# TRAFFIC CHARACTERISATION MECHANISM FOR DETECTING ROGUE ACCESS POINT IN LOCAL AREA NETWORK

**AMRAN BIN AHMAD**

**DOCTOR OF PHILOSOPHY**
**UNIVERSITI UTARA MALAYSIA**
**2015**

## Permission to Use

In presenting this thesis in fulfilment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the Universiti Library may make it freely available for inspection. I further agree that permission for the copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor(s) or, in their absence, by the Dean of Awang Had Salleh Graduate School of Arts and Sciences. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to:

Dean of Awang Had Salleh Graduate School of Arts and Sciences
UUM College of Arts and Sciences
Universiti Utara Malaysia
06010 UUM Sintok

# Abstrak

Titik Capaian Bangsat (RAP) adalah satu kerentanan rangkaian yang melibatkan penggunaan titik capaian tanpa wayar secara haram di dalam satu persekitaran rangkaian. Kewujudan RAP boleh dikenal pasti melalui pemeriksaan trafik rangkaian. Tesis ini bertujuan untuk membentangkan kajian penggunaan pencirian trafik rangkaian setempat (LAN) bagi mencirikan rangkaian trafik berwayar dan tanpa wayar melalui pemeriksaan pertukaran paket antara pengirim dan penerima, menggunakan penangkapan paket dengan cop masa masuk untuk menunjukkan kewujudan sesuatu RAP. Kajian ini adalah berdasarkan kepada analisis maklumbalas penyegerakan (SYN/ACK), maklumbalas penutupan sambungan (FIN/ACK), maklumbalas tolakan data (PSH/ACK) dan penghantaran data (PAYLOAD) oleh isyarat daripada pembekal yang dikaitkan kepada pasangan penerima akuan (ACK) masing-masing. Cop masa bagi setiap pasangan kemudiannya dikumpulkan menggunakan teknik Kumpulan Setara yang menghasilkan purata kumpulan. Ia kemudiannya dikategorikan kepada tiga zon untuk membentuk purata zon. Kemudiannya, purata zon ini telah digunakan untuk membentuk purata global yang bertindak sebagai nilai ambang dalam mengenal pasti sesuatu RAP. Sebuah tapak uji rangkaian dibangunkan di mana trafik rangkaian sebenar diperoleh dan dianalisis. Satu mekanisma untuk mencirikan trafik rangkaian berwayar dan tanpa wayar LAN menggunakan analisis purata global dalam proses pengesanan RAP telah dicadangkan. Nilai ambang pengesanan RAP bagi protokol rangkaian berwayar (IEEE 802.3) yang telah dikira oleh kajian adalah 0.002 ms manakala protokol tanpa wayar (IEEE 802.11g dan IEEE 802.11n) adalah masing-masing 0.014 ms dan 0.033 ms. Kajian ini menyumbang kepada satu mekanisma baru bagi mengesan sesuatu RAP melalui pencirian trafik dengan penelitian komunikasi paket dalam persekitaran LAN. Pengesanan RAP adalah penting dalam usaha untuk mengurangkan kerentanan dan memastikan integriti pertukaran data dalam LAN.

**Kata kunci:** Titik capaian bangsat, Cop masa masuk, Penangkapan paket, Penapisan paket, Keselamatan rangkaian.

# Abstract

Rogue Access Point (RAP) is a network vulnerability involving illicit usage of wireless access point in a network environment. The existence of RAP can be identified using network traffic inspection. The purpose of this thesis is to present a study on the use of local area network (LAN) traffic characterisation for typifying wired and wireless network traffic through examination of packet exchange between sender and receiver by using inbound packet capturing with time stamping to indicate the existence of a RAP. The research is based on the analysis of synchronisation response (SYN/ACK), close connection respond (FIN/ACK), push respond (PSH/ACK), and data send (PAYLOAD) of the provider's flags which are paired with their respective receiver acknowledgment (ACK). The timestamp of each pair is grouped using the Equal Group technique, which produced group means. These means were then categorised into three zones to form zone means. Subsequently, the zone means were used to generate a global mean that served as a threshold value for identifying RAP. A network testbed was developed from which real network traffic was captured and analysed. A mechanism to typify wired and wireless LAN traffic using the analysis of the global mean used in the RAP detection process has been proposed. The research calculated RAP detection threshold value of 0.002 ms for the wired IEEE 802.3 LAN, while wireless IEEE 802.11g is 0.014 ms and IEEE 802.11n is 0.033 ms respectively. This study has contributed a new mechanism for detecting a RAP through traffic characterisation by examining packet communication in the LAN environment. The detection of RAP is crucial in the effort to reduce vulnerability and to ensure integrity of data exchange in LAN.



**Keywords:** Rogue access point, Inbound timestamp, Packet capturing, Packet filtering, Network security.

## Acknowledgements

In the name of ALLAH, Most Gracious, Most Merciful.

First and foremost, I would like to profoundly praise The Almighty Allah, who has shown me the right path, provided me the strength and knowledge to complete this research.

There are so many wonderful and talented people whom I would like to thank for their help and patience that I am loss to where to begin.

I will start by thanking my supervisors Professor Dr. Suhaidi Hassan and Dr. Mohd Hasbullah Omar for their help, motivation, and encouragement throughout my study. Both of them are extremely talented person, and I have nothing but respect and admiration for them. They have helped me immensely, and I would like them to know that I appreciate all of their efforts and support.

Finally, my heartiest gratitude goes to my family, to my late father who passed away, to my mother who always has faith in me and prays for my success, to my beloved wife Hapizah Hussain for her understanding, support, and love, and last but not least to all my children, Amira, Hafizi, Amanina and Amalia Husna for being so sweet and loving.

