DECLARATION

I declare that this thesis entitled "Detection of Jamming Attack at Kolej Komuniti Masjid Tanah" is the result of my own research except as cited in the references. This thesis has not been accepted for any degree and is not currently submitted in the candidature of any other degree.

Signature: .....

Name: Haliza Binti Haron

Date: 11 January 2015

APPROVAL

I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in terms of scope and quality for the award of Master of Science in Security Science

Signature: …….....

Supervisor Name: Assoc. Prof. Dr Mohd. Faizal Bin Abdollah

Date: 11 January 2015

DEDICATION

I specially dedicate this thesis to my beloved husband,

"Mohd Fuad Bin Johari",

who has faith in me and

who has always staying with me,

despite all the pressure and stress I put him through during my study.

Dedication to "Hj. Haron Bin Johor" and "Hjh. Zainab Binti Samin",

who supported me throughout my study and who always prays for my success.

Dedication to my lovely kids,

"Danish" and "Dzaara",

Who always understand me during my hard time in completing my study

Dedicated to all my friends

who have always supported me in so many ways throughout my study.

ABSTRACT

Wireless network grows very fast; the flawed security of most of those networks becomes more apparent. People are extremely adopting to use wireless network to access Internet. The last ten years have seen an explosion in the use of wireless technology. The wireless network medium has become target to the attackers. This study will focus on jamming attack and the case study has been done at Kolej Komuniti Masjid Tanah (KKMT). This study will involve two important phases which are investigation and implementation phase. The investigation phase is the process of getting information from previous research to get an overview about the scope of the study. The simulation of the wireless network using Opnet Modeler has been done during implementation phase. The simulation is to get the result of the affected parameters that have been choosing in investigation phase. The results generated from the simulation process has analyze four parameters affected and can be used to detect jamming attack at KKMT are network load, delay, throughput and error rate.

ABSTRAK

Teknologi rangkaian tanpa wayar yang berkembang dengan pesat secara tidak langsung menyebabkan kelemahan keselamatan rangkaian tanpa wayar agak ketara. Rangkaian tanpa wayar juga menjadi satu keperluan yang sangat penting bagi masyarakat bagi mengakses internet. Teknologi rangkaian tanpa wayar telah mula popular dan berkembang pesat sejak sepuluh tahun yang lalu. Keadaan ini secara tidak langsung menjadikan rangkaian tanpa wayar menjadi sasaran kepada penyerang. Kajian ini akan memberi tumpuan kepada serangan 'jammimg' dan kajian kes telah dijalankan berdasarkan persekitaran rangkaian di Kolej Komuniti Masjid Tanah (KKMT). Kajian ini akan melibatkan dua fasa penting iaitu penyelidikan dan fasa pelaksanaan. Fasa penyelidikan adalah proses mencari maklumat megenai bidang kajian melaui kajian yang lalu untuk mendapat gambaran dan maklumat tentang skop kajian. Simulasi rangkaian tanpa wayar menggunakan Opnet Modeler telah dilakukan semasa fasa pelaksanaan. Simulasi ini adalah untuk mendapatkan hasil daripada parameter yang terlibat yang telah dipilih sewaktu fasa penyelidikan. Keputusan yang diperolehi daripada proses simulasi yang telah menunjukkan empat parameter terjejas dan boleh digunakan untuk mengesan serangan 'jamming' di KKMT adalah 'network load', 'delay', 'throughput' dan 'error rate'.

ACKNOWLEDGEMENT

Alhamdulillah, Thanks to Allah SWT, for giving me permission to complete this thesis. I would like to thank to all the support, encouragement and inspirations that I have received from everyone around me during completing my thesis.

I would like to express the greatest thanks and appreciation to my supervisor, Assoc. Prof. Dr. Mohd. Faizal Bin Abdollah for his valuable help, advices, patience and encouragement.

