise in wireless medium. Therefore the jamming nodes cause DoS attack with in the wireless channel. Jamming nodes transmit on a single frequency marked by a periodic pulse train in time.

The graph also represents that the packet delay time for voice application increases in the presence of the network attacks on the network. This indicates that, with malicious nodes in the normal network, the network performance degrades for voice traffic of the network.

6.6 Performance of Routing Protocols under Pulse Jammer Attack, under Misbehavior Node Attack and under Byzantine Attack for Voice Application in respect of Jitter Statistics

In this section, Pulse Jammer attack, Misbehavior Node attack and Byzantine attack were examined on DSR, AODV, OLSR, GRP routing protocols respectively. Some changes were applied in intruder nodes to act maliciously by dropping the data packets and by causing a delay in the transmission of the packets, while the data packets were being tried to send from the source node to the destination node on the network. Firstly, for each single scenario, the normal network traffic was generated with 30 mobile ad hoc nodes and later on five jamming nodes, five misbehaving nodes and five Byzantine nodes were placed in the network respectively. Then, the results were compared for voice application in respect of "jitter" statistics.

6.6.1 Jitter statistics of DSR protocol for voice application

Figure 2, represents the “jitter” statistics for voice application in the same graph. Jitter [19] is the ratio of transmission delay of the current packet and the transmission delay of the previous packet.

Figure 6.21 represents the “jitter” statistics for voice application on the normal network traffic with the average value of 0.006 seconds. It shows the jitter with jamming nodes in the network as 0.012 seconds, with Byzantine nodes as 0.009 seconds and with misbehaving nodes in the network as 0.007 seconds with respect to the DSR protocol.

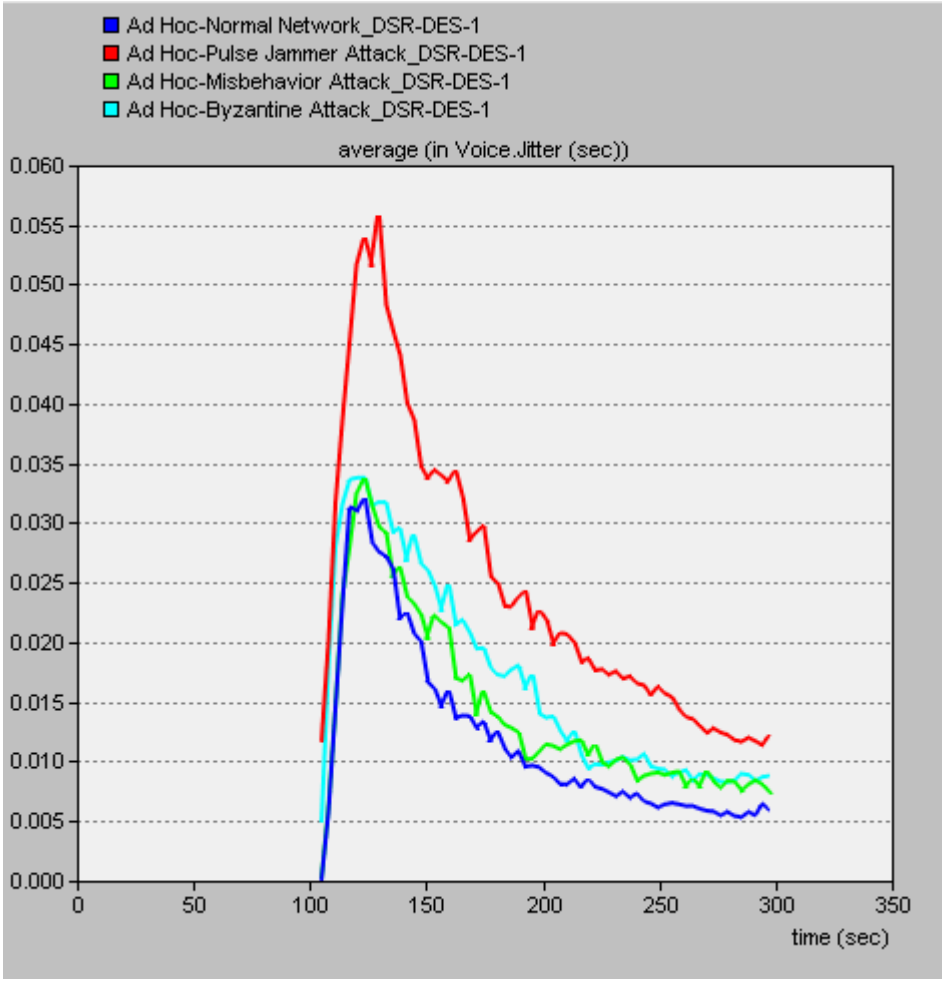


Figure 6.21 Jitter results of the normal network’s voice application with and without network attacks for DSR protocol

Analysis on the graph, it is seen that the largest increment of the “jitter” statistic for voice traffic is represented for the network with jamming nodes and the least increment is represented for the network with misbehaving nodes in respect of DSR protocol. That means, the DSR protocol is more vulnerable to the network with jamming nodes for jitter results of the normal network’s voice application. The graph shows that the security attacks have a significant impact on the network’s voice traffic for “jitter” statistic according to the DSR protocol. The network attacks reduce the reliability and performance of the network.

6.6.2 Jitter statistics of AODV routing protocol for voice application

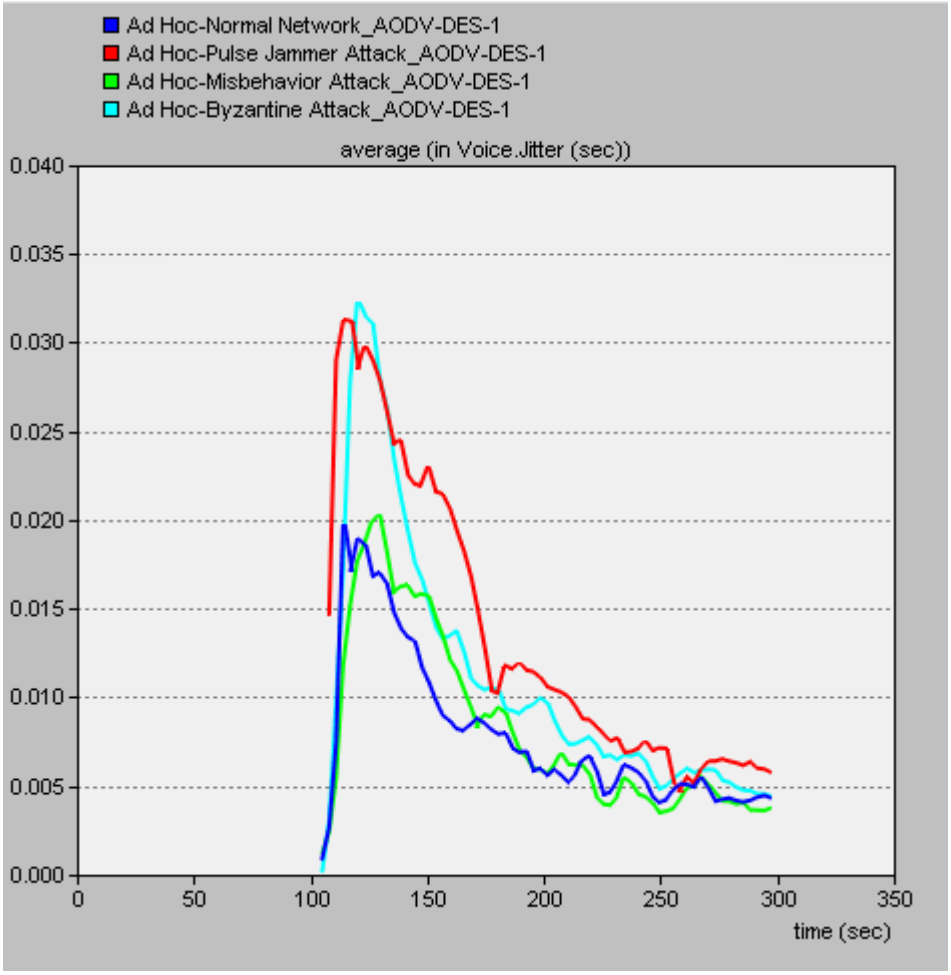


Figure 6.22 Jitter results of the normal network’s voice application with and without network attacks for AODV routing protocol

“Jitter” statistics are represented for voice application in the same graph. 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 6.22 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 jamming 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” statistic 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.

