MODELLING AND SIMULATION OF JAMMING ATTACKS IN WLAN

by

Tian Fu

April, 2012

Director of Thesis: Dr. Te-Shun Chou

Department of Technology Systems

Abstract

Wireless local area networks (WLAN) are one of the most widely used technologies in our daily lives. Instead of being limited to the range of wired equipment, users can communicate freely. However, since wireless networks are based on communication within radio channels, WLANs are susceptible to malicious attempts to block the channel. One of the most frequently used attacks is a Denial of Service (DoS) attack known as a jamming attack. Jamming attacks interfere with the transmission channels by constantly sending useless packets in order to disturb the communication between legitimate nodes. In real wireless networks where users communicate constantly, a jamming attack can cause serious problems. Because of this, a study of jamming attacks and how to prevent them is necessary. In this thesis, the jamming attacks were simulated in WLAN using OPNET Modeler, in order to provide a better understanding of jamming attacks. This study will be helpful for future research and development of a practical, effective way to avoid jamming attacks. The objectives of this thesis were to simulate client-server and ad-hoc networks and different jammers; launch jamming attacks in order to test how much influence different jammers have in WLAN communications; and to compare the performances of different ad-hoc routing protocols.

MODELLING AND SIMULATION OF JAMMING ATTACKS IN WLAN

A Thesis

Presented To the Faculty of the Department of Technology Systems

East Carolina University

In Partial Fulfillment of the Requirements for the Degree

Masters of Science in Technology Systems

by

Tian Fu

April 2012

MODELLING AND SIMULATION OF JAMMING ATTACKS IN WLAN

by

Tian Fu

APPROVED BY:

DIRECTOR OF DISSERTATION/THESIS:

_____

(Te-Shun Chou, Ph.D.)

COMMITTEE MEMBER:

_____

(Erol Ozan, Ph.D.)

COMMITTEE MEMBER:

_____

(J. Barry DuVall, Ph.D.)

CHAIR OF THE DEPARTMENT OF TECHNOLOGY SYSTEMS:

_____

(Tijjani Mohammed, Ph.D.)

DEAN OF THE GRADUATE SCHOOL:

_____

(Paul J. Gemperline, Ph.D.)

ACKNOWLEDGMENTS

Firstly, I would like to thank my advisor Dr. Te-Shun Chou. This thesis would be impossible without the insightful guidance he provided me. I would also like to thank Dr. Tijjani (TJ) Mohammed, Dr. Erol Ozan and Dr. J. Barry DuVall for being part of the committee to evaluate this work. Secondly, I want to thank my parents. Although they are far away, they still supported me through the process of obtaining my Master's degree. Finally, I would like to thank Mr. Storm Bryan Henry for reading through my thesis and giving me great suggestions.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS OR ABBREVIATIONS

WLAN: Wireless Local Area Network

DoS: Denial of Service

OPNET: Optimized Network Engineering Tool

AP: Access Point

IDS: Intrusion detection system

MAC: Medium access control

IEEE: The Institute of Electrical and Electronics Engineers

CS: Client-server

AH: Ad-hoc

PDR: Packet delivery Ratio

RSP: Received Signal power

MANET: Mobile Ad-hoc Networks

WMN: Wireless Mesh Networks

WSN: Wireless Sensor Networks

AODV: Ad-hoc On-Demand Distance Vector

DSR: Dynamic Source Routing

TORA: Temporally-Ordered Routing Algorithm

ELINT: Electronic Intelligence

CHAPTER 1: INTRODUCTION

Wireless Local Area Networks (WLANs) are becoming an increasingly important technology that is bringing the world closer together. WLANs are used in every area, such as education, agriculture, pharmaceuticals, manufacturing, transportation, military, and research. Therefore, the importance of WLAN security is significant.

There are two popular styles of WLANs: client-server networks and ad-hoc networks. The difference between these two networks is that client-server networks use access points or routers to transmit data, but ad-hoc networks do not rely on any pre-existing transmitters. Instead, all the nodes in an ad-hoc network participate in the routing process by forwarding messages to each other.

According to The Institute of Electrical and Electronics Engineers (IEEE) 802.11g standards (IEEE Org., 2012), all wireless network nodes transmit data packets in different channels. Since channels in WLANs are defined by frequencies, they are susceptible to malicious jamming attacks. It is easy for attackers to accomplish sending multitudes of useless packets in a specific frequency. Jamming attacks attempt to make the system crash by flooding it with useless traffic, and use all the resources in the network so users in the network cannot connect to the system. It is consistently used by hackers to break network systems, because of ease and security issues.

In this thesis, client-server networks and ad-hoc networks were simulated by using the simulation tool OPNET Modeler (OPNET Technologies, Inc., 2012). During the simulation, factors that may influence the result of the simulation were taken into consideration such as the distance, power level, and protocols used in ad-hoc networks.

1.1 Statement of the Problem

Previous research had found that jammers influence the performance of WLAN networks. However, most research could not demonstrate how different jammers and changed characteristics vary the result of jamming attacks. Jammers disturb networks in different situations in order to achieve various jamming effects. Also, because of the mobility of the WLAN, users cannot be simulated by only using a fixed node or a specific trajectory. Random trajectories in both nodes and jammers have to be considered a real world simulation Scenario. Finally, most research used single ad-hoc routing protocols in the network. A comparison of multiple routing protocols needs to be simulated.

The research problems of this thesis were:

- To compare how different jammers and changing characteristics vary the result of jamming attacks
- To compare the performance of switching channels to avoid jamming attacks under different jamming attacks
- To test the performance of popular ad-hoc network routing protocols with random trajectory jamming attacks

1.2 Research Questions

Three questions were asked in this research:

- How WLANs are affected differently based on different forms of jamming attacks and characteristics?
- Can switching channels in WLANs avoid jamming attacks?

- Which ad-hoc routing protocols, including Ad-hoc On-demand Distance Vector (AODV), Temporally-Ordered Routing Algorithm (TORA), and Dynamic Source Routing (DSR) is superior?

1.3 Methodology

OPNET Modeler was used to establish and analyze five scenarios which include three client-server and two ad-hoc network scenarios.

- Scenarios 1 to 3 were established basing on the wireless LAN models supported by OPNET Modeler library, in order to test how WLANs were affected by jammers and varying characteristics. Scenario 1 was established as a simple client-server network. By changing the parameters of the access point and the distance between the nodes and the access point, multiple experiments were simulated. For Scenario 2, a fixed pulse jammer was added to the network based on Scenario 1 for generating jamming attack in the network. How characteristics of the jammer vary the performance of jamming attack was compared in several experiments. In order to test mobile pulse jammer, Scenario 3 was simulated in OPNET Modeler. Scenario 3 was also based on client-server network with a mobile pulse jammer. Scenario 4 used ad-hoc network style.
- Different jammers were used in each experiment in Scenario 4. Including single band jammer, pulse jammer, and sweep jammer. After simulation with all possibilities and changed characteristics, a comparison of different jammers was drawn. Channels were switched in Scenario 4 to test if switch channel could be done in order to avoid jamming attacks.
- Communication channels in the networks were switched in order to avoid jamming attacks in Scenario 5. Experiments were done to test if switching channel works for every

type of jammer. In order to simulate random trajectories for users and jammers, a new method to generate networks and trajectories had been applied. This method was implemented in the ad-hoc experiment.

1.4 Significance of the Study

It is worth mentioning that the work presented here contributes several issues relevant in the field of jamming attacks in WLAN.

First this thesis had provided a better understanding of jamming behavior in WLANs. Multiple experiments had shown a comparison of different jammer performances. Second, this thesis demonstrated the use of different jammers in various environments, including the feasibility of switching channels to avoid jamming attacks. Third, it also provided a way to simulate random trajectory jamming attacks, and used it to simulate and compare the performance of multiple ad-hoc routing protocols.

1.5 Explanation of Parameters

In order to evaluate a network or a device, important parameters were used in the analysis. Including throughput, load, delay, traffic sent, traffic received, and data dropped. Following important parameters used in this thesis are presented for a better understanding of this thesis.

1.5.1 Throughput

Throughput (bits/sec) of a network or device is the total amount of data traffic that was successfully received and forwarded to the higher layer by the WLAN Media Access Control (MAC). It is the rate of successful message delivery of the network communication channel. For example, assume two nodes are transmitting data in a network. If the average data delivery in this network is 100 bits/sec, the throughput of the network is 100 bits/sec.

1.5.2 Load

Load (in bits/sec) of a network or a device is the average rate submitted to the wireless LAN MAC by its higher layers in this node. It is a measure of the amount of data networks or devices are transmitting in the system.

1.5.3 Delay

Delay (sec) represents the end-to-end delay of all the data packets that are successfully received by the WLAN MAC and forwarded to the higher layer. This delay includes the delays at the source, reception of all the individual fragments, and the delay of the frame via access point (AP). In the case of the source and destination, MACs are not AP MACs of the same infrastructure BSS.

1.5.4 Data Traffic Sent

Data traffic sent (bits/sec) presents WLAN data traffic transmitted by the MAC. Data traffic of a network is the rate of traffic transmitted by all the nodes. The data traffic sent from a node is the rate of data traffic transmitted by this single node.

1.5.5 Data Traffic Received

Data traffic received (bits/sec) in WLAN refers to the data traffic successfully received by the MAC from the physical layer. This statistic includes all data traffic received regardless of the destination of the received frames.

1.5.6 Data Dropped

Data dropped (bits/sec) is the data traffic in higher layer dropped by the WLAN MAC due to consistently failing retransmissions. This statistic reports the number of the higher layer packets that are dropped because the MAC cannot receive any ACKs of those packets or their fragments for the (re)transmissions.

1.6 Thesis Organization

The rest of the thesis is organized as follows: in Chapter 2, an overview of related works is discussed, and WLAN networks, including client-server networks and ad-hoc networks, are introduced. The research about jamming attacks, detection of jamming attacks, and the simulation tools are discussed in various literatures. Chapter 3 is the methodology of all the experiments in this thesis. There are three experiments which used client-server networks, while two experiments used ad-hoc networks. All the Scenarios are presented and explained; the purpose of each experiment is demonstrated. In Chapter 4, results of OPNET Modeler network simulations and an analysis of result comparisons is discussed. Chapter 5 contains the conclusion that is drawn from the analysis and the future work related to this research.

CHAPTER 2: LITERATURE REVIEW

In this Chapter, references of previous research that utilized the concepts in Chapter 1 are introduced. For each of the concepts, an overview of related literature is provided. In section 2.1, WLAN is introduced. Specifically, client-server and ad-hoc networks are explained. In section 2.2, DoS attacks, especially jamming attacks are presented. In Section 2.3, detection methods of jamming attacks are analyzed. Section 2.4 examines the simulation tools that can be used to simulate networks. In section 2.5, the simulation tool OPNET Modeler which is used in this thesis is introduced. Finally, in section 2.6, ad-hoc routing protocols are presented.

2.1 WLAN – Client-Server & Ad-Hoc Networks

Because WLAN provides users the mobility to move around within a local area without a wire and still connect to the network, it is widely used in many important areas. Banks, governments, corporations, and institutions transmit highly important data through WLANs. The security problems of WLANs become important for the users.

Most WLANs are based on the IEEE 802.11 standard, which transmits data in different channels based on frequencies. Due to the ease of installation and convenience, WLAN is regularly used in daily life. An introduction of WLANs was done by Gast (2005) and Mark (2005). They presented basic wireless LAN technology, why the technology had emerged, how it works, the architecture of WLANs, and the types of WLANs.

Because of the popularity of WLANs, security research must be done in various types of WLANs. Experiments were done by Varadarajan, Kumar, and Reddy (2011) about improving WLAN performance under DoS attacks. DoS attacks on the physical layer were analyzed and expanded to the security of the physical layer of the sensor network model. This research was done by using the ant system. By using Receiver Operating Characteristics (ROC) on nodes, DoS

attacks can be predicted by formulating the classification of jammers under various attack scenarios. This approach can help improving detecting DoS attacks in WLANs.

Research in this thesis was focuses on two types of WLANs: client-server and ad-hoc networks.

The advantages and disadvantages of client-server networks were analyzed in ianswer4u.com (2011). Client-server networks contain servers as a centralized control. Because of this, it is more convenient for the management of networks. Servers can help administrate the network by managing access rights, resource allocation, and the storing of data. Due to this architecture, access rights of nodes can be defined by established rules in the server, which makes the security problem easier to manage. However, this architecture also leads to too many requests for the server, which means an overload is more likely to happen in client-server networks. Overload can lead to the breaking-down of servers. Also, because it requires professionals to install and manage the network, it is more expensive to install and manage than other WLANs.

Ad-hoc networks can be grouped into three types of networks according to the application they carry: (1.) Mobile Ad-hoc Networks (MANET), (2.) Wireless Mesh Networks (WMN), and (3.) Wireless Sensor Networks (WSN). Introductions and examples of each network can be found as follows:

Nodes in MANET are all mobile nodes. They move independently in random trajectories. This network can be used to monitor and analyze data. Because of the cheap price of devices and installing, much research was based on MANET data monitoring. A research of air pollution monitoring in London used MANET technology (Ma et al., 2008). Mobile Sensor Nodes were

installed in cars running in London, and data was collected by Static Sensor Node all around the experiment area. Simulation of air pollution was done by data collected by the nodes.

An introduction of WMNs was done by Roos (2007). WMNs are based on mesh topology. Mesh nodes used in WMNs are small radio transmitters that can be used as routers or gateways. Due to the convenience and cheap price, WMNs are used in public devices such as street lights, which need to connect each other into a network. A physical real world based WMN was presented by Akyildiz, Wang, and Wang (2005). Different application scenarios of WMNs were tested, and implementation practice of WMNs was presented.

Wireless Sensor Networks (WSNs) security protocols were examined and compared, by a research of security of WNSs (Healy, Newe, and Lewis, 2009). It was focusing on their relative strengths and weaknesses. Because of the sensitive nature of WSNs it is becoming critical that if the data is protected. However, because of the processing requirements of traditional wireless networking, the security solutions are not viable. They reviewed the threats and attacks faced by WSNs and then dedicated the current situation of WSN security.

2.2 DoS – Jamming Attacks

Denial of Service attacks is the most common style of attacks. It is an attack attempting to make the network crash by flooding it with useless traffic, which then uses all the resources in the network so the legitimate users cannot connect to the system. It is constantly used by hackers to attack network systems, because it is easy to launch and hard to avoid. DoS attacks can be launched in various protocol layers and DoS attacks in different layers can vary.

Table 1 shows varying kinds of DoS attack in different protocol layers (Chaitanya and Arindam, 2010).

Table 1. DoS Attacks and Defenses to Combat At Different Protocol Layers

Protocol layer	**Attacks**	**Defenses**
Physical	Jamming	Sleep
	Node destruction	Hide nodes or tamper proof packaging
MAC	Denial of sleep	Sleep, authentication and anti-replay
Network	Spoofing, replaying	Authentication, anti-replay
	Hello floods	Geographic routing
	Homing	Header encryption
Transport	SYN flood	SYN cookies
	De synchronization attack	Packet authentication
Application	Path based DoS	Authentication and anti-replay protection
	Reprogramming attacks	

A study into DoS attacks and defense was done by Raymond and Midkiff (2008). Since WSNs are used in monitoring medical uses, homeland security, industrial automation, and military applications, security of WSNs must be guaranteed. Defeating many threats of DoS attacks on WSNs can be done by encryption and authentication, but some other techniques still need to be found to prevent from special DoS attacks, especially Denial of Sleep attacks, which are still critical threats in WSNs.

Out of all the DoS attacks, jamming is one of the most common styles. A jamming attack prevents legitimate users from accessing channel or disrupts communication between a sender

and a receiver. Jamming attacks are a problem that has been a challenge to overcome since World War II, when they were launched against radars. Nowadays, jamming attacks continue to remain a serious problem even for the most refined communication protocols implemented in the most sophisticated devices. Denial of Service attack, especially jamming attacks, is a popular research topic, and lots of research has been done in this area.

In an up-to-date survey (Pelechrinis, Iliofotou, and Krishnamurthy, 2011), jamming attacks can be shown as launching using off-the-shelf equipment. A simple example is when jamming attacks can be generated by transmitting a radio signal in order to block any access to the medium and/or interfere with reception.

In order to lower the possibility of being detected, new ways to generate jamming attacks were developed (Thuente and Acharya, 2005). This intelligent jamming attack was based on controlling the time packets are sent in routing protocols. It used CTS Corruption Jamming, ACK Corruption Jamming, DATA Corruption Jamming, and DIFS Wait Jamming. Simulations had been done using this intelligent jamming attack, and results showed it was more difficult to detect and had a better performance jamming the network.

One jamming experiment was done through a real system (Xu et al. 2005). Different jammers, including a constant jammer, a deceptive jammer, a random jammer, and a reactive jammer were tested in real systems (MAC and BMAC). The experiment utilized two nodes and a jammer in the network, and it also considered the effect distance would have on the nodes. Four different distances are considered: 38.6 inches, 54.0 inches, and 72.0 inches. The result of this experiment showed that when the distance of the nodes is 38.6 inches, the packet delivery ratio was the lowest. All of the jammers reduced packet delivery and sending ratios, but the deceptive jammer was the most effective, blocking all signals in the network.

2.3. Detection of Jamming

WLANs are built upon a shared medium that makes it easy to launch jamming attacks. These attacks can be easily accomplished by sending radio frequency signals that do not follow any MAC protocols. Detection of jamming attacks can be done in multiple ways. One of the most efficient ways is to jump channels. Because communication between two legitimate nodes is done through a specific frequency, the frequency can be changed if necessary.

While a jammer is attacking the wireless network, there are other effective ways to continue legitimate communication in the network. Engaging the jammer on the jammed channel and continuing communication in another channel was introduced by Beg, Ahsan, and Mohsin (2010). When the nodes detected the jamming in the wireless network, they jumped to another channel to continue legitimate communication. In the experiments, both 10 and 20 nodes experiments were done, and in both scenarios, after channels were jumped, the network resumes communications as normal. In both scenarios, the amount of packets dropped reduced immediately.

The research concluded that channel jumping will decrease the throughput of the network. Also, it was easier to detect jamming through intermitted channel jumping. Concluded, channel jumping was a superior method of combating network interference, rather than changing network protocols (Jeung, Jeong, and Lim, 2011).

A study on a channel migration scheme to mitigate wireless jamming attacks was done by four experiments (Hyun, Ning, and Liu, 2011). The first experiment was done without jammers in order to test the performance of network, and the second experiment tested a jamming attack in a single channel. The third experiment tested jamming attacks in multiple channels, while the last experiment of jamming attacks was varied in different channels in multiple regions. An

algorithm of channel migration was applied to the network system, which stated that when jamming attacks were launched in the channel, the communication of nodes should migrate to another channel and continue.

In order to prevent from multi-channel jamming attacks, a cross-layer jamming detection method was developed (Chiang and Hu, 2011). Cross-layer jamming detection is a tree-based approach. A jamming detection algorithm was utilized in all legitimate nodes; when the communication process began, all the nodes had the ability to report jamming attacks in different layers, and only the reports which were generated by nodes with jamming detection algorithm were accepted by the system in order to avoid error. Research was also done about multi-channel jamming attacks by Jiang and Xue (2010). The difference from the jamming detection algorithm was that it focused on network restoration and design of traffic rerouting.

Another way to lower the influence of jamming attacks is to set thresholds and priority to the network system (Fu et al. 2011). OPNET Modeler was selected as the simulation tool in the research. In the experiment, three legitimate nodes communicated in the network, while three jammers launched DoS attacks. A monitor node was set to watch the thresholds in the network. Legitimate nodes were set to a priority number, while the jammers' priority number was zero. When data transmitting in the network exceeded the threshold, packets sent by lower threshold were discarded first. In this case, useless messages in the network were dropped first when network is busy, and legitimate communication was continued. Through this method, data dropped by the nodes was largely decreased, and the transmission quality of the network was increased.

2.4. Simulation Tools

Network simulators attempt to portray an abstract model of a system in order to monitor the network. Simulation tools are programs available for users to build, configure, or monitor abstract systems.

For network simulation, many tools are available for use, such as: NS-2, TOSSIM, EmStar, OMNeT++, J-Sim, ATEMU, Avrora, and OPNET Modeler. The performance of some of the tools can be seen in Table 2 (Yu, 2011).

Table 2. A Comparison of Simulation Tools

Simulation Environment	**Version**	**License**	**Programming Language**
GIoMoSim/ QualNet	2.0 (Dec 2000)/ 5.0 (Nov 2009)	Free for academic research/ commercial	C and Parsec
OPNET Modeler Wireless Suite	16.0 (Dec 2009)	Commercial	Configuration by GUI internals C++
TOSSIM (part of TinyOS)	2.1.1 (Apr 2010)	BSD	nesC
OMNeT++	4.0 (March 2009)	Academic Public License	Basic modules C++; larger structures NED
NS-2	2.34 (Jun 2009)	GPL	C++; configuration OTcl
Avrora	Beta 1.7.106 (Aug 2008)	BSD	AVR micro-controller binaries
J-Sim	1.3 + patch4 (Jul 2006)	BSD-like	Java; configuration Tcl/Java
ATEMU	0.4 (2004)	BSD	AVR micro-controller binaries
EmStar	2.5 (Oct 2005)	Unknown	C
SENS	Jan31-2005b (Jan 2005)	Unknown	C++
SENSE	3.1 (Nov 2008)	BSD-like	C++
Shawn	Continuous SVN development (May 2010)	BSD	C++

An example of WLAN simulation with NS-2 can be found in the research done by Adaobi and Ghassemian (2010). The experiments were simulated by using the NS2 simulator. In all three of the experiments, when the DoS attacks were launched by the attackers, the packets dropped were significantly higher than the other scenario described. The performance of the Intrusion Detection System (IDS) used in the wireless sensor network is satisfactory, because the true positive was high and the False Positive Rate was low.