# Table of Contents

# List of Tables

# List of Figures

# List of Appendices

# List of Abbreviations

| | |
|---|---|
| ACK | Acknowledgement |
| AP | Access Point |
| ARP | Address Resolution Protocol |
| ASN.1 | Abstract Syntax Notation One |
| CSMA/CA | Carrier Sense Multiple Access/Collision Avoidance |
| DHCP | Dynamic Host Configuration Protocol |
| DoS | Denial of Service |
| FIN | No more data from sender |
| GUI | Graphical User Interface |
| IETF | Internet Engineering Task Force |
| IP | Internet Protocol |
| LAN | Local Area Network |
| MAC | Medium Access Control |
| MIB | Management Information Base |
| ms | Milliseconds |
| MyCERT | Malaysia Computer Emergency Response Team |
| NAT | Network Address Translation |
| NIC | Network Interface Card |
| NMS | Network Management System |
| OID | Object Identifier |
| OS | Operating System |

| | |
|---|---|
| OSI | Open Systems Interconnection model |
| PC | Personal Computer |
| PCAP | Packet Capturing |
| PHY | Physical |
| PSH | Push function |
| RADIUS | Remote Authentication Dial-In User Service |
| RAP | Rogue Access Point |
| RTT | Round Trip Time |
| SMI | Structure of Management Information |
| SNMP | Simple Network Management Protocol |
| SSID | Service Set Identifier |
| SYN | Synchronize sequence numbers |
| TCP | Transfer Control Protocol |
| UUM | Universiti Utara Malaysia |
| WEP | Wired Equivalent Privacy |
| WLAN | Wireless Local Area Network |
| WPA2 | Wi-Fi Protected Access 2 |

# CHAPTER ONE
# INTRODUCTION

Wireless technology provides users the freedom of mobility, gives network designers more options for connectivity, and gives many new devices the capability to connect to a network [1, 2, 3]. However, wireless technology brings significantly more threats or vulnerability than traditional wired networks. The issue of network vulnerabilities of wireless LAN is very critical in managing computer networks [4, 5, 6, 7, 8]. With increasing faults and attacks on network infrastructure, there is an urgent need to analyse network and service vulnerabilities under an organised fault attack in a more comprehensive manner [9, 10, 11, 12, 13].

Network extensibility can be achieved easily, with less effort, and become more cost effective through an implementation using wireless devices, such as by installing Access Points (APs) [14]. Many organisations spend greater effort in installing APs for widening the LAN coverage to enable greater access for staff, especially those located at various locations in different buildings. However, some staff prefer to access the organisational network through their private AP without realising the possible detrimental effects of doing so with regard to network security and also performance. This kind of private AP or Rogue AP does not belong to the organisation and it is also unmanageable because of the different configurations and without support by a specific tools in local area network. Thus, this has opened up the network and subjected it to many vulnerability related issues, for example intruders.

In relation to the above scenario, there should be a way to rectify the real problem of RAP, which is unknown to the network manager by using a special mechanism that has capabilities to detect RAPs in whatever event or situation [15, 16]. They are two types of LAN, namely wired and wireless. It can be considered that wired

is more suitable than wireless for detecting RAP which has many hosts located and scattered over an area in a campus network environment [17]. For this case, using a wireless approach may increase cost and also human effort. Meanwhile using a wired network implementation, specific tools can be deployed at the network cores, like routers, which are the transit points to many packets flowing through the network before they are routed to their destination.

The most suitable mechanism for a wired approach in detecting RAP is through packet capturing, which is when some specific interface and filter are set to capture whatever packets arriving at the router. The next step would be to perform an arrangement referencing algorithm that can be designed and developed for detecting a RAP. Hence, with the support of traffic analysis, the captured packet can be analysed for comparing between hosts in order to screen for the existence of RAPs. Here the situation can be deemed as the host going through RAP or otherwise, solely depending on the evaluation of all the results analysed through traffic analysis. However, the performance of the RAP Detection Mechanism implementation needs to also be taken into consideration before and after it is executed.

The aim of this research is to overcome RAP issues that originate from organisational staff members who deploy AP without permission and proper administration, which can cause a security breach and thus introduce network vulnerabilities for causing problems for the LAN. The next section will provide some detail of the reality of RAP that may exist in LAN and the possible solutions to prevent it from damaging whatever policy being imposed on the organisational LAN.

## 1.1 Current Rogue Access Point Scenario

Access points which are not accounted for in the network, meaning that they are not planned, can expose the enterprise network to a barrage of security vulnerabilities, even though they are typically connected to a network port behind a firewall [18, 19]. Unauthorised or rogue access points (RAPs) produce security vulnerabilities in enterprise/campus networks by circumventing inherent security mechanisms [20, 21] and these RAPs are installed on a secured network without the explicit permission of the appropriate network management authority [22, 23]. The popularity of the 802.11-based Wireless LAN (WLAN) also increases the risk of security attacks such as Denial of Service (DoS) attacks [24]. This can happen due to the characteristically open medium, insufficient software implementation, potential for hardware deficits, and improper configurations [21]. Even though APs are the best extensible device for network advancement, it is also the main contributor to network vulnerabilities, especially if it is connected without the proper security configuration [25].

The Simple Network Management Protocol (SNMP) forms part of the Internet protocol suite as defined by the (IETF) [26, 27]. It is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. It consists of a set of standards for network management, including an Application Layer protocol, a database scheme, and a set of data objects. The SNMP model consists of Network Management System (NMS), device management, and Management Information Base (MIB) [28]. NMS works as a Graphical User Interface (GUI) between the network environment and network administrator. Any given command or action taken can be performed through the NMS. The managed devices are managed by SNMP, which include devices such as switches, routers, gateways, computers or hardware that are related to and are supported by the MIB [29, 30, 31, 32, 27]. The MIB provides specific information

of managed devices, where each device has its own MIB provided by the product manufacturer.

This research investigated on finding a threshold or indicator that can be used for feeding into SNMP in detecting RAPs. However, throughout this thesis, the focus is on finding a threshold instead of discussing the actual SNMP. It is hoped that this outcome (threshold) could contribute towards better network management, in general, and more specifically, toward establishing a more improved SNMP.

## 1.2 Research Motivation

Sharing information has become more important to people when they connect to others. While this phenomenon continues to grow, the information properties need to be protected from any computer vulnerabilities, like intruders or hackers [9]. At the same time, computer and network professionals need to figure out remedies to resolve these issues, since this can potentially be a serious threat coming from mis-configured AP that is installed without permission, which has been touched upon previously.

In this section, this research will look into what has been done by the Malaysia Computer Emergency Response Team (MyCERT) at the national level to overcome those problems from a larger perspective of network vulnerabilities. The discussion will focus on MyCERT incident report in order to establish the severity for rectifying this critical network vulnerability from the larger national perspective.

