SECURITY PERFORMANCE ANALYSIS IN WIRELESS LANS

NURUL ANIS ANATI BINTI SARIPUDIN

Bachelor of Computer Science (Computer Systems & Networking)

UNIVERSITI MALAYSIA PAHANG

UNIVERSITI MALAYSIA PAHANG

DECLARATION OF THESIS AND COPYRIGHT

Author's Full Name : NURUL ANIS ANATI BINTI SARIPUDIN

Date of Birth : 961113-26-5156

Title : SECURITY PERFORMANCE ANALYSIS IN WIRELESS LANS

Academic Session : 2015/2016

I declare that this thesis is classified as:

☐	CONFIDENTIAL	(Contains confidential information under the Official Secret Act 1997)*
☐	RESTRICTED	(Contains restricted information as specified by the organization where research was done)*
☑	OPEN ACCESS	I agree that my thesis to be published as online open access (Full Text)

I acknowledge that Universiti Malaysia Pahang reserves the following rights:

1. The Thesis is the Property of Universiti Malaysia Pahang
2. The Library of Universiti Malaysia Pahang has the right to make copies of the thesis for the purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange.

Certified by:

_____
(Student's Signature)

961113-26-5156
Date: 26 December 2018

_____
(Supervisor's Signature)

Dr. Luhur Bayuaji
Date: 26 December 2018

NOTE : * If the thesis is CONFIDENTIAL or RESTRICTED, please attach a thesis declaration letter.

THESIS DECLARATION LETTER (OPTIONAL)

Librarian,
Perpustakaan Universiti Malaysia Pahang,
Universiti Malaysia Pahang,
Lebuhraya Tun Razak,
26300, Gambang, Kuantan.

Dear Sir,

CLASSIFICATION OF THESIS AS RESTRICTED

Please be informed that the following thesis is classified as RESTRICTED for a period of three (3) years from the date of this letter. The reasons for this classification are as listed below.

Author's Name
Thesis Title

Reasons (i)

(ii)

(iii)

Thank you.

Yours faithfully,

_____
(Supervisor's Signature)

Date:

Stamp:

Note: This letter should be written by the supervisor, addressed to the Librarian, *Perpustakaan Universiti Malaysia Pahang* with its copy attached to the thesis.

SUPERVISOR'S DECLARATION

I hereby declare that I have checked this thesis and in my opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Bachelor of Computer Science (Computer Systems & Networking).

(Supervisor's Signature)

Full Name : Dr. Luhur Bayuaji

Position : Senior Lecturer

Date : 26 December 2018

STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Universiti Malaysia Pahang or any other institutions.

(Student's Signature)

Full Name : Nurul Anis Anati Binti Saripudin

ID Number : Ca15087

Date : 26 December 2018

SECURITY PERFORMANCE ANALYSIS IN WIRELESS LANS

NURUL ANIS ANATI BINTI SARIPUDIN

Thesis submitted in fulfillment of the requirements
for the award of the degree of
Bachelor of Computer Science (Computer Systems & Networking)

Faculty of Computer Systems & Software Engineering

UNIVERSITI MALAYSIA PAHANG

DECEMBER 2018

ACKNOWLEDGEMENTS

All praise to the Almighty ALLAH S.W.T for His blessing which has given me strength, patience and wisdom and ability during the final year project developing period. Sincere thanks to the God for giving me the opportunity to complete this project on time.

I would like to express my deepest appreciation to all those who provided me possibility to complete this project. A special gratitude to I give to my supervisor, Dr. Luhur Bayuaji for his insightful comments, outstanding advice and suggestions, spend time and helped me to coordinate my project especially in writing this thesis report.

Furthermore, I would like also to acknowledge with much thanks and appreciation to my friends for sharing their good idea and knowledge with me, in order to assist myself to succeed this project. I have to appreciate the guidance given by other supervisors as well as the panels and all lecturers throughout the completion of this project. Moreover, I am very grateful to both of my family for their love and endless support.

ABSTRAK

Protokol keselamatan telah dilaksanakan dalam rangkaian untuk memastikan bahawa data yang dihantar adalah dalam integriti dan keselamatan. Oleh itu, eksperimen ini adalah untuk menganalisis protokol keselamatan dalam prestasi WLAN berdasarkan piawaian IEEE 802.11 g / n. Eksperimen ini dijalankan menggunakan testbed untuk mengukur prestasi LAN tanpa wayar dari segi throughput dan purata tangguhan. Ia juga akan mengkaji interaksi antara lapisan keselamatan yang berlainan dan prestasi kesan mereka rangkaian sesak dan tanpa jujukan. Kajian ini juga akan menilai kesan UDP terhadap prestasi rangkaian di bawah protokol keselamatan yang berbeza.

ABSTRACT

The security protocol has been implemented within the network to ensure that the data sent is in integrity and security. Therefore, this experiment is to analyze the security protocol in performance of WLANs based on the IEEE 802.11 g/n standard. This experiment is conducted using a testbed to measure wireless LAN performance in terms of throughput, and average delay. It will also study the interaction between different security layers and their effect performance of congested and uncongested networks. This research will also evaluate the effect of UDP on the network performance under different security protocols.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AES	Advanced Encryption Security
AP	Access Point
BSS	Basic Service Set
CBC-MAC	Cipher Block Chaining Message Authentication Code
CCMP	CBC-MAC Protocol
CMD	Command Prompt
CRC	Cyclic Redundance Unit
DSSS	Direct Sequence Spread Spectrum
ESS	Extended Service Set
ICV	Integrity Check Value
IV	Integrity Value
MIC	Michael or Message Integrity Code
MIMO	Multiple Input, Several Output
MPDU	MAC Protocol Data Unit
NR	Non-Roaming
OFDM	Orthogonal Frequency Division Multiplexing
RC4	Rivest Cipher 4
SDLC	System Development Life Cycle
SSID	Service Set Identifier
TKIP	Temporal Key Integrity
TP	Throughput
UDP	User Diagram Protocol
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WEP	Wired Equivalent Privacy

WLANs	Wireless Local Area Network

CHAPTER 1

INTRODUCTION

1.1 Background of Study

Wi-Fi abbreviated term for Wireless Fidelity which is general terms that referring to the IEEE 802.11 standard for Wireless Local Network or WLANs. WIFI is an alternative network for devices to connect in wireless mode rather than using the wired network. A local wireless network (WLAN) is a wireless distribution method for two or more devices using high- frequency radio waves, which often have an Internet access point. A WLAN enables users to move around the coverage area, often at home or in small office, while maintaining a network link. Sometimes a WLAN is called a local wireless network (LAWN). Development of WLAN standards based on the IEEE publication is 802.11a, 802.11b, 802.11g, and 802.11n where each standard has strengths and weaknesses in his application.

In WLANs around the world, security remained a major concern. Wireless networks offer comfort and flexibility, but they also increase network vulnerability. Security threats such as unauthorized access, denial of service attacks, spoofing of IP and MAC, hijacking and eavesdropping session can all be problems for WLANs. Various standard authentication and encryption techniques are combined with other access control mechanisms to address these threats. Collectively, these protocols, devices and techniques ensure the WLAN is equal to and even exceeds wired LAN security.

WEP (Wired Equivalent Privacy): An old standard for encryption used to overcome threats to security. WEP provides WLAN security by encrypting the information transmitted via the air so that only the receivers with the correct encryption key can decrypt the information. WPA (WI-FI Protected Access): Improved on the WEP by introducing Temporal Key Integrity Protocol (TKIP). While RC4 encryption is still

used, TKIP uses a temporal encryption key that is regularly renewed to make it harder to steal. Furthermore, the integrity of data has been improved through by using a more robust hashing mechanism. WPA2 (Wi-Fi Protected Access 2): improved on the WPA by introducing AES encryption algorithm. The AES is used in CBC-MAC Protocol (CCMP) to protect integrity and confidentiality in connection with AES key schedule. The CCMP use eight MIC bytes that are much stronger than Michael. Unlike WEP and TKIP, ICV is no longer needed.

The focus of the project is to examine the effect of security running on Wireless LANs. The project is test on the testbed in non-roaming network. Non-roaming network is access point (AP) and the clients are on the same network. While for roaming network, there are communication users in foreign networks for roaming network.

1.2 Problem Statement

Several security protocols and mechanisms to improve WLAN security are being developed. The implementations of security protocols therefore have an impact on network performance. However, there are no details on the extent to which degradation of network performance is affected by the security protocols in non-roaming networks.

Although the firmware of most wireless NICs can limit the interface for composing 802.11 standard packets, an attacker can still control any packet field using known techniques. It is therefore reasonable to assume that an attacker can generate any selected packet, modify packet's content, and fully control the packet's transmission.

At present, the wireless LAN system has a limited bandwidth, a longer response time and the wireless media is prone to error. This is caused by factors such as nature of the physical medium (air) itself, the number of users, the latency, the propagation factors like range and multipath. These can reduce LAN wireless performance.

1.3 Objective and Aim

The following are the objectives of this study to analyse the security performance in wireless LANs:

i. To compare the technique in Wi-Fi security protocol.

ii. To evaluate the effect of performance WLAN (IEEE 802.11g/n) for various security protocols

iii. To identify the effect of uncongested and congested network on UDP traffic stream.

1.4 Scope

The scope for the research is for the user that uses the wireless LANs to communicate with each other. The user who acts as a sender must be in one network to be able to send the data that they want to the receiver. The access point has the built-in DHCP server. It will assign the IP address to the devices that connect to the Wi-Fi.

The packet that sends from sender to receiver is capture by the Wireshark. The sender will generate the packet using TFGEN. This testbed is implemented in Windows 10.