6.6.3 Jitter statistics of OLSR protocol for voice application

The network scenarios for different attacks are depicted in Figure 6.23. The “jitter” parameter of the normal network’s voice application has the average value of 0.118 seconds and with the Byzantine nodes in the network it is noted as 0.183 seconds. For the network with misbehaving nodes, its average value is 0.167 seconds and the “jitter” statistics according to the network with jamming nodes is recorded as 0.133 seconds. The largest increment of the jitter statistic for voice application is represented for the network with Byzantine nodes and the least

reduction is represented for the network with jamming nodes with respect to OLSR protocol.

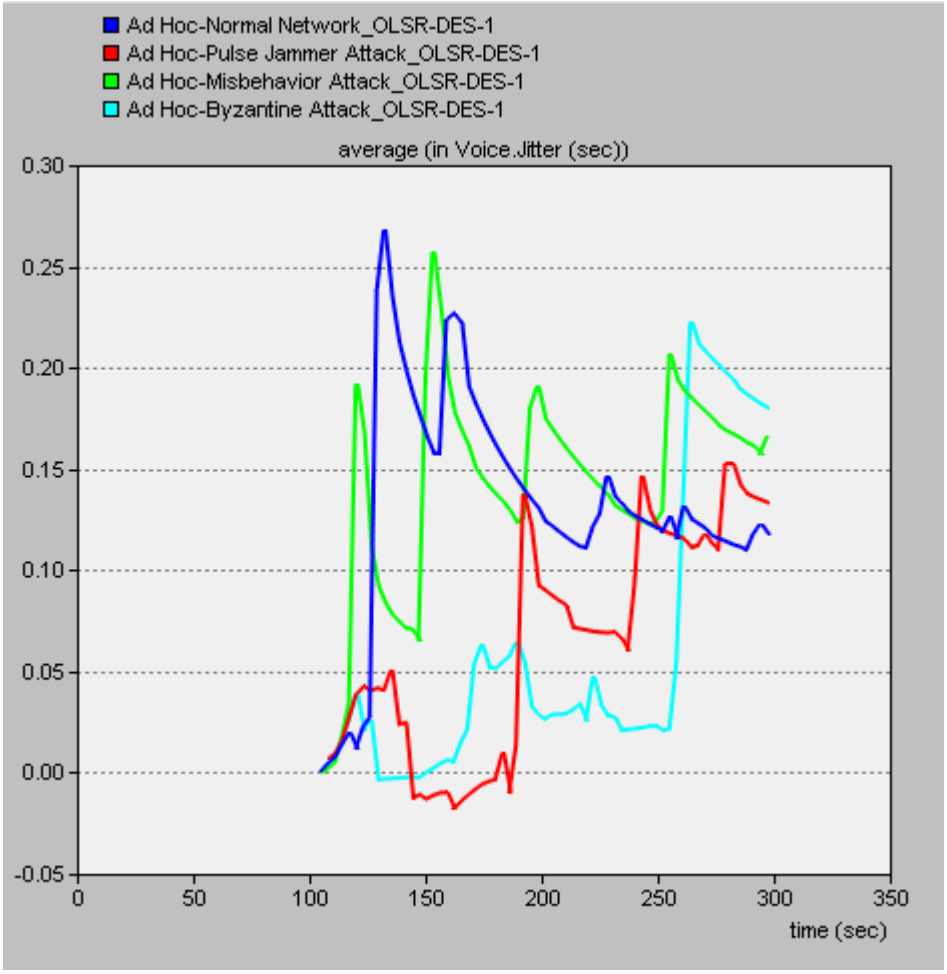


Figure 6.23 Jitter results of the normal network's voice application with and without network attacks for OLSR protocol

By examine the results, it is observed that the OLSR protocol is more vulnerable to the Byzantine nodes for "jitter" statistics of the network's voice application. The Byzantine attack shows that it drops the routing table for the other nodes and behaves malicious on purpose. The Byzantine nodes create routing loops and drop the data packets. The voice traffic delay of OLSR protocol under the network with and without security attacks notice up and down and it is unbalanced. The reason for this up and down rate of the voice traffic jitter could be that the network

nodes start to exchange the routing discovery, route request and routing table among each other in respect of the OLSR protocol.

6.6.4 Jitter statistics of GRP for voice application

The jitter results of the normal network's voice traffic with and without network attacks are compared in Figure 6.24 for GRP.

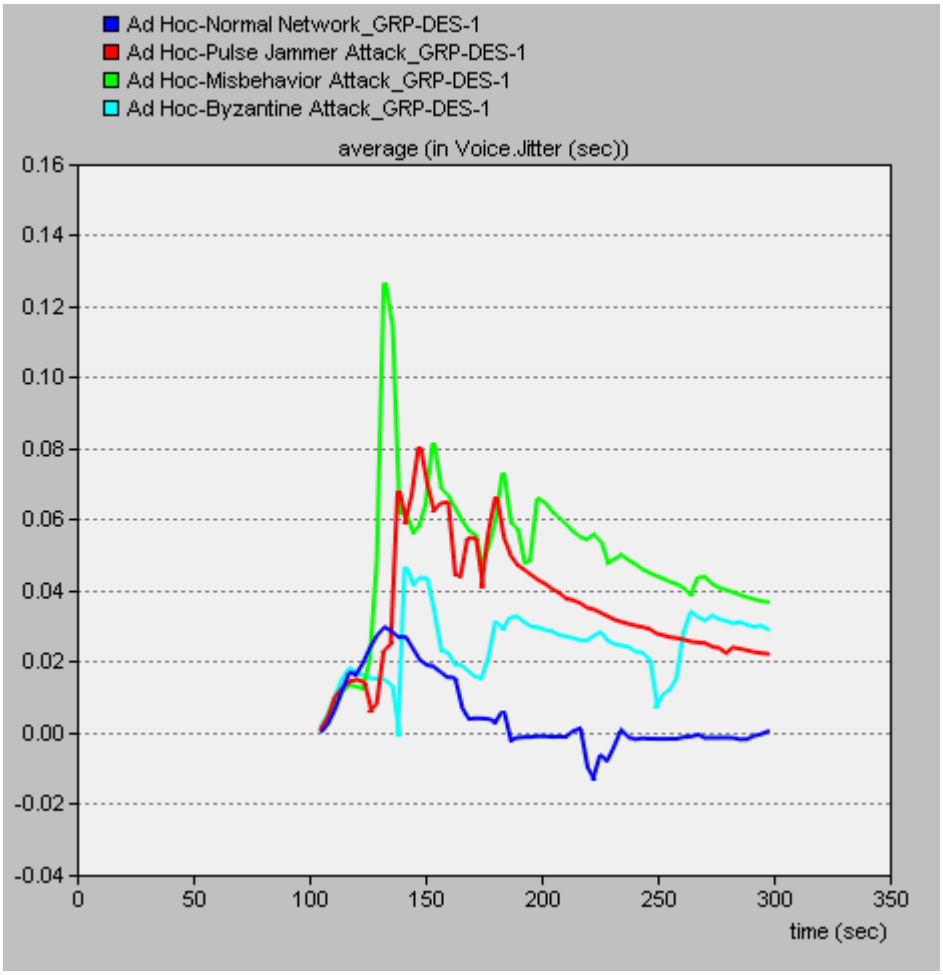


Figure 6.24 Jitter results of the normal network's voice application with and without network attacks for GRP

Jitter statistic of the network's voice application with normal traffic is recorded as 0.0004 seconds and the jitter parameter with misbehaving nodes is noted as 0.0368 seconds. On the other hand, the jitter of the network's voice traffic with

Byzantine nodes is noted as 0.0292 seconds and with jamming nodes as 0.0222 seconds.

The largest increment of the “jitter” statistic for voice application is represented for the network with misbehaving nodes and the least increment is represented for the network with jamming nodes with respect to GRP. This shows that the most malicious nodes in the network are misbehaving nodes. They don’t perform their duties, they lose the data packets and don’t forward the required data packets to the other nodes in the network.

The up and down voice delay of GRP under the network with and without network attacks is unbalanced and the reason for this has been mentioned pervious section.