I thanks sincerely to my best companions, who had always given me strength and supports to complete this thesis, Sharina, Waheeda, Fauzi, Zatul, Aiza, Ruby Nadiya, Asmarizan, and Mawardy, who had always been cheerful and fun despite the difficulties encountered during our study.

Last but not least, I would like to convey my deepest gratitude and sincerest love to my life supporters, Mohd Fuad Bin Johari, Muhammad Danish Irfan and Dzaara Nur Rifhan, to my beloved parents Hj Haron Bin Johor and Zainab Binti Samin, sisters and brothers for their uncountable supports, prayers and encouragement.

TABLE OF CONTENTS

CHAPTER		PAGE
	DECLARATION	
	DEDICATION	
	ABSTRACT	**i**
	ABSTRAK	**ii**
	ACKNOWLEDGEMENTS	**iii**
	TABLE OF CONTENTS	**iv**
	LIST OF TABLES	**v**
	LIST OF FIGURES	**vi**
1.	**INTRODUCTION**	**1**
	1.1 Introduction	1
	1.2 Background of the Study	4
	1.3 Problem Statement	5
	1.4 Research Questions	6
	1.5 Research Objective	6
	1.6 Research Scope	6
	1.7 Importance of the Thesis	7
	1.8 Organization of the Thesis	7
	1.8.1 Chapter 1: Introduction	7

1.8.2 Chapter 2: Literature Review 8

1.8.3 Chapter 3: Research Methodology 8

1.8.4 Chapter 4: Implementation 8

1.8.5 Result and Discussion 9

1.8.6 Conclusion 9

1.9 Summary 9

2. LITERATURE REVIEW 10

2.1 Introduction 10

2.2 Wireless History 10

2.3 Wireless Standards 13

2.4 WLAN Components 14

2.4.1 Access Points 15

2.4.2 Network Interface Cards / Client Adapters 15

2.4.3 Antenna 15

2.5 How WLAN Works 16

2.6 The Weaknesses of WLAN 18

2.6.1 Security 18

2.6.2 Range 18

2.6.3 Reliability 18

2.6.4 Speed 19

2.7 The Importance of Security in WLAN 19

2.8 Wireless Security Protocol 20

2.8.1 Wired Equivalent Privacy (WEP) 20

2.8.1.1 WEP Authentication 23

2.8.2 Wi-Fi Protected Access (WPA) 26

2.8.3 Wi-Fi Protected Access 2 (WPA2) 27

2.9 Methods of Attacking Wireless Network 29

2.9.1 Access Point Unauthorized Access 29

2.9.2 Information Eavesdropping / Interception 29

2.9.3 Data Changes / Replacement 30

2.9.4 Signal Interference / Inhibition 30

2.9.5 Denial of Service 31

2.9.5.1 Jamming Attack 31

2.10 Detecting Jamming Attack 36

2.10.1 Packet Delivery Ratio (PDR) 36

2.10.2 Packet Send Ration (PSR) 37

2.10.3 Bad Packet Ration (BPR) 38

2.10.4 Channel Utilization 38

2.10.5 Carrier Sensing Time (CST) 38

2.10.6 Jamming to Signal Ratio 39

2.10.7 Signal Strength (SS) 39

2.10.8 Signal to Noise Ratio (SNR) 40

2.10.9 Network Throughput 40

2.11 Propose Work 47

	2.12 Summary	48
3.	**RESEARCH METHODOLOGY**	**49**
	3.1 Introduction	49
	3.2 Research Methodology	51
	3.2.1 Phase One: Define Problem Statement	51
	3.2.2 Phase Two: Literature Review	51
	3.2.3 Phase Three: Analysis	53
	3.2.4 Phase Four: Design	53
	3.2.4.1 Simulation Tool: OPNET Modeler	53
	3.2.5 Phase Five: Project Simulation	54
	3.2.5.1 Project Simulation Workflow	55
	3.2.6 Phase Six Data Analysis	56
	3.3 Summary	56
4.	**IMPLEMENTATION**	**57**
	4.1 Introduction	57
	4.2 Create the Project	57
	4.3 Configure the Application Definition and Profile Definition	59
	4.4 Create the Scenario	61
	4.4.1 Scenario 1	62
	4.4.2 Scenario 2	64
	4.4.2 1 Jammer	65
	4.4.4.2 Antenna Pattern	67