1.5 Significance

The important of this analysis is to ensure your system meets security and performance requirements by conduct wireless LAN (WLAN) testing. Next, it can help the designers to choose which security protocol can be implemented in a given network scenario.

1.6 Thesis organization

Chapter 1 consists of the project introduction, which is the general introduction. Then the related problem statement continued. The objectives of the project are also clearly stated in conjunction with the aim. Finally, the project's scope to show the related field according to project title.

Chapter 2 is the review of the project literature. In this chapter, information on the research study in general is described.

Chapter 3 deals with the methodology of research used to develop this project. In this chapter, phases such as planning, analysis and design are required. The used software and hardware will also be explained.

Chapter 4 literally deals with implementation, testing and discussion of results. In addition, there will be a model for the project flow and also some data collection for research process. This chapter for PSM II will be done next semester.

Chapter 5 is the last chapter that deals with the entire work required for PSM II and concludes the entire project from the beginning.

CHAPTER 2

LITERATURE REVIEW

2.1 Overview

In Chapter 1, we discussed the introduction of research which consists of the problem statement, the objective and the scope. In this chapter, we will discuss on the relevant literature review to understand about the system technology and how the security performance analysis process in WLANs is carried out. It will therefore be developed to justify the current work.

2.2 Security Protocols

There are three security protocols that have been developed. Below are the descriptions of the existing systems that have been implemented before. These are Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and Wi-Fi Protected Access 2 (WPA2).

2.2.1 WEP

The objective of this protocol is to provide security in line with the level of security mechanisms for wired wires. In addition, it is used to protect the MAC Protocol Data Unit (MPDU). WEP employs RC4 (Rivet Cipher 4) algorithm from RSA Data Security to decrypt MPDUs and CRC-32 on the data link layer. RC4 is an algorithm to generate keys to encrypt from plain text to cipher text. RC4 is always mistaken as encryption algorithm. It is a flowchart and consists of 24-bit vector start (IV) combined with a key to be a packet key. RC4 is very fast and use small amount of energy source due to the insufficiency count of cycle.

For CRC-32 which also known as Cyclic Redundancy Check, this is a method to detect error by using redundant bits to hold information about the amount and level of bits in packet delivered. CRC-32 is used to calculate the Integrity Check Value (ICV) against MPDU and to ensure the integrity of the data. The 32-bit of ICV will be combined at the end of MPDU before it is been encrypted. MPDU and IV will be encrypt using per-pack key. IV and ID keys will be merged in front of MPDU making it as WEP Protocol Data Unit.

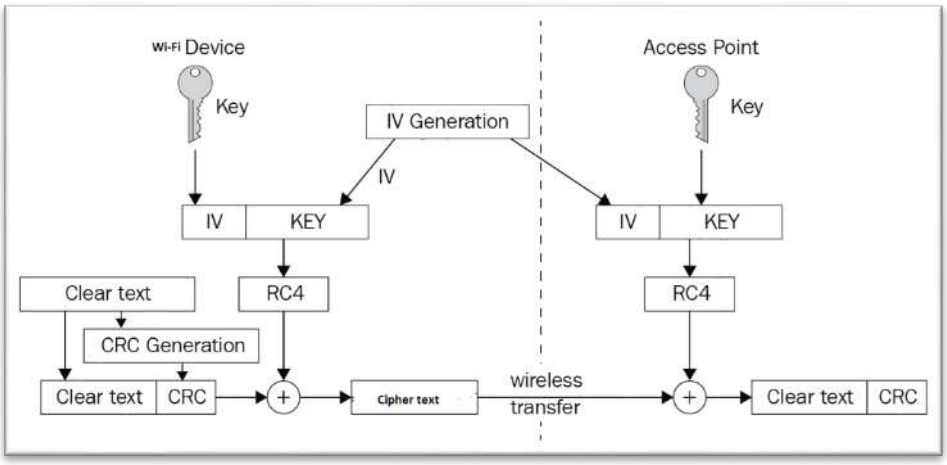


Figure 2.1 WEP Mechanism

Referring to Figure 2.1, before transmission of data happen, the Wi-Fi device or the sender will have one key ID which same with the access point or receiver. IV (24 bits) and key (40 bits) will be merged together to become a packet key of 64 bits. The key will processed through RC4 algorithm to generate random numbers. The plain text contains MPDU and ICV. That plain text undergoes or exclusive with a random number that has been generate before with RC4. Thus, cipher text will generate to send to the recipient.

On the receiving side, the received text will be decrypted into plain text. It is a reverse process on the sender's side. The received text will undergo OR EXCLUSIVE with the same packet key to become plain text. The CRC will calculate whether the received ICV is the same as delivered by the sender.

2.2.1.1 Authentication

WEP security consists of two, authentication and encryption parts. Encryption parts already discussed at the above. WEP Authentication means authentication of a device when it join the LAN first. The wireless networking authentication process using WEP prevents devices/stations from joining the network unless they now the key.

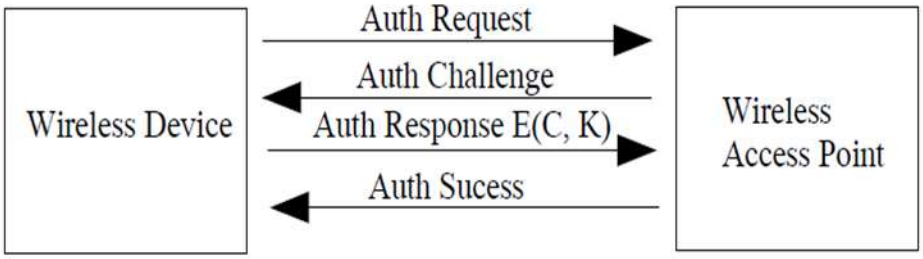


Figure 2.2 WEP Authentication

2.2.2 WPA

The security mechanism of second mechanism to provide more reliable communication is 802.11i, but a short-term solution called WPA was developed. In this solution, the Temporary Key Integrity Protocol (TKIP) was designed as a WEP patch. TKIP requires two distinct of keys namely 64 MIC and 128 bits for combining functionality to generate an encryption key per packet. The elements that contained in this algorithm are Michael or Message Integrity Code (MIC), packet sequencing disciplines and per-packet mixing functions.

Referring to Figure 2.3, in brief, Michael will calculate the Message Integrity Control (MIC) key and combined with MPDU. This MIC replace the RC4 that found in the WEP. Basically, the RC4 and MIC have similar function. Normal text will consist of MPDU and MIC will be placed in pieces and next combined with sequence parcel numbers. Temporal keys and MAC address will undergo first phase mixing to produce intermediate keys and continue with the second phase mixing to produce per-pack WEP key. The key is used by RC4 to generate keys to encrypt pieces.

Message Integrity Control (MIC) works to protect the integrity of a data. It uses 64 bit size of key and shifts, exclusive ORs, and addition. Every 32-bit block is processed into two 32-bit registers representing the final output, a 64-bit authentication tag. MIC are sent to the recipients as tag with the data. MIC that tied to the data will be recalculated

by the receiver. If the two tag match then data will received as authentic by receiver, if not the data will rejects as a forgery.

Per-packet mixing function is intended to produce more random keys. Basic key (encryption key), MAC address transmitter and input packet sequence numbers. The output is also new WEP is key per-packet. The mixing function is divided into two steps to minimize the calculation requirement, namely the non-linear substitution table, and the intermediate value is mixed. Combining the base key, the MAC transmitter address and the four most important bytes of the packet sequence number for the first phase to generate an intermediate value. Then, the intermediate value for the second phase is combined with smaller bytes of the packet sequence number to produce the key per packet.

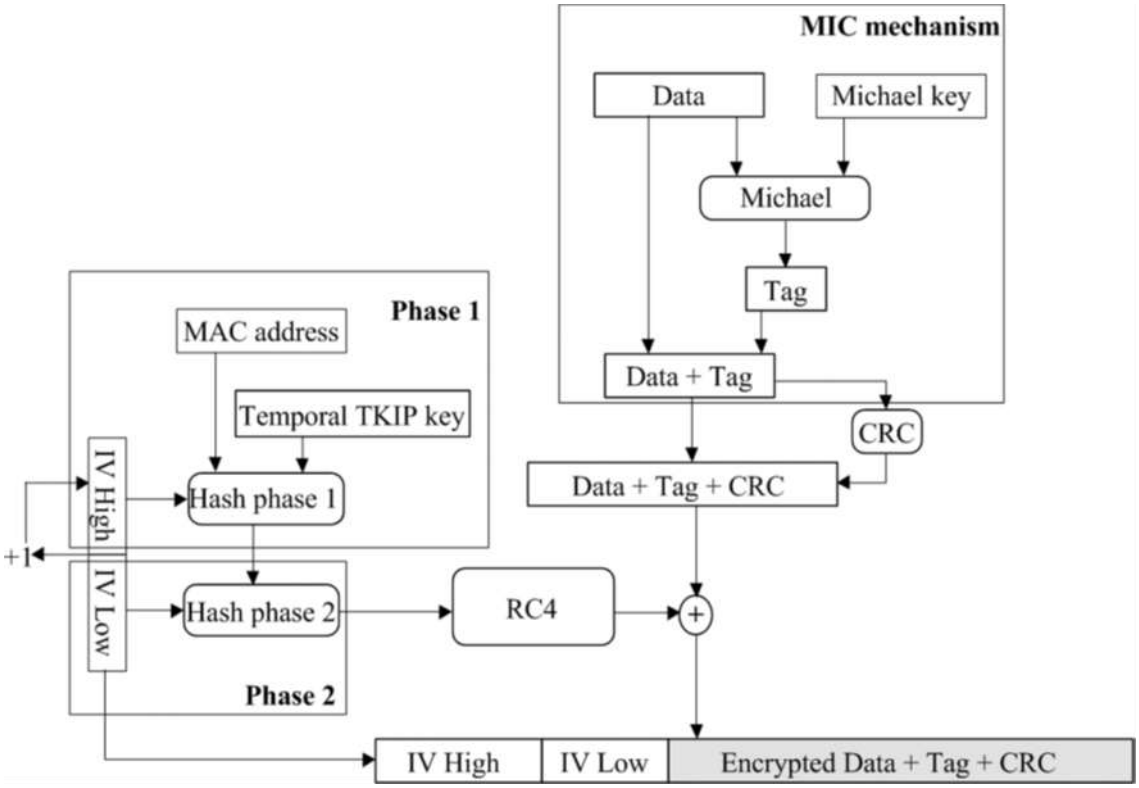


Figure 2.3 WPA Mechanism

2.2.3 WPA2

WPA2 enhances WPA with stronger cryptographic properties such as the CBC-MAC Protocol Counter Mode (CCMP) using AES encryption algorithm.