6.7 Performance of Routing Protocols under Pulse Jammer Attack, under Misbehavior Node Attack and under Byzantine Attack for Email Application in respect of Traffic Received Statistics

In this section, the performance of routing protocols was compared under Pulse Jammer attack, under Misbehaviour Node attack and under Byzantine attack. First of all, a normal network traffic was generated using DSR, AODV, OLSR and GRP routing protocols respectively, then each network scenario was duplicated with different security attacks which were mentioned before. Five jamming nodes, five misbehaving nodes and five Byzantine nodes were placed in the network respectively. Four scenarios were occured in OPNET simulator by using 30 ad hoc nodes with IEEE 802.11b standard for email application in respect of “traffic received” statistics.

6.7.1 Traffic received statistics of DSR protocol for email application

The traffic received of the network’s email application is shown in Figure 6.25. When the normal network’s email application and the email application of the networks with intruder nodes are compared, it is seen that the “traffic received” statistics decreases with security attacks on the network.

Figure 6.25 represents that the average value of the normal network's email traffic received is 180.53 bytes/sec. On the other hand, the average value of the network's traffic received for email applicaiton with jamming nodes is 13.33 bytes/sec, with Byzantine nodes the value is recorded as 66.93 bytes/sec and with misbehaving nodes it is noted as 126.93 bytes/sec with respect to the DSR protocol.

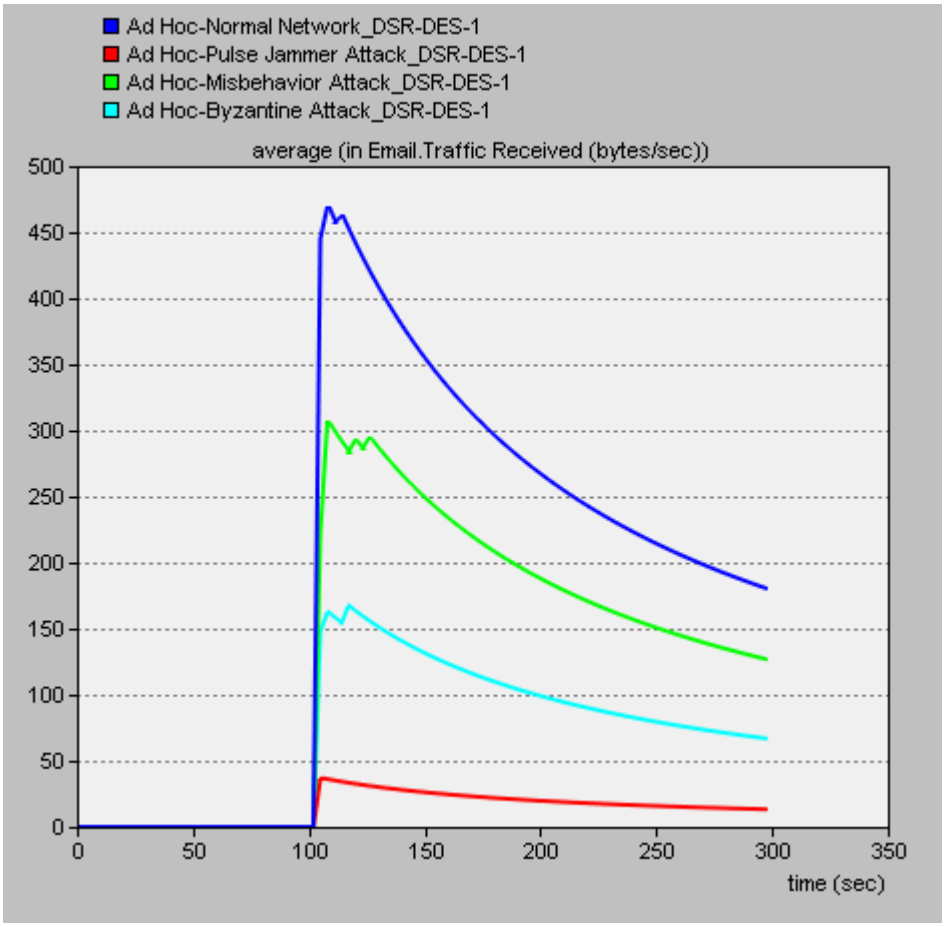


Figure 6.25 Traffic received results of the normal network's email application with and without network attacks for DSR protocol

The largest reduction of the traffic received statistic for email application is represented for the network with jamming nodes and the least reduction is represented for the network with misbehaving nodes with respect to DSR protocol. The vulnerable activities of the malicious nodes decrease the traffic received

gradually and the traffic received of the network's email application reduces more if the simulation time is extended more than 300 seconds.

6.7.2 Traffic received statistics of AODV routing protocol for email application

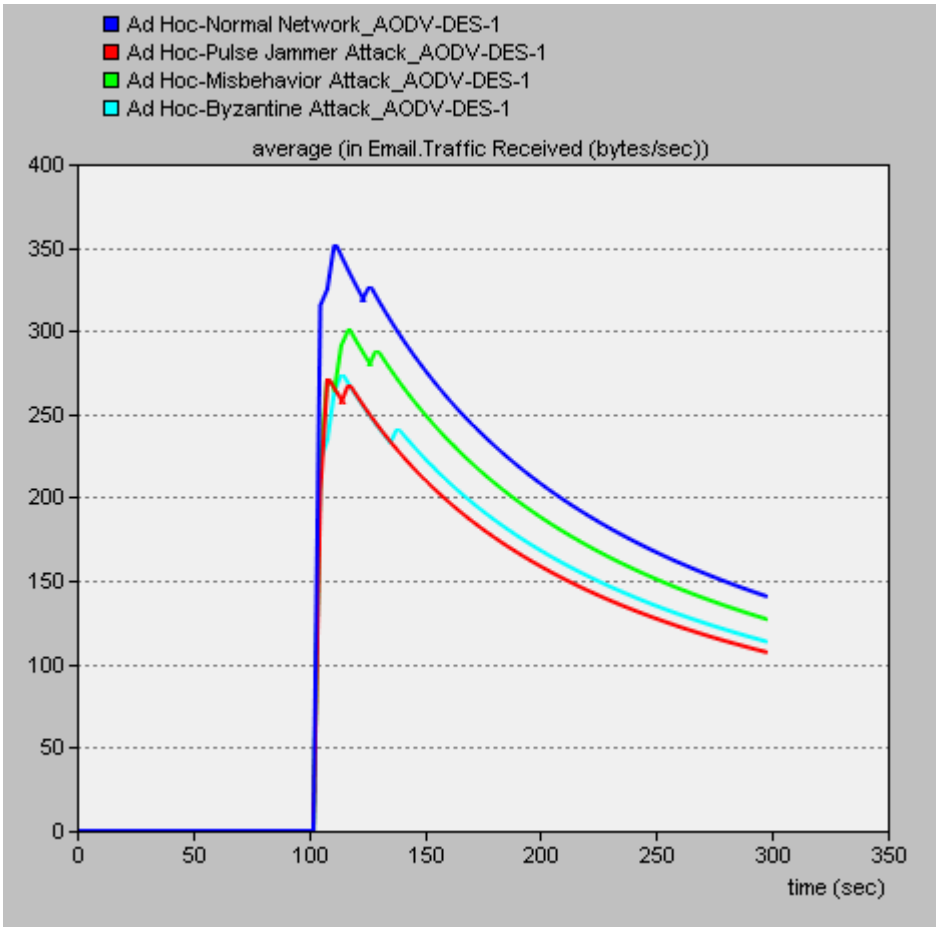


Figure 6.26 Traffic received results of the normal network's email application with and without network attacks for AODV routing protocol

In Figure 6.26, the traffic received is represented for the normal network's email application with and without network attacks in respect of the AODV routing protocol.

In the graph below, it is seen that the traffic received for email application increases in the beginning of the simulation up to a certain point and from that point it degrades rapidly. This is due to the fact that the utilization of the network

reaches a steady state after some time. And because of the abnormal activities of the intruder nodes, the traffic received reduction is more than the normal network's email traffic received for AODV routing protocol.

The "traffic received" statistic of the normal network's email application is recorded as 140.8 bytes/sec. Then, it is noted as 107.25 bytes/sec with jamming nodes in the network. The average value of the "traffic received" statistics for email traffic is 113.65 bytes/sec with Byzantine nodes and with misbehaving nodes in the network its value is noted as 127.15 bytes/sec with respect to the AODV routing protocol.