### 1.2.1 MyCERT Incident Report

The Incident Report is an initiative toward achieving the mission and vision of MyCERT at the national level [33]. Currently, MyCERT operates the Cyber999 computer security incident handling and response help centre as well as the

Cybersecurity Malaysia Malware Research Centre [34].This activity had started in 1997 and continues to provide pertinent security information until today. However for the scope of this study, the reporting was compiled and analysed from 2007 to 2015 (June) (see Table 1.1). The reporting was based on a monthly basis and also summarised as a yearly basis in order to differentiate the result between the years starting from 2007 and ending in 2015 (June).

Table 1.1
*MyCERT: General Reported Incident Year 2007 - 2015 (June)*

| Categories | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 (June) | Total |
|---|---|---|---|---|---|---|---|---|---|---|
| Content Related | - | - | 17 | 39 | 59 | 20 | 54 | 35 | 15 | 239 |
| Cyber Harassment | 68 | 72 | 174 | 419 | 459 | 300 | 512 | 550 | 228 | 2782 |
| Denial of Service | 8 | 12 | 28 | 66 | 78 | 23 | 19 | 29 | 16 | 279 |
| Fraud | 364 | 907 | 1022 | 2212 | 5328 | 4001 | 4485 | 4477 | 1747 | 24543 |
| Intrusion | 31 | 766 | 1766 | 2160 | 3699 | 4326 | 2770 | 1125 | 729 | 17372 |
| Intrusion Attempt | - | - | - | 685 | 734 | 67 | 76 | 1302 | 108 | 2972 |
| Malicious Codes | 182 | 277 | 283 | 1199 | 1012 | 645 | 1751 | 716 | 189 | 6254 |
| Spam | - | - | - | 1268 | 3751 | 526 | 950 | 3650 | 2906 | 13051 |
| Vulnerabilities Report | 31 | 89 | 182 | 42 | 98 | 78 | 19 | 34 | 10 | 583 |
| **Total** | 684 | 2123 | 3472 | 8090 | 15218 | 9986 | 10636 | 11918 | 5948 | 68075 |

Table 1.1 shows the incident type on the left most column and the number of occurences on a yearly basis from 2007 to 2015 (June). The report projected the difference between each incident type occurrences which can be seen as a total either by yearly or incident type. Figure 1.1 shows the increase or decrease of each incident type, based on yearly reporting.

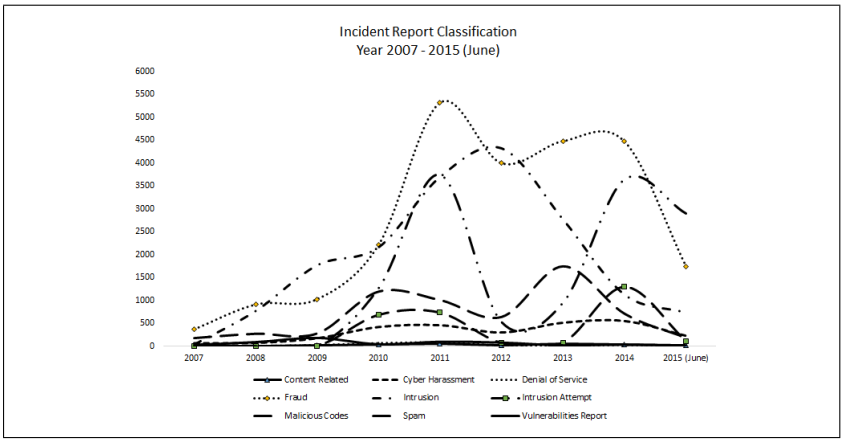



*Figure 1.1.* MyCERT: General Reported Incident Year 2007 - 2015 (June)

The graph (Figure 1.1) demonstrates that fraud has increased and become the highest threat by year 2011 and gradually decrease until June 2015. The second ranked incident goes to intrusion, followed by spam, even though it was small in number just a few years before. In addition, the rest of the incidents were not as higher as previously stated (fraud, intrusion and spam), but they cannot be disregarded because each of these incidents will play a vital role in affecting the Internet community. Figure 1.2 highlights the overall incident type starting from 2007 and up to 2015 (June).

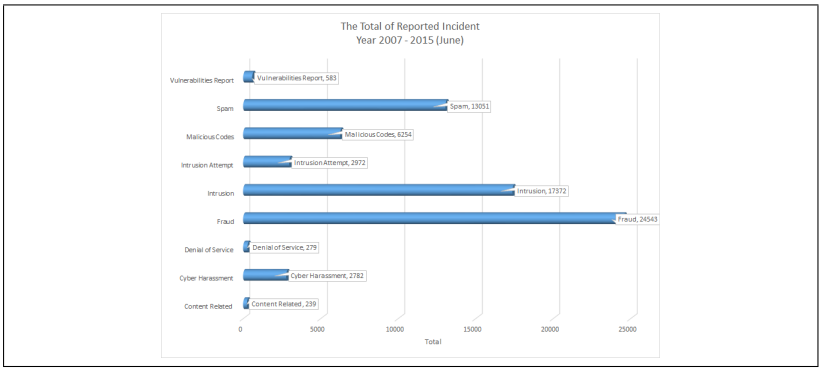



*Figure 1.2.* MyCERT: The Total of Reported Incident Year 2007 - 2015 (June)

The biggest reported was Fraud (24543 cases). There is much valuable information that can be disguised when users start to do an on-line transaction [35, 36, 37, 38]. The best choice for financial transaction in e-commerce is by using the credit card, even though there are a few other alternatives. Consequently, many network engineers feel threatened when facing the intrusion (17372 cases) phenomenon that appears in their network site. In addition to addressing this unwanted appearance, this thesis presents a possible viable solution on how to stop this intruder from breaking through a network barrier. The network engineer will discover that many intruders will start entering through the network edge (host) using two kinds of links, namely wired or wireless. The easiest is through wireless where it is welcomed by an AP. Moreover, a RAP can characteristically open the door to the network core (switches or routers) or another edge (servers and hosts). Detecting this kind of AP will reduce the potential

for intrusion and fraud, and also minimise the threat to other Internet communities if it is stopped at an early stage (where they are coming from).