A different jammer analyzing experiment was done by using Matlab (Reddy, Varadarajan, and Kumar, 2011). Various jammers, including a single-tone jammer, a multiple jammer, a pulsed jammer, and an ELINT jammer were analyzed. 16 nodes were simulated using Matlab 6.5. Changing numbers of nodes were attacked by the jammer in the experiments. Experiment results displayed packet loss and average packet delivery of the network when 3, 6, 9, and 12 nodes were under attack, respectively. The more nodes that were under attack, the more packets that are lost in the network. The most significant effected was when 12 nodes were attacked by the ELINT jammer. In this scenario, the packet loss was 92%, the average packet delivery was only 0.0071.

Different simulation tools and their functions and performances were compared by Yu (2011). This research contained the comparison of general simulator or specific simulator, and if the tool included graphical user interface (GUI), and their function details.

Table 3 shows the comparison of the simulation tool functions, including the comparison of if the simulation tool is Discrete-Event simulations or Trace-Driven simulation; if the simulation tool includes GUI, if the simulation tool is an open source tool.

Table 3. Comparison of Seven Main-Stream Simulation Tools

Simulation Tool	**Discrete-Event Simulations or Trace-Driven Simulation**	**GUI**	**Open source and Online documents**	**General simulator or Specific Simulator**
NS-2	Discrete-Event Simulation	No	Yes	General simulator
TOSSIM	Discrete-Event Simulation	Yes	Yes	Specifically designed for WSNs
EmStar	Trace-Driven Simulation	Yes	Yes	Specifically designed for WSNs
OMNeT++	Discrete-Event Simulation	Yes	Noncommercial or commercial license	General simulator
J-Sim	Discrete-Event Simulation	Yes	Yes	General simulator
ATEMU	Discrete-Event Simulation	Yes	Yes	Specifically designed for WSNs
Avrora	Discrete-Event Simulation	No	Yes	Specifically designed for WSNs

2.5 OPNET Modeler

In this research, OPNET Modeler was used as the simulation tool. OPNET Modeler contains the fastest simulation engine, and it has many models of wireless protocol and devices in the OPNET Modeler model library. By using OPNET Modeler, the parameters of wireless models can be customized. This function largely expanded abilities of experiments. Furthermore, OPNET Modeler is also a powerful analyzer. It runs on a C compiler and has GUI-based

debugging and analyzing. By using the debugging function in OPNET Modeler, experiments can be visualized; network simulation results can be monitored in an integrated environment.

Because OPNET Modeler is one of the best simulation tools, many experiments and analysis were done by using it. Chaitanya and Arindam (2011) analyzed Denial of Service attacks in wireless sensor networks by using OPNET Modeler. They used a tree topology as their model in the experiment, created an environment that included a router, a coordinator and end nodes. Attacks launched into the router and coordinator. The result of this research showed that the number of packets dropped during DoS attack is close to 1,200, as compared to less than 100 when there was no attack on the router. When a DoS attack occurred on the coordinator, the load during an attack was higher (27500 bits/sec), as compared to the load during an attack on router i.e. (9100 bits/sec).

A group of experiments of WLANs simulation were done by Malhotra, Gupta, and Bansal (2011). Different wired and wireless network performances were analyzed by using OPNET Modeler. For wired networks, different transmission links, such as 10 Base T, 100 Base T and 1000 Base X Ethernet links were tested; the performance of networks with and without load balancing policy were compared. For wireless network, Fragmentation Threshold, Data rate and buffer size were tested in OPNET Modeler simulator.

OPNET Modeler was used to simulate WLAN environments and all the jammers as well as jamming attacks. One of the examples of a jamming attack scenario was tested by using OPNET Modeler (JESÚS, 2007). In the example, Scenario 1 was a client-server experiment; when the jammer was introduced to the network, the packets were dropped. The number of packets that dropped was based on the distance between the jammer and the nodes, as well as the power of the jammer. Scenario 2 had 19 nodes and one server. After the jammer was engaged in

the network, the network was influenced by the jammer. Also, when the jammer was switched from a consistent jammer to a random jammer, the influence of the jammer on the network can still be seen. The throughput of the network dropped due to the introduction of the jammer. The same situation can be seen in Scenario 4, which established as ad-hoc network. After the jammer is introduced in the network, the throughput of the nodes dropped immediately. In Scenario 5, there was not a jammer, but one of the nodes was noticed as malfunctioning. After the node acted malfunctioned, the throughput of the network started to act inconsistently, which established that one malfunctioning node can influence the network as if it was a jammer.

2.6 Routing Protocols

Different routing protocols were compared in experiments using OPNET Modeler by Ali and Sarwar (2011). DSR, AODV, and TORA were compared by looking at the throughput, delay, load, FTP Traffic sent, FTP traffic received, and download response time by simulating the same wireless network that was used in OPNET Modeler experiment. Also, the maps of network traffic were analyzed. When there was an intruder in the network, the traffic automatically routed to another node to avoid sending packets to the intruder node. Lastly, networks with and without firewall were simulated. The firewalls which used network had a lower response time value and higher security.

Ad-hoc protocols DSR, AODV, TORA, FSR, ZPR, and WRP were compared and discussed in MANET (Soujanya, Sitamahalakshmi, and Divakar, 2011). Each routing protocol had advantages and disadvantages. For example, because DSR routing protocol saved all the information in the IP head, there was no need to keep the routing table in the routing process. However, it was not efficient for larger networks because of a large amount of IP head information. AODV was an efficient routing protocol that supports constant movements of nodes

and had quick responses to topology changes. But it required that the nodes in the broadcast medium can detect each other in order to make transmissions.

CHAPTER 3 EXPERIMENTAL METHODOLOGY

In Chapter 3, experiment designs are stated. It starts with explanations of applications used in the networks, and characteristics of common nodes. Later in this Chapter, each Scenario and experiment will be demonstrated.

3.1 Application Definition/Model Specification

In every Scenario, a low-load video application was used in order to generate traffic in the networks. Experiments in this thesis contained two types of networks. One was a client-server network, and the other was an ad-hoc network. The first three Scenarios used the client-server network, and the fourth and fifth Scenarios used the ad-hoc network. All node models were based on "wireless_LAN_adv", "ethernet" and "jammer" shared object palettes. All the following tables and figures were screenshots from experiments within OPNET Modeler.

3.1.1 Application Definition and Profile Definition Characteristics.

Defining Application and Profile Characteristics in OPNET Modeler was done by using the Application Configuration and Profile Configuration in OPNET Modeler. Application Configuration allows users to define the application running in the network. The application can be things such as e-mail, database, ftp, http or print. Users can also customize the application required in the network. In order to allow all users to be able to use the defined application, a profile must be created by using Profile Configuration.

All the experiments and Scenarios used a low-load video application, which was defined as "128×120 pixels, 9 bits per pixel, and 10 frames per second" in OPNET Modeler. The Application Definition and Profile Definition Characteristics are shown in Table 4:

Table 4. Application Definition and Profile Definition Characteristics

Application Definition Characteristics

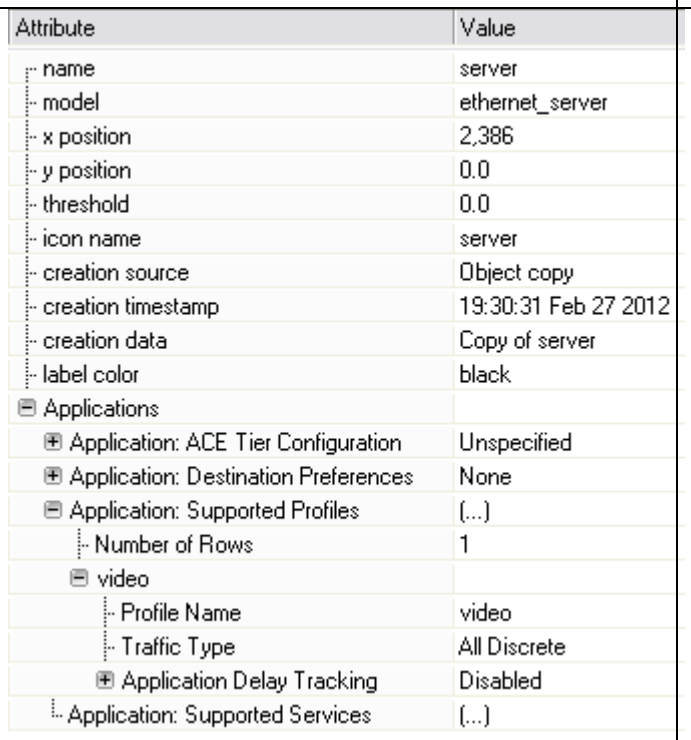
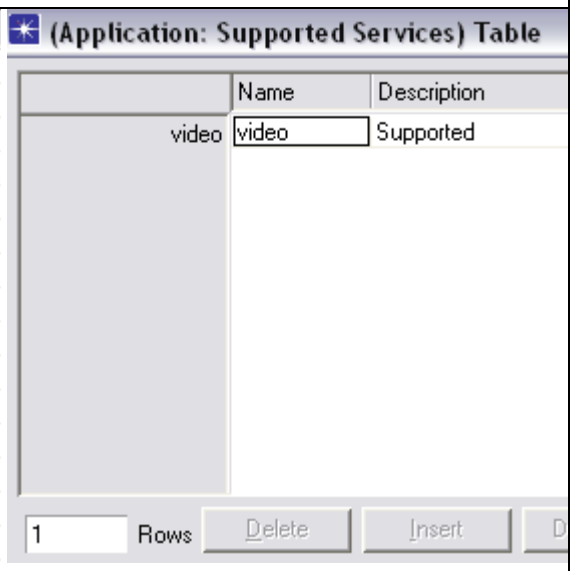
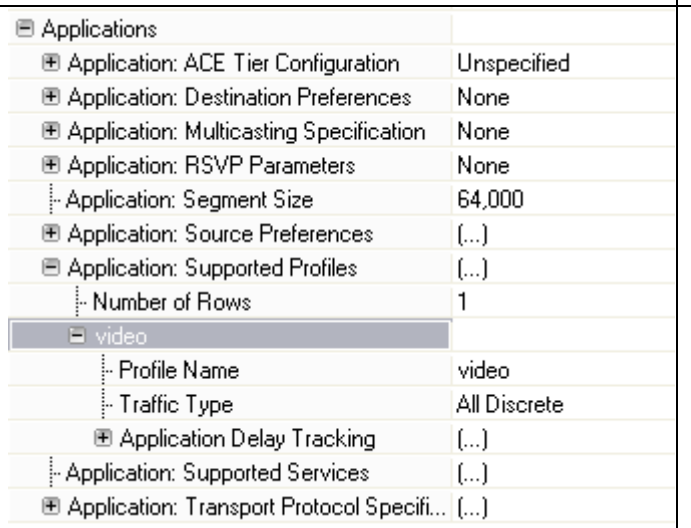
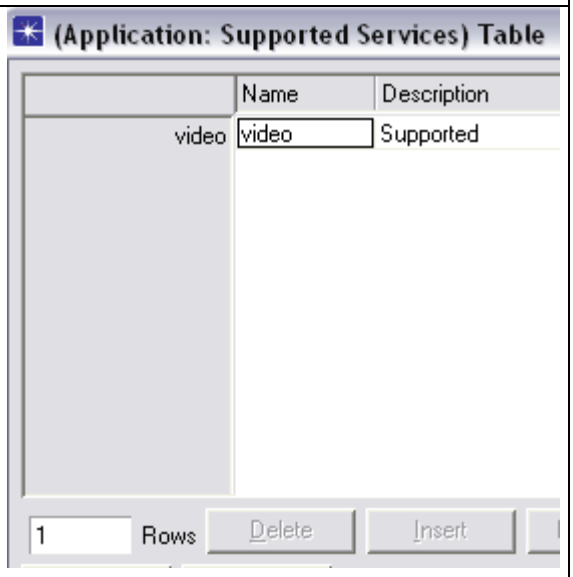
Attribute	Value
name	appConfig
model	Application Config
x position	-2,101
y position	1,125
threshold	0.0
icon name	util_app
creation source	Object copy
creation timestamp	19:31:02 Feb 27 2012
creation data	Copy of appConfig
label color	black
Application Definitions	(...)
Number of Rows	1
video	
Name	video
Description	(...)
Custom	Off
Database	Off
Email	Off
Ftp	Off
Http	Off
Print	Off
Remote Login	Off
Video Conferencing	Low Resolution Video
Voice	Off
MOS	
Voice Encoder Schemes	All Schemes
hostname	
minimized icon	circle/#708090
role	

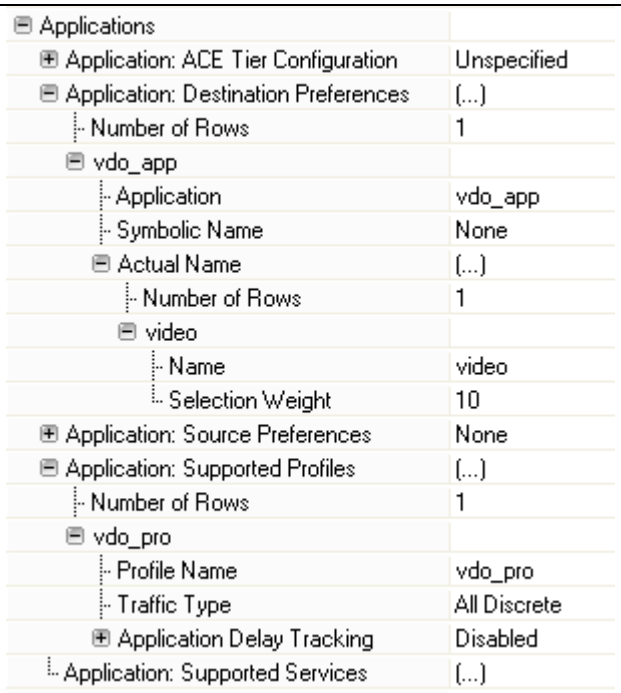
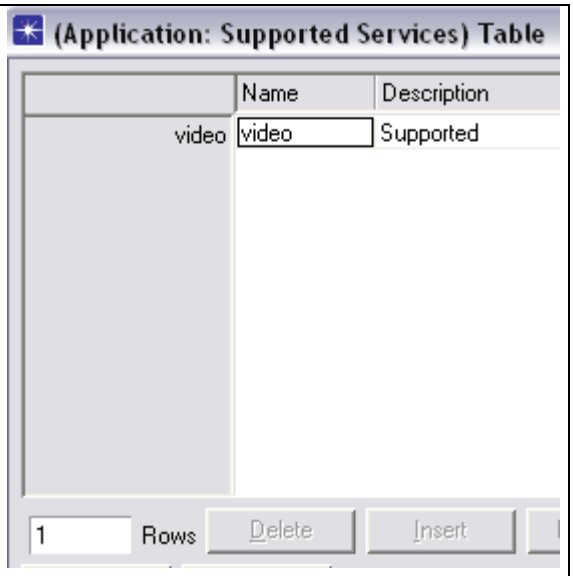
Profile Definition Characteristics

Attribute	Value
name	pro_config
model	Profile Config
x position	-2,115
y position	509
threshold	0.0
icon name	util_profiledef
creation source	Object copy
creation timestamp	19:31:02 Feb 27 201
creation data	Copy of pro_config
label color	black
Profile Configuration	(...)
Number of Rows	1
video	
Profile Name	video
Applications	(...)
Number of Rows	1
video	
Name	video
Start Time Offset (seconds)	No Offset
Duration (seconds)	End of Profile
Repeatability	(...)
Inter-repetition Time (secon...	exponential (300)
Number of Repetitions	Unlimited
Repetition Pattern	Serial
Operation Mode	Serial (Ordered)
Start Time (seconds)	constant (0)
Duration (seconds)	End of Simulation
Repeatability	Once at Start Time

After the application of the network was defined, nodes which application can be configured must be defined to support the video application and profile. Table 5 shows the application definition in server, the fixed work station, and the mobile work station.

Table 5. Characteristics and Application Definition of the Nodes

	Application configuration	Application: supported services
Server		
Fixed work station		

Mobile work station		

All the nodes were set to support the application used in the network. The server generated low-load video as defined in the system. Data transmitted in the network represented packets of a video conference.

3.1.2 Nodes Characteristics

The server node in the Scenario was based on the model "ethernet _server" under the "ethernet" shared object palette. The characteristics of the server are shown in Figure 1:

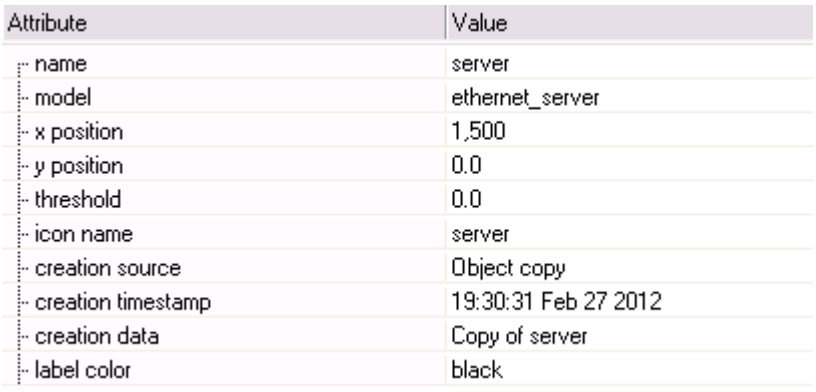
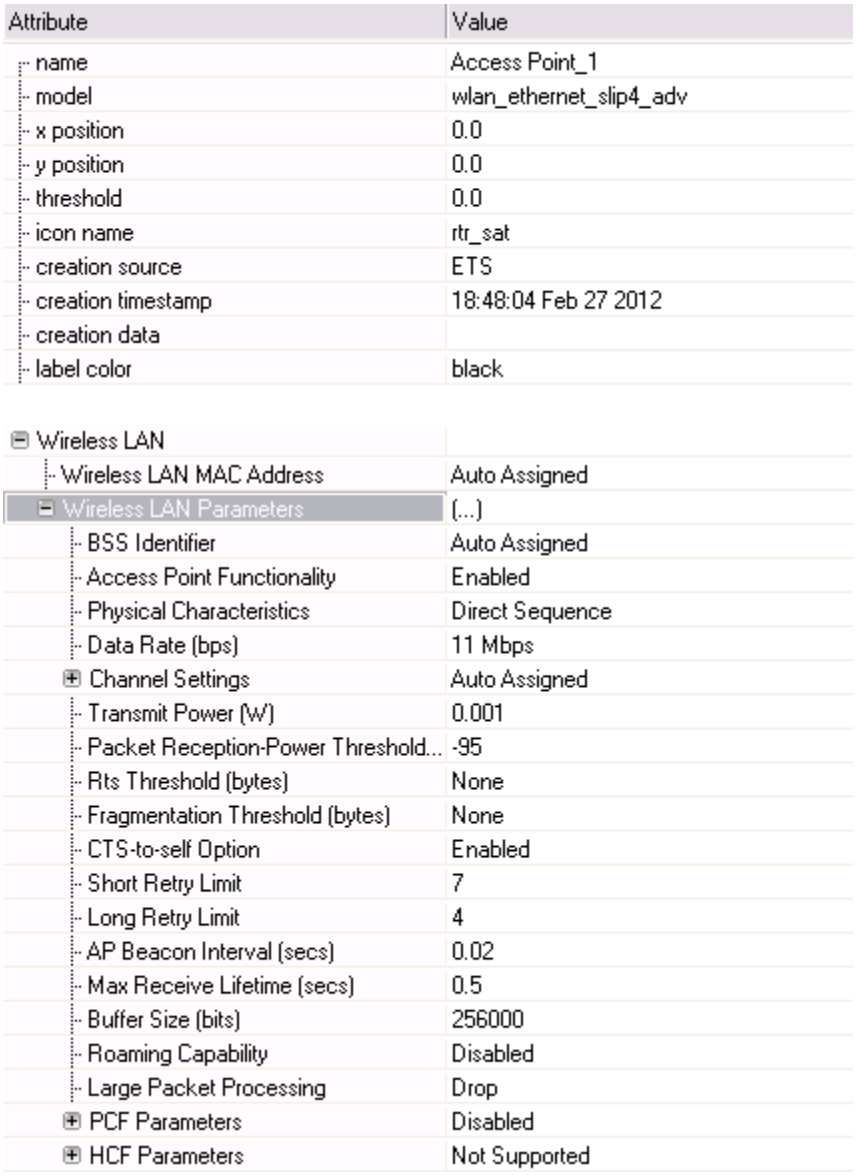


Figure 1. Characteristics of the Server

The switch, which was represented by model "ethernet32_switch," was a bridge that connects the server and access point. 1000BaseT acted as the connecting link between the switch and the server, as well as the switch and access point. The access point was defined using the wlan_ethernet_split4_adv model. The characteristics of the switch and the access point are shown in Figures 2 and 3.