The largest reduction of the traffic received statistic for email application is represented for the network with jamming nodes and the least reduction is represented for the network with misbehaving nodes with respect to AODV routing protocol.

6.7.3 Traffic received statistics of OLSR protocol 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 6.27, 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 jamming 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 protocol.

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.

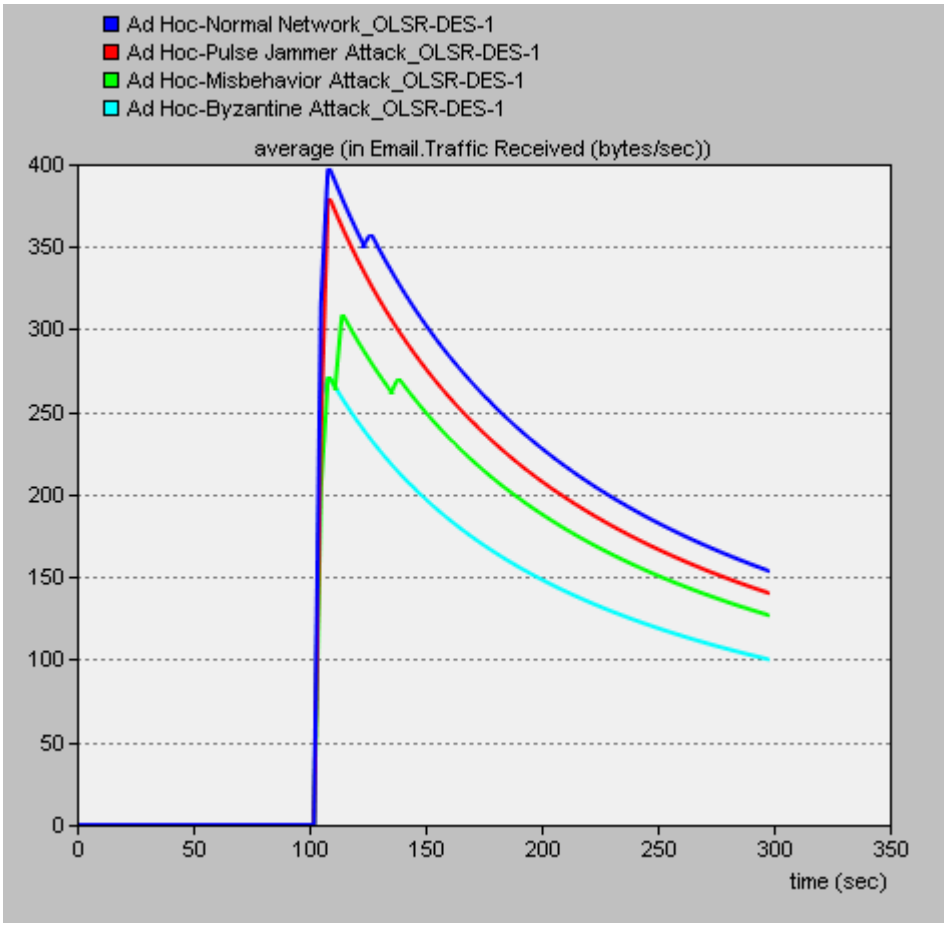


Figure 6.27 Traffic received results of the normal network's email application with and without network attacks for OLSR protocol

6.7.4 Traffic received statistics of GRP for email application

The normal GRP network's email traffic received is lower than the GRP network's email traffic received under pulse jammer attack and the captured results are shown in Figure 6.28.

There is a difference between the network's email traffic with and without malicious nodes in the network. Intruder nodes clearly reflects the availability and reliability of mobile ad hoc nodes in terms of security. The largest reduction of the traffic received statistic for email application is represented for the network with jamming nodes and the least reduction is represented for the network with misbehaving nodes with respect to GRP.

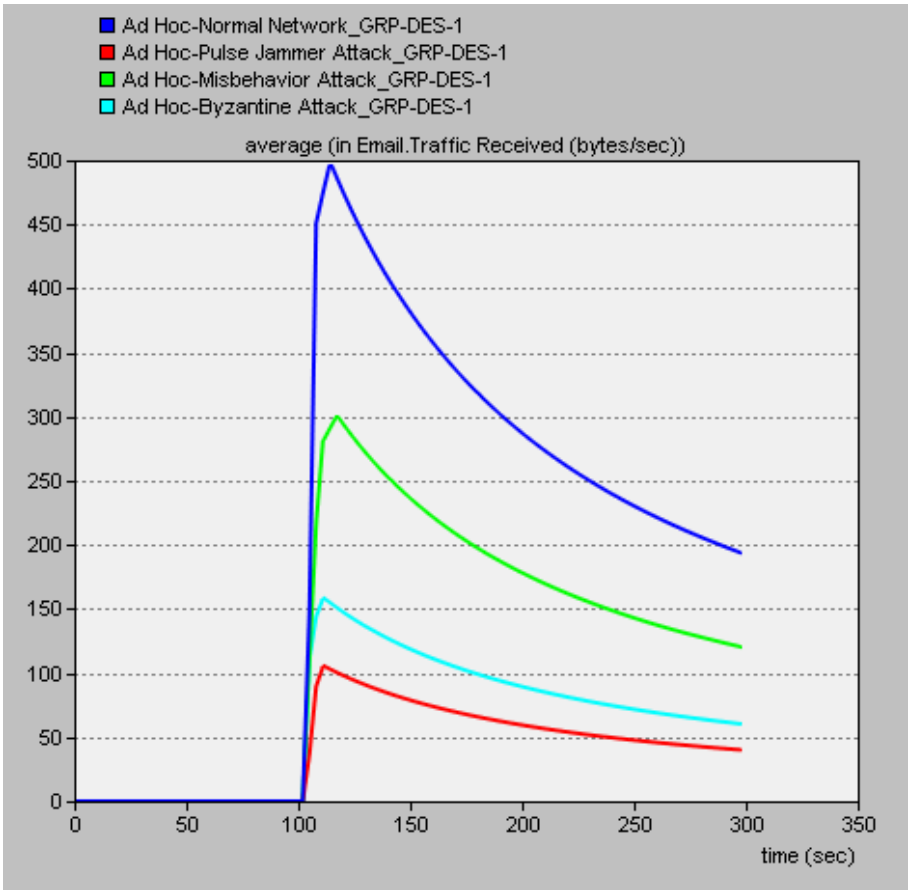


Figure 6.28 Traffic received results of the normal network's email application with and without network attacks for GRP

Traffic received of the network's email application is analyzed with and without intruder nodes. The normal email traffic received is recorded as 194.027 bytes/sec and later with jamming nodes in the network, the email traffic received is noted as 40.107 bytes/sec. For the network with Byzantine nodes, its average value is 60.373 bytes/sec and the "traffic received" statistics according to the network with misbehaving nodes is recorded as 120.587 bytes/sec.

6.8 Performance of Routing Protocols under Pulse Jammer Attack, under Misbehavior Node Attack and under Byzantine Attack for Video Conferencing Application in respect of Traffic Received Statistics

In this section, the networks using DSR, AODV, OLSR and GRP routing protocols were generated with 30 mobile ad hoc nodes respectively. Application

configuration, profile configuration and mobility configuration were defined. The mobile ad hoc nodes were configured to use mentioned routing protocols in OPNET. The normal network traffic results were collected, then five jamming nodes, five misbehaving nodes and five Byzantine nodes were placed in the network respectively and the captured results were compared for video conferencing application in respect of “traffic received” statistics.

6.8.1 Traffic received statistics of DSR protocol for video conferencing application

Figure 6.29 shows the email traffic received with and without security attacks in the network.

By examine the graph, it is observed that the rate of traffic received with intruder nodes on the network is decreased steadily. The largest reduction of the traffic received statistic for video conferencing application is represented for the network with jamming nodes and the least reduction is represented for the network with Byzantine nodes with respect to DSR protocol.