## 1.3 Problem Statement

In many network environments, the use of AP is given priority for widening the network service to users. However, without proper configuration, it will create vulnerabilities to the existing network. Network vulnerabilities refer to the impact of attacks and fault on a computer network [39, 40]. It is a point where the network is susceptible to attack. The network vulnerability analysis is a systematic examination of the computer network to determine the adequacy of security measure, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation [12].

The method used for tracking these wireless vulnerabilities is through War Driving. Azzali (2009) and Ahmad (2013) in [41] and [42] conducted War Driving at UUM (refer Figure1.3) and discovered a total of 38 access point units and seven ad hoc units. However, all APs and ad hoc devices were found to have the Encryption OFF (open mode) setting, which meant that no access security key (password) is required and anybody can easily gain access through these AP devices. Four access points had been detected using the default setting for the service set identifiers (SSID). Moreover out of the 45 APs, 29 were registered and legal APs, while the rest were unauthorised APs (RAPs) (refer Table 1.2).

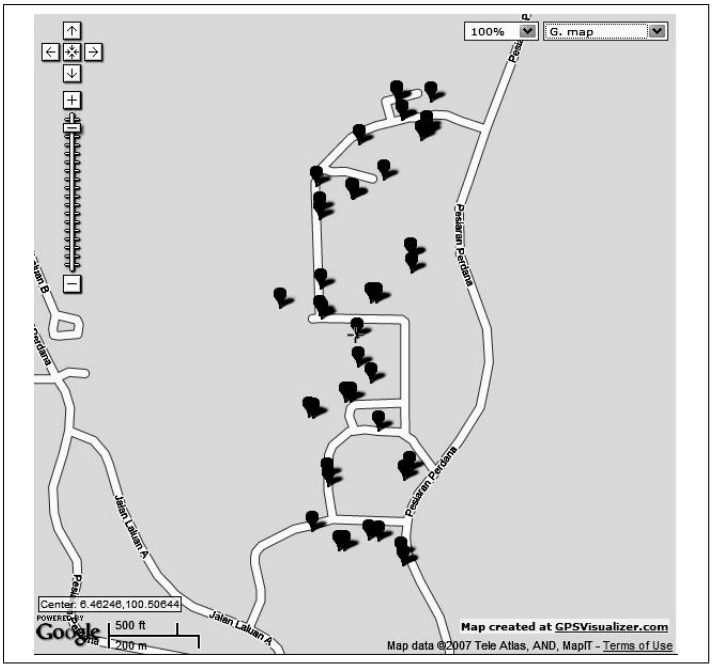



*Figure 1.3.* War Driving Route

Table 1.2
*Vulnerabilities Analysis*

| **Categories** | **No.** |
|---|---|
| ALL (AP & Ad-hoc | 45 |
| Encryption OFF | 45 |
| Encryption ON | 0 |
| Access Point | 38 |
| Ad-hoc | 7 |
| Default SSID | 4 |
| Authorize AP | 29 |
| Rogue AP | 16 |

In spite of the 802.1a/b/g/n for wireless LAN, 802.1X is also being used for security purposes at the UUM campus. 802.1X is also known as RADIUS, which is a centralised authentication system within the wireless perimeter. Each user will be prompted for a user name and password. Without passing this stage they will not be given access to the wireless LAN. At UUM, 802.1X is implemented for all campus APs. Figure 1.4 shows the windows prompt for the user to authenticate.

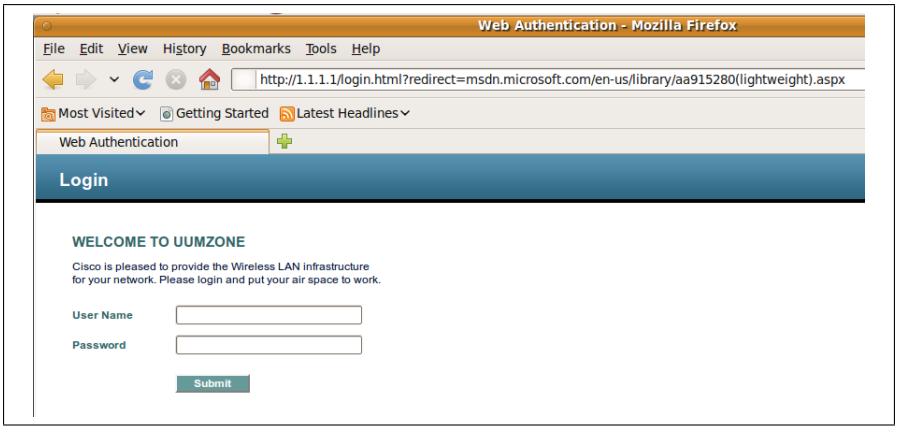



*Figure 1.4.* UUM's RADIUS Authentication

Consequently, this security will be avoided if any AP other than the campus APs is connected to the wireless LAN. The user can use the network services without having to authenticate beforehand. Figure 1.5 shows the RAP in action without detecting the connection to UUM LAN. Even though it is configured by legal staff members, it is still considered illegal since it does not meet the security requirements as imposed by the security policy. Ironically some of them are using the default configuration of these devices. From Figure 1.5, it shows that the RAPs using the default as SSID, without changing and enforcing a certain security level (i.e., more vulnerable without security).

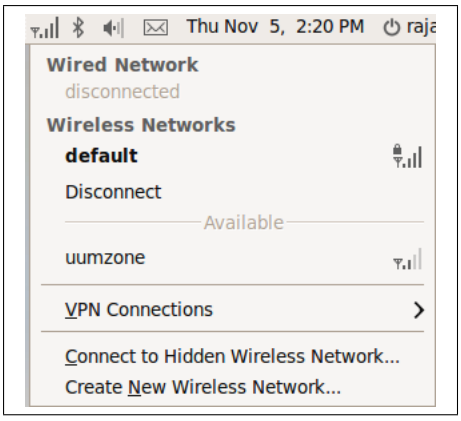



*Figure 1.5.* Wireless Connection

The rise in numbers of RAP will give many detrimental effects, and such vulnerabilities can become very complex to be managed, especially by each administrator (network engineer) [43, 44]. Rapid action should be taken to resolve the issue of RAPs, and an alternative is through traffic characterisation between the wired and wireless networks.