Attribute	Value
name	switch
model	ethernet32_switch
x position	1,000
y position	0.0
threshold	0.0
icon name	switch
creation source	Object copy
creation timestamp	19:30:31 Feb 27 2012
creation data	Copy of switch
label color	black
⊟ Bridge Parameters	(...)
Priority	32768
Spanning Tree Protocol	RSTP (802.1w)
⊞ QoS Parameters	None
⊞ Timers	Default
BPDU Service Rate (packets/sec)	100000
Packet Service Rate (packets/sec)	500000
⊞ Switch Port Configuration (32 Rows)	(...)
⊞ Switch Port Group Configuration	None
⊞ VLAN Parameters	(...)
altitude modeling	relative to subnet-platform
condition	enabled
financial cost	0.00
hostname	
minimized icon	circle/#708090

Figure 2. Characteristics of Switch



Attribute	Value
name	Access Point_1
model	wlan_ethernet_slip4_adv
x position	0.0
y position	0.0
threshold	0.0
icon name	rtr_sat
creation source	ETS
creation timestamp	18:48:04 Feb 27 2012
creation data	
label color	black
Wireless LAN	
Wireless LAN MAC Address	Auto Assigned
Wireless LAN Parameters	(...)
BSS Identifier	Auto Assigned
Access Point Functionality	Enabled
Physical Characteristics	Direct Sequence
Data Rate (bps)	11 Mbps
Channel Settings	Auto Assigned
Transmit Power (W)	0.001
Packet Reception-Power Threshold...	-95
Rts Threshold (bytes)	None
Fragmentation Threshold (bytes)	None
CTS-to-self Option	Enabled
Short Retry Limit	7
Long Retry Limit	4
AP Beacon Interval (secs)	0.02
Max Receive Lifetime (secs)	0.5
Buffer Size (bits)	256000
Roaming Capability	Disabled
Large Packet Processing	Drop
PCF Parameters	Disabled
HCF Parameters	Not Supported

Figure 3. Characteristics of Access Point

The fixed node used wlan_wkstn_adv (fixed) model. The wlan_wkstn_adv (mobile) model was used as the mobile node in the Scenario. The 'wlan_wkstn_adv' model both used in node_1 and mobile_node_1 required application configuration and profile configuration for generating traffic in the network.

The characteristics of the fixed work station node and the mobile work station node are listed below:

Table 6. Characteristics of Work Stations

Fixed node (node_0)

Attribute	Value
name	node_0
model	wlan_wkstn_adv
x position	-4.0
y position	277
threshold	0.0
icon name	wkstn_wless_wlan
creation source	Object Palette
creation timestamp	19:33:37 Feb 27 2012
creation data	
label color	black
Wireless LAN	
Wireless LAN MAC Address	Auto Assigned
Wireless LAN Parameters	(...)
BSS Identifier	Auto Assigned
Access Point Functionality	Disabled
Physical Characteristics	Direct Sequence
Data Rate (bps)	11 Mbps
Channel Settings	Auto Assigned
Transmit Power (W)	0.005
Packet Reception-Power Threshold...	-95
Rts Threshold (bytes)	None
Fragmentation Threshold (bytes)	None
CTS-to-self Option	Enabled
Short Retry Limit	7
Long Retry Limit	4
AP Beacon Interval (secs)	0.02
Max Receive Lifetime (secs)	0.5
Buffer Size (bits)	256000
Roaming Capability	Disabled
Large Packet Processing	Drop
PCF Parameters	Disabled
HCF Parameters	Not Supported
altitude	0.0
altitude modeling	relative to subnet-platform
condition	enabled
financial cost	0.00
hostname	
minimized icon	circle/#708090
role	

Mobile node (mobile_node_0)

name	mobile_node_0
model	wlan_wkstn_adv
x position	-923
y position	69
trajectory	lte_east
color	white
bearing	0.0
ground speed	
ascent rate	
threshold	0.0
icon name	wkstn_wless_wlan
creation source	Object Palette
creation timestamp	19:33:40 Feb 27 2012
TCP	
Wireless LAN	
Wireless LAN MAC Address	Auto Assigned
Wireless LAN Parameters	(...)
BSS Identifier	Auto Assigned
Access Point Functionality	Disabled
Physical Characteristics	Direct Sequence
Data Rate (bps)	11 Mbps
Channel Settings	Auto Assigned
Transmit Power (W)	0.005
Packet Reception-Power Threshold...	-95
Rts Threshold (bytes)	None
Fragmentation Threshold (bytes)	None
CTS-to-self Option	Enabled
Short Retry Limit	7
Long Retry Limit	4
AP Beacon Interval (secs)	0.02
Max Receive Lifetime (secs)	0.5

The signal range of the access point in this experiment was 500×500 meters. The mobile node had a west-to-east trajectory through the work space.

3.2 Client-Server Network Scenarios

A typical client-server network includes a server, a switch, an access point, and nodes. The server can be any type, such as Ethernet server, ftp server, or an E-mail server. Nodes receive service based upon the type of server that supports the network. For example, an Ethernet server will provide Ethernet service to all the nodes in the network, while an ftp server provides ftp service to the nodes.

A switch is a device that exchanges information in network systems. The switch in a client-server network is used to transmit information from the server to the nodes in an appropriate route to meet transmission requirements. In client-server scenarios, the switch was used to transmit data from the server to the access point.

Access points in client-server networks give service to nodes. IEEE 802.11g states that the access point coverage is 75 meters. Since the default setting of access point transition power is larger than 802.11 standards, the signal range of access point in this experiment can cover the area of 500×500 meters. Multiple access points can be used in one client-server network by using different BSS numbers. Nodes can utilize different access points to get service by connecting to the correct BSS numbers.

End nodes in client-server networks can be various network devices, such as mobile phones, computers, or laptops. In this thesis, wireless work stations (fixed nodes and mobile nodes) were used as end devices. “client_server” models and “wireless_lan” models in OPNET Modeler were used to build the client-server network used in Scenario CS-1 to CS-3. All the

experiments in client-server network Scenarios used the low-load video application, which was defined by using Application Configuration and Profile Configuration.

3.2.1 Scenario CS-1

The objective of this Scenario was to compare throughput in different situations, varying access point power levels, and varying distances between the access point and nodes. Scenario CS-1 simulated a simple client-server network, which included one server, one switch, one access point, one fixed node (node_0) and a mobile node (mobile_node_0). The methodology of Scenario CS-1 is shown in Figure 4:

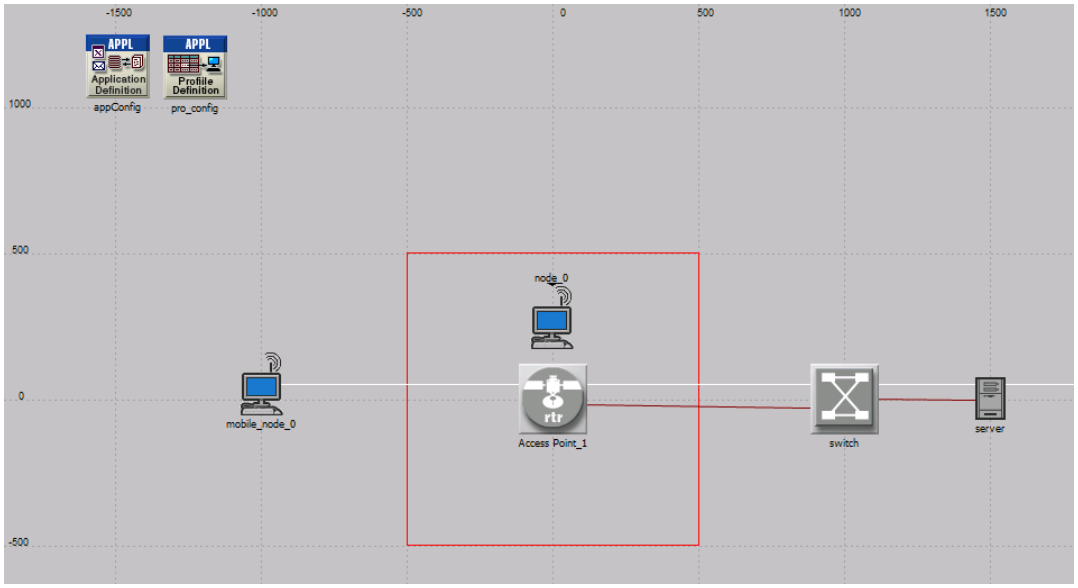


Figure 4. Scenario CS-1 Methodology

The mobile node followed a straight line running through the middle of the work space from the west to the east. The trajectory of the mobile node is shown in Figure 5:

Trajectory name: lte_east

	X Pos (km)	Y Pos (km)	Distance (km)	Altitude (m)	Traverse Time	Ground Speed	Wait Time	Accum Time	Pitch (degrees)
1	0.000000	0.000000	n/a	0.000000	n/a	n/a	00.00s	00.00s	Autocomputed
2	3.500000	0.000000	3.500000	0.000000	3m00.00s	43.495983	00.00s	3m00.00s	Autocomputed

Figure 5. Trajectory of Mobile Node in Scenario CS-1

3.2.2 Scenario CS-2

This Scenario included three experiments. The objective for the first experiment was to compare jamming results for the fixed node. The second experiment compared jammer results for the mobile node while movement occurred. For the third experiment, comparisons were made between differentiating jammer power levels. The methodology of the Scenario CS-2 is shown in Figure 6.

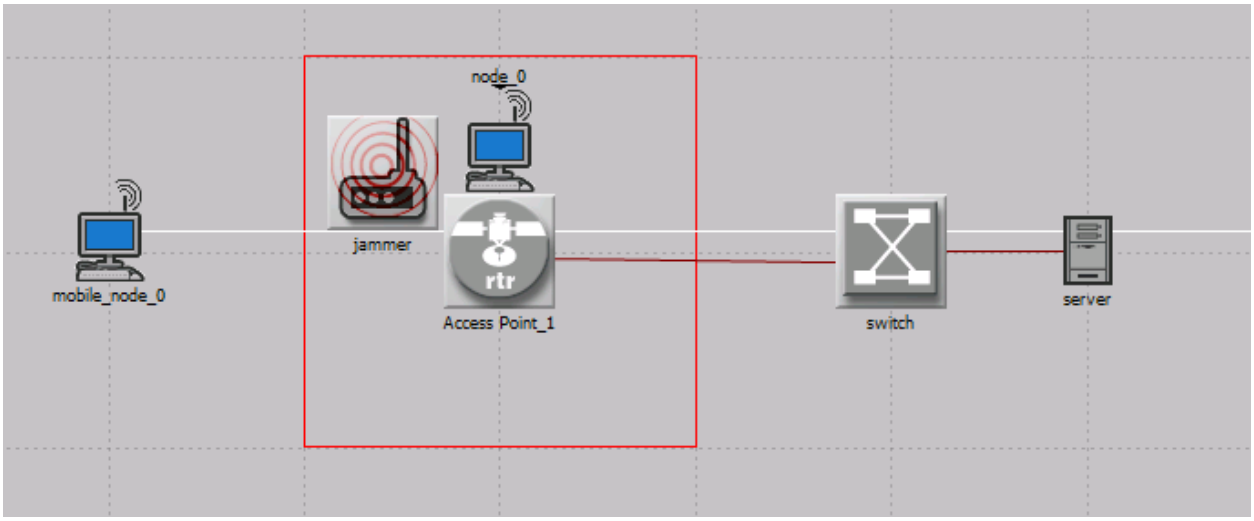


Figure 6. Methodology of Scenario CS-2

In this Scenario, a fixed pulse jammer was added to the network used in the Scenario CS-1. All the models of the nodes were the same as those used in Scenario CS-1. The jammer was represented by the model ‘jam_pulsed’ in OPNET Modeler. The jammer was composed of a source and a radio transmitter. Figure 7 shows the components of the pulse jammer used in this Scenario.

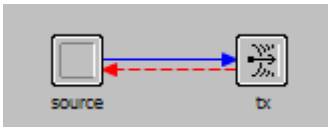


Figure 7. The Components of Pulse Jammer

The source of the jammer was a pulsed_source signal generator. The process of the source model is showed in Figure 8:

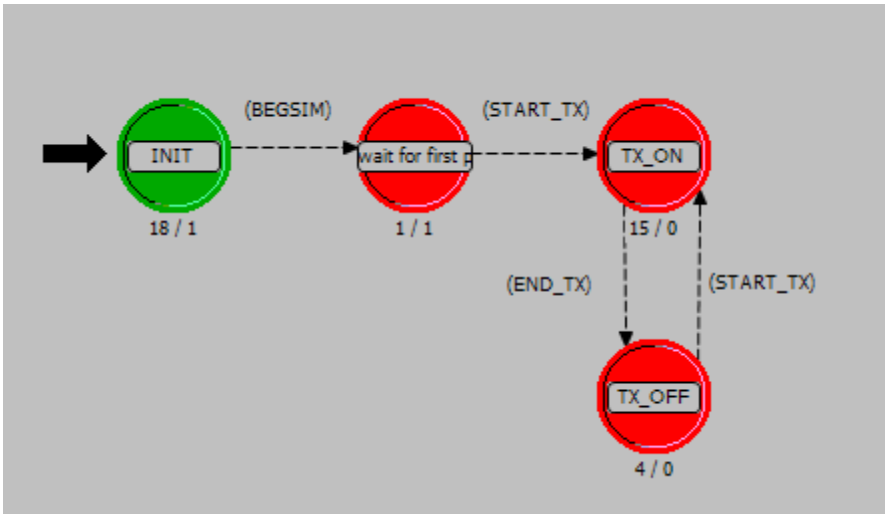


Figure 8. Process Model of Pulsed Source Generator

The signal generated in the source was controlled by three different states. The first, ‘wait for the first pulse,’ state controlled if packets were allowed to be sent. The TX_ON state controlled the start of packets sent from the source to the radio transmitter. The TX_OFF state was responsible for generating and scheduling pulses. The signal must go through the first state to be confirmed if the packets should be sent or pulsed. The code of this pulse source generator is listed in APPENDIX.

The characteristics of the pulse jammer are shown in Figure 9:

Attribute	Value
name	jammer
model	jam_pulsed
x position	-300
y position	150
threshold	0.0
icon name	wless_jammer
creation source	Object Palette
creation timestamp	23:58:48 Mar 13 2012
creation data	
label color	black
Altitude	0.0
Jammer Band Base Frequency	2,402
Jammer Bandwidth	22,000
Jammer Transmitter Power	0.001
Pulse Width	1.0
altitude modeling	relative to subnet-platform
condition	enabled
financial cost	0.00
hostname	
minimized icon	circle/#708090
role	

Figure 9. Characteristics of Pulse Jammer

All the jammers had similar transmitters. The characteristics of the transmitters are shown in Figure 10.

Attribute	Value
name	tx
channel	(...)
Number of Rows	1
Row 0	
data rate (bps)	1,000,000
packet formats	unformatted
bandwidth (kHz)	promoted
min frequency (MHz)	promoted
spreading code	disabled
power (W)	promoted
bit capacity (bits)	infinity
pk capacity (pks)	1,000
modulation	jammod
rxgroup model	dra_rxgroup
txdel model	dra_txdel
closure model	dra_closure
chanmatch model	dra_chanmatch
tagain model	dra_tagain
propdel model	dra_propdel
icon name	ra_tx
channel [0].bandwidth	promoted
channel [0].min frequency	promoted
channel [0].power	promoted

Figure 10. Characteristics of Jammer Transmitter

According to the IEEE 802.11 standard, all wireless network nodes transmit data packets in different channels. The differences between each channel are defined by transmission frequencies. Figure 11 shows all the channels and their corresponding frequencies that exist in WLAN (Wikipedia, 2007).

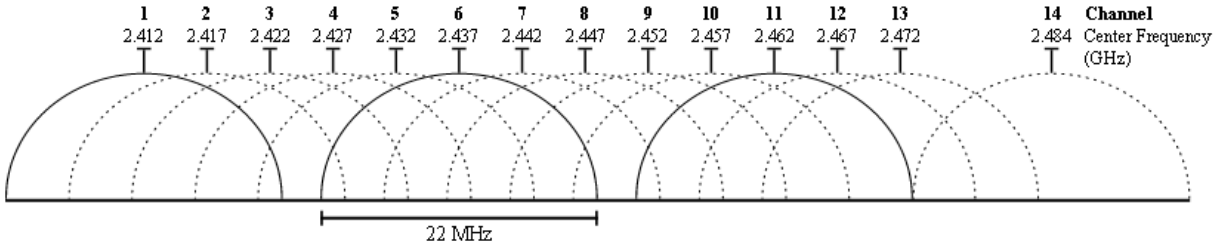


Figure 11. WLAN Channels And Frequencies

The first channel starts from the frequency of 2401 MHz. Intervals between each channel occur at every 5 MHz. Because of this, there are only 3 channels that are completely independent of one another. These are channels 1, 6 and 11. In this Scenario, the BSS numbers of all nodes were auto-assigned by OPNET Modeler at channel 1. Jammer characteristics automatically established band base frequency at 2401 MHz, in order to influence communication in channel 1. According to the theory of channels in WLAN, the bandwidth of each channel is 22 MHz, which is 22,000 KHz.

3.2.3 Scenario CS-3

The objective of this Scenario was to compare the influence of the jammer on the nodes at different times. Because the jammer was moving in an octagonal path, the influence on the nodes should be different from time to time, depending on the distance between the node and the jammer. The jamming results were compared depending on the location of the jammer in relation to the nodes. The methodology of this Scenario is shown in Figure 12:

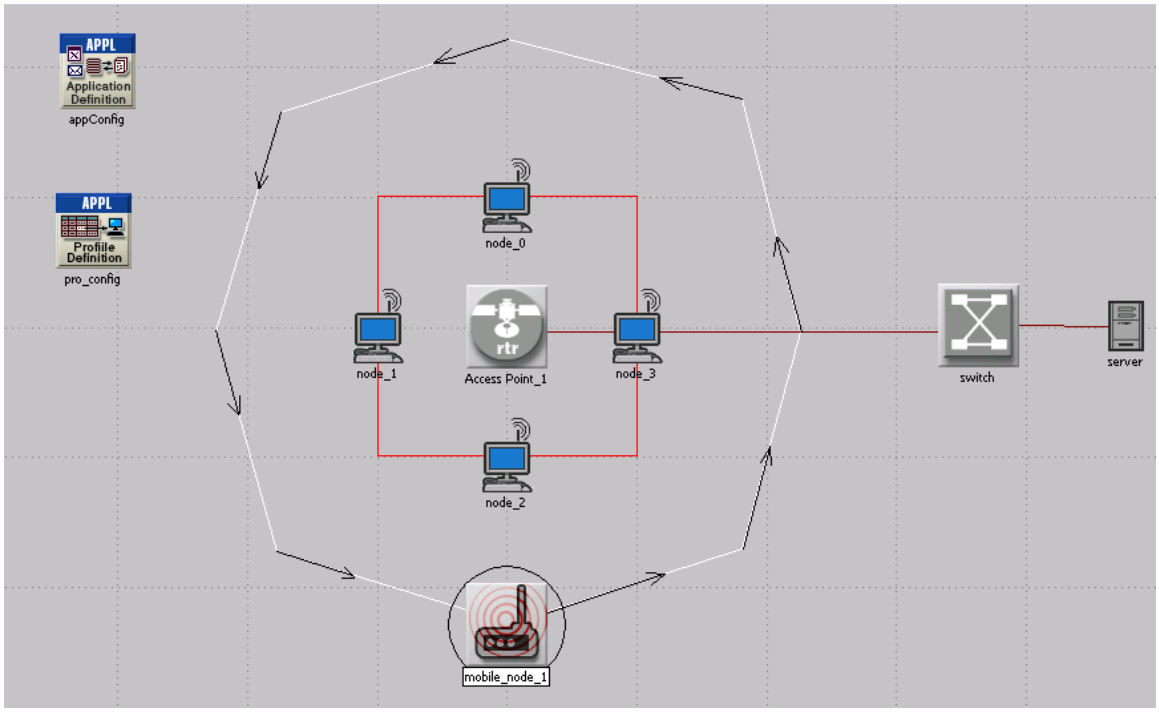


Figure 12. Methodology of Scenario CS-3

In this Scenario, the model of the server, switch, and access point were the same as in previous Scenarios. All four work stations were fixed nodes, and utilized the same model as the fixed work station nodes as in Scenario CS-1 and CS-2. It also used a low-load video application. Four fixed work stations were used in the experiment. The distance between each node and the access point was 500 meters. A mobile pulse jammer was used in this Scenario. This jammer had a trajectory that moved in the work space of OPNET Modeler. The trajectory of the pulse jammer is shown in Figure 12 as the black arrows.