4.4.2.3 Trajectory 68

4.5 Select Statistic of Interest 68

4.6 Summary 69

5. RESULT AND ANALYSIS 70

5.1 Introduction 70

5.2 Demonstration of Results 71

5.3 Global Statistics 71

5.3.1 Network Load 72

5.3.2 Delay 73

5.4 Object Statistics 75

5.4.1 Throughput 75

5.4.2 Error Rate 77

5.5 Summary 80

6 CONCLUSION 81

6.1 Introduction 81

6.2 Concluding Remarks 81

6.3 Research Contribution 82

6.4 Future Recommendation 83

REFERENCES

APPENDICES

LIST OF TABLES

TABLE	TITLE	PAGE
2.1	Wireless Evolution	11
2.2	IEEE Standards	13
2.3	Comparison of WPA, WPA2 and WEP	28
2.4	Characteristics of Various Jammers	34
2.5	PSR / PDR for Jamming	35
2.6	Summary of Wireless Jamming Attack Literature Review	41
2.7	Comparative Study of Existing Parameter	46
3.1	Project Methodology	56
4.1	Application Definition Profile	59
4.2	Characteristics of the Nodes	60
4.3	Project Scenario Details	61
4.4	Workstations & Access Point Characteristics	63
4.5	Transmitter Power Attributes	66
5.1	Simulation Performance Metrics	71
5.2	Wireless LAN Network Load Statistics	72
5.3	Wireless LAN Delay Statistics	74

5.4 Throughput Statistics 76

5.5 Error Rate Statistics 78

5.6 Comparison of Affected Parameters under Jamming Attack 79

LIST OF FIGURES

FIGURE	TITLE	PAGE
2.1	WEP Encryption Process	21
2.2	WEP Decryption Process	22
2.3	Open Key Authentication Process	23
2.4	Shared Key Authentication Process	25
2.5	RTS/CTS Standard of CSMA/CA	27
3.1	Project Scenario	50
3.2	Phase Two Components	52
3.3	Project Simulation Workflow	55
4.1	Wireless Project	58
4.2	Scenario 1 Network Diagram	62
4.3	Scenario 2 Network Diagram	64
4.4	The Components of Jammer	65
4.5	Jammer Process Model	65
4.6	3D Antenna Pattern	67
4.7	Jammer Trajectory Parameter	68

CHAPTER 1

INTRODUCTION

1.1 Introduction

Wireless network transmission process is through the air, this situation increase the possibilities of attack are more high in wireless network compare to wired network. The communication through wireless network also has a high risk of being interrupted by the attackers in the signal range. The interceptions of wireless network are difficult to detect, this resulted to the high cases of sniffing activities by attacker and the owner or the network administrator are not aware of attackers activities. The low security of Wired Equivalent Privacy (WEP) encryption makes it easy to crack. There are thousands of software available to crack WEP keys. The very challenging issue is how the hacker can find the access point key and share the bandwidth.

The main security issue should cover by wireless network is by defending the network from unauthorized access and eavesdropping by increasing the confidentiality (Lashkari, Mohammad, et al. 2009) . Besides that, the integrity of the data needs to be protected from the man in the middle attack. The security issues that always being discussed regarding wireless network are:

i. **Access:** this issue referred to the access control using wireless security protocols such as WPA/WPA2. This is to make sure only authorized user can access to wireless network. The improper access control will encourage the attack from the surrounding area.

ii. **Privacy:** the attackers can sniff the data transfer or communication during the transmission process. There are very important to ensure that the wireless emvironment is safe from the sniffing activities.