## 1.4 Research Questions

In conjunction to the problem statement above, there are three major research questions to be highlighted in this research. Each question consists of other sub-questions.

i. How can a suitable testbed be designed for detecting RAPs by bridging packet capturing and traffic analysis structures together?
    a. How can a packet capturing structure be designed for grabbing a packet flowing inside the LAN?
    b. How can a traffic analysis structure be designed for analysing captured data packets?
    c. How can a logical network testbed be laid out by integrating packet capturing and traffic analysis structures?

ii. How can a detection mechanism be developed using a design testbed that consists of packet capturing and traffic analysis structures?
    a. How can a physical network testbed be deployed that refers to 1(a), 1(b), and 1(c)?
    b. How can a packet capturing engine be coded by modifying the existing packet capturing library to suit the RAP detection mechanism?

c. How a traffic analysis structure be built from selected traffic characteristics for analysing captured data packets?

iii. How can a newly developed RAP detection mechanism be evaluated based on the combination of packet capturing and traffic analysis structures?

a. How can the differences between wired and wireless traffic characteristics in detecting RAP be evaluated?
b. How can a performance of a proposed RAP detection mechanism be evaluated?

## 1.5 Research Objectives

This thesis derived the research objectives from the same research questions, which consisted of three major goals, which are:

i. to design a suitable logical network testbed for detecting RAP using packet capturing and traffic analysis structures.
ii. to develop a detection mechanism using the design testbed that consists of packet capturing and traffic analysis structures
iii. to evaluate a new RAP detection mechanism developed based on the combination of packet capturing and traffic analysis structures.

## 1.6 Research Scope

This research focused on how to detect RAPs from the perspective of two major structures, which are packet capturing and traffic analysis. In addition, the research also observed three major processes, which are designing, developing, and evaluating the mechanism for packet capturing and traffic analysis. The design process covers the design of a testbed to support the packet capturing and traffic analysis design structure.

The development then follows this design, which is highlighted by the coding process of packet capturing and traffic analysis, and a combination of both shall become the new workable Traffic Characterisation Mechanism (TCM). The next section lists the research steps taken to achieve the research objectives.

## 1.7 Research Steps

This research work had several steps to be accomplished toward achieving the research objectives and thus answering the research questions, as listed below:

i. survey of existing RAP detection mechanism from other related work to find research gap,
ii. design a network testbed for housing RAP detection mechanism,
iii. develop packet capturing and traffic analysis engine for characterising in wired and wireless environments, and
iv. evaluate the differences between wired and wireless traffic characterisation.

## 1.8 Research Contribution

The overall contribution of this thesis is to develop a TCM for detecting RAP through differentiating between wired to wireless traffic. This mechanism is supported by a packet capturing structure which is used to capture filtered TCP flags and time stamped at the inbound network point. Next, the time stamped is processed through the traffic analysis structure, handling by equal grouping and averaging to produce a zone mean. An average of different zone mean can generate a global mean or threshold. The lowest threshold either from wired or wireless is selected as the RAP detection indicator. The detail of research contribution are listed below.

i. The design of a suitable testbed for detecting RAP by bridging packet capturing and traffic analysis structures together.

   a. The design of packet capturing structure for grabbing a packet that flows in the LAN.
   b. The design of traffic analysis structure for analysing a captured data packet.
   c. The layout of logical network testbed by integrating packet capturing and traffic analysis structures.

ii. The development of a detection mechanism using the design testbed that consists of two structures: packet capturing and traffic analysis structures.

   a. The deployment of a physical network testbed that refers to 1(a), 1(b), and 1(c).
   b. The development of a packet capturing engine by modifying the existing PCAP library to suit with the RAP detection mechanism.
   c. The building of traffic analysis structure from selected traffic characteristics for analysing captured data packets.

iii. The evaluation of a newly developed RAP detection mechanism based on the combination of packet capturing and traffic analysis structures.

   a. The comparison of differences between wired and wireless traffic characteristics in detecting RAP.
   b. The evaluation of performance of RAP detection mechanism before and after the implementation.

## 1.9 Organisation of the Thesis

This thesis is organised into six chapters, as follows:

**Chapter One** provides an overview on the thesis as a whole. It outlines the issues

related to the research and highlights the importance of the research. This chapter forms the problem statement of the research and addresses the motivation in doing this research. The chapter also states the scope of the research, its objectives, steps in completing the research, and key contributions of the research.

**Chapter Two** consists of a literature review that examined background materials on Rogue Access Point detection, which defines the general framework for this research. It describes traffic characteristic as a key for RAP detection in wired LAN and its main function in the RAP detection. The chapter reviews and classifies currently available RAP detection schemes. The chapter then concludes by comparing various types of RAP detectors, algorithms, and testbeds used for rectifying RAP.

**Chapter Three** addresses the design and experimentation of RAP detection mechanism used in carrying out this research. The chapter begins by introducing three models used in designing the mechanism which are training, verification, and mathematical models. The three models are very important in a research prototype development where a testbed is used to experiment on traffic characteristics between 802.3 to 802.11g, and 802.11n. The experimentation of the testbed is discussed in greater detail.

**Chapter Four** emphasises on threshold discoveries, which is a reflection of chapter three. The result from a prototype experimentation between wired and wireless traffic characterisation is channelled toward generating an indicator or threshold for differentiating between 802.3 to 802.11g, and 802.11n.

**Chapter Five** presents the verification of two different wireless modes; 802.11g and 802.11n. All TCP flags are covered and discussed in their respective zone like in the

third chapter, namely the training stage. The verification between this threshold to the two wireless modes (802.11g and 802.11n) is to look for an existence of a genuine RAP, Potential RAP, or Non-RAP. This is measured through a percentage dissimilarity between those wireless to the threshold. This chapter also highlights the importance of the verification stage in order to detect RAP.

**Chapter Six** is the concluding chapter of this research in detecting RAP using a traffic characterisation mechanism. This chapter starts by summarising the research importance that has become the core component that made this project successful. Additionally, the importance of training and verification stages that this research focused upon has been marked as the main contribution toward the body of knowledge. This thesis ends by offering two viable future research directions where the threshold that this research contributed can be injected to, which are SNMP Agent and Management Information Base (MIB).