The characteristics of the mobile pulse jammer are shown in Figure 13:

Attribute	Value
name	mobile_node_1
model	jam_pulsed
x position	0.0
y position	-1,147
trajectory	xclock_circle_south
color	white
bearing	0.0
ground speed	
ascent rate	
threshold	0.0
icon name	wless_jammer
creation source	Object copy
creation timestamp	16:43:23 Feb 28 2012
creation data	Copy of mobile_node_1
pitch	0.0
yaw	0.0
roll	0.0
label color	black
Altitude	0.0
Jammer Band Base Frequency	2,401
Jammer Bandwidth	22,000
Jammer Transmitter Power	0.001
Pulse Width	1.0
altitude modeling	relative to subnet-platform
condition	enabled
financial cost	0.00
hostname	
minimized icon	circle/#708090
role	

Figure 13. Characteristics of Mobile Pulse Jammer

The pulsed jammer was set to 2,401 MHz frequency, and the jammer bandwidth was 22,000 KHz. The power of the jammer was set to 0.001 W. This jammer was set to have an octagonal path around the access point and four work stations. The path of the mobile jammer is shown as Figure 14:

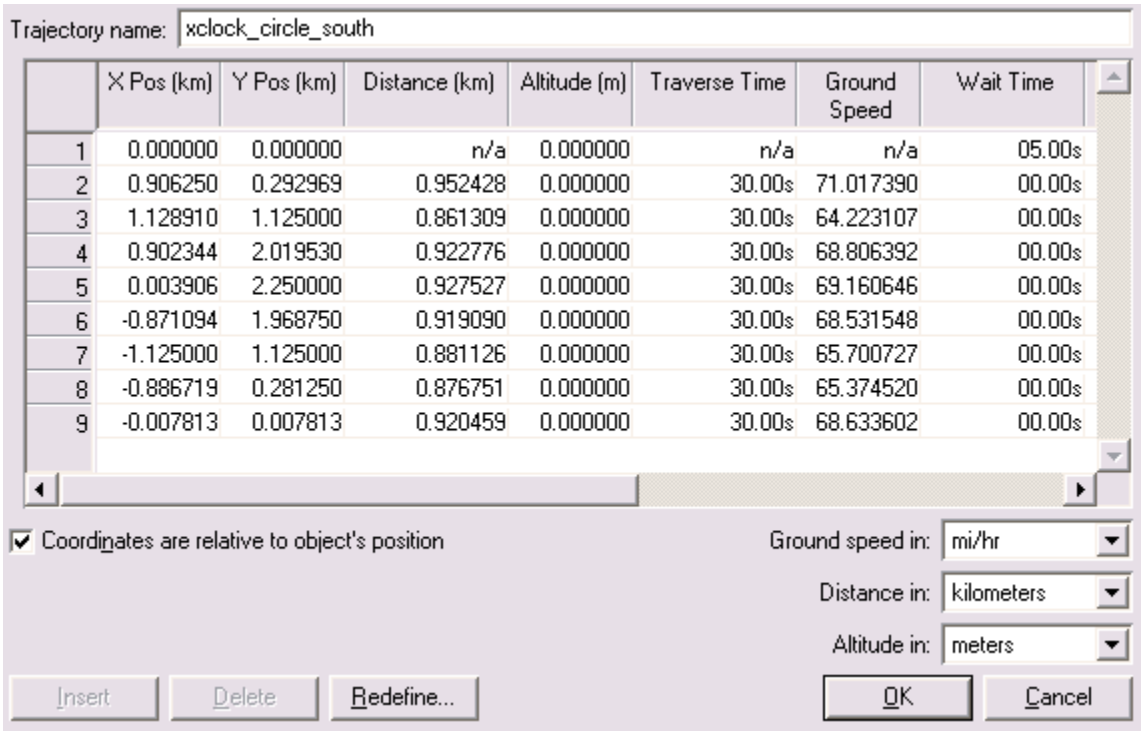


Figure 14. Trajectory of Mobile Pulse Jammer

Each side of the octagon required the mobile jammer 30 seconds to complete. The total time to travel the octagon was 4 minutes. The red square around the access point was located 500 meters away from the access point. Each of the work stations was located in the middle of the access point signal range. The black arrow represents the movements of the mobile jammer.

3.3 Ad-hoc network Scenarios

Scenarios based on ad-hoc networks were very different from the ones based on client-server network fashion. Server, switch, access point, and physical links which were utilized in client-server networks were no longer used. Because of the flexibility of its decentralized nature, ad-hoc networks are used in a large number of various areas.

The application was defined only on work station devices using the same low-load video application as described in Table 5.

3.3.1 Scenario AH-1

The objective of this Scenario was to compare the differences between different types of jammers. The methodology of this Scenario is shown in Figure 15:

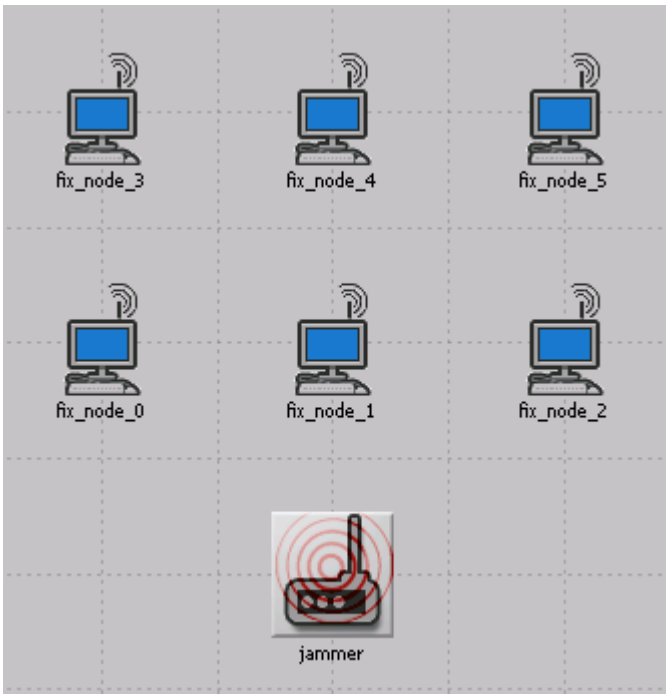


Figure 15. Methodology of Scenario AH-1

In this Scenario, six work station nodes were simulated. All of them were created by using the ‘wlan_skstn_adv (fixed node)’ model in OPNET Modeler. The application and profile definition are described in Scenario CS-1.

The distance between each work station was 10 meters. Instead of only using the pulse jammer as in the previous scenarios, a sweep jammer and a single band jammer were utilized in separate experiments. All jammers were fixed nodes.

The pulse jammer was introduced in Chapter 4.1, and the characteristics of the pulse jammer can be found in Figure 16.

Attribute	Value
name	single_band_jammer
model	jam_sb
x position	45.49
y position	30.1
threshold	0.0
icon name	wless_jammer
creation source	Object copy
creation timestamp	02:35:47 Mar 14 2012
creation data	Copy of single_band_jammer
label color	black
Altitude	0.0
Jammer Band Base Frequency	2,401
Jammer Bandwidth	22,000
Jammer Packet Interarrival Time	constant (1.0)
Jammer Packet Size	constant (1024)
Jammer Start Time	10.0
Jammer Stop TIme	Infinity
Jammer Transmitter Power	0.001
altitude modeling	relative to subnet-platform
condition	enabled
financial cost	0.00
hostname	
minimized icon	circle/#708090
role	

Figure 16. Characteristics of Single Band Jammer

The components of single band jammer included a source and a radio transmitter, which are shown in Figure 17.

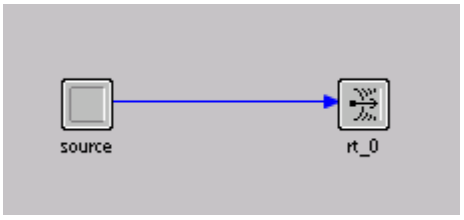


Figure 17. Components of Single Band Jammer

The single band jammer generated signal in a different way than pulse jammers. Single band jammers generate customized packets by using a process shown in Figure 18:

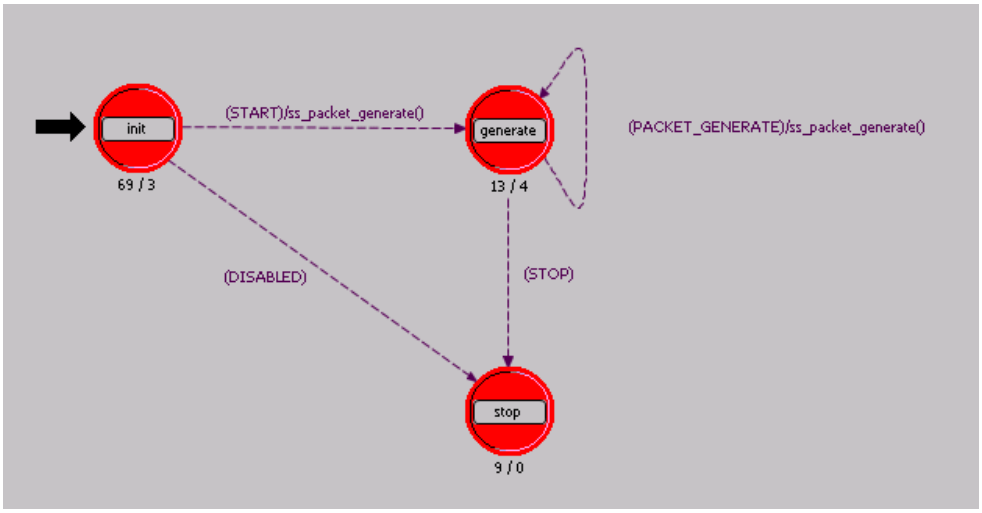


Figure 18. Process Model of Single Band Jammer

The state generated packets which were then customized by the users. The packets used in experiments are shown in Figure 16, the packet size was constantly 1024 bits, and the jammer started to work 10 minutes after the simulation started. The code of single band jammer source generator can be found in APPENDIX.

Another jammer used in the experiment was the sweep jammer. Figure 19 shows the characteristics of the sweep jammer.

Attribute	Value
name	swept_jammer
model	jam_swept
x position	20
y position	30
threshold	0.0
icon name	wless_jammer
creation source	Object copy
creation timestamp	02:35:47 Mar 14 2012
creation data	Copy of swept_jammer
label color	black
Altitude	0.0
Cycle Time	60
Jammer Band Base Frequency	2,401
Jammer Bandwidth	22,000
Jammer Transmitter Power	0.001
Number of Frequencies	60
altitude modeling	relative to subnet-platform
condition	enabled
financial cost	0.00
hostname	
minimized icon	circle/#708090
role	

Figure 19. Characteristics of Sweep Jammer

A sweep jammer was built up from a source signal generator and a signal transmission. The components of the sweep jammer are shown in Figure 20:

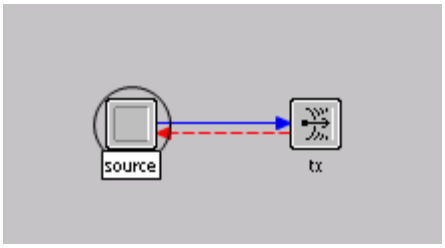


Figure 20. Components of Sweep Jammer

It was composed of a signal source node and a signal transmitter. The difference between the sweep jammer and the pulse jammer was the process of sending data from the source node. The process model of the sweep jammer is shown in Figure 21:

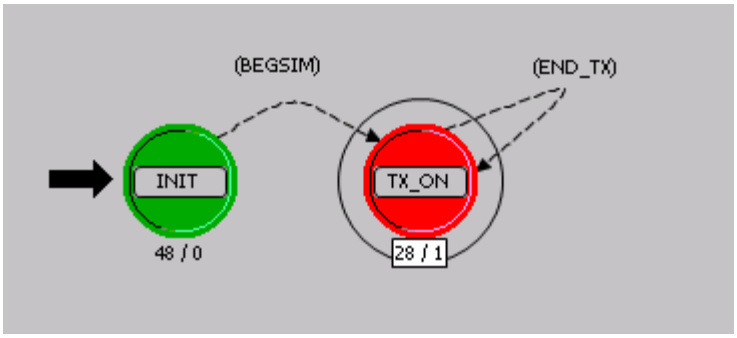


Figure 21. Process Model of Sweep Jammer

The TX_ON state was responsible for allowing data to be sent to different frequencies. The code of changing frequency in this jammer is shown in Appendix.

This Scenario included two groups of comparisons. The first set was a comparison of how different jammers styles influence the network. Later in the experiment, the communication between nodes was switched to channel 6. The second comparison occurred after the switch had been made.

3.3.2 Scenario AH-2

In this Scenario, different ad-hoc routing protocols were compared in a MANET network. Mobile nodes were set to travel in random trajectories, which were established using the mobility configuring node in OPNET. The methodology of this Scenario is shown in Figure 22:

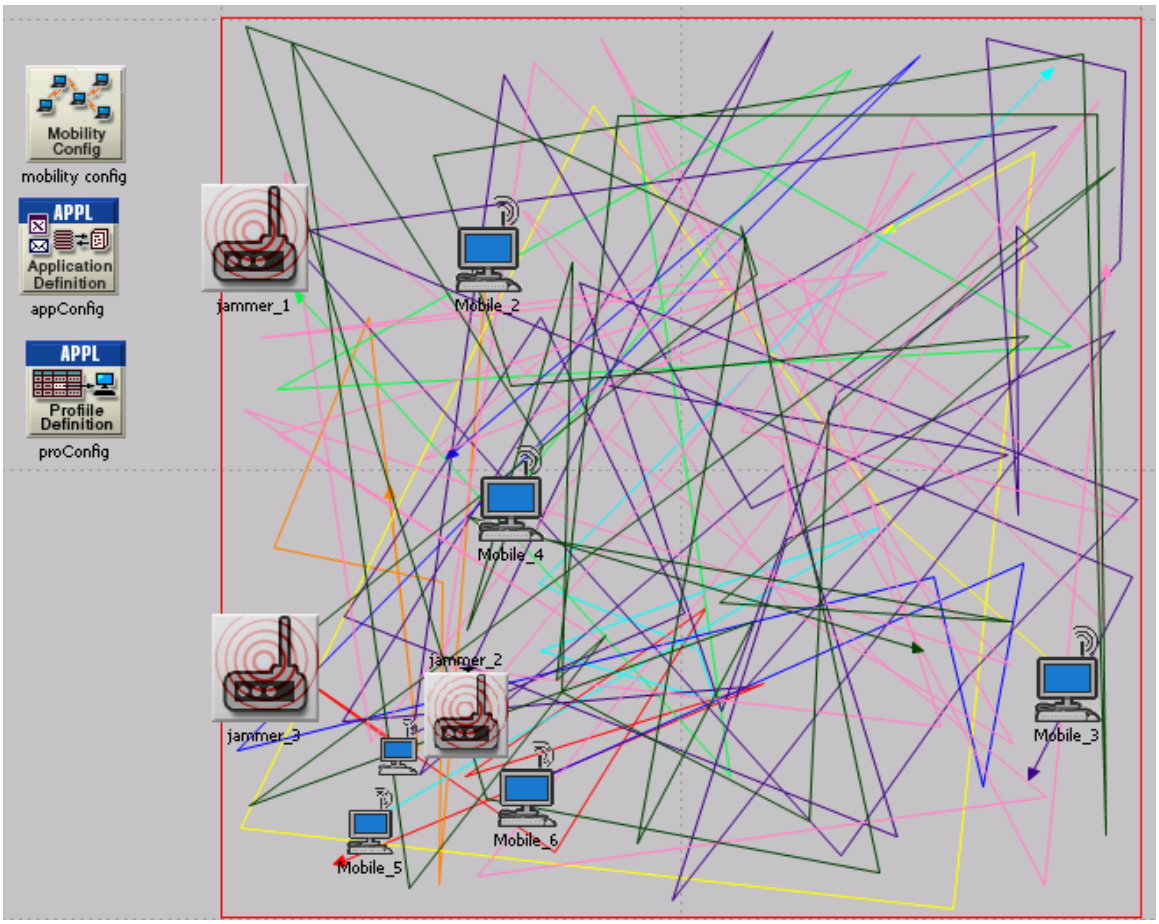


Figure 22. Methodology of Scenario AH-2

3.3.2.1 Random Trajectory Generation

In Figure 22, the color of the trajectories are: red: mobile_node_1; orange: mobile_node_2; yellow: mobile_node_3; green: mobile_node_4; cyan: mobile_node_5; blue: mobile_node_6; purple: jammer_1; pink: jammer_2; dark green: jammer_3. The mobile nodes used the ‘wlan_wksn_adv (mobile node)’ model; the pulse jammer was utilized. All the mobile nodes were supporting low-load video application defined in Chapter 3.1.

In order to generate random trajectories for the nodes and jammers, the mobility configuration node was used. It defined mobility profiles that separated node references to model mobility. It controlled the movements of nodes based on configured parameters. Figure 23 shows the definition setting of the mobility for the nodes in this Scenario.

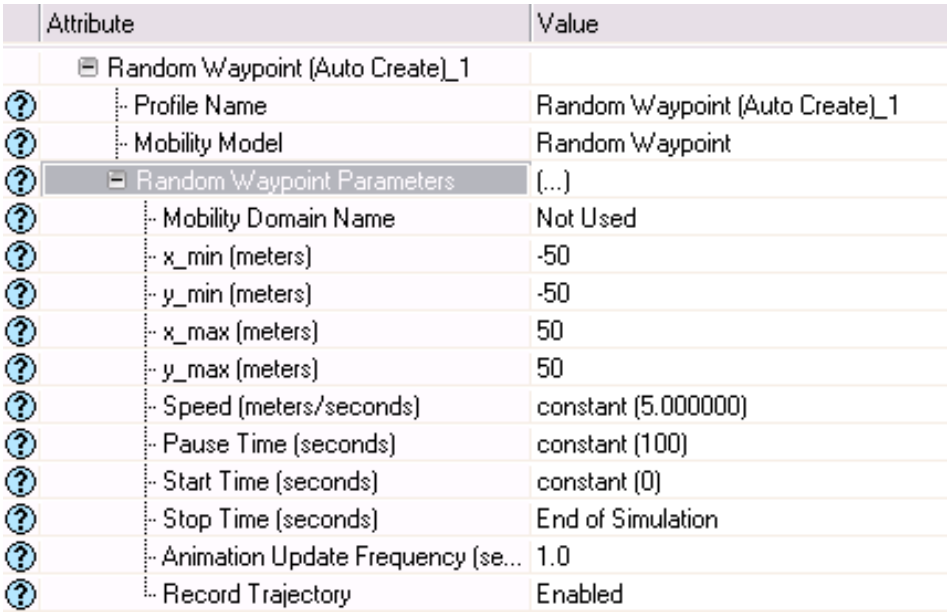


Figure 23. Definition Setting of the Mobility

The trajectories were set to a random waypoint in a 50×50 meter area. They started from the beginning of simulation, and ended at the end of the simulation. The speed of the nodes was constantly 5 meters/second, and when the node finished a movement to a random destination, it would stop and pause for 100 seconds. The random trajectories used by each node were recorded by the OPNET Modeler library. When the jammers needed to generate random trajectories, the jammers could use the random trajectory generated for the nodes saved in the library.

The algorithm of the random trajectory is shown in Figure 24:

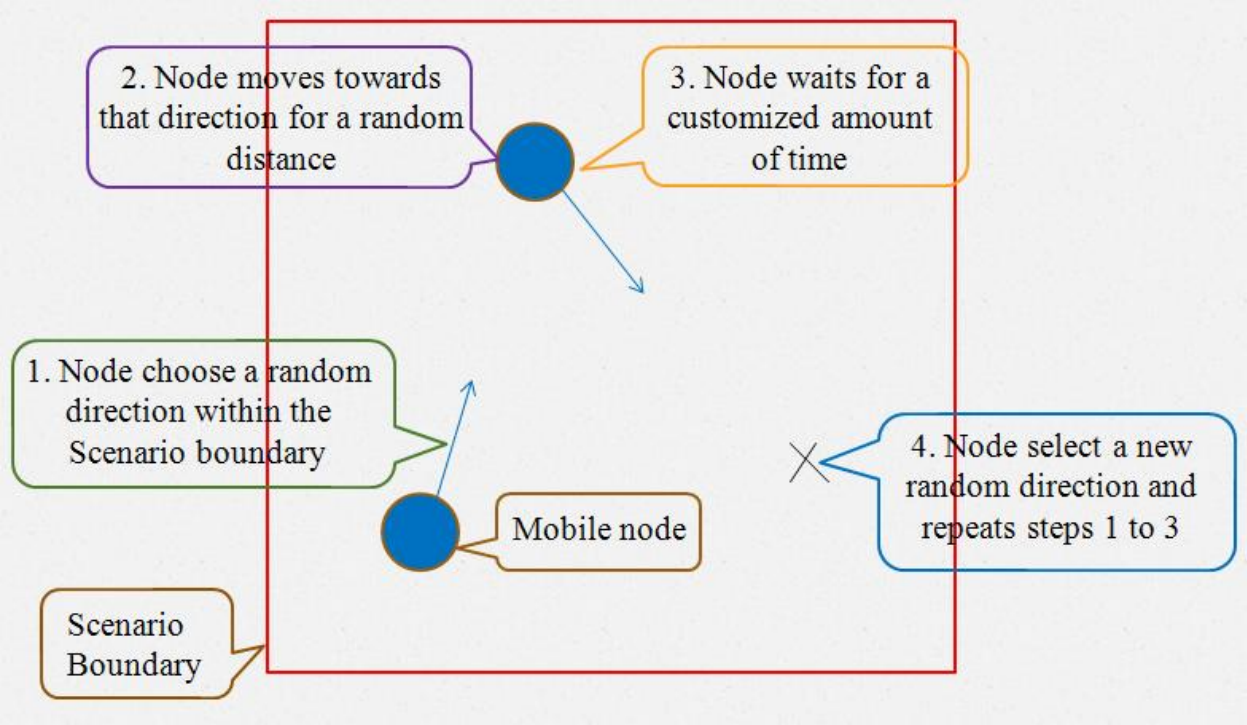


Figure 24. Algorithm of Random Trajectory

The red line in Figure 24 represents the boundary of the scenario. The blue sphere represents the mobile node used in the experiments. The algorithm of generating random trajectory included four steps:

1. The node chose a random direction within the scenario boundary, which was set to a 50×50 meter area.
2. The mobile node moved with a customized speed for a random distance towards the random direction chosen in the first step.
3. The node waited for a customized amount of time, which was set to 100 seconds in the experiments.
4. The mobile node chose another random direction and repeats step one to 3.