The CCMP uses the 48-bit IV as a sequence number to contribute detect replays. This protocol ensures the lifecycle of AES keys is prolonged. Two widely used CCMP techniques are counter mode for encryption and the Cipher Block Chaining Message Authentication Code (CBC-MAC) for the protection of integrity. Unlike TKIP, CCMP uses the same key for confidentiality and integrity, which uses two different key for both processes.

The encryption algorithm that used in this CCMP is Advanced Encryption Standard (AES). AES prelude a need for a packet key because CCMP does not have a key function per packet. The AES key is used in CCMP to protect integrity and confidentiality in connection with the AES key schedule. The CCMP use eight MIC bytes that are much stronger than Michael. Unlike WEP and TKIP, ICV is no longer needed.

Referring to Figure 2.4, a sequence packet number is required to build IV and counter (CTR). The sequence packet function to check if the packet received is new or repeated packet. IV is used in CB to generate random number for the first encryption because the following encryption will depend on the random number that has generated before. Basically, IV is used to calculate the MAC using AES algorithm. CTR is used for encryption. The plain text that have combined with the sequence packet number will be encrypted in CBC mode and the resulting of the last block is MAC in 128-bit size. The following MAC will be combined with the plain text. The values (CTR) have been established. Therefore, the text that consists of plain text, sequence packet number and MAC will be encrypted in counter mode and resulting of cipher text.

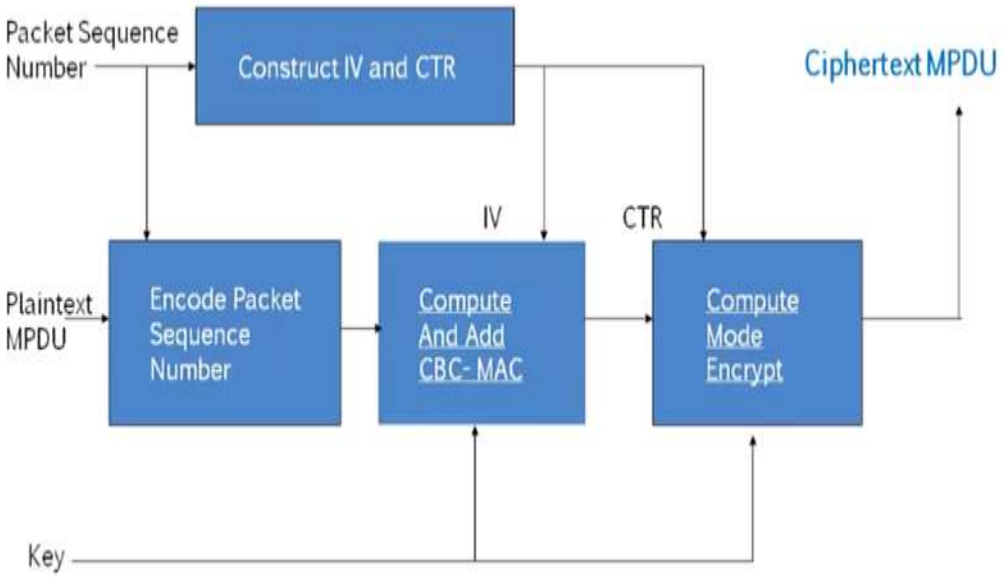


Figure 2.4 CCMP Mechanisms

Table 2.1 Comparative Analysis of WLAN

	WEP	**WPA**	**WPA2**
Authentication	Open authentication and key authentication is shared (use same key for encryption)	Key authentication is shared and have strong authentication that based on 802.1x and EAP	Authentication based on 802.1x and EAP and pre-authentication, RSNA
Encryption	Thoroughly researched and documented deficiencies	All WEP deficiencies is removed	WEP and WPA deficiencies are removed
	40 bit key	128 bit key	128 bit key
	Use same key	Does not use the same key	
	Use RC4 algorithm encryption		Use AES algorithm encryption
Integrity	CRC32	MIC	CBC-MAC

2.3 Encryption Method

In each of the security protocol, there is an encryption algorithm that implemented on the security protocol. The encryption algorithm that use are RC4 and AES algorithm.

2.3.1 RC4

RC4 is the best most familiar of all sequential systems. It uses variable value keys and is oriented to bytes. It is a very simple and easy-to-use algorithm. The key length variable between 1 to 256 bytes is used to initialize the 256 bytes S array. It contains all 8 permutations, from 0 to 255. It also produce stream K encryption and decryption of stream K by selecting one of the 255 unique stream conditions.

There are three execution phase in RC4 algorithm

i. Initializing of S array

- In the ascending hierarchy, it is initialized with values from 0 to 255. For instance, S (0) = 0 until S (255) = 255. On the same time, T array fields are filled with K key value depending on the initialization point and key length.

ii. Initial permutation of S array

- It uses the T array by swapping the S (i) value with the S (j) value, where the T array calculates the j.

iii. Cipher Stream Generation

- It is all about the elements of S. The value of the S (j) element is replaced by the value S (i). The S (i) computes the j. After that step, the S stream elements is indicate the value for the cipher stream.

2.3.2 AES

This algorithm belongs to the block cipher algorithms group. It supports 128 to 256-bit keys and blocks in a 32 bits sequence. The key length and block length will be selected separately. The encryption and decryption processes of the AES algorithm occur in a number of rounds, each round consisting of one permutation and three substitutions:

Substitution of bytes: AES defines of 16x16 byte matrix with permutation of any 256 8 bit value. It is called S-box. It is intended to withstand crypto analytic attacks.

ShiftRows Permutation: it is carried out according to the original matrix rows. The first row will stay the same. It shift 1 byte to the left for the second row. Left 2-byte shift to the third row and left to the last 3-byte row shift.

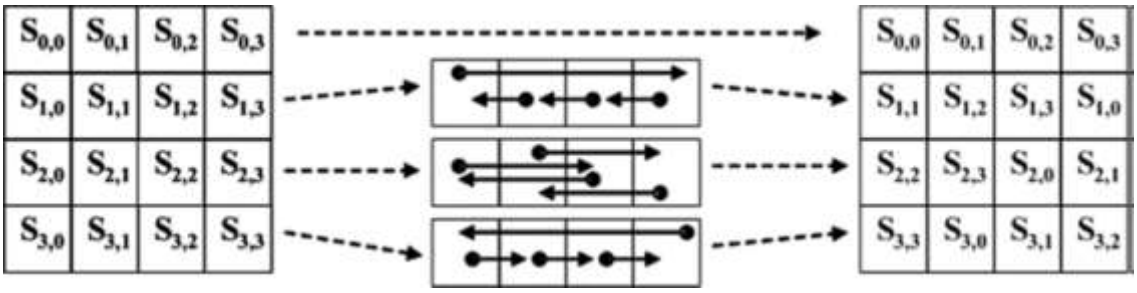


Figure 2.5 ShiftRows Permutation

MixColumn Substitution: Each column is performed by this substitution. The bytes of the column are mapped to a new value that used by all columns.

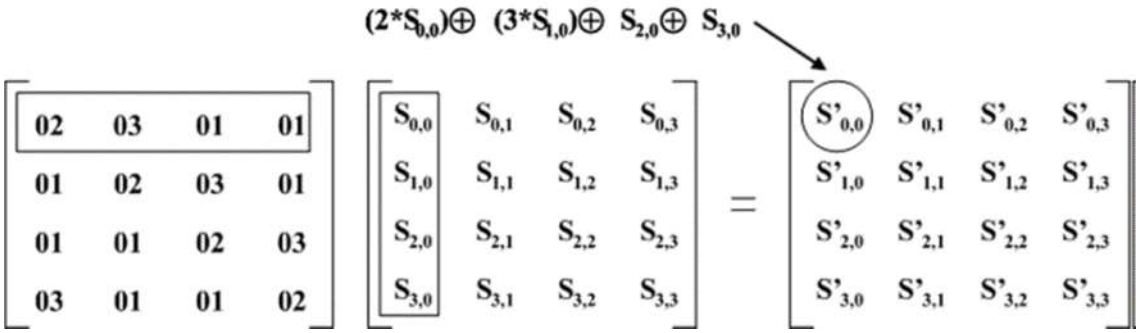


Figure 2.6 MixColumn Substitution

AddRoundKey Substitutions: XOR function is applied between the previous transformation results of round key of bit 128. The original matrix is affected by the substitution of each bit.