# CHAPTER TWO
# LITERATURE REVIEW

## 2.1 Introduction

This chapter will discuss RAP in greater detail from several aspects, such as RAP terms, the implication of RAP to the network, and how it is detected by looking at previous related works. The discussion scope also covers a method to overcome the RAP problem through finding differences between wired and wireless traffic characteristics. Furthermore, this chapter highlights the role of packet capturing, packet filtering, and equal grouping for analysing network traffic in detecting RAP that is hiding within the network territory.

In addition, the discussion also points to related works being done by other researchers. Their approaches have been reviewed and analysed for supporting this research in developing a new RAP detection mechanism to detect RAP either through wired or wireless environment, which is also further elaborated upon in this chapter. At the end of the chapter, the RAP detection algorithm and testbed are listed down and aggressively reviewed to support the design and development of a novel RAP detection mechanism.

## 2.2 Rogue Access Point (RAP)

RAP is defined as an unauthorised Access Point or illegal Access Point being setup without a permission and even unknown to the management and authorised individuals, like the network administrator, within the organisation [45, 19, 46, 47, 48, 49]. In normal RAP cases, the device is setup by two types of users, namely intruders or hackers, and the organisational staff who have their own respective intentions. On the one hand, intruders or hackers use RAP for breaking into any

network security system and executing illegal activities, such as stealing, spying, or tapping valuable organisational information [50, 51, 52, 53, 54]. While on the other hand, organisational staff members would use APs for extending their network connection without any malicious intent, but without proper configuration of the extra AP, this would contribute towards network vulnerabilities for the LAN. For example, a staff member who buys a new computer or network printer with wireless capabilities will require an extra network connection point which is already occupied. He or she would overcome this limitation by plugging in AP into the current data point. Even though this approach solves their problem, without secured configuration and proper deployment strategy, it will generate a bigger crisis to the organisational LAN [19, 55, 56, 52]. Whatever devices that are connected to LAN and not belonging to the organisation are considered as rogue devices, regardless of whether it is malicious or otherwise.

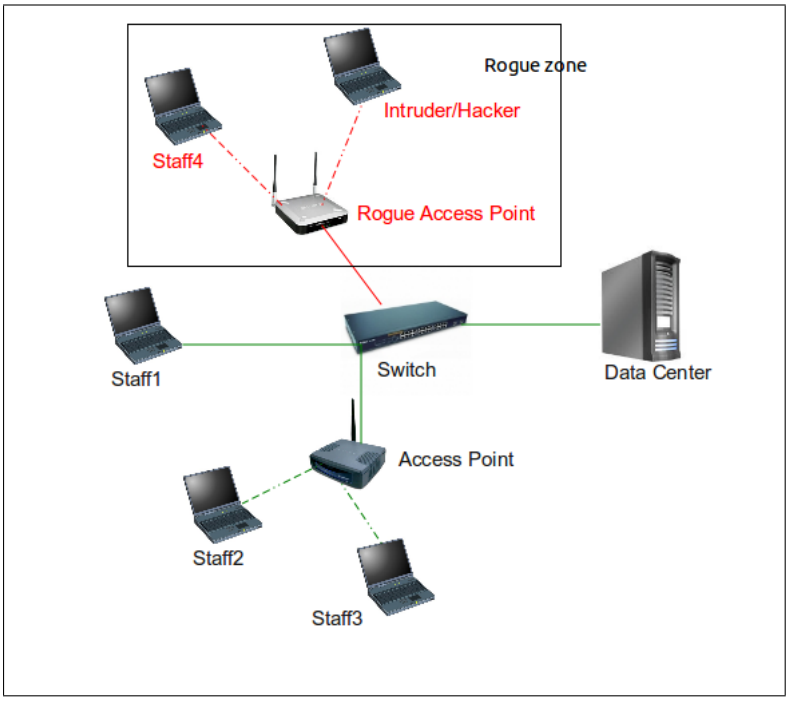



*Figure 2.1.* Wired-Wireless Network

Figure 2.1 shows a simple LAN that consists of a data centre server, switch, wireless

access point, client machines (computers), and users. Users may access the data centre through APs which are deployed by the organisation. However there is another AP which cannot be used by authorised parties. The RAP concern is that the AP is an unauthorised wireless device which is connected without permission and illegally creates a "rogue zone". Even though it looks the same (if it is configured to use the same device specifications), it is not permitted. Users might accidentally connect to the RAP and their computer would be vulnerable to rogue users like hackers. It is also breaching LAN security and overruling some critical network security mechanisms, such as the firewall [57].

Whatever network vulnerabilities that could possibly occur in LAN is facilitated by the RAP [19, 46, 47, 48, 49, 55]. Any intruders or rogue users will not get any chances to penetrate the network if the RAP is stopped as soon as possible. The next section will discuss several implications of RAP if it is connected to the organisational LAN.

## 2.3 RAP Implications

It would be a worst case scenario if the RAP is silently connected to one of the organisation's data point without anybody being aware of its existence. In the proceeding sections, a discussion on two major implications, namely AP with default configuration and overruled RADIUS security implementation, which have the potential of causing problems to the organisational LAN, shall be presented.

### 2.3.1 AP with Default Configuration

AP with default configuration means that the device is being used with the default Service Set Identifier (SSID), where the name is actually "default" or the product name, like "dlink". In addition, default configuration of AP solely appear and work without any specific configuration and also without any specific security barrier

(encryption pass-phrase). This phenomenon is very critical where an intruder can easily connect to that particular AP without having to identify or authorise themselves [58, 59, 60, 61, 62, 41].

A good approach for implementing AP security is by using WEP with a proper pass-phrase, but this sometimes does not guarantee airtight security to prevent attempts by attackers [14]. Moreover, a strong encryption key like WPA or WPA2 can be used for increasing the security. Unfortunately, the existence of RAP attached to LAN would be bypassing the security policy, i.e., the AP itself is not permitted to attach itself to the LAN, and the worst case is that it is implemented using the default configuration. Even though having more APs can be of benefit to the organisational staff, it exposes a vulnerability of the LAN to someone who may have malicious intentions and want to get into the network [63, 64, 65, 66, 41].