One of the random trajectories generated by the system is shown in Figure 25:

	X Pos (m)	Y Pos (m)	Distance (m)	Altitude (m)	Traverse Time	Ground Speed	Wait Time	Accum Time	Pitch (degrees)
1	-23.315902	-27.517021	n/a	0.000000	n/a	n/a	00.00s	00.00s	Autocomputed
2	25.368656	32.960884	77.638614	0.000000	15.53s	5.000000	00.00s	15.53s	Autocomputed
3	6.407964	4.130266	34.506532	0.000000	06.90s	4.999962	1m40.00s	2m02.43s	Autocomputed
4	26.977467	0.182824	20.944773	0.000000	04.19s	4.999794	1m40.00s	3m46.62s	Autocomputed
5	48.767860	-5.847381	22.609527	0.000000	04.52s	5.001149	1m40.00s	5m31.14s	Autocomputed
6	2.678485	27.727197	57.021662	0.000000	11.40s	5.000076	1m40.00s	7m22.54s	Autocomputed
7	-28.169663	0.930399	40.861830	0.000000	08.17s	5.000068	1m40.00s	9m10.72s	Autocomputed
8	22.378360	21.628233	54.621420	0.000000	10.92s	5.000023	1m40.00s	11m01.64s	Autocomputed
9	-45.719698	14.394854	68.481184	0.000000	13.70s	5.000000	1m40.00s	12m55.34s	Autocomputed
10	5.393328	21.197335	51.563488	0.000000	10.31s	5.000000	1m40.00s	14m45.65s	Autocomputed
11	-33.763799	-30.492250	64.846548	0.000000	12.97s	4.999968	1m40.00s	16m38.62s	Autocomputed
12	-43.134311	32.760213	63.942831	0.000000	12.79s	4.999989	1m40.00s	18m31.41s	Autocomputed
13	39.757691	-36.493866	108.014906	0.000000	21.60s	5.000000	1m40.00s	20m33.01s	Autocomputed
14	-22.235778	-45.463869	62.639224	0.000000	12.53s	5.000023	1m40.00s	22m25.54s	Autocomputed
15	45.435057	40.930163	109.741871	0.000000	21.95s	4.999992	1m40.00s	24m27.49s	Autocomputed
16	12.183306	-7.845962	59.032034	0.000000	11.81s	4.999987	1m40.00s	26m19.29s	Autocomputed
17	10.910556	3.189898	11.109714	0.000000	02.22s	4.999817	1m40.00s	28m01.51s	Autocomputed
18	25.313340	39.078820	38.671324	0.000000	07.73s	5.000106	1m40.00s	29m49.25s	Autocomputed
19	44.311626	14.726311	30.886927	0.000000	06.18s	5.000095	1m40.00s	31m35.43s	Autocomputed
20	46.135957	-17.153665	31.932013	0.000000	06.39s	5.000000	1m40.00s	33m21.81s	Autocomputed
21	-16.059134	44.994625	87.924055	0.000000	17.58s	5.000009	1m40.00s	35m19.40s	Autocomputed
22	-25.921715	-22.131034	67.846357	0.000000	13.57s	4.999995	1m40.00s	37m12.97s	Autocomputed
23	28.250960	-28.670516	54.565909	0.000000	10.91s	4.999985	1m40.00s	39m03.88s	Autocomputed
24	12.911044	21.353796	52.323513	0.000000	10.46s	4.999984	1m40.00s	40m54.34s	Autocomputed
25	-43.972270	3.759177	59.542132	0.000000	11.91s	4.999987	1m40.00s	42m46.25s	Autocomputed
26	-7.609933	-19.959074	43.413855	0.000000	08.68s	5.000036	1m40.00s	44m34.94s	Autocomputed
27	-47.526683	6.505877	47.893070	0.000000	09.58s	5.000059	1m40.00s	46m24.51s	Autocomputed

Figure 25. One of Random Trajectory Generated By Mobility

Specific trajectory parameters such as travel time, distance, speed and wait time were established. All of the trajectories in this Scenario were auto-computed with the algorithm of a random trajectory defined in the mobility configuration.

3.3.2.2 Ad-hoc Routing Protocols

Because ad-hoc networks do not have any router or access point, nodes are not established in a specific network structure. Therefore, a routing protocol is needed in the ad-hoc network. Ad-hoc routing protocols are used to set up the path for nodes to transmit data. When a network is established, a transmission path has to be discovered according to different settings of ad-hoc routing protocols. The routing protocols networks use varies the performance of the networks. Tables 7-9 shows parameters used in protocols.

Table 7. Parameter of AODV Routing Protocol

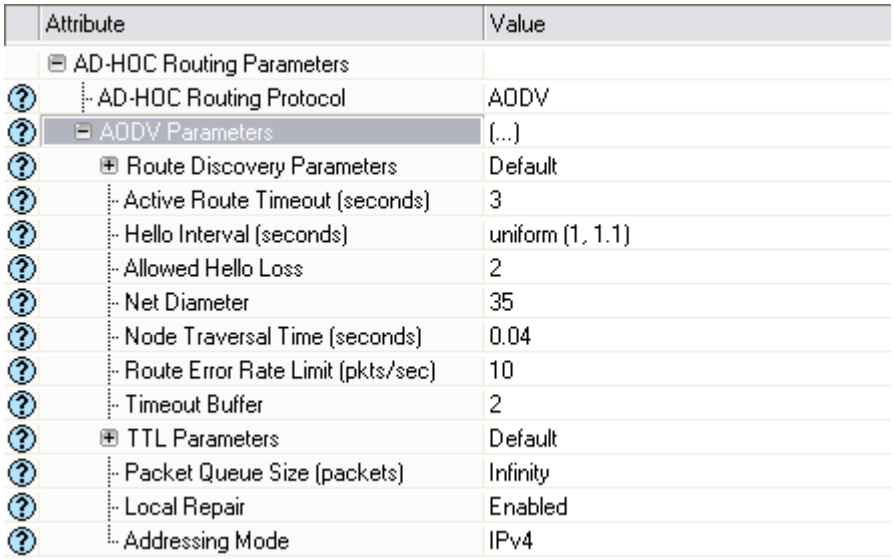
Protocol	Parameter settings
AODV	

Table 8. Parameter of TORA Routing Protocol

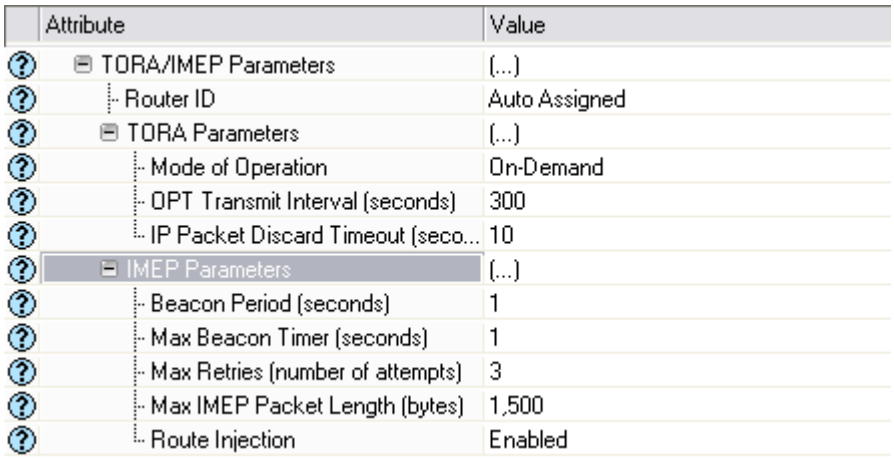
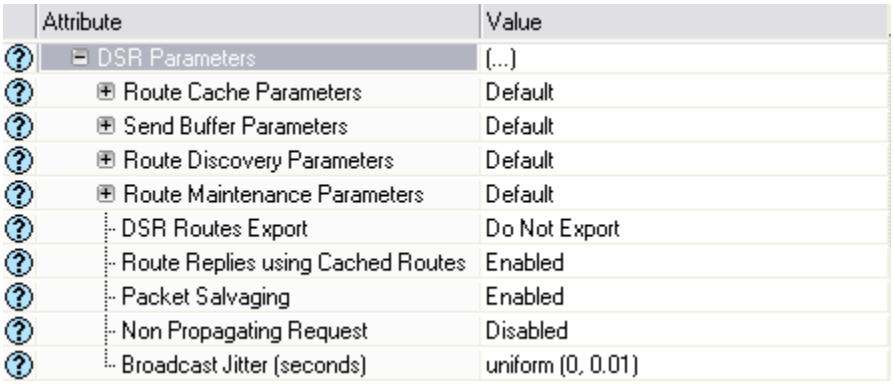
Protocol	Parameter settings
TORA	

Table 9. Parameter of DSR Routing Protocol

Protocol	Parameter settings
DSR	

All the protocols tested in this Scenario were using the ad-hoc routing protocol models from OPNET Modeler. The purpose of this experiment was to test and compare the performance of each routing protocol while there was jamming attack in random trajectories. Both jammers and mobile nodes traveled in random trajectories. Average throughput of the network assisted in evaluating listed protocols.

CHAPTER 4 SIMULATION ANALYSIS

Chapter 5 analyzed the results of the 5 Scenarios described in the previous Chapter. The simulation results were displayed in the order that they appeared in Chapter 4. The results were accompanied with an analysis.

4.1 Scenario CS-1

Scenario CS-1 included three different comparisons. The first was a comparison of fixed work station and mobile work station simulation results. The second experiment was a comparison of throughput when transmitting power level of access points vary. The third experiment compared the throughput of the mobile node while located at varying distances from the access point. The simulation time for each experiment was 2 minutes.

4.1.1 Experiment 1 in Scenario CS-1

With normal network traffic, throughput of fixed node (node_0) and mobile node (mobile_node_0) were compared and the result was shown in Figure 26. Fixed node was located within the bounds of the access point signal range located outside of the signal range. It then traveled within the bounds of the signal range. The start position of the mobile node was 1000 meters away from the access point, which was out of the signal range of the access point, but then travels into the signal range.

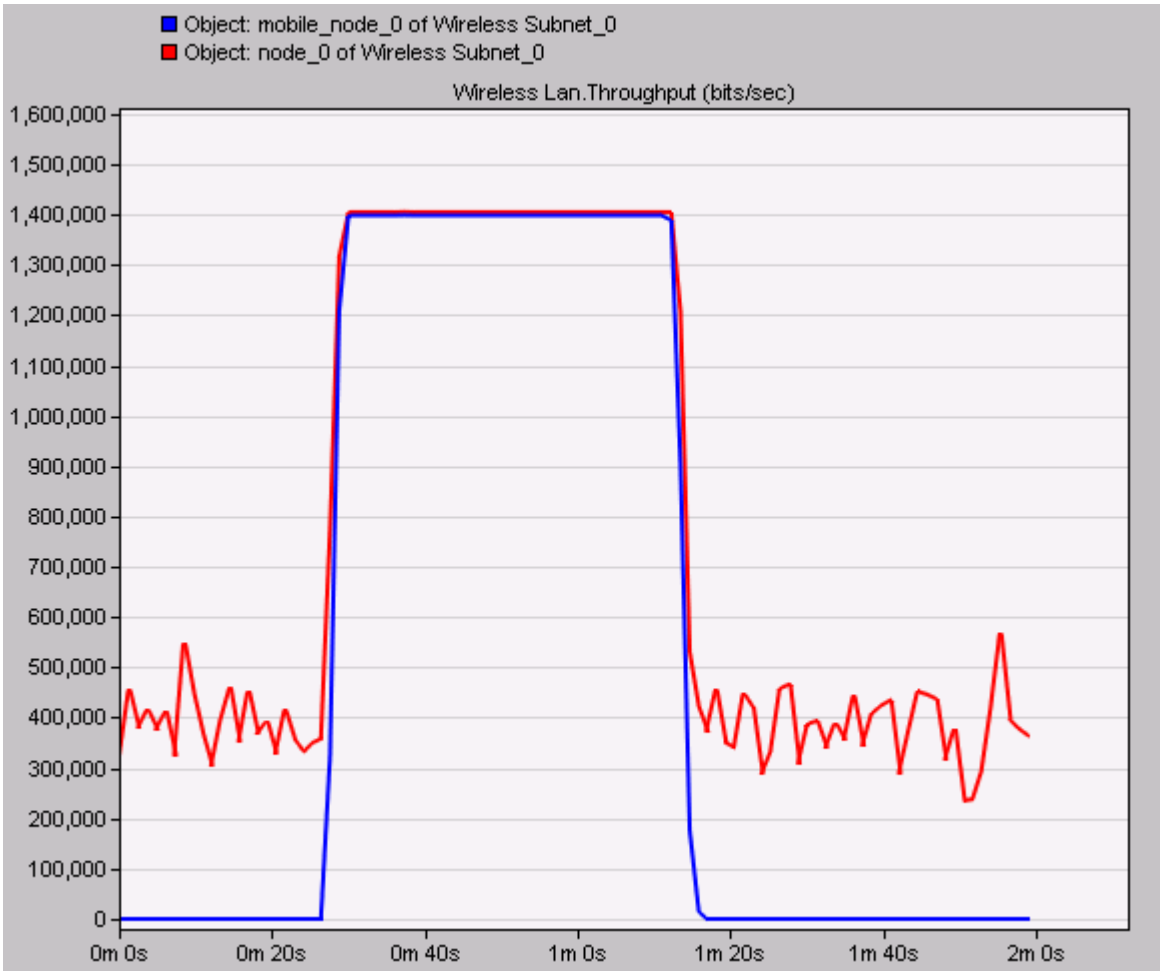


Figure 26. Comparison of Throughput of the Fixed Node and Mobile Node without Jammer

Fixed node; Mobile node

When the mobile node traveled into the signal range, the video conference application communication activated. The throughput of both nodes increased immediately as effect. When the mobile node moved out of range, the fixed node still received a signal from the access point, but the throughput dropped because the video conference communication ended.

4.1.2 Experiment 2 in Scenario CS-1

The effect that carrying power had on the nodes is compared in Figure 27. Green, blue, and red lines represent the throughput of the mobile node while the power level of access point was 0.0005W, 0.001W, and 0.005W, respectively.

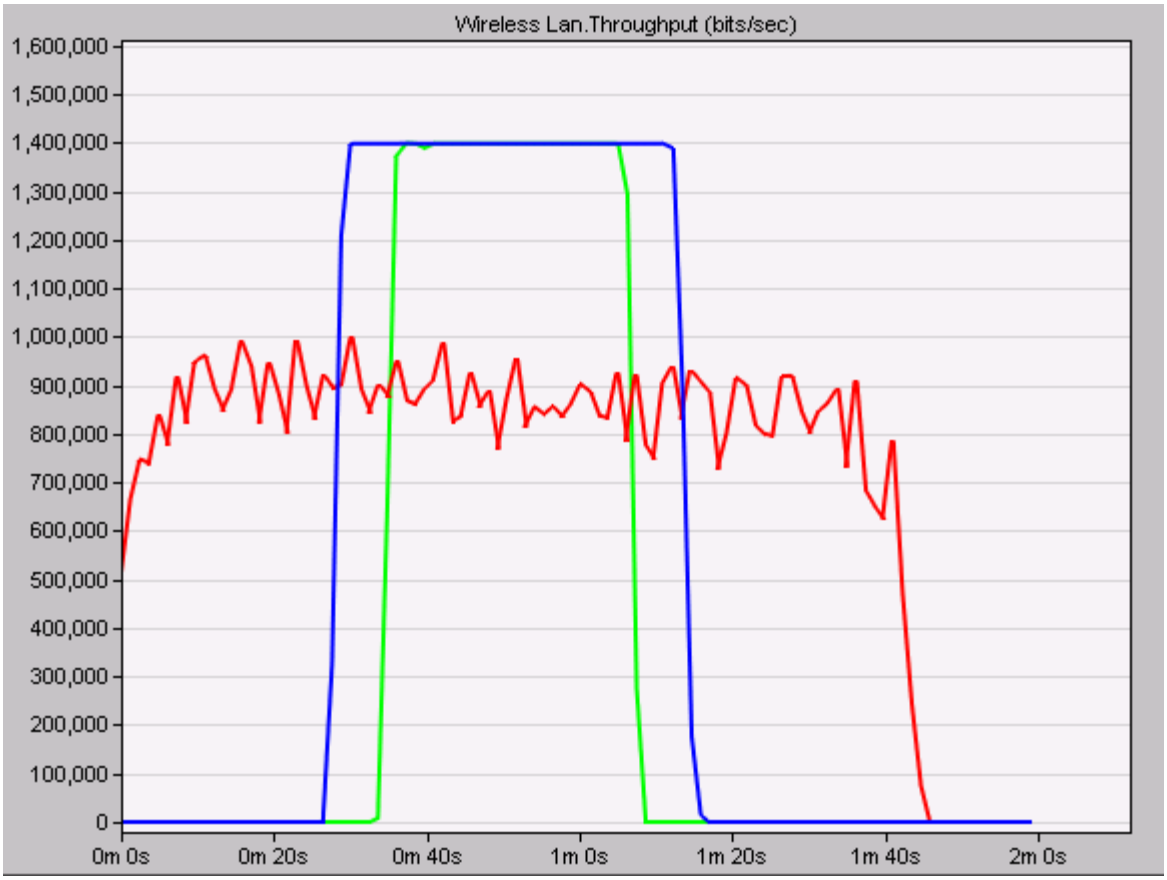


Figure 27. Throughput of Different Access Point Powers

0.0005W; 0.001W; 0.005W

In Figure 27, the green line represents the throughput of the mobile work station when the access point power was 0.0005W; the blue line represents a 0.001W power level, and the red line represents a 0.005W power level. When power was decreased, the signal range for the mobile node was decreased. When power reached 0.001W, the signal range from the access point was visibly increased. When power became 0.005W, the mobile node received signal up to 1000 meters away from the access point, which was the starting position.

4.1.3 Experiment 3 in Scenario CS-1

Figure 28 compared the effect on the nodes according to the distance from the access point. In this experiment, access point power was limited to 0.001W. The distance between the

access point and the mobile node varied from 50 meters to 400 meters. The blue line represents the throughput of the mobile node when the distance was 50 meters; the red line represents the simulation result of 300 meters; and the green line represents 400 meters.

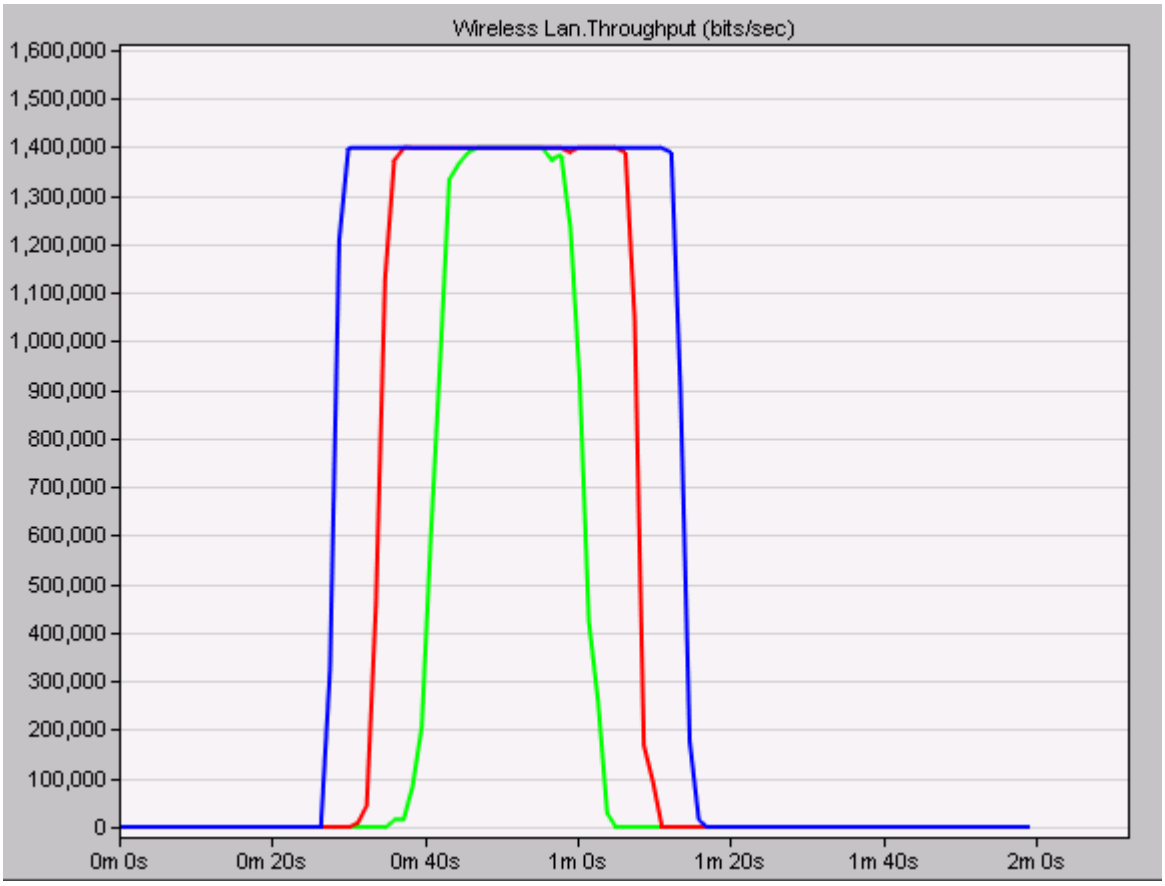


Figure 28. Throughput Comparison in Different Distances

50 M; 300 M; 400 M

In Figure 28, when the distance increased from 50 to 300 meters, the time it took for mobile nodes to receive a signal decreased by about 5 seconds, and when distance was increased once more to 400 meters, signal decreased again. In conclusion the further the distance was, the worse the signal became.