Wireless network is exposed to jamming attacks. Jamming is defined as the emission of radio signals aiming at disturbing the transceivers' operation. The objective of a jamming attack is to interfere with legitimate wireless communications. The goals are either preventing a real traffic source from sending out a packet, or by preventing the reception of legitimate packets. The jamming attack is one of the security threats that can lead to great damage in the real world. Jamming is one of DoS attacks which is used in wireless networks, where an attacker is respects the medium access control (MAC) protocol and transmits on the shared channel either continuously or periodically to target all or some communication respectively.

The most efficient and easy way to interfere the communication of two parties by using jamming method (Wang & Wyglinski 2011). Continuous jamming has been used as a denial-of-service (DoS) attack against voice communication since the 1940s (Divya & Gosul 2012). All wireless networks, regardless of security features, are prone to this type of attack. Radio frequency jamming may have been first used in World War II. False instructions would be broadcast to enemy pilots to confuse them.

Nowadays, internet is like a heart of a life. Everything in this world need to the internet access. Many activities would be stuck if there are no internet accesses. There are variety of activities that rely on internet connection.

There are different methods use to connect to the internet either using cable, DSL or wireless devices. The configurations of wireless devices are simpler and easy compare to the wired services. The importance's of the internet at the same time increase the risk to the user. The secret informations can easily being stealing by the irresponsible person. These risks are not taking seriously by certain internet user.

Wireless networks are not having any fixed infrastructure so that any number of hosts can enter and leave the network at anytime(Dorus 2013). The mobility of wireless network makes it more popular compare to wired network. Wireless network also increase the business productivity. The use of wireless network will decrease the network installation cost.

The IEEE 802.11 wireless Ethernet standard has solved the big issues of single-vendor proprietary problem in 1997, where the product of different vendors cannot communicate with each other. The standards permit the communication between different wireless products from different vendors (Shukla et al. 2010). 802.11a, b and g is the well known and most commonly use standards (Ali et al. 2011). 802.11a is an extension to 802.11 that applies to wireless LANs and provides up to 54-Mbps in the 5GHz band. 802.11a uses OFDM (Orthogonal Frequency Division Multiplexing), where it will not face any problem in performing multitasking job at

once although during crowded time. 802.11b (also referred to as 802.11 High Rate or Wi-Fi) is an extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission in the 2.4 GHz band. 802.11b has the straight addition of modulation technology same as in 802.11.Mostly 802.11b suffered from the intrusion of other products. 802.11g applies to wireless LANs and is used for transmission over short distances at up to 54-Mbps in the 2.4 GHz bands. 802.11g was authorized in 2003 as a third modulation device with 2.4 GHz band. It provide maximum data rate with 54Mbit/s at physical layer. The hardware of 802.11g is totally compatible with 802.11b. 802.11n recognized in 2009 as a final endorsement in 802.11 Standards family. All type of enterprises was previously transferred to 802.11n networks. These all enterprises based on Wi-Fi Alliance's. Wi-Fi is a certified product for 802.11n application to make 802.11 standard families more useful and compatible to new era because Wi-Fi fulfill the requirements of new era where no need to spend time for the arrangement of wires or cables and so on.

1.2 Background of the Study

Current wireless network is vulnerable to many attacks, hackers can break wireless network security protocols and access protected wireless without owner’s knowledge. Wireless networks make use of shared transmission medium; therefore, they are open to several malicious attacks. Since a large number of people had been adopted extremely using Internet through wireless connection, security is one of the notable problems.

Jamming attack is one of the wireless attacks that can disrupt wireless communication by generating high-power noise across the entire bandwidth near the transmitting and receiving nodes. Jamming attack can drastically reduce the wireless network performance.