A sniffing tool like Netstumbler can easily discover the RAP that can be manipulated easily for gaining access into the network without having to provide a specific SSID key and tight security pass-phrase [67, 68, 69, 70, 14, 71, 72, 63, 73]. As a result, the network is widely open to anybody and produce high levels of vulnerabilities which are difficult to be controlled and thus need more effort to block them.

### 2.3.2 Overruled RADIUS Security Implementation

Some organisations use a centric authorisation approach like 802.11X to control their legal users, in other words for them to gain access to the corporate LAN, they need to get permission from a centralised server. This mechanism is also called the RADIUS Server (see Figure 2.2). Users will be routed to the RADIUS server through the AP and prompted for a login and password to be checked by the RADIUS server. If it is valid then they can stay connected to the network through the AP.

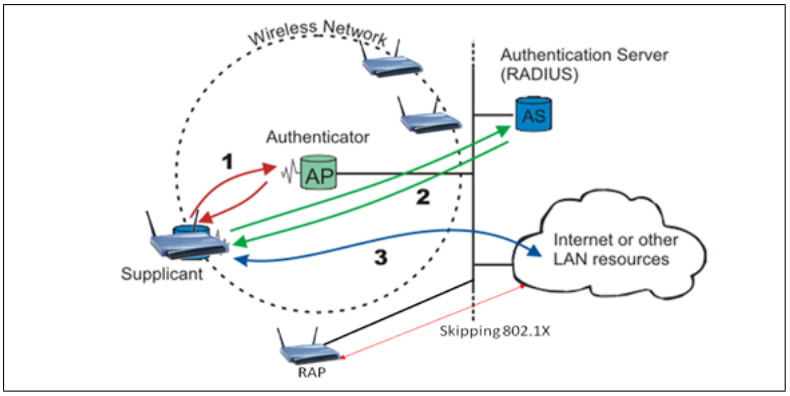



*Figure 2.2.* Avoiding 802.1X

RAP will break this rule by skipping the RADIUS server authorisation process because RAP is not setup to connect to the RADIUS server and its presence is not known to network administrator [74, 75]. Activating 802.1X should be done manually at the AP itself and this does not necessarily occur in the RAP. As a result, the RAP is beyond their control and even though it never has a chance to be configured, it has already penetrated and gained illegal access to the LAN. However, there is a way to stop this RAP from entering the network. The next topic will elaborate how to detect RAP while it is connected to the organisational LAN.

## 2.4 RAP Detection Approaches

The existence of RAP within the network environment is sometimes undetectable and could lead to becoming the worst case scenario for the organisation. Even though the network is readily equipped with a robust high-end security mechanism, RAP will break this security gate by bypassing them as discussed previously. This thesis shall now look into some related work that focused on detection approaches, all of which shall be categorised into three different categories, as presented in the following sections.

### 2.4.1 Passive Monitoring

Generally network traffic that flows within the wired and wireless environment is known to have different characteristics. Both of them operate using different media and the traffic volume is not static and always dynamic, depending on how frequent users demand information retrieval. Because of this inherently dynamic nature, there should be a special monitoring approach to monitor the traffic movement, such as passive monitoring. This passive monitoring should immediately take place at the switch where the AP is connected. The difference between wired and wireless Round Trip Time (RTT) can be observed and RAPs can be detected using this approach.

Passive monitoring utilises a wait-and-scan method of network traffic that bypasses a specific point, and it can be achieved using RTT [20]. RTT means that whichever party sends a packet with specific TCP flags must send back a return packet with acknowledgment flags. This round trip is measured by time stamping at the beginning and end point at both sides. The time difference is compared to characterise either it is a wired or wireless network.

Another approach was proposed by Wei (2007) in [76], which consisted of two different algorithms, namely passive monitoring with training and without training using sequential hypothesis testing. This technique is used to capture packet headers to look for TCP ACK–pairs, which are then analysed. Both algorithms exploited the fundamental properties of 802.11 CSMA/CA MAC and half duplex wireless channel to find the different characteristics between wired and wireless networks.

### 2.4.2 Using Visualisation

The most important in identifying RAP is to find its actual location [77, 47]. The first approach, passive monitoring, uses scanned network traffic as a way to detect RAP and

point to its location where its setup is known. In normal circumstances, the location of the AP is not known especially in the wireless LAN environment, but the AP can be used as a scan device to detect other APs. Schweitzer (2007) in [22] used APs as a mechanism to scan other organisational AP and built a graphical "profile map". This visualisation approach analyses the strength of wireless signal received by legal APs and plot its location on the map. This profile is then used to identify any APs that is not shown on the legal map, thus these can be concluded as RAPs.

### 2.4.3 Traffic Characteristics

When traffic is flowing inside a medium, it looks similar and cannot be differentiated as being wired or wireless. Both use the same protocol, TCP/IP, which is the de facto protocol implemented by many manufacturers involved in developing network devices. Even though both 802.3 and 802.11 structures have the same network traffic packets, the way both behave is quite different, especially relating to time factors. These differences can be found through studying traffic characteristics that they both have, and by doing this, it is easy to assume that a wireless device found in wired structured as a potential RAP.

There are three kinds of traffic characteristics as mentioned in [19, 55]; one to one corresponding, link speed, and inter-packet switching. One to one corresponding refers to one MAC address for one device. If a recorded MAC with their respective wired device is detected different, then the traffic is being sent by different devices, which could potentially be RAP. Of course this is only an assumption made toward the unknown MAC address, which is not recorded in the legal AP list.

Another traffic characteristic category that can assist in finding differences between wired and wireless network is link speed. As usual, the wired medium is faster and

better compared to wireless medium. With fast ethernet technology, a wired packet can be transmitted up to one billion bits per second, whereas a wireless network can send packets around 300 million bits per second. Moreover, an ethernet network can transport about 100 million bits per second while 802.11g is capable of about half of that amount. With this difference, something can be done to differentiate between those different technologies.