4.2 Scenario CS-2

Scenario CS-2 included three different comparisons. The first one was the comparison of the throughput of fixed nodes with and without jammer simulation results. The second experiment was a comparison of mobile nodes' throughput with and without a jammer. Finally, the third experiment compared mobile node throughput with varying jammer power. The simulation time for each experiment was 2 minutes.

When a jammer was used in the Scenario, the communication between the access point and the node were affected. Because the jammer was a pulse jammer, the attack had a pulsed effect. When the jammer was sending useless packets to flood the network, the throughput of the node dropped. When the jammer pulsed, which stopped the packet flooding, the throughput returned to normal, and communication continued. For the fixed node, the jammer and access point were always in the signal range.

4.2.1 Experiment 1 in Scenario CS-2

The fixed node always received a signal from the access point, but the jamming attack always influenced communication between the fixed node and the access point. When the mobile node ventured into the area, the communication between the fixed node and the mobile node caused an increase in network throughput, but communication between these two nodes was affected by the jammer as well. Figure 29 shows the simulation result for this experiment.

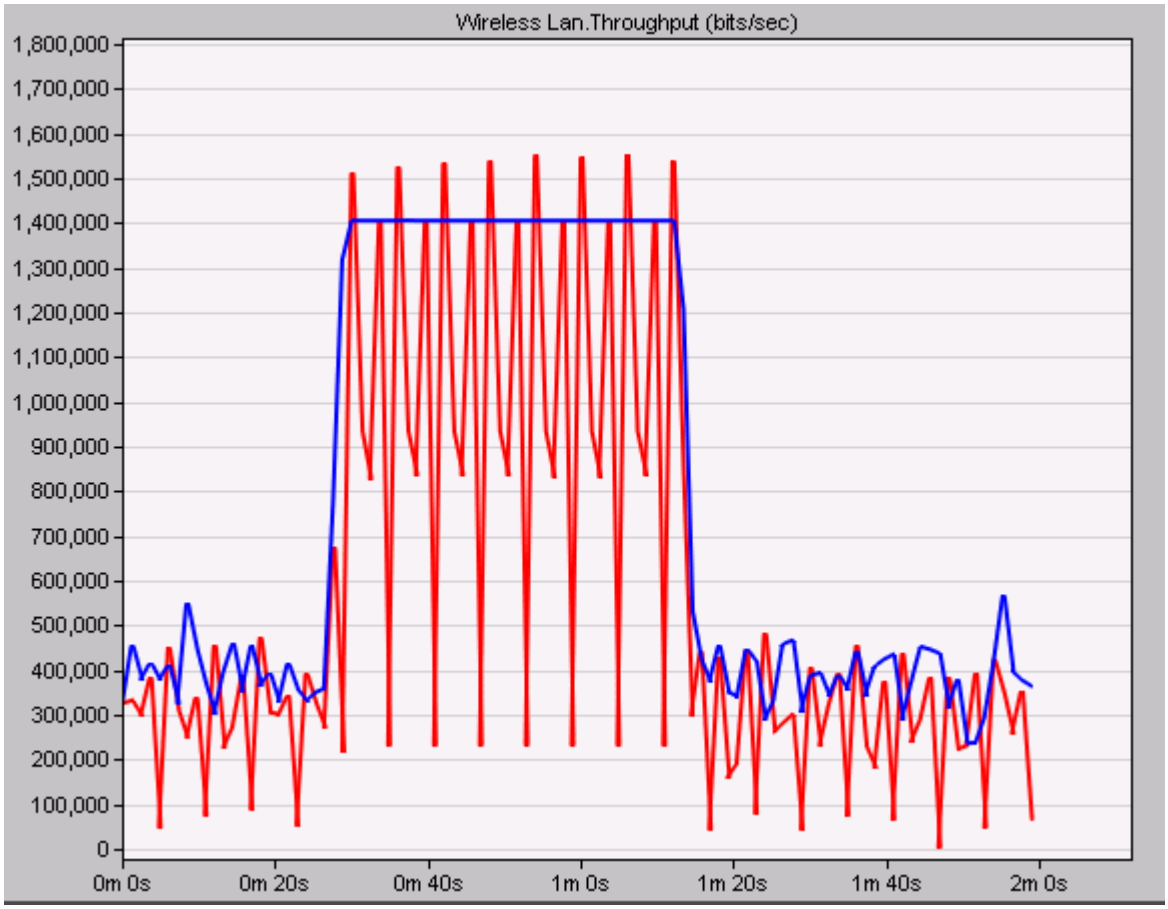


Figure 29. Comparison of Throughput of Fixed Node With/Without Jammer

The blue line represents the throughput before the jammer was applied in the network, and the red line represents the throughput after the jammer was applied in the network. The jammer constantly jammed the fixed node.

4.2.2 Experiment 2 in Scenario CS-2

When the mobile node was out of the range of the access point, there was no signal received from the access point or fixed node. But when it moved into the access point signal boundary, the jammer began affecting communication immediately. Figure 30 shows the throughput of the mobile node.

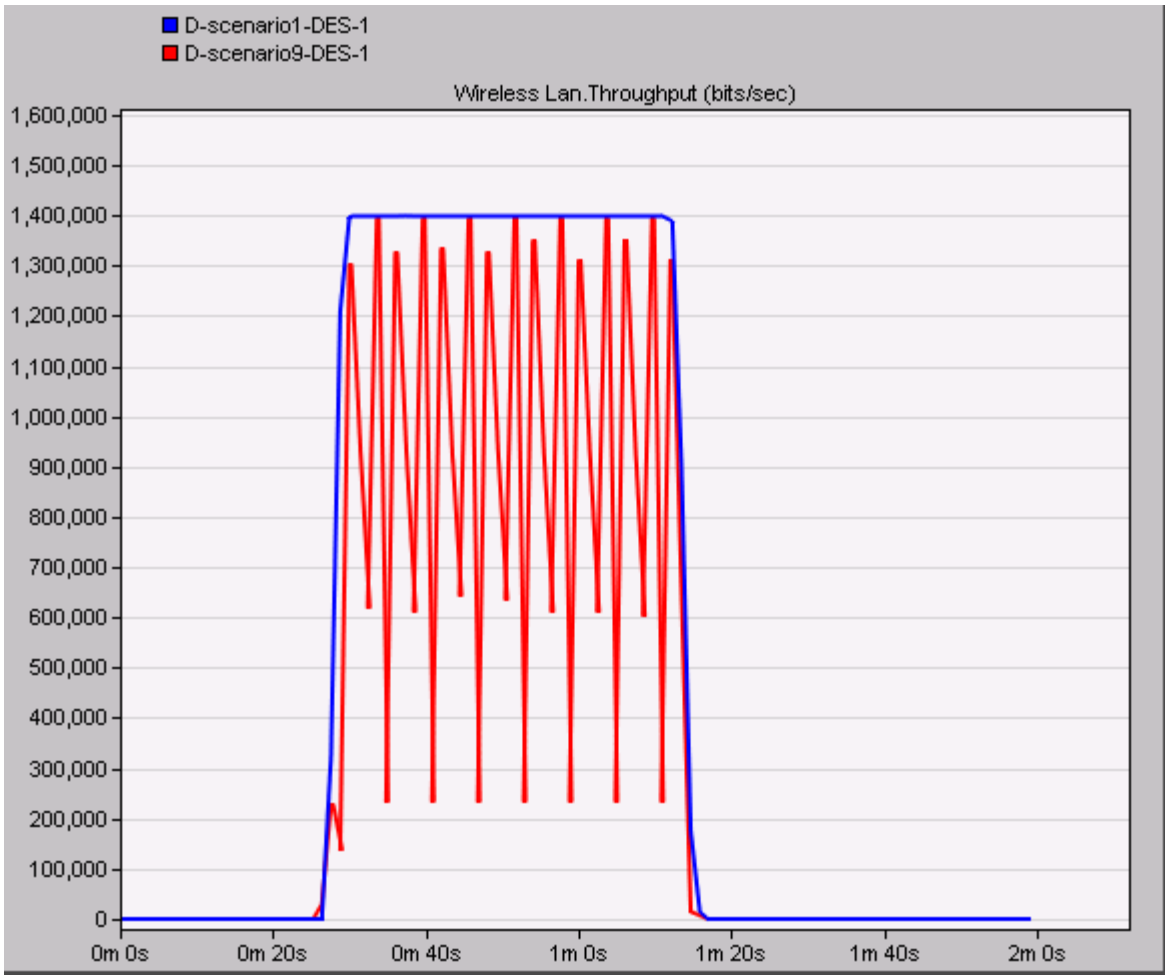


Figure 30. Comparison of Mobile Node Throughput With/Without Jammer

The blue line represents throughput before the jammer was utilized, and the red line is the throughput after the jammer attacks the network. The jammer affected the mobile node immediately after it moved into the signal boundary of the access point.

4.2.3 Experiment 3 in Scenario CS-2

For the third experiment, different power levels were used in the jammer. Figure 31 shows the comparison of mobile node throughput in different jammer power levels.

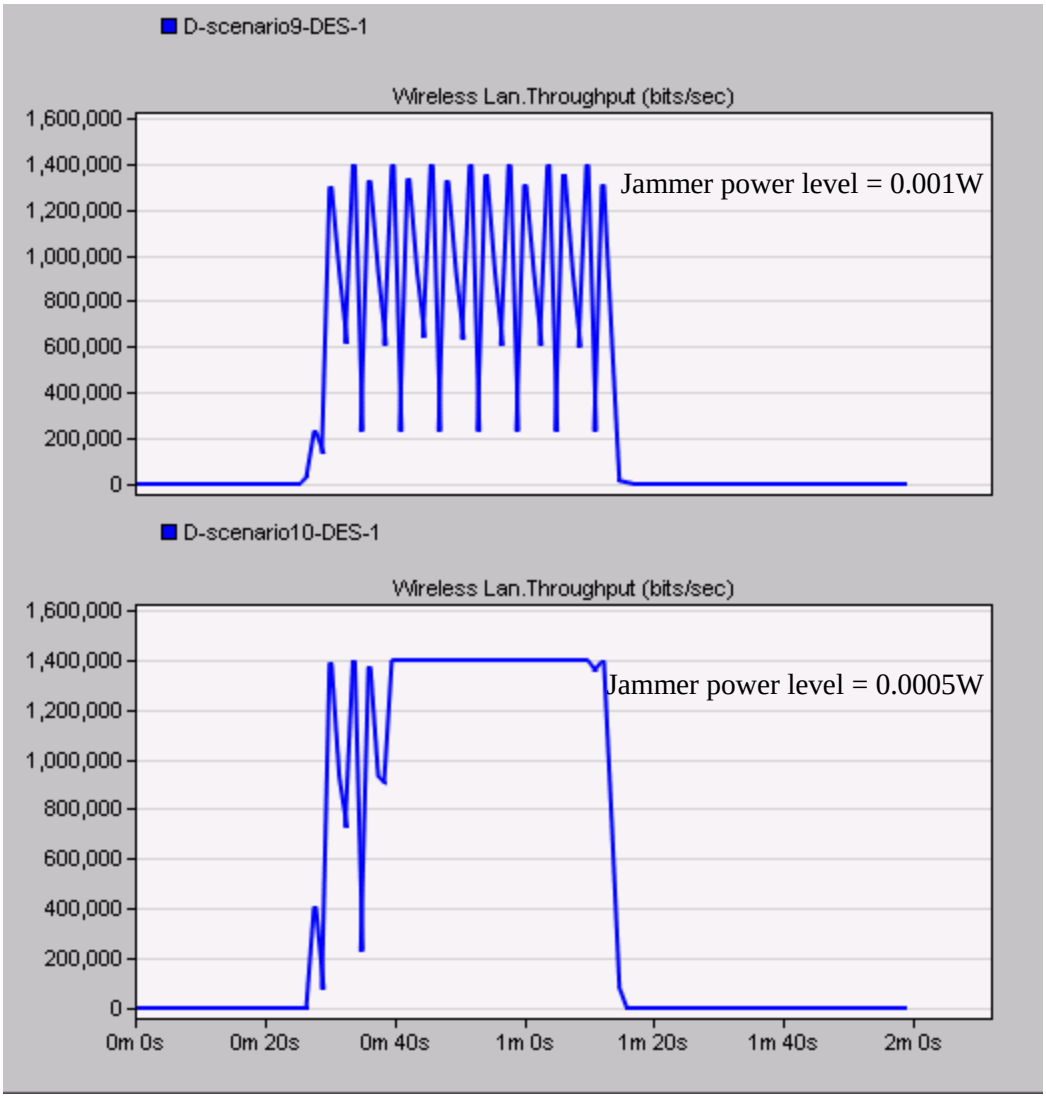


Figure 31. Comparison of Mobile Node Throughput in Different Jammer Powers

In Figure 31, the first simulation result used jammer power level 0.001W, and the second had a power level of 5E-005W. When the power of the jammer was small, the range which the jammer could influence was smaller. When the mobile node moved into the work space, it was in close proximity to the jammer, and therefore affected. But while the mobile node was moving away from the jammer, it moved out of the jamming range, and back to normal communications.

4.3 Scenario CS-3

Scenario CS-3 simulated a client-server network with 4 fixed nodes and a mobile pulse jammer. The objective of this Scenario was to test and help understand the jamming attack launched by a mobile pulse jammer. The simulation time for the experiment was 4 minutes.

The experiment in this Scenario compared throughput of different nodes while the jammer was moving around the nodes. The jammer was moving in an octagonal pattern around four fixed nodes. It took the jammer 30 seconds to travel on each side of the path. The shortest distance possible between a node and the jammer was 1125 meters. When the jammer moved towards a certain node, the communication of this node was jammed. The throughput of this node dropped during the time which the jammer was affecting it. But as the jammer moved away from this node, the throughput returned to normal. Figure 32 shows the simulation result for experiment 1.

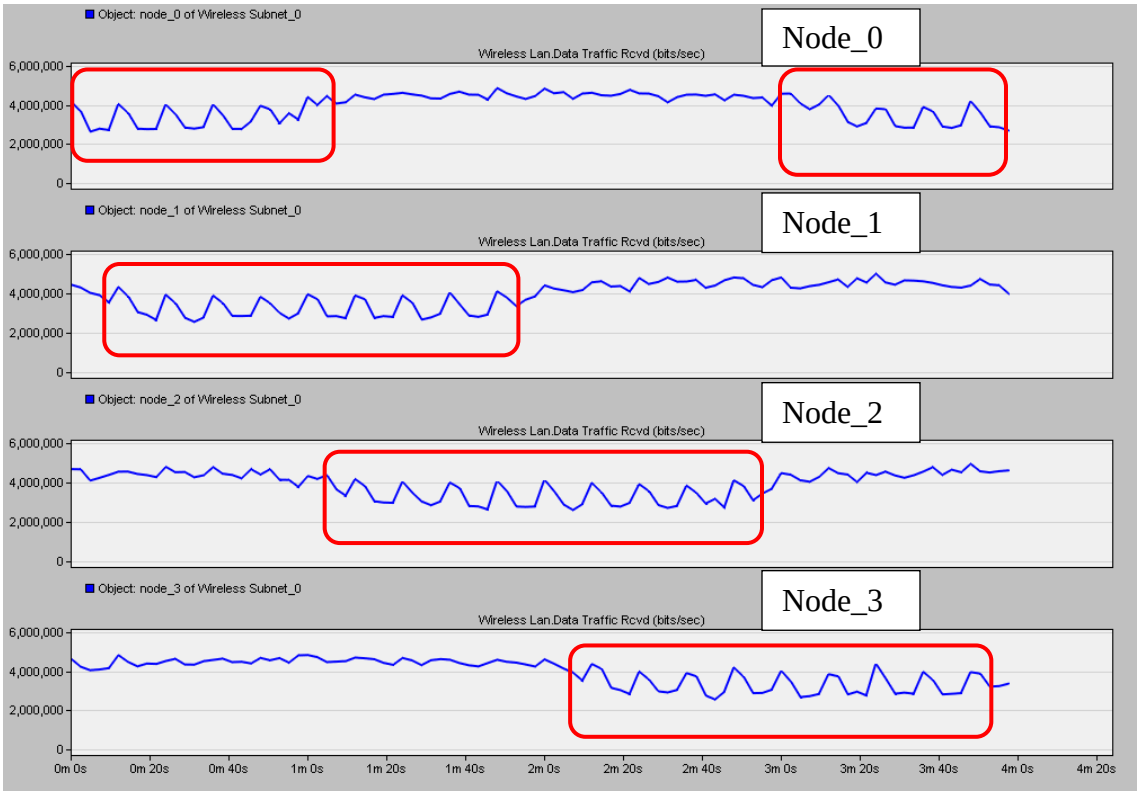


Figure 32. Traffic Reception of Fixed Nodes

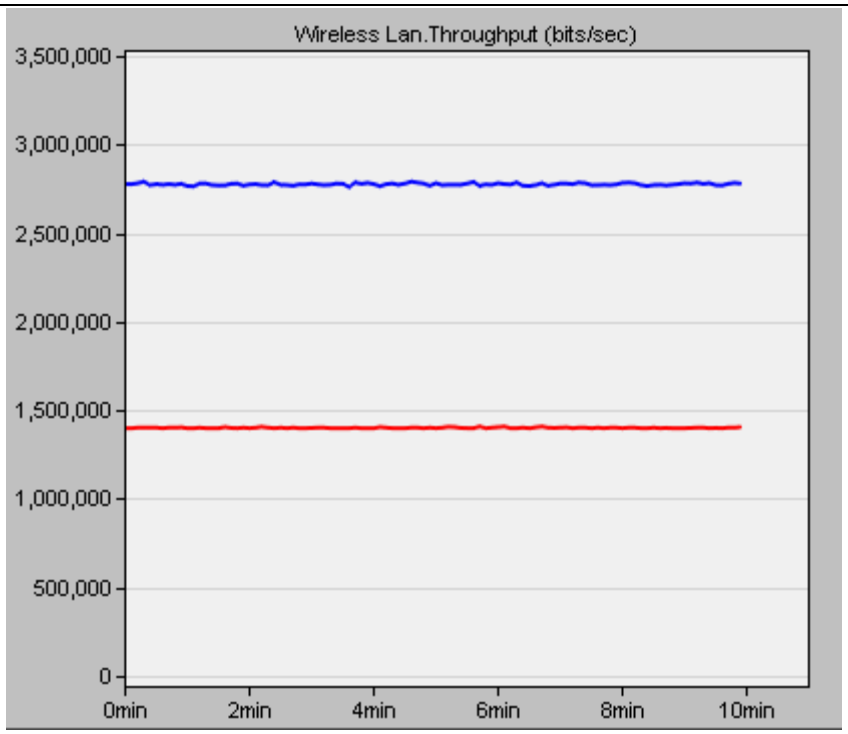
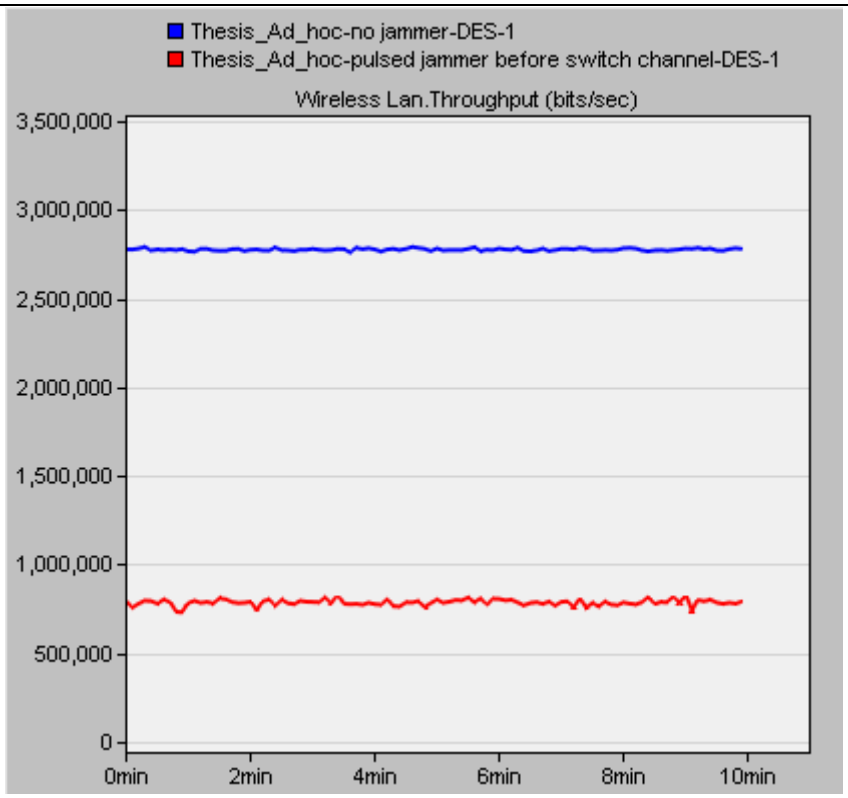
The lines in Figure 32 represent the packets received by each node through time. The jammer started moving beneath node_0. Only node 0 was affected by the jammer in the beginning of the simulation. Because of the influence of the pulse jammer, the traffic received by node_0 dropped and returned back to normal. When the jammer came towards it, the traffic received by node_0 dropped again. When the jammer travelled to node_1, the traffic received by node_1 began to be influenced by the jamming attack. At 2 minutes, the jammer was located at the position located right above node_2. The traffic received by node_2 dropped. This process was repeated for all nodes in this Scenario.