Kolej Komuniti Masjid Tanah (KKMT) is one of the education centers that provided with wireless connection environment. Wireless network nodes transmit data packets in different channels. Channels in WLAN technologies are defined as frequencies, and it has risk to malicious jamming attack. There are many effects and defense strategy has been study to overcome jamming attack. However, each method is suitable for only a limited range of network(Li et al. 2012). Therefore, the proper technique to detect jamming attack for KKMT needs to be study in order to protect the wireless environment from jamming attack.

1.3 Problem Statement

The medium of wireless networks make it easy to be attack (Pelechrinis et al. 2011). There are many parameters used to identify the performance of wireless network. Stated in (Sufyan et al. 2013) that the detection of jamming attack base on single parameter is not accurate. Therefore, the suitable parameters that suite with KKMT wireless network environment need to be define

1.4 Research Questions

Based on the background of the study and the problem statement, the research questions in this study are as follows:

i. How to identify jamming attack?

ii. What are the affect of jamming attack to KKMT wireless network?

1.5 Research Objective

i. To study jamming attack categories.

ii. To identify and select the parameter to detect jamming attack.

iii. To analyze the affects of jamming attack to KKMT wireless network.

1.6 Research Scope

The study will focus on KKMT wireless network as case study. Wireless network are susceptible to malicious jamming attack. Jamming attack can disrupt the wireless network and it will reduce the work effectiveness among staffs and students.

1.7 Importance of the Study

At the present time there are so many attacks against wireless network including KKMT. The jamming attack is one of the vulnerabilities that will disrupt the network. Identifying the suitable parameter in detecting jamming attack will help increasing the KKMT network performance.

1.8 Organization of the Thesis

This study provides six chapters of the project report. The report structure is as follows:

1.8.1 Chapter 1: Introduction

Chapter 1 is the introduction part of this study. The background of study is briefly explained in this chapter followed by problem statement, research question, research objectives, research scope and importance of the study.

1.8.2 Chapter 2: Literature Review

Chapter 2 contains the literature review part. In this chapter, the related study to jamming attack will be explained in more details. The in depth study on parameters regarding jamming attack base on previous research will be held in this chapter. All references such as books, journals and papers that are related in getting information regarding this research will be use.

1.8.3 Chapter 3: Research Methodology

Chapter 3 is the methodology of this study. This chapter discussed about the methodology that have been chose to achieve the research objectives. The flow of the process in completing the project will discuss in details. The research design is important in order to ensure the successful of the project implementation.

1.8.4 Chapter 4: Implementation

Chapter 4 is about implementation where the focus in on the process of completing the project simulation until the result is successfully generated. In this chapter the actual implementation of the research method will discuss to get the needed result. The step by step of the implementation will be included.

1.8.5 Chapter 5: Result and Discussion

Chapter 5 is describing about result from the simulation phase in chapter 4. The output generated will be analyze and discuss for the process of verification and validation for all the data in the previous chapter.

1.8.6 Chapter 6: Conclusion

Chapter 6 will be the conclusion of this study. This section will provide a conclusion and summarize all the content of this report and also provides some suggestion and recommendation for future work.

1.9 Summary

This chapter provides the whole overview of the project. The background of study, problem statement, research question, research objectives, research scope and Importance of the study are stated. In the next chapter, the literature review related to wireless network and jamming attack will be explained in details.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter covers several literature reviews about wireless local area network (WLAN) security and jamming methods issues. The literature search is a very significant step in the research process. (Liu & Houdek 2006) stated that many people out there face the same problem. The literature review gives the overall understanding regarding the topic of the research base on the previous studies that have been made. This chapter is very important in order to make sure there are no similarity in the research topic and at the same time to develop a better understanding about the research scope.

2.2 Wireless History

More than 100 years ago, an Italian physicist and inventor name Guglielmo Marconi (Raychaudhuri & Mandayam 2012) was the first person to successfully transmit information over radio waves. Since that, wireless technology has gone through the revolution in line with computer technology revolution. Table 1 below shows a timeline for wireless technology evolution (Technologies 2003):