Table 2.2 Comparison of Encryption Algorithm

	AES	**RC4**
Cipher Type	Block Cipher	Stream Cipher
Characteristic	Operates on discrete block of data using fixed key and formula	Does not have discrete block size
Speed	Slower than RC4	Very fast

2.4 Integrity Algorithm

To make sure the data sent is in integrity and safe. The integrity algorithm is very important to solve the problem.

2.4.1 TKIP

To improve and solve WEP security problems, TKIP has been introduced as a collection of algorithms. RC4 is an encryption device that is used in wireless network adapter's hardware and cannot be replaced. So, TKIP is introduced to solve the problem, TKIP uses the RC4 device to change the shared key usage methods. In WEP, in encryption directly and other keys are generated in TKIP. The improvements of TKIP are:

i. To prevent message from falsification, message integrity code is encrypted.

- MIC is encrypted. It is hash-based encryption mechanism to work on existing wireless network adapters. False messages are to be detected. There are three components in MIC mechanism:

a) Authentication key

- It uses Michael key for both for the sender and receiver. They are using the same key.

b) Tag function

- The function is to generate the tag which is based on the message and key authentication.

c) Verification

ii. To prevent from replay attacks, strict IV is sequences.

- False message appearing when an attacker meets and send the message as his own. It resolves by connecting the MIC key to the IV counter.

iii. Key generation.

- Temporal key is called because the duration is temporary and changes when the time elapses. The packet has its own unique key based on unchanged of key and IV sequence concatenation. Therefore, the TKIP key has function will generate key.

iv. In order to prevent from attacks that are related to the key repetition, a mechanism is used to refresh the keys.

TKIP has two steps for key generation:

Step 1: The MAC address of the sender is used to calculated hash function, temporal key and high 32 bits of IV. This step is step when the temporal key changed.

Step 2: The step 1 output and the low 16 bits of IV is used to calculate the hash function. The output will produce the 128 bits of key stream. The bits that compatible with WEP that has the IV is the first three. The remaining bit is compatible with WEP. This step is to make the attacker hard to hack the security protocol.

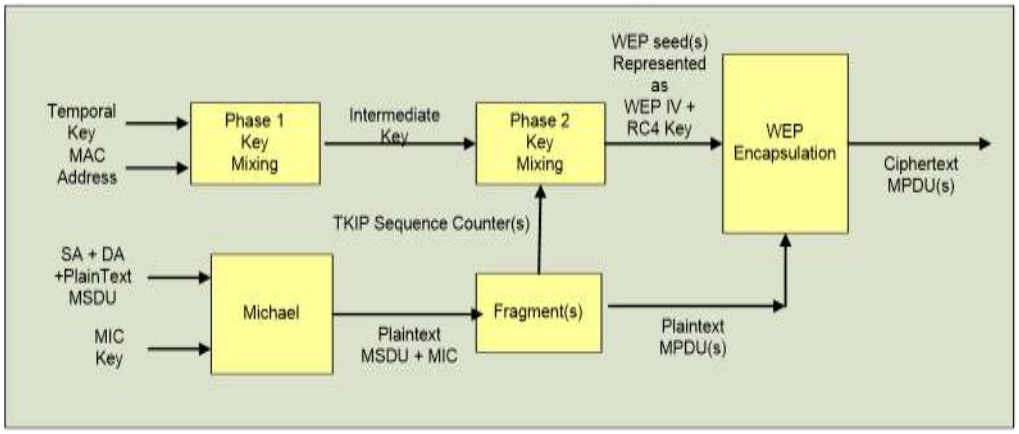


Figure 2.7 TKIP Structure

2.5 IEEE 802.11 WLAN Standards

The 802.11 standard defines the distribution system as an element that links BSS through access points within the ESS. The distribution system supports the 802.11 mobility types by providing the logical services needed to map address to the destination and integrate multiple BSS in a seamless manner.

2.5.1 IEEE 802.11g

The standard IEEE 802.11g provides the 802.11a speed, 802.11b range, and 802.11b backward compatibility and WEP security encryption. It is using 2.4 GHz band yet has between 6 and 54 Mbps rates of signalling. It also achieves its speed by using the modulation of the Orthogonal Frequency Division Multiplexing. It also using direct-sequence spread-spectrum (DSSS). A technique that distributes the data to transmitted in smaller pieces.

2.5.2 IEEE 802.11n

Up to date for previous IEEE standard. It is created to boost the about (IEEE 802.11 g) throughput, the volume of bandwidth supported through the use of multiple wireless signals in addition to antennas name MIMO engineering (Multiple Inputs, Several Outputs) rather than a single. The MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput via spatial multiplexing and increased range by exploiting the spatial diversity.

Table 2.3 WLAN Standard Comparison

	IEEE 802.11g	**IEEE 802.11n**
Band (GHz)	2.4	2.4
Bandwidth	20	20, 40
Modulation	DSSS,OFDM	SC, OFDM
Advanced Antenna Technology	N/A	MIMO up to 4 spatial
Maximum Data Rate	54 Mbps	300 Mbps

2.6 Wireshark

Wireshark is a packet analyser for the network. A network packet analyser tries to capture network packets and will try to display data in the most detail.

The Wireshark features:

a) Live packet data captured by the network device.

b) Open packet data capture program files.

c) Import packets from text files containing packet data hex dumps.

d) Display very detailed information protocol packets.

e) Save packet with very information on the protocol package.

f) Captured packet data is saved.

g) Export a number of capture file formats for some or all packets.

h) Multiple criteria filter packets.

Benefits:

User-friendliness: The packet-sniffing should be understood using the interface. It is based on GUI with clearly written context menus and simple layout. It is also offers a number of features to improve usability, such as colour coding based on protocol and detailed graphical representations of raw data.

Program support: Wireshark is one of the most active open source projects in the world.

Operating system support: Supports all major modern operating systems, including Windows, Mac OS X, and Linux-based platforms. A complete list of supported operating systems can be viewed on the homepage of Wireshark.

2.7 TFGEN

TFGEN is a packet generator tool. It generate the UDP packet at the sender and send to the receiver destination. We can set the utilization in the TFGEN to test the congested and uncongested network. The utilization is in Kbps, so if we want to use in Mbps set the value in thousands. It is because 1000 Mbps equal to 1 Kbps. We also can set the traffic pattern in continuous and constant to keep the tool generate the packet.

2.8 TL-WR1043ND Access Point

TL-WR1043ND 300Mbps Wireless N Gigabit Router Integrates 4-Port Switch, Firewall, NAT-Router and Wireless AP. The 300Mbps Wireless N Gigabit Router offers exceptional range and speed that fully meet of Small Office/Home Office (SOHO) networks and the high network performance users.

The benefits of the TL-WR1043ND are:

1. Incredible Speed

   - This IEEE 802.11g and IEEE 802.11b compatible router. It offers a wireless connection of up to 300Mbps to 802.11n wireless clients. This makes it ideal for handling a lot of data streams simultaneously. It is stable and smooth network.

2. Multiple Security Protections

   - Because WEP encryption, WPA-PSK, WPA2-PSK and advanced firewall protection provide complete data privacy.

3. Flexible Access Control

   - Children or staff may have restricted access policies. With the remote management function, the network administrator can control and monitor the network in real time.

4. Simple Installation

   - It is very easy to manage because the router is practically compatible with entire OS.

CHAPTER 3

METHODOLOGY

3.1 Introduction

This chapter will be discuss the methodology for the analysis to be carried out for this study. The analysis including a study of the existing Wi-Fi security mechanism such as WEP, WPA, and WPA2 and standard WLAN. The strategies and approaches used are described as part of this chapter. We will therefore discuss the methodology, approaches or techniques used in this research. The chosen model for this project is the methodology of waterfall.

3.2 Research Methodology

In completing a project SDLC plays an important role in guiding the developer on what deliverables that must be created? How will the deliverable created? Who will create the deliverables? When will the deliverables be created and also where will everything be documented? Without the guidance of SDLC the project will not proceed smoothly as the developers may miss the due date or forget to develop require documentations. In simple language, SDLC will act as the reminders for the developer.

For this project, the selected SDLC process model is the waterfall model. It is one of the traditional and oldest and most traditional process models in SDLC. It is also referred to as linear-sequential life cycle model. The model itself progresses linearly through discrete which are very simple to understand and use. In this model there are planning, analysis, design and implementation phase.

As true as its name each phase must be completed before the next phase can begin and no overlap occurs in the phase refers Figure 3.1. Despite that it is identical as the waterfall itself, as it keep on flowing without reversing, continuing its journey downwards. It is wrong to believe that the waterfall model prohibited previous phases from returning.

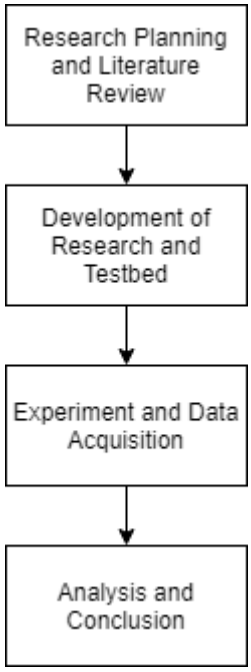


Figure 3.1 Research Methodology

This methodology allow changes to make from time to time to any stages to solve problems faced during current stage. Lastly, this research methodology gives advantage to researchers as it allow researchers to adapt easily to the needs of the research project.

3.3 Research Planning and Literature Review

The first phase of the research methodology is the research planning and literature review on the subject. The conceptualization is completed before examining the existing studies to determine the type of relevant research topic. When the research topic is selected, related journals, articles and studies are collected to be studied. This enables the problem statement, objective, and scope of this research to be defined. We find related security information in Wi-Fi mechanism for this research.