The “traffic received” statistics for video conferencing application of the normal network is recorded as 2,131 bytes/sec with respect to the DSR protocol. Ad hoc nodes exchange the routing table to the other nodes and few packets are dropped or discarded. After implementing the jamming nodes, it decreases to 979.5 bytes/sec. Jamming nodes deny the network transmission services. The graph represents the “traffic received” statistics of video conferencing application as 1,440 bytes/sec for the network with misbehaving nodes. Because of the misbehaving nodes don’t forward the data packets to other nodes, they drop the data packets and the entire network lead to congestion in terms of network performance. Figure 6.29 shows that the traffic received of the video conferencing application with Byzantine nodes in the network is noted as 1,901 bytes/sec in respect of the DSR. The Byzantine nodes don’t perform their basic tasks for the fulfilment of the network’s requirements in good means and these activities decrease the performance of the network.

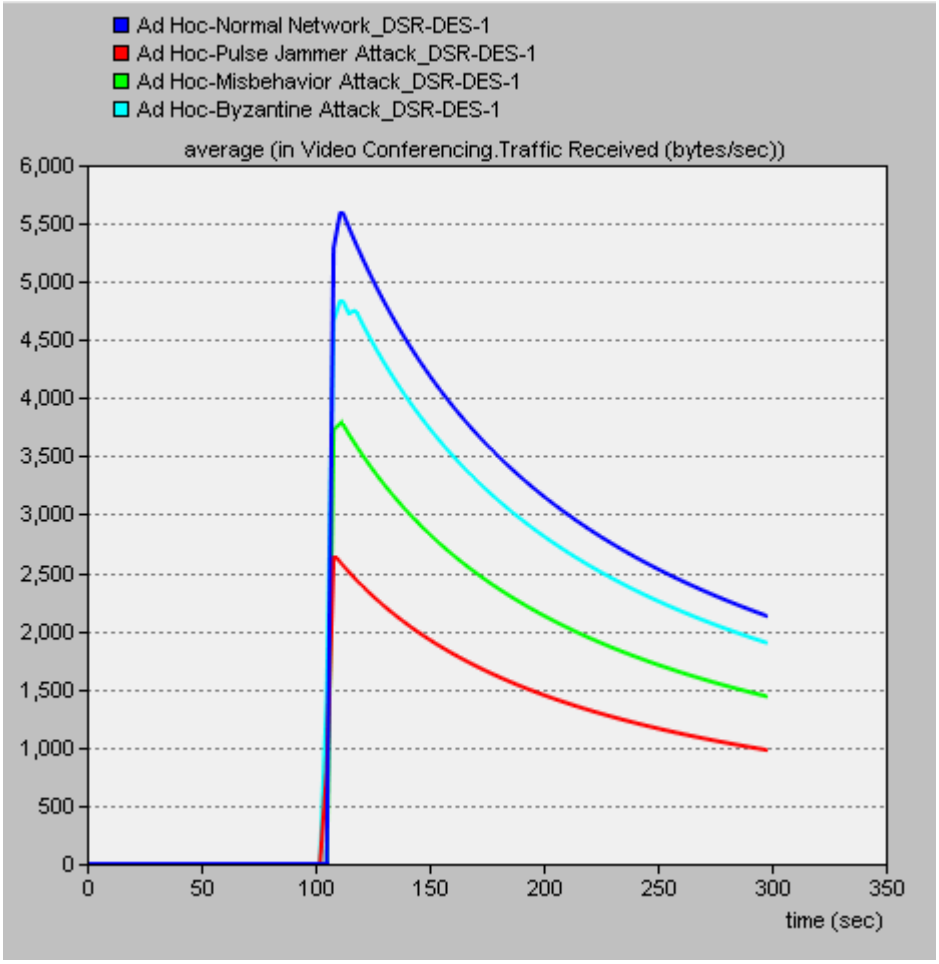


Figure 6.29 Traffic received results of the normal network's video conferencing with and without network attacks for DSR protocol

6.8.2 Traffic received statistics of AODV routing protocol for video conferencing application

Figure 6.30 represents that the average value of the normal network traffic received in video conferencing application is noted as 6,451 bytes/sec. Introducing the jamming nodes affectively reduce the traffic received of the network video conferencing at the rate of 979.2 bytes/sec. This result shows a poor performance of the video conferencing traffic. The misbehaving nodes decreases the video conferencing traffic received by causing corruption of the packets and keep dropping the packets randomly. The performance of the jamming nodes have a significant affect on the network's video conferencing traffic received. On the other

hand, the network with misbehaving nodes shows the average value of the video conferencing traffic received with 3,628 bytes/sec; with Byzantine nodes the value is noted as 4,320 bytes/sec in respect of the AODV routing protocol.

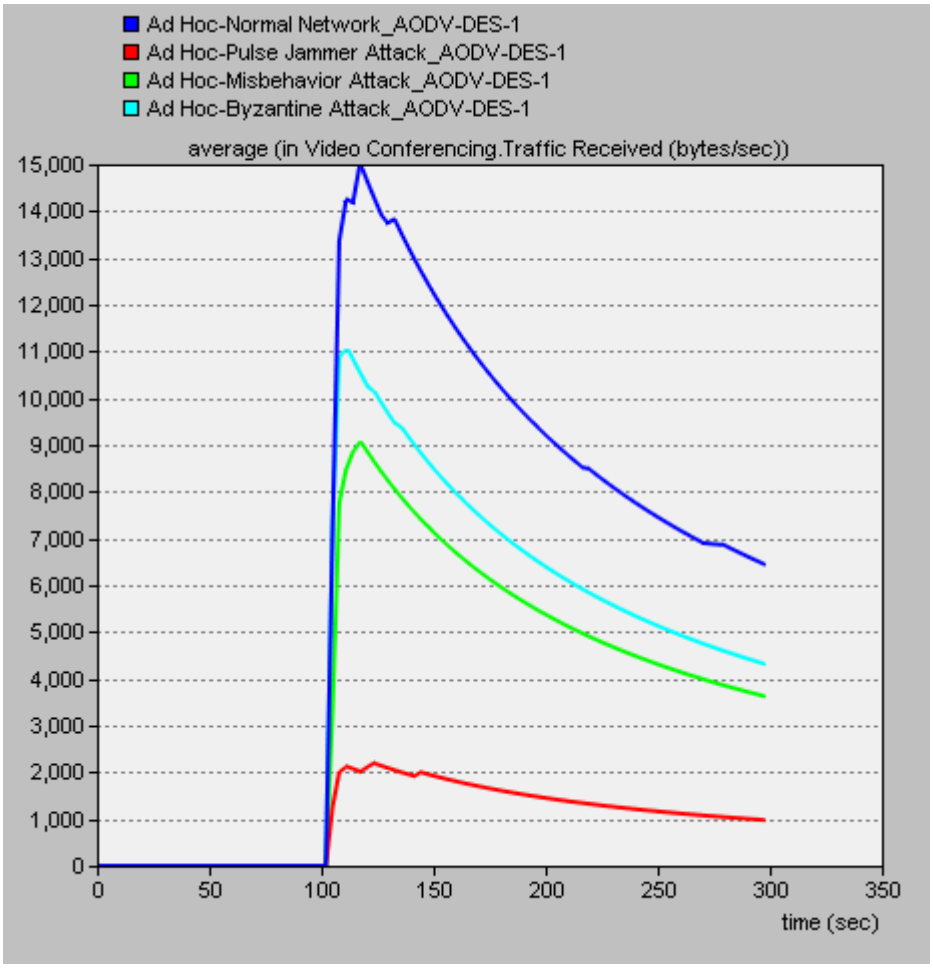


Figure 6.30 Traffic received results of the normal network's video conferencing with and without network attacks for AODV routing protocol

The reliability of the network reduces in terms of the network security. The largest reduction of the traffic received statistic for video conferencing application is represented for the network with jamming nodes and the least reduction is represented for the network with Byzantine nodes in respect of the AODV routing protocol.