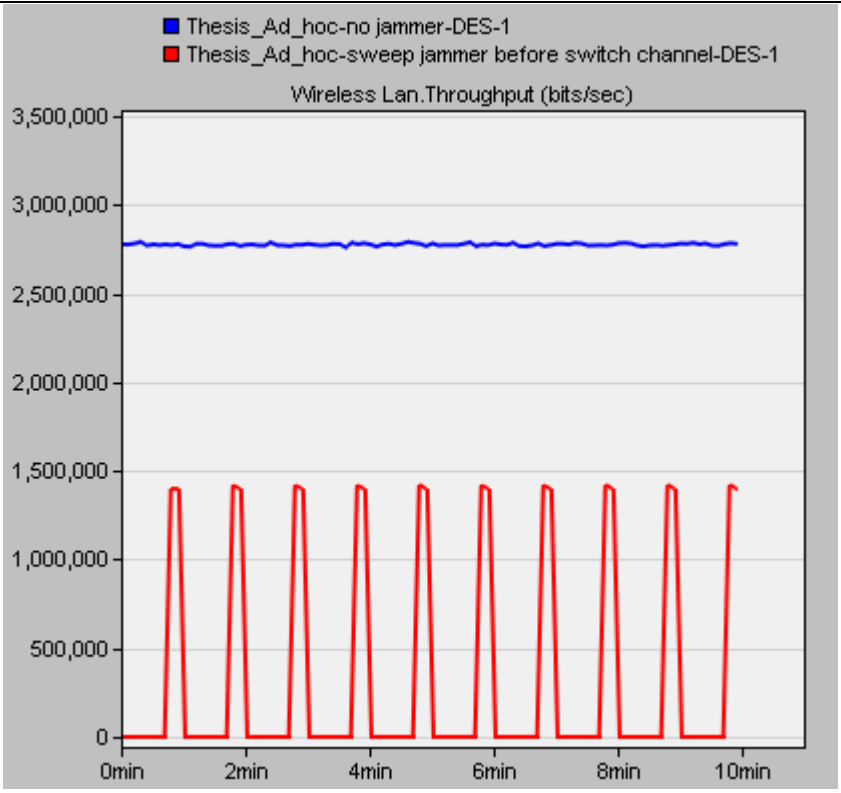
4.4 Scenario AH-1

In Scenario AH-1, an ad-hoc network was simulated by using the fixed nodes described in previous scenarios. Six fixed work stations and one fixed jammer were distributed into the work space. The distance between each node was 50 meters. Two groups of experiments were done in this scenario. The first group of experiments compared the performance of three types of jammers, including single band jammer, pulse jammer, and sweep jammer. The second group of experiments tested the performance of switching channels to avoid jamming attacks method for each jammer. The simulation time for each experiment was 10 minutes.

In the first group of experiments, each jammer was simulated separately. The throughput of a fixed node before and after the jamming attacks was compared. Table 10 shows the performance of three types of jammers. The blue lines represent the throughput before the jammer was introduced into the network, and the red lines represent the throughput after each jammer is used in the network.

Table 10. Comparison of Throughput With/Without Different Jammers

Single band jammer	
Pulse jammer	

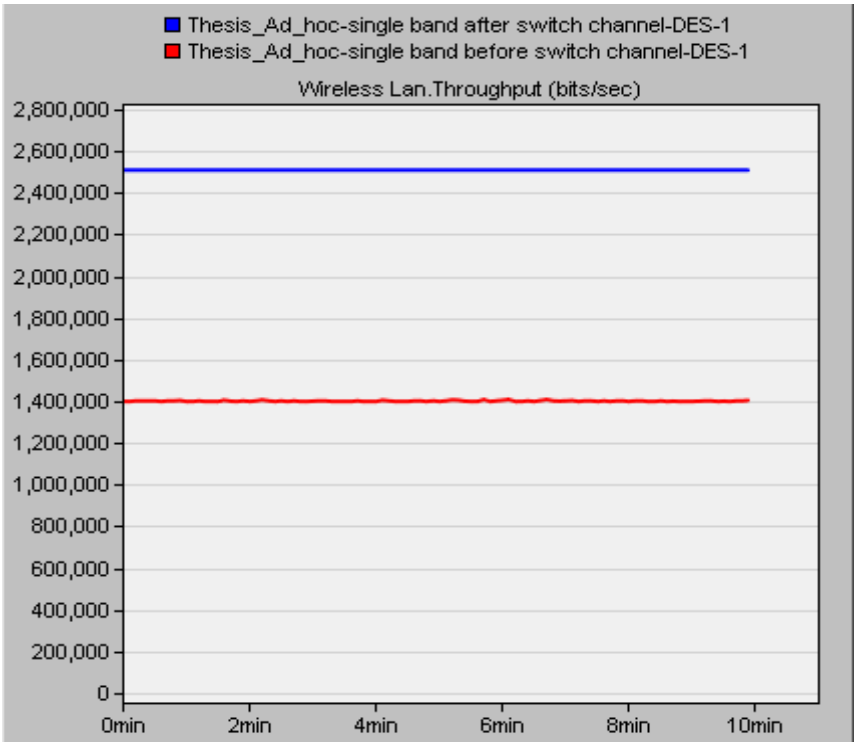
Sweep jammer	

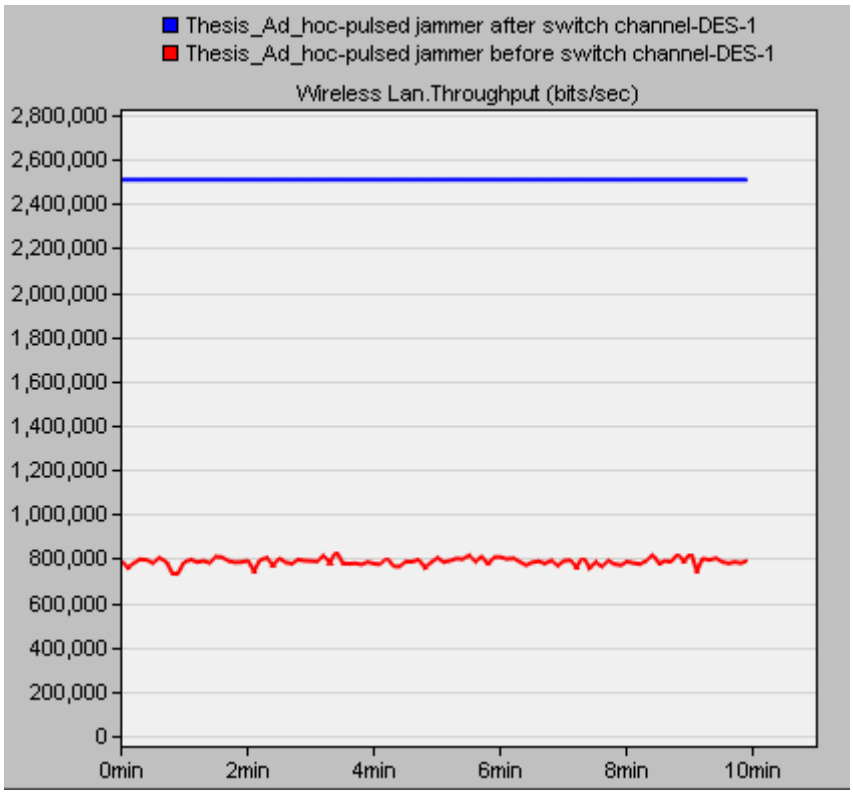
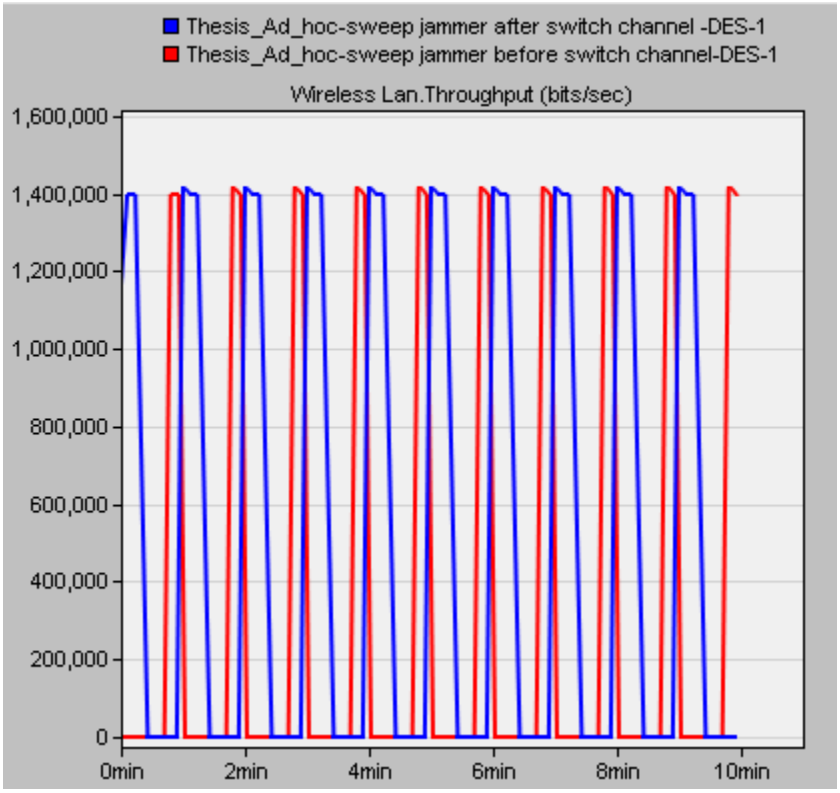
All the throughputs shown in Table 10 are derived from a fixed node. After a single band jammer was used, the throughput of the fixed node dropped from over 2,750,000 bits/sec to an average of 1,400,000 bits/sec. In the same situation, pulse jammers influenced the throughput of the fixed node to drop to an average of below 800,000 bits/sec. The performance of the pulse jammer was superior to the single band jammer. Jamming attacks launched by the pulse jammer effectively blocked communications in the network. The performance of the sweep jammer showed that its effects can vary from dropping throughput from 2,750,000 bits/sec to 1,850,000 bits/sec, to not having an influence at all. If a sweep jammer was utilized correctly, by using techniques such as increasing the sweep speed, it can block more data transmission in all channels of the network.

As a user, in order to prevent from being attacked by jammers, switching channels is one of the most effective methods, according to the previous research. Because of the channel communication of WLANs, when communications are blocked in one channel, nodes can be switched to another channel in order to continue the data transmission. The purpose of the second group of experiments was to test if this method is effective for every type of jammer. In the previous experiments, all the communications were transmitted in channel 1. In this group of experiments, fixed_node_0 and fixed_node_1 were switched from channel 1 to channel 6. Other nodes were set to continue to communicate in channel 1.

Table 11 shows the comparison in the second group of experiments. The throughput used in the comparison was the throughput of the fixed_node_0, which was switched from channel 1 to channel 6. The red lines in Table 11 represent the throughput of the fixed node before channel was switched, and the blue lines represent the throughput after the channel was switched.

Table 11. Comparison of Throughput Before/After Switching Channel under Different Jammers

Single band jammer	

Pulse jammer	
Sweep jammer	

For the single band jammer and pulse jammer, the jamming frequency was set at 2401 MHz, with a bandwidth of 22 MHz, which can only affect channel 1 to channel 5. After the nodes were switched out of the jammer's jamming frequency range, from channel 1 to channel 6, the throughput of the fixed node went up from 1,400,000 bits/sec to 2,500,000 bits/sec. Again, the fixed node under pulse jamming attacks went up from 800,000 bits/sec to 2,500,000 bits/sec after channel switching. After the communication channel was switched, both nodes avoided single band and pulse jamming attacks.

When traffic was not being sent in channel 1 or channels that not overlapped with channel 1, jamming attacks did not affect the nodes. If the jamming frequency is also switched to channel 6, the network would be jammed again.

On the other hand, the performance of the sweep jammer was not influenced by channel switching. Because of its characteristics, the sweep jammer could jump from frequency to frequency throughout the simulation process. It covered all frequencies from channel 1 to channel 14. When communication was switched from channel 1 to channel 6, it was still be affected by the sweep jammer. From the last figure in Table 11, the blue line and the red line represent the throughput under jamming attacks in two completely non-overlapped channels. After a particular time, jamming attacks were generated in channel 6 as well. If attackers use sweep jammers to disturb a network, switching channels to avoid the jamming attack will be futile.

4.5 Scenario AH-2

In Scenario AH-2, an ad-hoc network was simulated by using the mobile nodes traveling in random trajectories. The ad-hoc network included six mobile nodes and three pulse jammers, also traveling in random trajectories. Six experiments were done in order to draw four

comparisons. The first comparison showed the performance of AODV, TORA, and DSR routing protocols in the ad-hoc network without jamming attacks, and the second to fourth comparisons showed the performance of the ad-hoc routing protocols AODV, TORA, and DSR. The simulation time for each experiment was 10 minutes. Figure 33 shows the performances of three routing protocols tested in Scenario AH-2:

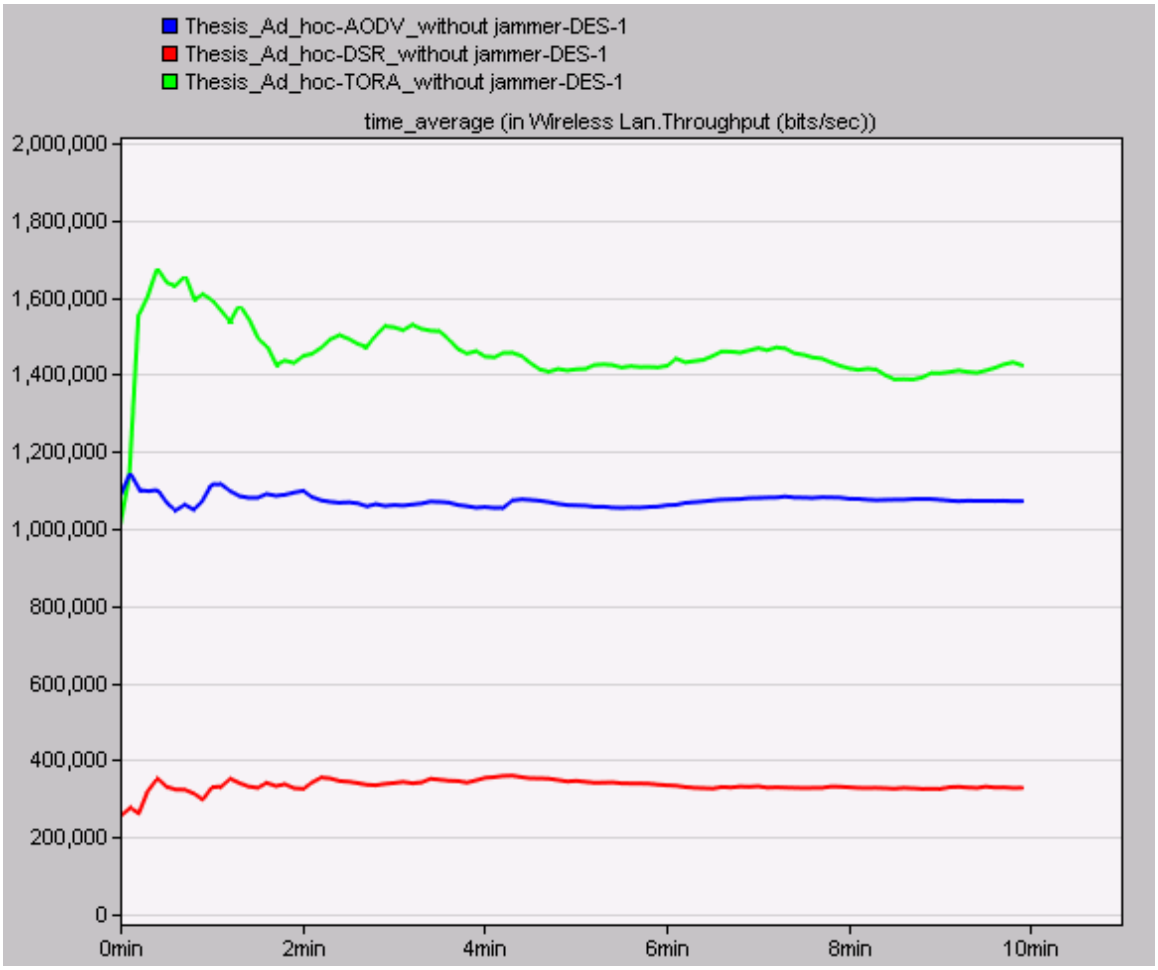


Figure 33. The Throughput Using AODV, TORA, and DSR Ad-hoc Routing Protocols
TORA; AODV; DSR

This experiment compared the performance of the three ad-hoc routing protocols. The throughput of the same node was compared under the three routing protocol. The blue line in Figure 33 represents the throughput of the mobile node using the AODV routing protocol. The

average throughput was around 1,100,000 bits/sec. The green line in Figure 33 demonstrates the throughput under the TORA routing protocol, the average of which was over 1,400,000 bits/sec. The red line in Figure 33 represents throughput under the DSR routing protocol, which only had a 350,000 bits/sec throughput in the same network.

Figure 34 shows the delay of a mobile node in the network under the three ad-hoc routing protocols.

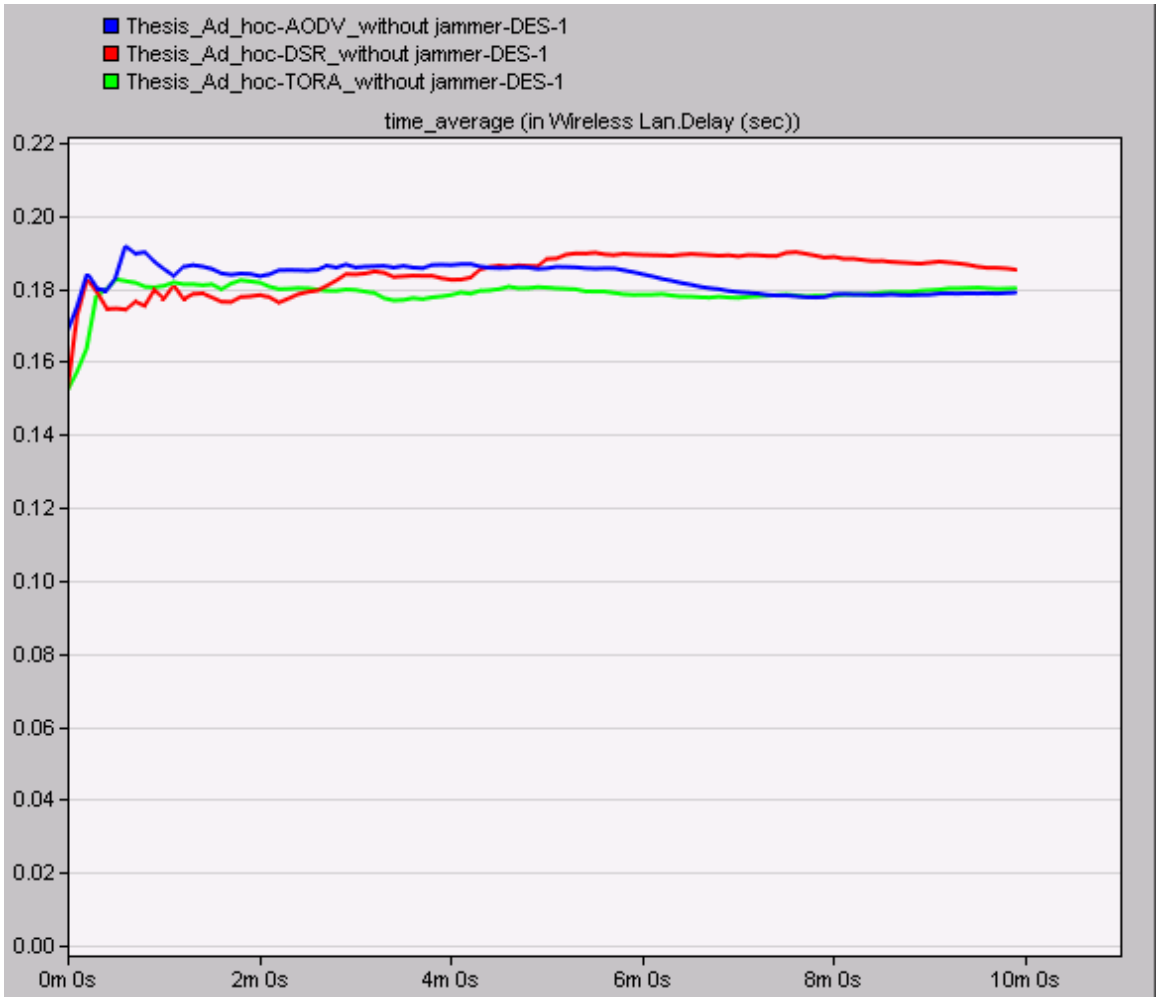


Figure 34. Delay of A Mobile Node in The Network Using AODV, TORA, and DSR Ad-hoc Routing Protocols

TORA; AODV; DSR

In Figure 34, the delay of the same mobile node in the ad-hoc network in three different routing protocols is similar. Because the delay in three experiments was the same, the routing protocol with higher throughput in the network was superior. The network that used the TORA routing protocol had the best performance because it had a greater throughput than the others. The DSR routing protocol performed the worst since it only gave the network one fifth of the throughput in comparison to the TORA routing protocol.