The resources we have collected are via internet journals, previous students references, and websites. The existing security studies in the Wi-Fi mechanism are carefully analyse and filtered in accordance with the relevance of the research topic.

Based on the information collected, learn about the difference of security protocol and standard WLAN to identify how the implementation of security protocol effect the performance of the network. This information is very important because can determine the methodology used by the researchers in carrying out their experiment testing.

3.4 Development of Research and Testbed

We decided to analyse the performance of the security protocol on wireless LANs on the basis of the security protocol and the WLAN standard we studied.

3.4.1 Experimental Testbed

To study the impact of different security protocols on WLAN performance in non-roaming networks, an experimental testbed is built-up for mobility users.

3.4.2 Non-Roaming Network.

Non-roaming network scenario, also known as NRS, deals with the situation when mobile node, also called as a wireless node, PC-B is connecting to Wi-Fi from access point. The PC-A is connecting to the access point at the Ethernet port using the RJ45. It is to able access point to give IP address at both PC. So that, both devices can communicate with each other.

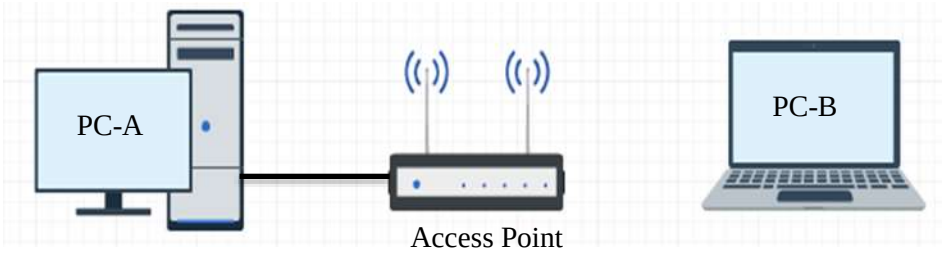


Figure 3.2 Experimental Testbed on Non-Roaming Network

3.4.3 Configure Network

After setting up the testbed, open CMD and type “ipconfig” and the press “Enter”, to see whether the IP address for both PC has changed according the IP address of the network. If not, type “ipconfig/release” and press “Enter” and then type “ipconfig/renew” and press “Enter”, here the new IP address will be given according to the network.

3.4.4 Setting Access Point

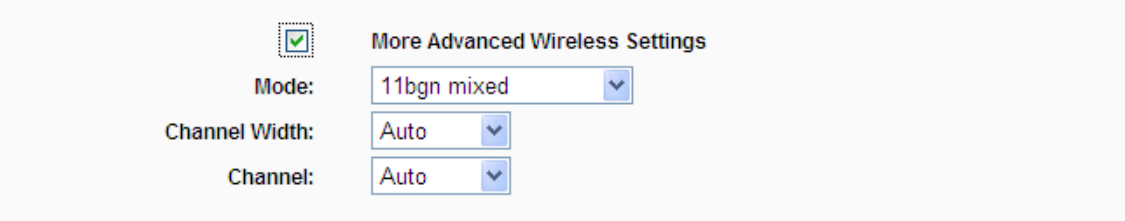


Figure 3.3 Wireless Setting

The mode is to determine the wireless mode which router works on.

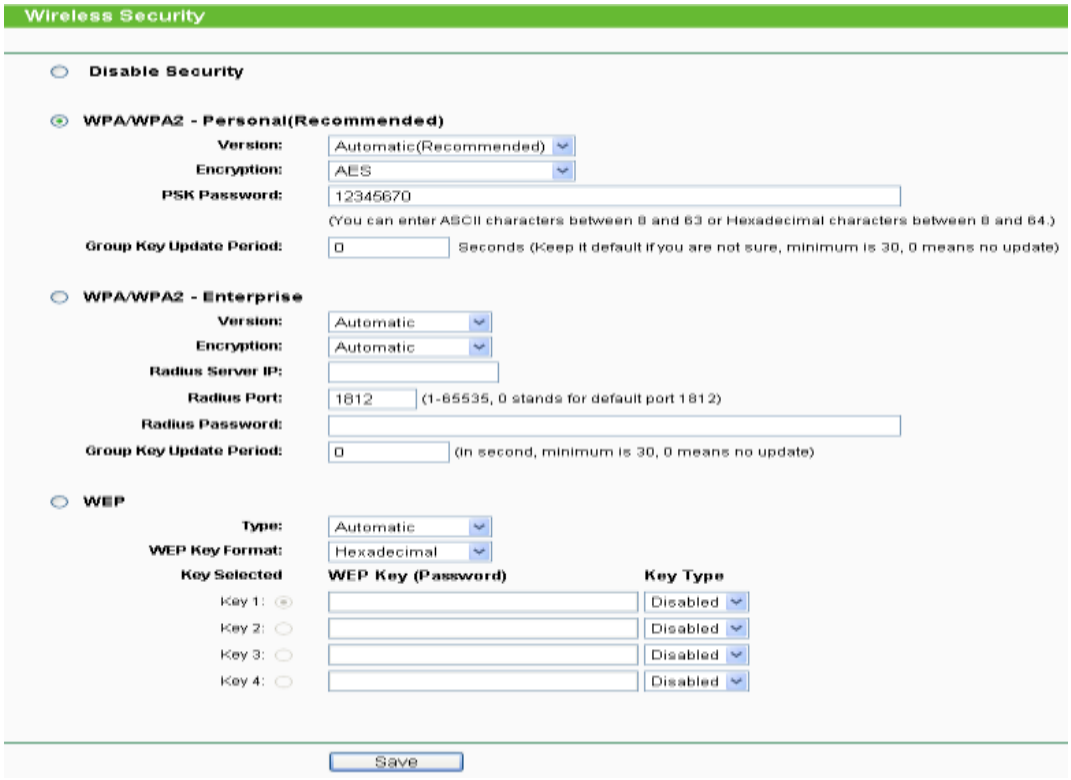


Figure 3.4 Wireless Security Settings

Setting the Wireless Security and choose the security protocol that want to test and click button “save”.

3.4.5 Setup the Wireshark

We need to set up the Wireshark, to make sure that the Wireshark is clean from capturing packet that we do not want. Stop and disable all the ports that running in the PC, so that it will be clear.

3.4.6 Setup the TFGEN

The TFGEN is generate packet tool. It only can generate UDP traffic stream.

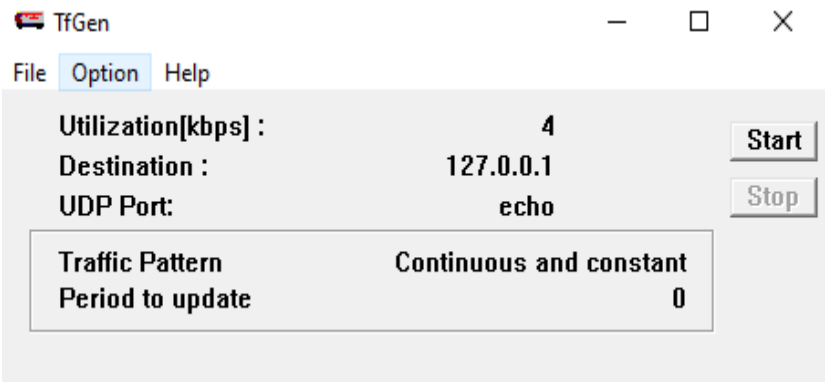


Figure 3.5 TFGEN Tool

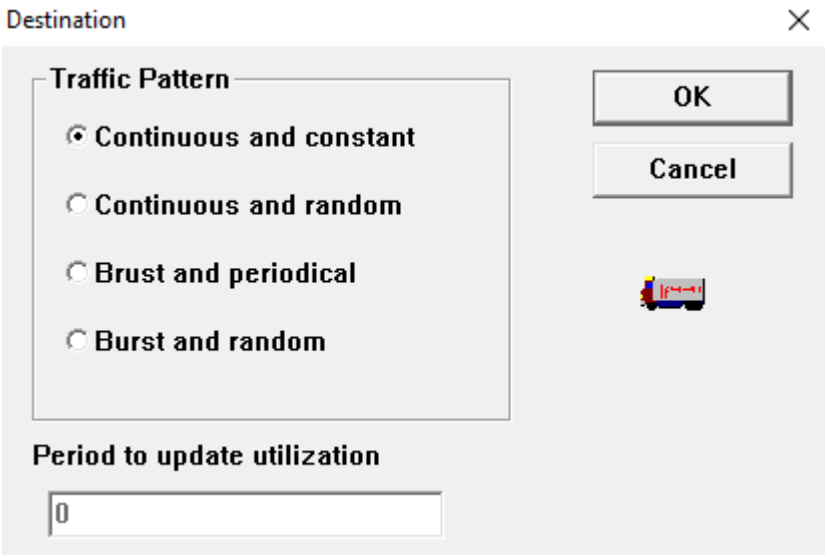


Figure 3.6 Traffic Pattern

Before generating the packet, click the "Option" tab to setting the Utilization, Destination, and the UDP Port. The utilization is for the bandwidth, since it is in Kbps, we need to set the number in thousand, because we read the data in Mbps. For the

Destination, we enter the IP address of the destination that we want to generate the packet. Lastly, for the traffic pattern, choose continuous and constant.