6.8.3 Traffic received statistics of OLSR protocol for video conferencing application

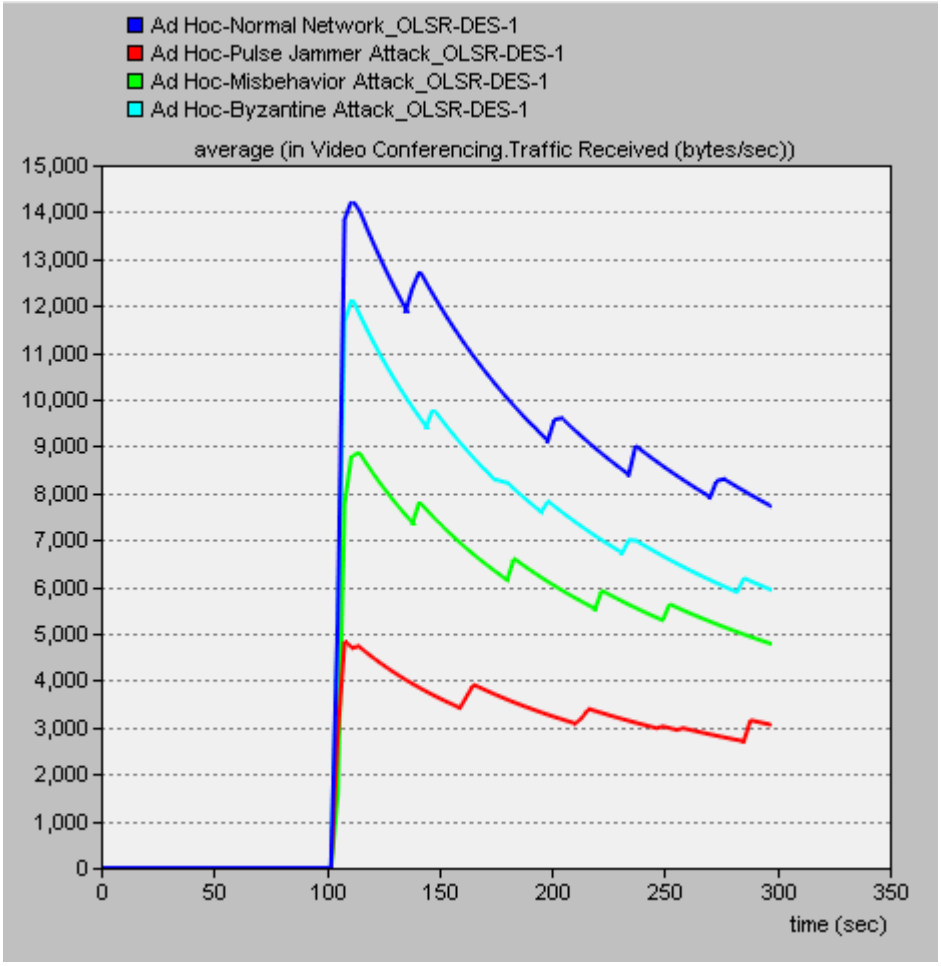


Figure 6.31 Traffic received results of the normal network's video conferencing with and without network attacks for OLSR protocol

The "traffic received" parameters for video conferencing application are represented in Figure 6.32 for the networks with and without network attacks with respect to the OLSR protocol.

In Figure 6.32, the normal network's video conferencing traffic received statistics is noted as 7,718 bytes/sec. Then, it is recorded as 3,052 bytes/sec with jamming nodes in the network. The average value of the video conferening traffic received statistics is recorded as 4,780 bytes/sec with misbehaving nodes and with

Byzantine nodes in the network its value is noted as 5,932 bytes/sec according to the OLSR protocol.The largest reduction of the traffic received statistic for video conferencing application is represented for the network with jamming nodes and the least reduction is represented for the network with Byzantine nodes in respect of the OLSR protocol.

The captured results show that the intruder nodes failed the network performance in every aspect. OLSR video conferencing traffic received decreases when the intruder nodes damage the network by their malicious activities.

6.8.4 Traffic received statistics of GRP for video conferencing application

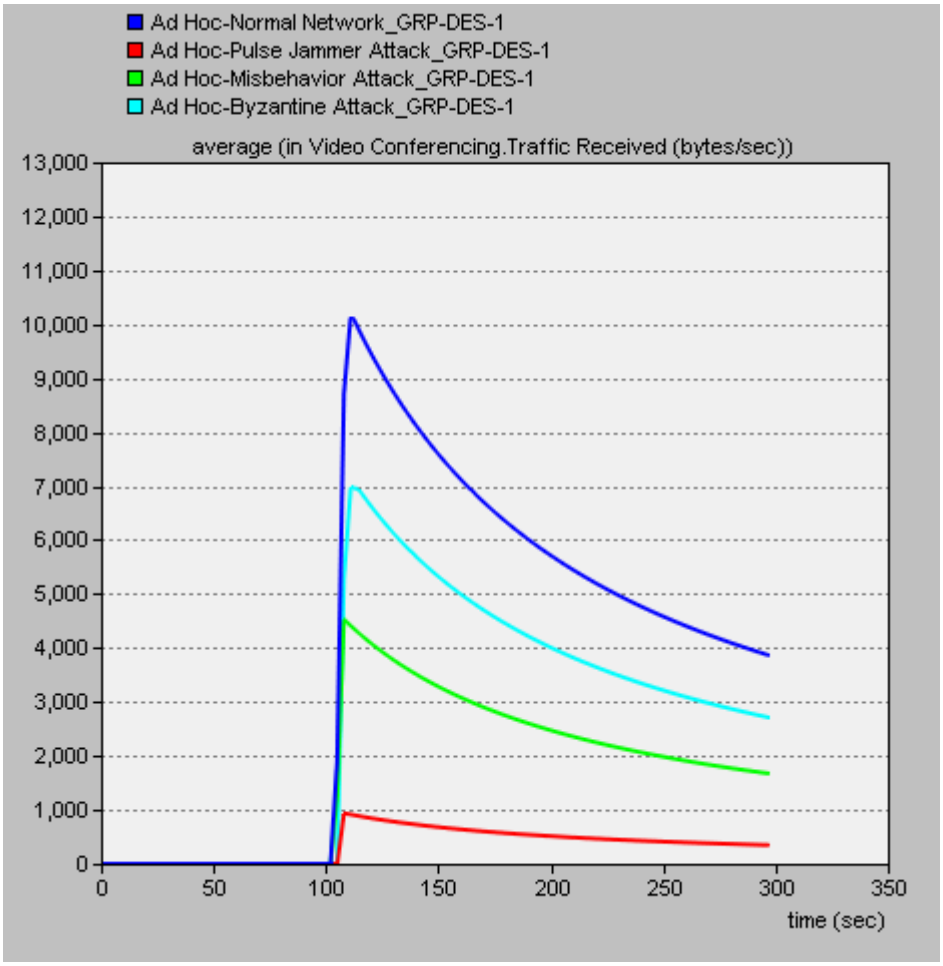


Figure 6.32 Traffic received results of the normal network's video conferencing with and without network attacks for GRP

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 “traffic received” statistics for video conferencing application of the normal network is noted as 3,859 bytes/sec at the duration time of simulation 300 seconds in Figure 6.32. After implementing the five jamming nodes, it decreases to 345.6 bytes/sec. The reason for this is because jamming nodes generate a noise on radio frequency in pulse time which decreases the “traffic received” statistics on the network for GRP. The graph represents the traffic received statistics of video conferencing application as 1,640 bytes/sec for the network with misbehaving nodes. Due to the misbehaving nodes, the network becomes congested. Figure 6.32 shows the traffic received with Byzantine nodes in the network as 2,707 bytes/sec with respect to the GRP. The Byzantine attack has a negative impact on the transmission and network traffic.

The largest reduction of the traffic received statistic for video conferencing application is represented for the network with jamming nodes and the least reduction is represented for the network with Byzantine nodes according to the GRP.

6.9 Simulation Results

In this thesis, the performance of routing protocols has been compared under jamming nodes, misbehaving nodes and Byzantine nodes. The impact of Pulse Jammer Attack, Misbehavior Node Attack and Byzantine Attack has been investigated on DSR, AODV, OLSR and GRP routing protocols.

Fistly, the performances of Reactive Routing Protocols such as DSR and AODV routing protocols has been compared under jamming nodes, under misbehaving nodes and under Byzantine nodes for the whole network. By analyzing the results, the largest reduction is represented for the network with jamming nodes and the least reduction is represented for the network with Byzantine nodes according to

the network load and throughput statistics and for the delay statistics the largest increment is represented for the network with jamming nodes and the least increment is represented for the network with Byzantine nodes in respect of DSR and AODV routing protocols. According to the results, it seems that DSR and AODV routing protocols are more vulnerable to the network with jamming nodes and placing the malicious nodes in the network reduces the performance of the network. In addition, Reactive Routing Protocols, i.e., DSR and AODV routing protocols behave in a similar manner.