The performance of each protocol was tested and compared under random trajectory jamming attacks. Three mobile pulse jammers were used in the same network defined in Chapter 3.2.2.1. Figures 35 to 37 show the throughput of the same mobile node before and after the jammer was applied in the network with AODV, TORA, and DSR routing protocols.

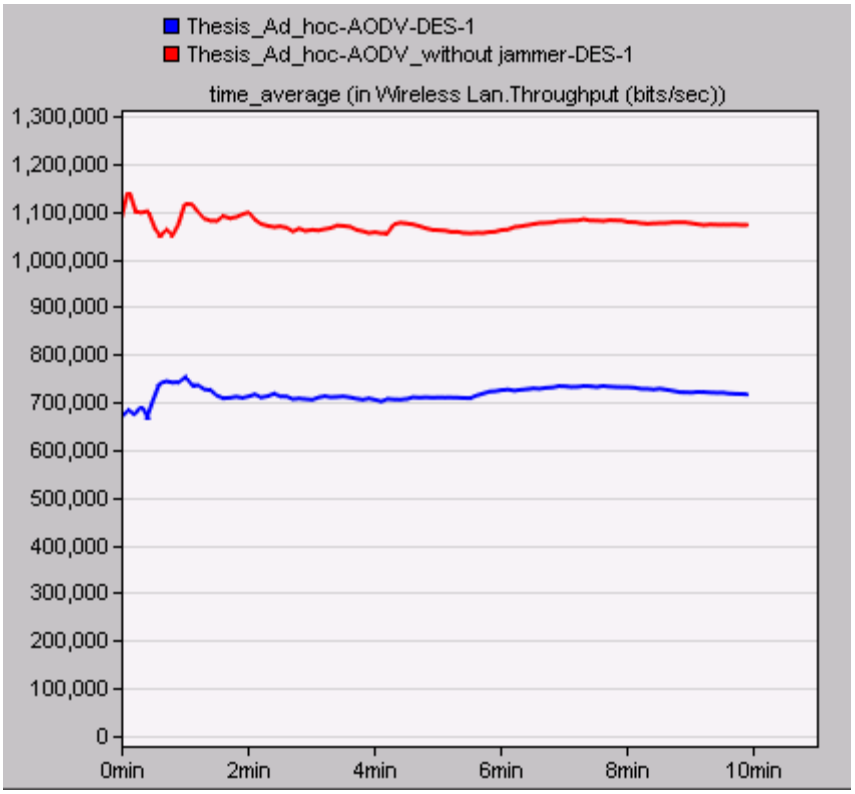


Figure 35. Throughput With/Without Jamming Attacks Using AODV Routing Protocol

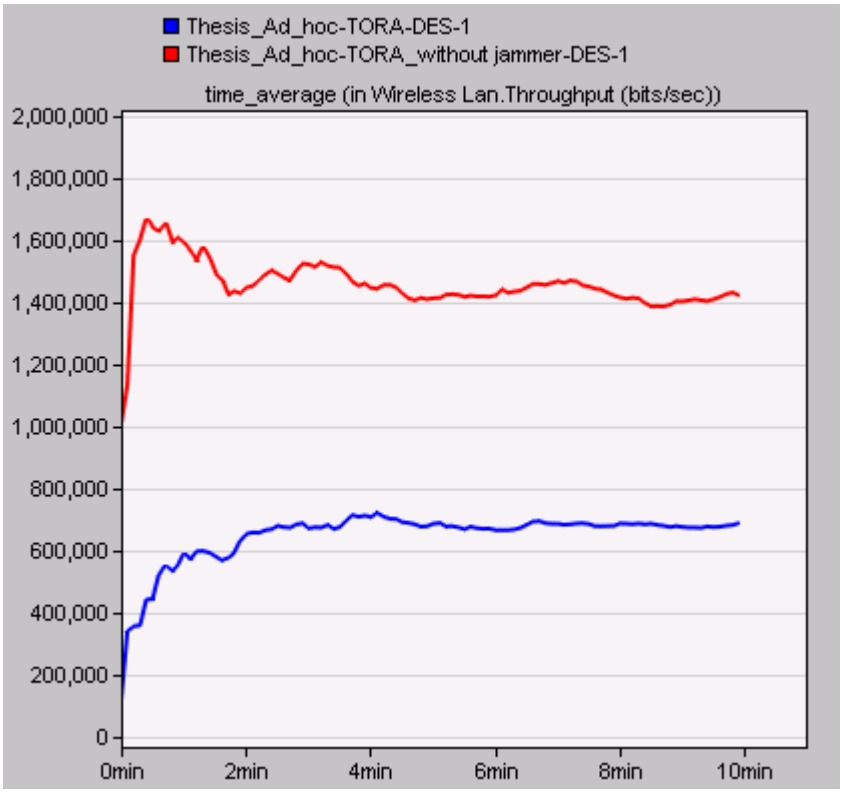


Figure 36. Throughput With/Without Jamming Attacks Using TORA Routing Protocol

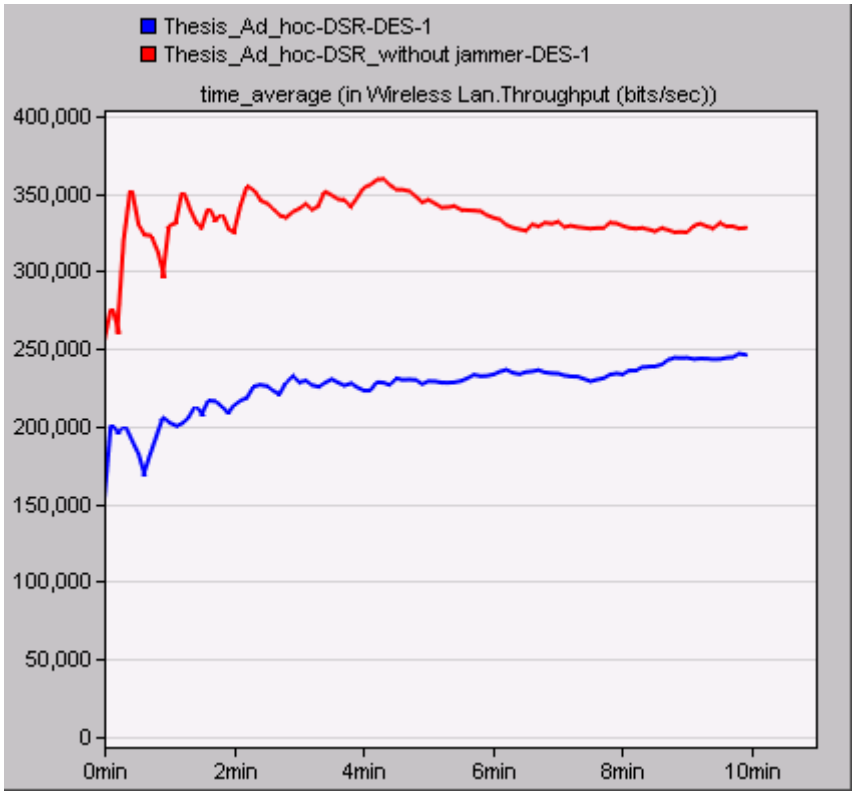


Figure 37. Throughput With/Without Jamming Attacks Using DSR Routing Protocol

In Figures 35 – 37, the red lines represent the throughput in the network without jammers, while the blue lines represent the throughput with jammers. After the random trajectory jamming attacks were launched in the network, throughput of the mobile node dropped in both networks. Throughput of the mobile node with the AODV routing protocol applied in the network dropped from an average of 1,100,000 bits/sec to 700,000 bits/sec; the TORA routing protocol reduced from 1,400,000 bits/sec to 700,000 bits/sec; while the experiment used DSR routing protocol dropped from 350,000 bits/sec to 225,000 bits/sec.

The TORA routing protocol had the best overall performance when applied in ad-hoc networks. When there were jamming attacks in the network, it maintained a satisfactory throughput. AODV also managed to maintain good data transmission. But when jamming attacks were not launched, it had a lower throughput in the network. The DSR routing protocol had the worst performance in the ad-hoc network compared to the AODV and DSR routing protocols.

CHAPTER 5 CONCLUSIONS AND FUTURE WORK

The goal of this research was to compare the performance of jamming attacks generated by differing types of jammers, and to compare ad-hoc routing protocols. The conclusions drawn from the research was divided in between three sections.

5.1 Jamming Attacks in WLANs

The research began from understood the elements that influence the performance of WLANs. Experiments were done in order to demonstrate that distance and power levels from the access points were the main factors that vary the throughput of nodes. The larger the distance between nodes and access points were, the weaker the signal would be. Also, the smaller the power of an access point was, the weaker the signal would be.

Jamming attacks launched by different jammers in WLANs were studied and analyzed. In Scenario 2, a pulse jammer was used in a client-server network. The result proved that jamming attacks did influence the communication between legitimate nodes. When a node traveled toward the pulse jammer, the throughput of the node dropped significantly. The data dropped by the node increased depending on the distance between the node and jammer. The closer the distance was, the more data was dropped. Also, the power level of the jammer varied the performance of the nodes as well. The more powerful a jammer was, the wider the influence would be.

A mobile jammer was utilized in a client-server network. The result of this experiment demonstrated how much jamming attacks can influence a network. The legitimate nodes received fewer packets while the mobile jammer was in close proximity, and communications returned to normal as the jammer traveled out of range.

5.2 Switching Channels to Avoid Jamming Attacks

Previous research had shown that the switch channel method in WLANs can avoid jamming attacks. This research also demonstrated that not every jamming attack can be avoided by switching the communication to another frequency. Three different jammers' attack performances were compared. Pulse jammers were superior within one channel. It caused the greatest impact on the network within one frequency. But pulse jammers could only be assigned to a single frequency. When communications between nodes were switched to another channel, single band jammers could not affect the network anymore. Sweep jammers worked best when channel switching was involved. No matter what frequency nodes transmitted at, sweep jammers could always influence communications.

5.3 Ad-Hoc Routing Protocols

In order to generate a real WLAN network and jamming attacks, random trajectories in both nodes and jammers were implemented. A comparison of 3 widely used ad-hoc routing protocols were drawn under the random trajectory jamming attacks. The TORA routing protocol had the best overall performance in the data transmission process in ad-hoc networks. It provided a more satisfying throughput in the network when jammers were not used in the network. Also, it remained a good data transmitter when random trajectory jamming attacks were launched in the network. The AODV routing protocol also provided a good transmission rate. Whether the situation included a jammer or not, the DSR routing protocol performed worse in comparison to other ad-hoc routing protocols. It provided one fifth of the throughput in the network than the TORA routing protocol, and it only contained less than one third of the throughput in the network when jammers were utilized.

5.4 Future Work

This research compared different jamming attacks in WLANs and their performances when the channel of communication was switched, as well as the performance of ad-hoc routing protocols. However, there was still much research that could be done in this area.

Jamming attack IDS: It was demonstrated that because not all the jamming attacks could be avoided by switching transmissions, jamming attacks are still a big problem in WLANs. A method of avoiding sweeping jamming attacks needs to be found. We believe that a method of detection can be found by developing a jamming attack IDS in the future.

Real world system jamming attacks: Random trajectory WLANs and jamming attacks were tested in the research, but other factors, such as physical obstructions, other magnetic field, Radio transmitting towers, and weather in real world can also influence the function of devices. Physical equipment based jamming attacks deserve to be tested.

Three ad-hoc protocols were tested in the research, but more protocols exist that require study. More routing protocols should be included and investigated.

REFERENCES

Acharya, M., Sharma, T., Thuente, D., & Sizemore, D. (2004, August). Intelligent Jamming in 802.11b Wireless Networks. *proceeding of OPNETWORK*.

Adaobi, O., & Ghassemian, M. (2010, December). Analysis of an Anomaly-based Intrusion Detection System for Wireless Sensor Networks. *1st international conference communications engineering*, 59-63.

Akyildiz, I. F., Wang, W., & Wang, W. (2005, January). Wireless mesh networks: a survey. *Computer Networks Journal*, *47*(4), 445-487.

Beg, S., Ahsan, F., & Mohsin, S. (2010, October). Engaging the Jammer on the Jammed Channel in MANET. *International Conference on Emerging Technologies*, *6*, 410-413.

Chaitanya, K. C., & Ghosh, A. (2010). Analysis of Denial-of-Service attacks on Wireless Sensor Networks Using Simulation. *Middlesex University*, 1-13.

Chiang, J. T., & Hu, Y. Cross-Layer Jamming Detection and Mitigation in Wireless Broadcast Networks. *IEEE/ACM Transactions on Networking*, *19*(1), 286-296.

Client Server Network: Advantages and Disadvantages. (2011, May). In *ianswer4u.com*. Retrieved April 2, 2012

Fu, Y., Yang, J., Xiao, P., Luan, L., & Peng, L. (2011, June). Research on Detection Scheme for Denial of Service Attacks in Wireless Mesh Networks. *International Journal of Digital Content Technology and its Applications*, *5*(6), 290-296.

Gast, M. (2005). *802.11 Wireless Networks: The Definitive Guide* (2nd ed., pp. 14-61). Sebastopol, CA: O'Reilly Media.

Healy, M., Newe, T., & Lewis, E. (2009, February). Security for Wireless Sensor Networks: A Review. *IEEE Sensor Application Symposium*, 80-85.

Hyun, S., Ning, P., & Liu, A. Mitigating Wireless Jamming Attacks via Channel Migration. *International Conference on Distributed Computing Systems Workshops, 31*, 313-322.

IEEE. (n.d.). *IEEE 802.11™: Wireless Local Area Networks (LANs)*. In . (Ed.). Retrieved April 2, 2012, from http://standards.ieee.org/about/get/802/802.11.html

Jeung, J., Jeong, S., & Lim, J. (2011). Anti Jamming – Based Medium Access Control Using Adaptive Rapid Channel Hopping in 802.11. *Graduate School of Ajou University*, 70-82.

Jiang, S., & Xue, Y. (2009, October). Providing survivability against jamming attack for multi-radio multi-channel wireless mesh networks. *Journal of Network and Computer Applications, 34*(2), 443-454.

Konstantinos, P., Iliofotou, M., & Krishnamurthy, S. V. (2011, April). Denial of Service Attacks in Wireless Networks: The case of Jammers. *Communications Surveys & Tutorials, IEEE, 13*(2), 245-257.

Ma, Y., Richards, M., Ghanem, M., Guo, Y., & Hassard, J. (2008). Air Pollution Monitoring and Mining Based on Sensor Grid in London. *Sensors*, *8*(6), 3601-3623.

Malhotra, R., Gupua, V., & Bansal, R. K. (2010, March). Simulation &Performance Analysis of Wired and Wireless Computer Networks. *Global Journal of Computer Science and Technology*, *XI*(III), 11-17.

Mark, C. (2005). *CWNA Guide to Wireless LANs* (2nd ed., pp. 1-544). Stamford, CT: Course Technology.

OPNET Technologies, Inc. (2012). *OPNET Modeler* (16.0 ed.). In . (Ed.). Retrieved April 2, 2012, from http://www.opnet.com/

Raymond, D. R., & Midkiff, S. F. (2008, January). Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses. *IEEE CS*, *7*(1), 74-81.

Reddy, K. S., Varadarajan, S., & Kumar, M. S. (2011, June). Improving QOS Under DDoS Attacks in Wireless Sensor Networks. *International Journal of Engineering Science and Technology (IJEST)*, *3*(6), 5057-5065.

Roos, D. (2007, June). How Wireless Mesh Networks Work. In *HowStuffWorks.com*. Retrieved April 2, 2012, from http://computer.howstuffworks.com/how-wireless-mesh-networks-work.htm

Soujanya, B., Sitamahalakshmi, T., & Divakar, C. (2011, April). STUDY OF ROUTING PROTOCOLS IN MOBILE AD-HOC NETWORKS. *International Journal of Engineering Science and Technology (IJEST)*, *3*(4), 2622-2631.

Wi-Fi channels (802.11b,g WLAN). (2007). In *Wikipedia*. Retrieved April 2, 2012, fromhttp://en.wikipedia.org/wiki/File:2.4_GHz_Wi-Fi_channels_(802.11b,g_WLAN).png

Xu, W., Zhang, Y., & Wood, T. (2005, May). The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks. *MobiHoc'05*, *3*(5), 1-12.

Yu, F. (2011, April). A Survey of Wireless Sensor Network Simulation Tools. In *Washington University in St. Louis, Department of Science and Engineering.* Retrieved April 2, 2012, from http://www.cse.wustl.edu/~jain/cse567-11/ftp/sensor/index.html

APPENDIX

Code of pulse source generator:

For the TX_ON state:

```
/* Begin a new transmission. */

/* Create a packet of size such that it will*/

/* occupy 'pulse on time' seconds on the channel.*/

pkptr = op_pk_create (pk_len);

if (pkptr == OPC_NIL)

        jam_pulse_error ("Unable to create jamming packet.");

/* Set the corresponding encapsulation bit to mark  */

/* this packet as a "jammer generated" packet.*/

op_pk_encap_flag_set (pkptr, OMSC_JAMMER_ENCAP_FLAG_INDEX);

/* Send the packet to the transmitter. */

op_pk_send (pkptr, 0);
```

For the TX_OFF

```
/* Schedule the start of the next pulse. */

evh = op_intrpt_schedule_self (op_sim_time () + silence_dur, 0);

if (op_ev_valid (evh) == OPC_FALSE)

        jam_pulse_warn ("Unable to schedule next pulse.");
```

Code of single band signal generator:

```
/* At this initial state, we read the values of source attributes*/

/* and schedule a selt interrupt that will indicate our start time*/

/* for packet generation.*/

/* Obtain the object id of the surrounding module.*/

own_id = op_id_self ();

/* Read the values of the packet generation parameters, i.e. the*/

/* attribute values of the surrounding module.*/

op_ima_obj_attr_get (own_id, "Packet Interarrival Time", interarrival_str);

op_ima_obj_attr_get (own_id, "Packet Size", size_str);

op_ima_obj_attr_get (own_id, "Start Time", &start_time);

op_ima_obj_attr_get (own_id, "Stop Time", &stop_time);

/* Load the PDFs that will be used in computing the packet*/

/* interarrival times and packet sizes.*/

interarrival_dist_ptr = oms_dist_load_from_string (interarrival_str);

pksize_dist_ptr              = oms_dist_load_from_string (size_str);

/* Make sure we have valid start and stop times, i.e. stop time is    */

/* not earlier than start time.*/

if ((stop_time <= start_time) && (stop_time != SSC_INFINITE_TIME))

        {

        /* Stop time is earlier than start time. Disable the source.    */

        start_time = SSC_INFINITE_TIME;

        /* Display an appropriate warning.*/
```

```
	op_prg_odb_print_major ("Warning from simple packet generator model
(simple_source):", "Although the generator is not disabled (start time is set to a finite value),", "a
stop time that is not later than the start time is specified.", "Disabling the generator.", OPC_NIL);
	}
/* Schedule a self interrupt that will indicate our start time for*/
/* packet generation activities. If the source is disabled,*/
/* schedule it at current time with the appropriate code value.*/
if (start_time == SSC_INFINITE_TIME)
	{
	op_intrpt_schedule_self (op_sim_time (), SSC_STOP);
	}
else
	{
	op_intrpt_schedule_self (start_time, SSC_START);
	/* In this case, also schedule the interrupt when we will stop*/
	/* generating packets, unless we are configured to run until*/
	/* the end of the simulation.*/
	if (stop_time != SSC_INFINITE_TIME)
		{
		op_intrpt_schedule_self (stop_time, SSC_STOP);
		}
	next_intarr_time = oms_dist_outcome (interarrival_dist_ptr);
	/* Make sure that interarrival time is not negative. In that   */
```

```
	/* case it will be set to 0.*/
	if (next_intarr_time <0)
		{
		next_intarr_time = 0.0;
		}
	}
/* Register the statistics that will be maintained by this model.*/
bits_sent_hndl = op_stat_reg ("Generator.Traffic Sent (bits/sec)",OPC_STAT_INDEX_NONE,
OPC_STAT_LOCAL);
packets_sent_hndl = op_stat_reg ("Generator.Traffic Sent
(packets/sec)",OPC_STAT_INDEX_NONE, OPC_STAT_LOCAL);
packet_size_hndl = op_stat_reg ("Generator.Packet Size (bits)", OPC_STAT_INDEX_NONE,
OPC_STAT_LOCAL);
interarrivals_hndl    = op_stat_reg ("Generator.Packet Interarrival Time (secs)",
OPC_STAT_INDEX_NONE, OPC_STAT_LOCAL);
```

Code of sweeping frequencies of sweep jammer:

```
/* Begin a new transmission. */

/* Compute the frequency of transmission.   */

freq_tx = freq_base + freq_slot * freq_interval;

/* Advance the frequency slot for next transmssion. */

freq_slot = (freq_slot + 1) % num_intervals;

/* Assign the selected frequency to the transmitter   */

/* channel. */

if (op_ima_obj_attr_set (txch_objid, "min frequency", freq_tx) ==

OPC_COMPCODE_FAILURE)

        jam_swproc_error ("Unable to set minimum frequency in transmitter channel.");

/* Create a packet of size such that it will occupy     */

/* 'dwell_time' seconds on the channel.*/

pkptr = op_pk_create (pk_len);

/* Set the corresponding encapsulation bit to mark  */

/* this packet as a "jammer generated" packet.*/

op_pk_encap_flag_set (pkptr, OMSC_JAMMER_ENCAP_FLAG_INDEX);

/* Send the packet to the transmitter. */

op_pk_send (pkptr, 0);
```