3.4.7 Security Policies

Based on the security protocol we have studied, we decided to perform experiments on different security protocol. Six security layers performance analysis is performed. The six security layers are: SSID (no security layer), WEP/64 (WEP used with 64 bit keys), WEP/128 (WEP used with 128 bit keys), WPA/AES (WPA used with Advanced Encryption Standard), WPA2/AES (WPA used with Advanced Encryption Standard), and WPA2/AES/TKIP (WPA2 mixed with both AES and TKIP).

3.4.8 Performance Metric

Measuring the performance of local wireless network in terms of throughput, transmission delay and average delay. These parameters can be defined as:

a. Throughput (TP) (Mbps): The measurement of total number of bytes transmitted over a network at certain time.

b. Average Delay in (ms): the average measuring of how long the bit of data travel across the network from one node to another node.

$$Average\ Delay = \frac{Total\ Time\ Delta\ from\ Displayed\ Frame}{Total\ Packet\ Capture} \times 1000$$

3.5 Experiment and Data Acquisition

After developing the research framework, therefore, a procedure was design to test the accuracy of analysing the security performance in WLAN method. The design procedure shown in Figure 3.3 and Figure 3.4 was developed to test theory before we physically proceed with sender and receiver personal computers.

The design model consist of five components which are setup testbed, configure access point, setup Wireshark, capture packet, and result for the personal computer that act as receiver. While, for the sender the design model only consists of set up test testbed, setup TFGEN and generate packet. This is because configure access point can just be

configure at one of the personal computer and for the result only on the receiver side after capture the packet.

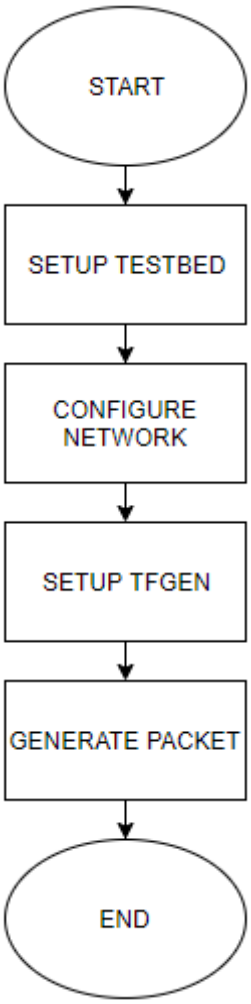


Figure 3.7 Procedure to Generate Packet at Sender

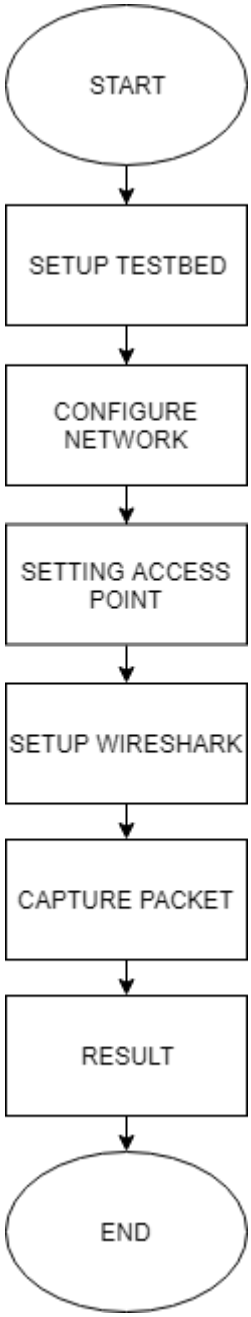


Figure 3.8 Procedure to Capture Packet at Receiver

The experiment is the step before analysis and conclusion. In here, the design model is used a guide for the experiment of proposed solution before proceed to the next step. Firstly, to prepare the hardware and software required by this project.

3.5.1 Hardware and Software

In order to carry out the research experiment, we must specify the hardware and software requirements for setting up the experiment. This setup is essential for research, since software and hardware is used to conduct the research experiment and to test and evaluate the experiment in the next phase.

3.5.1.1 Hardware Specification

The hardware requirement for this research.

Table 3.1 Hardware Requirement

Hardware	Descriptions
One unit of laptop • **Processor: Intel® Core™ i-3** • **RAM: 4 GB** • **System Type: 64-bit Operating Systems, x-64 based processor**	Used for the entire research project in which resources are found, implemented, tested and documented. During implementation and testing, it act as a sender to send packet using TFGEN.
One unit of PC • **Processor: Intel® Core™ i-7-7700** • **RAM: 16 GB** • **System Type: 64-bit Operating Systems, x-64 based processor**	Used only during implementation and testing, it act as a receiver to receive the packet and capture it using Wireshark.
Access Point (TL-WR1043ND)	Used to for a wireless connection to wireless clients
RJ45	Used to connect the PC-A to the access point's Ethernet port. It is for able the Ethernet on the PC.

3.5.1.2 Software Specification

The software specification for this research

Table 3.2 Software Requirement

Software	Descriptions
Windows 10 Professional	The operating system used for research.
Wireshark	To capture the packet that receive from sender
TFGEN	To generate packet from sender to receiver. It is using UDP traffic stream.
Microsoft Words 2013	Document the result of research.
GanttProject	To plan the Gantt Chart
Google Chrome	Collect information relating to this research.

The experiment is tested for this stage because all components are combined. Experiment and data acquisition are conducted to solve the problems statement and determine whether the limitation of existing journals is avoided. The main purpose of this test is to demonstrate the proposed authentication scheme in real time in order to ensure the accuracy of the result and claims made in this research. In addition, the experiment and data acquisition phase allows the research experiments to identify errors and limitations so that further improvements can be made to obtain the desired result.

3.6 Analysis and Conclusions

This analysis and conclusion phase is the final step in implementation of this research project. After getting the data that required, we analyse the performance of security protocol in wireless LANs, the result is thoroughly discussed. On the basis of the result, a conclusion is drawn as to whether the hypothesis accepted or not for this project.

Finally, a project thesis that clearly describes the entire project process is completed. The result are also discussed and recorded to demonstrate whether or not the hypothesis has been proven. In the next chapter you will find a more detailed explanation for the implementation phase.

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Overview

The design methodology, tests and the discussion of outcome planned in Chapter 3 will be implemented. The outcome of the execution concluded. This stage is the most important in the development of the tools because it discusses how the tools analyse the impact of security protocols on the wireless network.

4.2 Non-Roaming Network

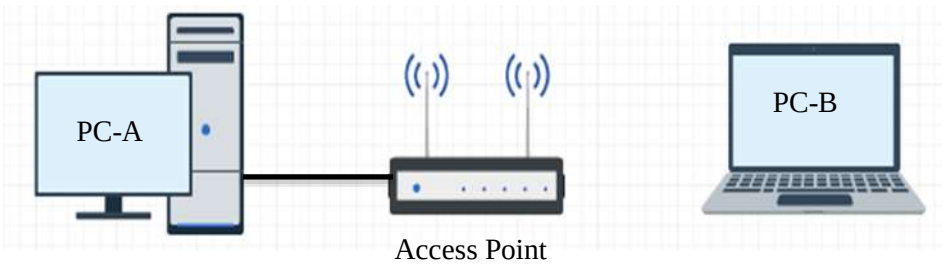


Figure 4.1 Non-Roaming Network

Table 4.1 IP Address for each devices

	IP Address	Subnet Mask	Default Gateway
PCA	192.168.0.100	255.255.255.0	192.68.0.1
PCB	192.168.0.101	255.255.255.0	192.68.0.1
Access Point (TL-WR403ND)	192.168.0.1	255.255.255.0	192.68.0.1

4.3 Systems Parameters

We have selected various system parameters in order to perform experimental analysis. Table 4.2 shows system parameters for system modelling during experiments.

Table 4.2 System Parameters

Systems Parameters	
Bandwidth	The nominal bandwidth of IEEE 802.11g is 54 Mbps and for IEEE 802.11n is 74 Mbps.
Traffic Type	UDP traffic stream
Packet Length	1500 bytes
Total Number of Packets	The packets are transmitted continuously as long as the session is "on". So the parameter is "0".
Traffic Generation	TFGEN tool used to generate WLAN traffic, IP packets are transferred predefined number, size and content to measure the performance impact of security algorithm in wireless LANs

Table 4.3 Security Protocols

Term	**Security Protocols**
P1	SSID
P2	WEP/64
P3	WEP/128
P4	WPA/AES
P5	WPA2/AES
P6	WPA2/TKIP

4.4 Results and Discussion

The result of the security performance analysis will be discussed here

4.4.1 Performance Analysis is in the Non-Roaming Scenario

Experiments are performed to study the impact of implemented security protocols on the performance WLAN in the non-roaming environment where the PC-A, PC-B and access point are in the same network. Results are obtained.