The performance of OLSR protocol has been investigated under Pulse Jammer attack, Misbehavior Node Attack and Byzantine Attack and the results are compared in terms of performance metrics, i.e., data droped, delay, network load and throughput. By observing the results, it can be said that OLSR protocol is more vulnerable to Pulse Jammer attack and less vulnerable to Byzantine attack in general. It is clearly seen in the network results that the malicious nodes drop the data packets and don't forward the data packets to the other nodes and the network performance is affected badly.

The performance of GRP has been examined under security attacks that is mentioned before. The network traffic results are compared with and without jamming nodes, misbehaving nodes and Byzantine nodes in the network. Performance metrics, i.e., data droped, delay, network load and throughput are observed for analyzing the captured results. According to the results, GRP is acting a little different from the others, the largest reduction is represented for the network with jamming nodes and the least reduction is represented for the network with Byzantine nodes according to the network load and throughput statistics. However, for the delay and data dropped statistics, the largest increment is represented for the network with misbehaving nodes and the least increment is represented for the network with jamming nodes in respect of GRP. These kind of malicious activities spoil the transmission and the network traffic suffer badly.

The performances of for DSR, AODV, OLSR and GRP routing protocols have been compared under Pulse Jammer attack, under Misbehavior Node attack and under Byzantine attack for voice application in respect of packet end-to-end delay statistics. The network traffic results are compared with and without intruder nodes in the network. It is clearly seen in the network results that the packet end-to-end delay statistics with intruder nodes increases when it is compared to the normal network. Reactive Routing Protocols, i.e., DSR and AODV routing protocols behave in a similar manner. These routing protcols usually are more vulnerable to the network with jamming nodes and less vulnerable to the Byzantine nodes for voice application in packet end-to-end delay statistics. Nevertheless, GRP and Proactive Routing Protocol, i.e., OLSR Protocol are more influenced against Pulse Jammer attack, but less affected against Byzantine attacks for voice application in respect of packet end-to-end delay statistics. The network attacks drope the packets in the network and degrade the network routing services.

The performances of DSR, AODV, OLSR and GRP routing protocols have been compared under Pulse Jammer attack, under Misbehavior Node attack and under Byzantine attack for voice application with respect to jitter statistics. Analysis on the results, it is seen that DSR and AODV routing protocols give a similar response against the network attacks. They are more affected against jamming nodes, whereas GRP and OLSR routing protocols are less influenced against jamming nodes for jitter statistics of the network's voice application. Jitter statistics with intruder nodes increases when it is compared to the normal network. The jitter of the network with intruder nodes notice up due to the malicious activities on the network.

The performances of DSR, AODV, OLSR and GRP routing protocols have been compared under Pulse Jammer attack, under Misbehavior Node attack and under Byzantine attack for email application according to traffic received statistics. By observation the results, it can be said that DSR, AODV and GRP routing protocols give similar results. These protocols are more affected against the Pulse Jammer attack and they are less affected against the Misbehavior Node attack for traffic

received statistics of the network's email application. However, Proactive Routing Protocol, i.e., OLSR Protocol is less influenced against the Pulse Jammer attack for email application according to the traffic received statistics. The traffic received decreases systematically to lower level by placing the intruder nodes in the network.

The performances of DSR, AODV, OLSR and GRP routing protocols have been compared under Pulse Jammer attack, under Misbehavior Node attack and under Byzantine attack for video conferencing application in respect of traffic received statistics. It is seen in the network results that four routing protocols which are mentioned before give a similar response against the security attacks. They are more vulnerable to the network with jamming nodes and less vulnerable to the Byzantine nodes for video conferencing application in respect of traffic received statistics. The traffic received results decreases by placing the intruder nodes in the network for video conferencing traffic load. The decrease in traffic received affects the reliability and availability of the network.

7 CONCLUSION AND FUTURE WORK

In this research, Position-based Routing Protocol (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, under Misbehavior Node attack and under Byzantine attack is investigated.

The network with manet_station mobile nodes contains ftp, email (medium load) and low database traffic analyzing and the network with wlan_wkstn nodes contains http (heavy browsing), ftp (high load), email (high load), voice (PCM Quality Speech) and video conferencing (low resolution video) applications. The normal networks are compared with the networks which include 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. In addition, the performance of the routing protocols are compared under Pulse Jammer attack, under Misbehavior Node attack, and under Byzantine attack.

Results show that routing protocols are more vulnerable to the networks with jamming nodes, and placing the intruder nodes in the network reduces the reliability, availability and the performance of the network. In addition, when the performance of the routing protocols are compared under Pulse Jammer attack, under Misbehavior Node attack, and under Byzantine attack, based on the research and analysis of the simulation results, DSR has the worst performance compared with the other three routing protocols AODV, GRP and OLSR.

Jammer attack generates noise on the wireless radio frequency medium to stop the communication in order to trigger the network. A controlling transmitter can generate signal that will be strong to overcome the target signal and can disrupt communications. Subsequently, messages are lost due to the high noise in the spectrum. 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. Misbehaving nodes affects the network in several different

security aspects. Also, Byzantine attack drops, modifies and mis-route the forwarding packets in an attempt to disrupt the routing service.

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.

Security is a primary concern in mobile ad hoc networks. The use of computer networks becomes a necessity for government, industry, and personal businesses. As communication technology networks continue to grow, potential vulnerabilities are under greater threat. Everyday, attackers are trying to find a new security vulnerability in mobile ad hoc networks. A single weak point may give the attacker the opportunity to gain the access of the system and perform malicious tasks, so security must be provided for the entire system.

Research in this field continues for many years, but still in an early stage. There are many unanticipated attacks remaining undiscovered. Cyber attacks, including hacking, of business websites and computer systems are increasingly common. These attacks can be extremely damaging for businesses, computer information systems, computer networks or personal computer devices. So, protection and defense against cyber attacks become inadequate as attackers become more sophisticated. The ability to track and trace attackers is crucial. As cyber attacks change, new defenses need to be developed. Additionally, more research needs to be done on data security in different levels, secure routing protocols, efficient key agreement and distribution, and trust management for large mobile ad hoc networks. Today's security architecture must be agile, flexible, and deeply integrated. It must offer a far-reaching view of threats to prevent attacks and avert their worst effects.

REFERENCES

[1] LIU, C., and KAISER, J., “A Survey of Mobile Ad Hoc Network Routing Protocols,” The University of Magdeburg, 36p, October 2005.

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

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

[4] SALIM, S., “Mobile Ad Hoc Network Security Issues,” M.Sc. Thesis, University of Central Lancashire, 81p, 2010.

[5] JHA, R.K., BHOLEBAWA, I.Z., DALAL, U.D., and WANKHEDE, A.V., “Detection and Fortification Analysis of WiMAX Network: With Misbehavior Node Attack,” International Journal on Communications, Network and System Sciences, vol. 5, pp. 353-367, 2012.

[6] PROANO, A. and LAZOS, L., “Selective Jamming Attacks in Wireless Networks,” Department of Electrical and Computer Engineering, University of Arizona, 6p.

[7] PANI, N.K., “A Secure Zone-Based Routing Protocol for Mobile Ad Hoc Networks,” Department of Computer Science and Engineering, National Institute of Technology, 85p, May 2009.

[8] RAZAK, S.A., FURNELL, S.M., and BROOKE, P.J., “Attacks against Mobile Ad Hoc Networks Routing Protocols,” Network Research Group, University of Plymouth, 6p.

[9] DENG, H., LI, W., and AGRAWAL, D.P., “Routing Security in Wireless Ad Hoc Networks,” IEEE Communications Magazine, vol. 40, pp. 70- 75, Oct. 2002.

[10] NEHRA, E. and SINGH, E.J., “Performance Comparison of AODV, TODV,OLSR and ABR using OPNET,” International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 5, pp. 984-990, May 2013.

[11] TAMIZHSELVI, A. and BANU, Dr. R.S.D.W., “Performance Evaluation of Geographical Routing Protocol under Different Traffic Scenario,” International Journal of Computer Science and Telecommunications, vol. 3, no. 3, pp. 64-67, March 2012.

[12] VENKATESH, INDRA, A., and MURALI, R., “Routing Protocols for Vehicular Adhoc Networks (VANETs): A Review,” Journal of Emerging Trends in Computing and Information Sciences, vol. 5, no. 1, pp. 25-43, January 2014.