4.4.2 Throughput measurement on the basis of applied security protocol

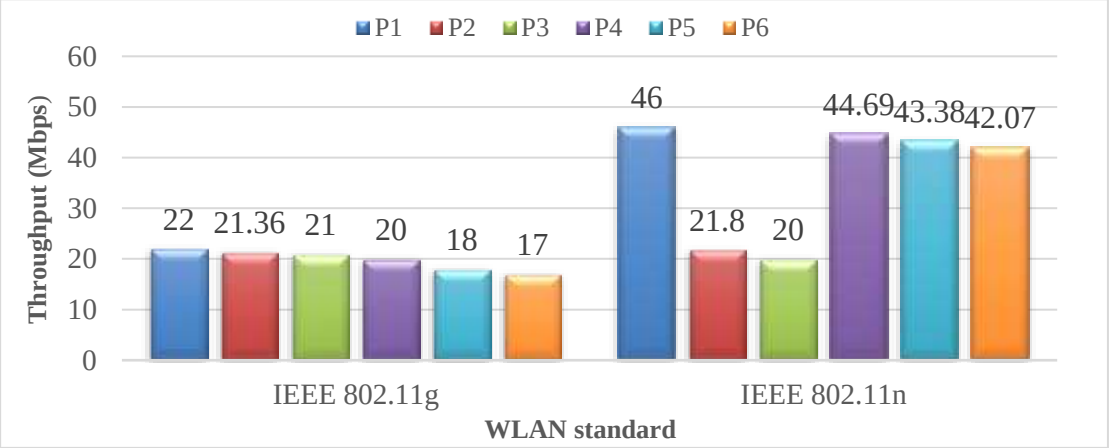


Figure 4.2 Impact of Security Protocol on Throughput

Two IEEE 802.11g/n standards have been used to get throughput readings in non-roaming network. Each standards has been set to 54 Mbps for IEEE 802.11g, while IEEE 802.11n is 74 Mbps. The diagram shows that the SSID has the highest throughput. This is because the SSID has no security and is used as a benchmark for each protocol security. This shows that increasingly complexity of securities, decreasing throughput. For IEEE 802.11g, P1 – P3 decreased by 3.13%, while for P4 – P6 decreased by 2.44 %. This is because of increase in computations of the security protocols, which consume more system resources.

But for IEEE 802.11n deny the observations that, increasingly complexity of securities, decreasing throughput. This shows in the Figure 4.2, where throughput degradation occurs with protocols P2 – P3 (WEP 64/128) approximately 36% higher than P1. It is happen because IEEE 802.11n does not support RC4 encryption algorithm that used in WEP. It therefore prohibits the use of high throughput and reduces rates to 54 Mbps. From security protocol, P1, P4-P6 throughput decreased about 1.44% with an increase in the security strength of protocol.

4.4.3 Throughput for UDP stream on the basis of congested and uncongested network.

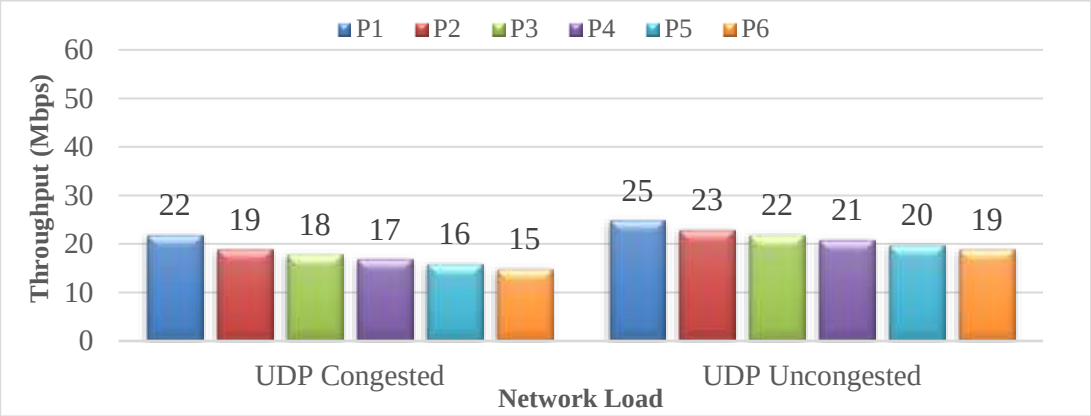


Figure 4.3 Uncongested and Congested Network for IEEE 802.11g on UDP Traffic

Each standards has been set to 54 mbps for IEEE 802.11g, while 74 mbps for IEEE 802.11n. The traffic generate rates for IEEE 802.11g uncongested is 30 Mbps and for congested is 55 Mbps. For security protocol P1 maximum throughput obtained for the UDP uncongested network is 25 Mbps and throughput for the congested network is 22 Mbps. From the results, its shows that throughput for the uncongested network is higher than congested network, based on figure that plotted, the average throughput degradation in the UDP congested network is 3.8 % more than the UDP uncongested network. It is depicted that throughput in the congested is less as compared to the uncongested network and this is due to the congestion caused in the network by high traffic generation rates.

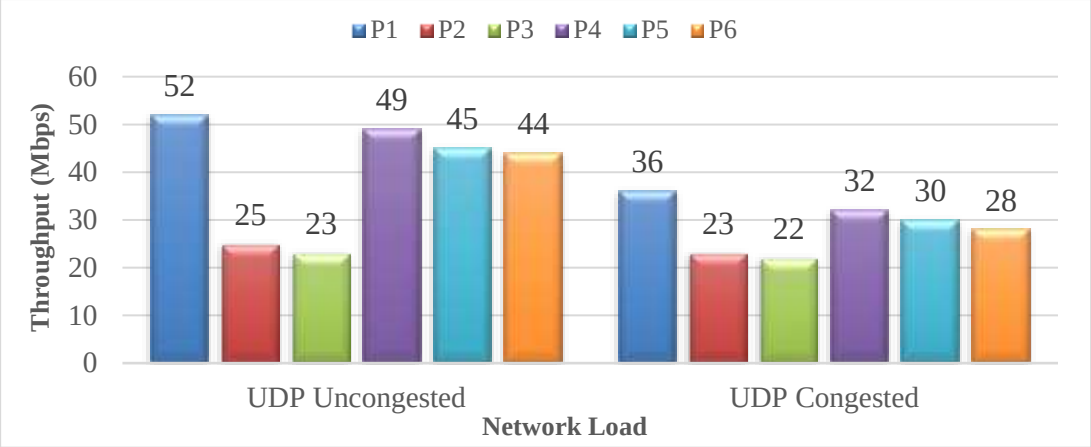


Figure 4.4 Uncongested and Congested Network for IEEE 802.11n on UDP Traffic

In IEEE 802.11n based network on the traffic was generated at 50 Mbps and 75 Mbps to make network congested and uncongested. From the figure above shows that average throughput decreased about 1.13% for security protocol P1 while for P4-P6 is 2.73% in the UDP congested network compared to the uncongested network. Throughput degradation is maximum for P2-P3 in both congested and uncongested network. It is the same as in section 4.4.2.

4.4.4 Average Delay

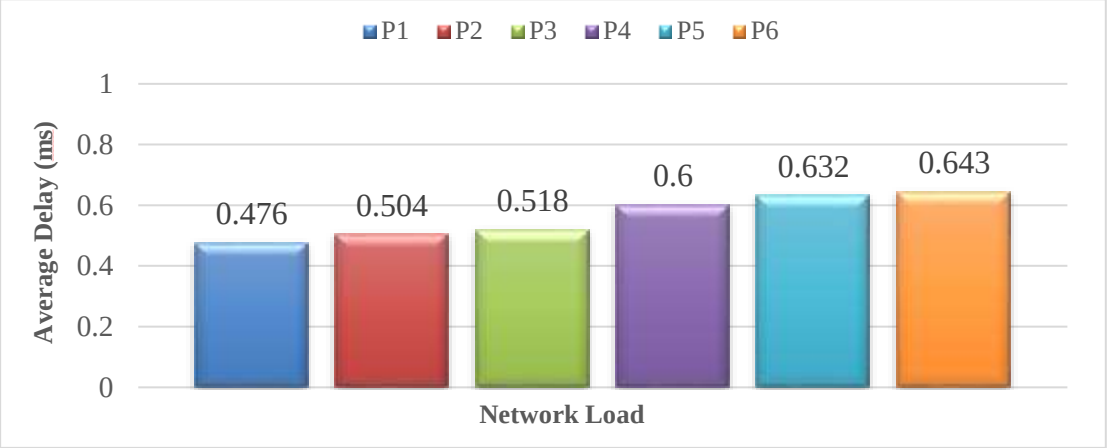


Figure 4.5 Average Delay for IEEE 802.11g

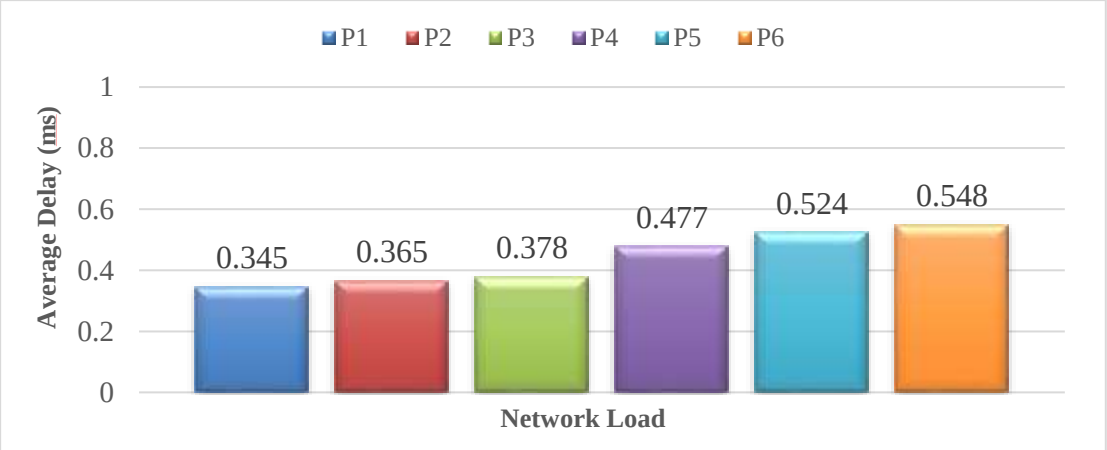


Figure 4.6 Average Delay for IEEE 802.11n

Experiment results also obtained to study the impact of different security protocols on average delay. It is observed that different security protocols have impact on average delay values. Increase completion of security mechanisms, increasing the average delay. This is because encryption overheads increase. Furthermore, the increasing of data rates also increase the average delay. The average delay increases with the increase of authentication message. Therefore, the improved data rates and the strongest encryption method have the highest average delay. So, the WPA2/TKIP in IEEE 802.11n comes at the expense of the increased the average delay.

CHAPTER 5

CONCLUSION

5.1 Introduction

In this chapter, the research will be concluded and we will also discuss whether or not the aim of this research was achieved. In this chapter also, a brief discussion of the future work will also be discussed.

5.2 Conclusion

In this paper, we have presented the experimental results on the security performance of 802.11 standards of WLAN. The analysis has been performed to study the impact of different security protocols in terms of throughput and average delay.

The first objective of this research was to compare the technique in Wi-Fi security protocol. This objective is successfully achieved as in the literature review has told how the encryption algorithm encrypt the data and differences of each protocol.

The second objective is to identify the effect of performance WLAN (IEE 802.11g/n) for various security protocols. This objective is successfully achieved as shown in Figure 4.2. This shows that increasingly complexity of securities, decreasing performance.

Lastly, the third objective is to identify the effect of uncongested and congested network on UDP traffic stream also has been achieved. The results of the successful is shown in Figure 4.3 and 4.4. This shows that throughput on the uncongested network is higher than congested network. Furthermore average delay increase when the encryption of security protocols increase.

Lastly, from the analysis discussion, we can say that for the application where security is less concern but a network with a better performance is required lower security layer (WEP, WPA/AES) can be used.

The limitations of this research is to make sure the Wireshark is clean from capturing other than required packet. We need to search where the not required packet come and disable it from running. So, it do not capture it. Next, the other limitations is to choose the packet generator tool that can operates on Windows and can set the bandwidth to generate the packet.

5.3 Future Work

In the near future, analysis of security performance of wireless LANs can be performed for TCP traffic. We can compare between TCP and UDP on congested and uncongested network. Next, can compare with the other router to see the difference of security performance on each of the router WLAN.

REFERENCES

Jindal, Poonam, and Brahmjit Singh. 2017. "Quantitative Analysis of the Security Performance in Wireless LANs." *Journal of King Saud University - Computer and Information Sciences* 29(3): 246–68. http://dx.doi.org/10.1016/j.jksuci.2014.12.012.

Local, On Wireless. 2006. "Security Impacts Networks." : 123–27.

Baghaei, N, and R Hunt. 2004. "IEEE 802.11 Wireless LAN Security Performance Using Multiple Clients." *Proceedings 2004 12th IEEE International Conference on Networks ICON 2004 IEEE Cat No04EX955* 1: 299–303. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1409151.

Butty, Levente. "WiFi Security : WEP and Its Flaws Why Security Is More of a Concern in Wireless ? Introduction to WiFi."

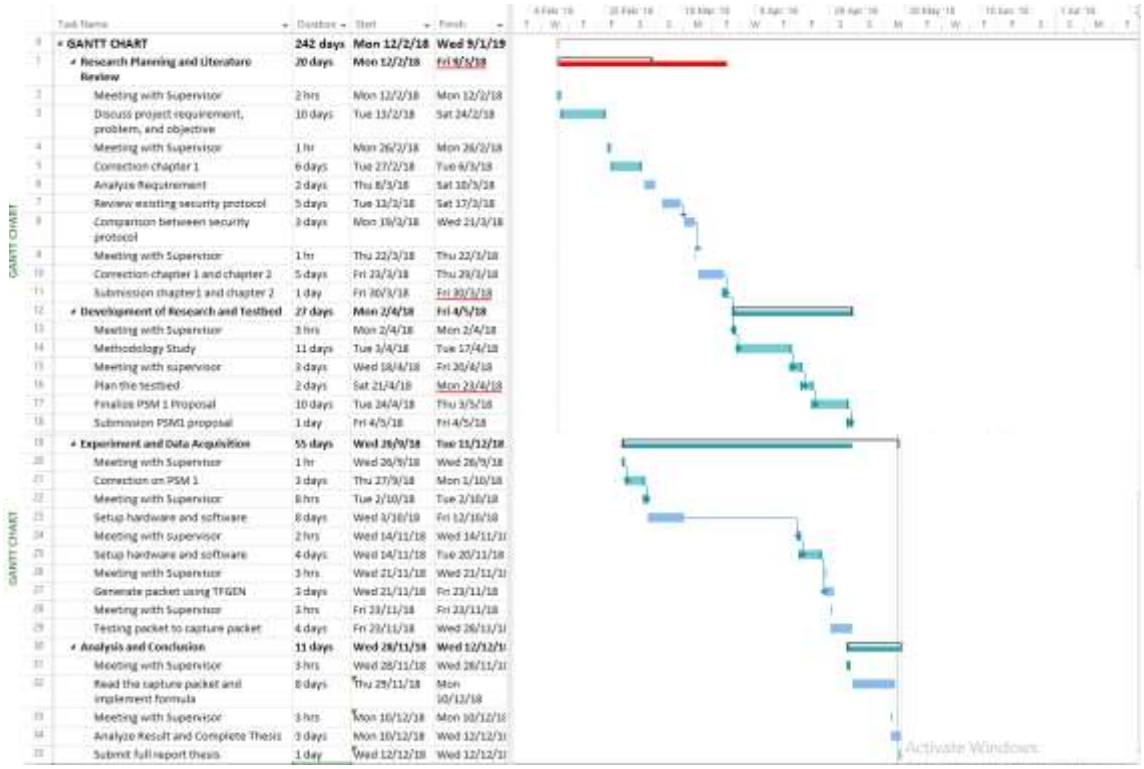
Cam-winget, By Nancy, Russ Housley, David Wagner, and Jesse Walker. "No Title." 46(5): 35–39.

Government, The, Hong Kong, Special Administrative, and Region The. 2010. "Wireless Networking Security."

Potlapally, N. R., S. Ravi, A. Raghunathan, and N. K. Jha. 2006. "A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols." *IEEE Transactions on Mobile Computing* 5(2): 128–43.

Sheldon, Frederick T., John Mark Weber, Seong Moo Yoo, and W. David Pan. 2012. "The Insecurity of Wireless Networks." *IEEE Security and Privacy* 10(4): 54–61.

APPENDIX A
GANTT CHART



	Task Name	Duration	Start	Finish
0	GANTT CHART	242 days	Mon 12/2/18	Wed 9/1/19
1	Research Planning and Literature Review	20 days	Mon 12/2/18	Fri 9/3/18
2	Meeting with Supervisor	2 hrs	Mon 12/2/18	Mon 12/2/18
3	Discuss project requirement, problem, and objective	10 days	Tue 13/2/18	Sat 24/2/18
4	Meeting with Supervisor	1 hr	Mon 26/2/18	Mon 26/2/18
5	Correction chapter 1	6 days	Tue 27/2/18	Tue 6/3/18
6	Analyze Requirement	2 days	Thu 8/3/18	Sat 10/3/18
7	Review existing security protocol	5 days	Tue 13/3/18	Sat 17/3/18
8	Comparison between security protocol	3 days	Mon 19/3/18	Wed 21/3/18
9	Meeting with Supervisor	1 hr	Thu 22/3/18	Thu 22/3/18
10	Correction chapter 1 and chapter 2	5 days	Fri 23/3/18	Thu 29/3/18
11	Submission chapter1 and chapter 2	1 day	Fri 30/3/18	Fri 30/3/18
12	Development of Research and testbed	27 days	Mon 2/4/18	Fri 4/5/18
13	Meeting with Supervisor	3 hrs	Mon 2/4/18	Mon 2/4/18
14	Methodology Study	11 days	Tue 3/4/18	Tue 17/4/18
15	Meeting with supervisor	3 days	Wed 18/4/18	Fri 20/4/18
16	Plan the testbed	2 days	Sat 21/4/18	Mon 23/4/18
17	Finalize PSM 1 Proposal	10 days	Tue 24/4/18	Thu 3/5/18
18	Submission PSM1 proposal	1 day	Fri 4/5/18	Fri 4/5/18
19	Experiment and Data Acquisition	55 days	Wed 26/9/18	Tue 11/12/18
20	Meeting with Supervisor	1 hr	Wed 26/9/18	Wed 26/9/18
21	Correction on PSM 1	3 days	Thu 27/9/18	Mon 1/10/18
22	Meeting with Supervisor	8 hrs	Tue 2/10/18	Tue 2/10/18
23	Setup hardware and software	8 days	Wed 3/10/18	Fri 12/10/18
24	Meeting with supervisor	2 hrs	Wed 14/11/18	Wed 14/11/1
25	Setup hardware and software	4 days	Wed 14/11/18	Tue 20/11/18
26	Meeting with Supervisor	3 hrs	Wed 21/11/18	Wed 21/11/1
27	Generate packet using TFGEN	3 days	Wed 21/11/18	Fri 23/11/18
28	Meeting with Supervisor	3 hrs	Fri 23/11/18	Fri 23/11/18
29	Testing packet to capture packet	4 days	Fri 23/11/18	Wed 28/11/1
30	Analysis and Conclusion	11 days	Wed 28/11/18	Wed 12/12/1
31	Meeting with Supervisor	3 hrs	Wed 28/11/18	Wed 28/11/1
32	Read the capture packet and implement formula	8 days	Thu 29/11/18	Mon 10/12/18
33	Meeting with Supervisor	3 hrs	Mon 10/12/18	Mon 10/12/18
34	Analyze Result and Complete Thesis	3 days	Mon 10/12/18	Wed 12/12/1
35	Submit full report thesis	1 day	Wed 12/12/18	Wed 12/12/1