[13] GU, D. and ZHANG, J., Mitsubishi Electric Research Laboratories, “QoS Enhancement in IEEE802.11 Wireless Local Area Networks,” IEEE Communications Magazine, pp. 120-124, June 2003.

[14] TAHERI, M., KAZEMI, M.A.A., and TOLOIE-ESHLAGHY, A., “Improvement of Mobility Management in Heterogeneous Wireless Networks by Using Multiple Attribute Decision Making,” Computer and Information Science, vol. 4, no. 4, July 2011.

[15] MOHAPATRA, P., LI, J., and GUI, C., “Qos In Mobile Ad Hoc Networks,” University Of California, IEEE Wireless Communications, pp. 44-52, June 2003.

[16] BAYAN, A.F., WAN, T.C. and RAMADASS, S., “Delay Analysis and System Capacity Control for Mobile WIMAX Relay Networks,” Journal of Computer Science, vol.6, no.10, pp. 1137-1143, 2010.

[17] KALE, V. and GULHANE, V., “Detection of Misbehavior Nodes using Efficient Comparison of Multiple Route Set in Performance Routing Protocols in WSN,” International Journal of Computer Science and Telecommunications, vol. 3, no. 12, pp. 43-49, December 2012.

[18] GENC, V., “Performance Analysis of Transparent Mode IEEE 802.16j Relay –based WIMAX Systems,” M.Sc. thesis, University College Dublin, pp. 20-67, 2010.

[19] PAUL, H. and SARKAR, P., “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, pp. 370-374, August 2013.

[20] ÖZTÜRK, Ş., “Improvement of Performance of Heterogeneous Wimax Systems by using Relay Networks,” M.Sc. thesis, Başkent University, 89p, 2013.

[21] EDEMEN, Ç., “Channel Adaptive User Cooperation Strategies for Fading Wireless Channels,” M.Sc. thesis, Işık University, June 2006.

[22] BAŞTÜRK, İ., “Iterative Channel Estimation Techniques for Multiple Input Multiple Output Orthogonal Frequency Division Multiplexing Systems,” M.Sc. thesis, İzmir Institute of Technology, 78p, July 2007.

[23] MAUVE, M., WIDMER, J. and HARTENSTEIN, H., “A Survey on Position-Based Routing in Mobile Ad Hoc Networks,” IEEE Network, pp. 30-39, November/December 2001.

[24] THAKARE, A.N. and JOSHI, Mrs. M.Y., “Performance Analysis of AODV & DSR Routing Protocol in Mobile Ad hoc Networks,” IJCA Special Issue on “Mobile Ad-hoc Networks” MANETs, pp. 211-218, 2010.

[25] KHOKHAR, R.H., NGADI, M.A., and MANDALA, S., “A Review of Current Routing Attacks in Mobile Ad Hoc Networks,” International Journal of Computer Science and Security, vol. 2, no. 3, pp. 18-29, 2008.

[26] BADGUJAR, V.S. and DHAGE, S.N., “Effect Of Blackhole Intrusion in Wireless Networks,” International Journal of Computer Engineering and Applications, vol. 7, no. 3, pp. 9-18, September 2014.

[27] HAAS, Z.J., PEARLMAN, M.R., and SAMAR, P., “The Zone Routing Protocol (ZRP),” IETF Internet Draft, draft-ietf-manet-zone-zrp-04.txt, July 2002.

[28] PERVAIZ, M.O., CARDEI, M., and WU, J., “Routing Security in Ad Hoc Wireless Networks,” Florida Atlantic University, 32p, 2005.

[29] KAPLAN, E., “Understanding GPS,” Artech House, 1996.

[30] CAPKUN, S., HAMDI, M., and HUBAUX, J., “Gps-free Positioning in Mobile Ad Hoc Networks,” Proc. Hawaii Int’l. Conf. System Sciences, Jan. 2001.

[31] PERKINS, C.E., ROYER, E.M., DAS, S.R., and MARINA, M.K., “Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks,” IEEE Personal Communications, pp. 16-28, February 2001.

[32] BIHANI, A., “An Analysis of Routing Protocols in MANETs,” International Journal of Engineering Trends and Technology (IJETT) , vol. 7, no. 1, pp. 31-35, Jan. 2014.

[33] SHIVAHARE, B.D., WAHI, C., and SHIVHARE, S., “Comparison of Proactive and Reactive Routing Protocols in Mobile Adhoc Network using Routing Protocol Property,” International Journal of Emerging Technology and Advanced Engineering, vol. 2, no. 3, pp. 356-359, March 2012.

[34] EHRAMPOOSH, S. and MAHANI, A.K., “Secure Routing Protocols: Affections on MANETs Performance,” First International Conference on Communications Engineering, pp. 77-82, 22-24 December 2010.

[35] SANCHEZ, J.A., RUIZ, P.M., and MARIN-PEREZ, R., “Beacon-Less Geographic Routing Made Practical: Challenges, Design Guidelines, and Protocols,” IEEE Communications Magazine, pp. 85-91, August 2009.

[36] KARP B.N., “Geographic Routing for Wireless Networks,” Doctoral thesis, Harvard University, 118p, October 2000.

[37] ULLAH, I. and REHMAN, S.U., “Analysis of Black Hole Attack on MANETs using Different MANET Routing Protocols,” M.Sc. thesis, Blekinge Institute of Technology, 51p, September 2010.

[38] SHARMA, V. and MITTAL, S., “Load Balancing in MANETs: A Review,” International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, no. 5, pp. 1-32, pp. 1245-1249, May 2014.

[39] GAGANDEEP, AASHIMA, and KUMAR, P., “Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review,” International Journal of Engineering and Advanced Technology (IJEAT), vol. 1, no. 5, pp. 269-275, June 2012.

[40] BISWAS, K. and ALI, Md. L., “Security Threats in Mobile Ad Hoc Network,” M.Sc. thesis, Blekinge Institute of Technology, 48p, March 2007.

[41] WU, B., CHEN, J., WU, J., and CARDEI, M., “A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks,” Department of Computer Science and Engineering, Florida Atlantic University.

[42] AWERBUCH, B., HOLMER, D., NITA-ROTARU, C., and RUBENS, H., “An On-Demand Secure Routing Protocol Resilient to Byzantine Failures,” ACM Workshop on Wireless Security (WiSe’02), Atlanta, Georgia, USA pp. 21-30., September 2002.

[43] RAJARAM, A. and PALANISWAMI, Dr. S., “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.

[44] JAWANDHIYA, P.M., MANGESH, A., and GHONGE, M., “A Survey of Mobile Ad Hoc Network Attacks,” International Journal of Engineering Science and Technology, vol. 2, no.9, pp. 4063-4071, 2010.

[45] LI, W. and JOSHI, A., “Security Issues in Mobile Ad Hoc Networks - A Survey,” Department of Computer Science and Electrical Engineering, University of Maryland, 23p.

[46] KÄRPIJOKI, V., “Security in Ad Hoc Networks,” Telecommunications Software and Multimedia Laboratory, Helsinki University of Technology, 16p.

[47] BURG, A., “Ad Hoc Networks Specific Attacks,” Technische Universität München, Institut für Informatik, Seminar Paper, Seminar Ad Hoc Networking: concept, applications, and security, November 2003.

[48] CHALABIANLOO, N., “Routing And Security In Wireless Sensor Networks, An Experimental Evaluation of A Proposed Trust Based Routing Protocol,” M.Sc. Thesis, Middle East Technical University, 71p, February 2013.

[49] JHA, R.K., BHOLEBAWA, I.Z., DALAL, U.D., and WANKHEDE, A.V., "Detection and Fortification Analysis of WiMAX Network: With Misbehavior Node Attack," International Journal on Communications, Network and System Sciences, vol. 5, pp. 353-367, April 2012.

[50] ZHANG, Y., LAZOS, L., and KOZMA, W. Jr., “AMD: Audit-based Misbehavior Detection in Wireless Ad Hoc Networks,” IEEE Transactions on Mobile Computing, 14p.

[51] HATWARE, I.V., KATHOLE, A.B., and BOMPILWAR, M.D., “Detection of Misbehaving Nodes in Ad Hoc Routing,” International Journal of Emerging Technology and Advanced Engineering, vol. 2, no. 3, pp 6-11, 2012.

[52] Opnet Technologies, Inc. “Opnet Simulator,” www.opnet.com