In addition to the two above categories, the difference between wired and wireless environment also can be detected through measuring the gap between packets. This process is called inter-packet switching measurement. As previously discussed, the link speed between wired and wireless structures have a difference and this will affect the packet interrelation (packet gaps). This packet gap can be measured for differentiating wired and wireless networks. If the gap is small and very close among packets, it can predict to be corresponding to a wired structure, otherwise it is considered to be wireless.

## 2.5 Packet Capturing

*Tcpdump* [78] was originally written in 1987 by Van Jacobson, Craig Leres, and Steven McCanne who were at the time, working in the Lawrence Berkeley Laboratory Network Research Group. By the late 1990s, there were numerous versions of *tcpdump* distributed as part of various operating systems, and numerous patches that were not well coordinated.

*Tcpdump* is used to solve and troubleshoot network problems during that time. They were working at the Lawrence Berkeley Laboratory Network Research Group. Starting from that time, *tcpdump* had evolved until the late 1990s with many patches to various operating systems, not just limited to Unix, but also to Windows and Mac.

In 1999, Michael Richardson and Bill Fenner created www.tcpdump.org.

The core library of *tcpdump* is *libpcap* [78, 79, 80, 81]. PCAP is an acronym of Packet Capture and very relevant for network administrators to monitor and control how traffic moves from users to the server. By observing the traffic flow, this may assist the network engineer to plan and execute a more organised network packet movement [81, 82, 83, 84]. Additionally, it also can be used for future trend and forecasting when the need to expand the network and to downsize for optimisation arises. Without having a clear picture of what really occurs within the network, it would be difficult to formulate and implement a network design, especially when there is newly invented technology which need to be implemented [85].

The original *libpcap* is written in C, however for other languages, a wrapper is used to minimise the interfacing problem between other languages and the C programming language. *Libpcap* comes with a nice GUI and its capabilities will help any newbie programmer easily by facilitating the process of adopting any module into their program.

In this research, project *libpcap* has become compulsory in designing, developing, and evaluating a Packet Capturing Mechanism. This work adopted the complete cycle of capturing procedure from *libpcap* into the RAP detection structure starting from packet capturing configuration, open packet capturing state, capturing arriving packet, processing packet into host centric, pass to Traffic Analysis, and close state. The packet capturing itself will capture traffic data while being in promiscuous/hidden mode. While this process is taking place, packet filtering needs to fully select which packets are required for solving network security issues [86, 80, 87]. Then, a time stamp is executed between those selected packets while being scooped, as suggested

by Orosz (2010) in [81].

The existence of Packet Capturing (*libpcap*) is not enough without knowing what kind of traffic is to be captured and processed. The next section will shed further light on this topic.

## 2.6 Traffic Characterisation

Heterogeneous networking environment is far more unpredictable than a homogenous one. It is difficult to find one homogenous network unless it is built within a small scale environment, many differences can be controlled, such as small differences in OS, hardware specification, NIC, and etc. When mentioning about traffic, it is not out of scope of heterogeneity in its functioning. A difference in network layers could also contribute to this difference. However, for the purpose of this research, the focus is data flow at Layer 3 and Layer 4 which are network layer and transport layer of the OSI model. This two layers play an important in this research which captures a packet (Layer 3) or segment (Layer 4) in a passive mode. Passive means waiting for the packet to arrive at the network interface where it is then grabbed. A cleansing process is then executed afterwards.

Cleansing is a method of how a packet or segment is arranged according to a filter that is imposed at the opening of a packet capture. Layer 3 information like IP is extracted and represents a host. Whereas Layer 4 is scoped into TCP flag differences like SYN, SYN/ACK; FIN, FIN/ACK; PSH, PSH/ACK, and Payload/ACK [88, 89, 90, 91]. Figure 2.3 shows where these TCP flags are located in the TCP packet.

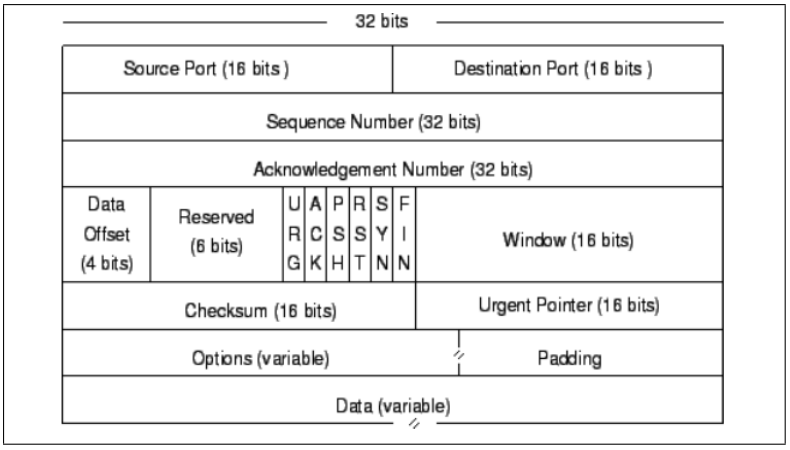



*Figure 2.3.* TCP Packet Format (adopted from [88])

TCP flag is labelled as FIN on the rightmost of the figure, SYN on the second, third is RST or reset, followed by PSH or PUSH, then ACK (Acknowledge), and URG (Urgent). Only FIN, SYN, PUSH, and ACK were considered in this research. Other parts like Source, Destination, Sequence Number, Acknowledgment Number, and Windows is part of packet capturing information for analysing whether there is any difference between wired and wireless structures. Table 2.1 briefly elaborates each TCP flag in the TCP packet.

Table 2.1
*TCP Packet Structure*

| **Field** | **Explanation** |
|---|---|
| Source port | TCP port of sending host |
| Destination port | TCP port of destination host |
| Sequence number | Ensures all bytes have been received |
| Ack number | The sequence number of the next byte |
| Data length | Length of the TCP segment |
| Reserved | Reserved |
| Flags | What content is in the segment |
| Windows | How much space is in the TCP windows |
| Checksum | Ensures validity of the header |
| Urgent Pointer | If urgent data is being sent, this specifies the end of that data in the segment |

As mentioned earlier, this research will only look at SYN, FIN, PUSH, and data exchange (PAYLOAD) for packet capturing purposes. Normally, communication between source and destination occurs involving a few sequence steps, as shown in Figure 2.4.

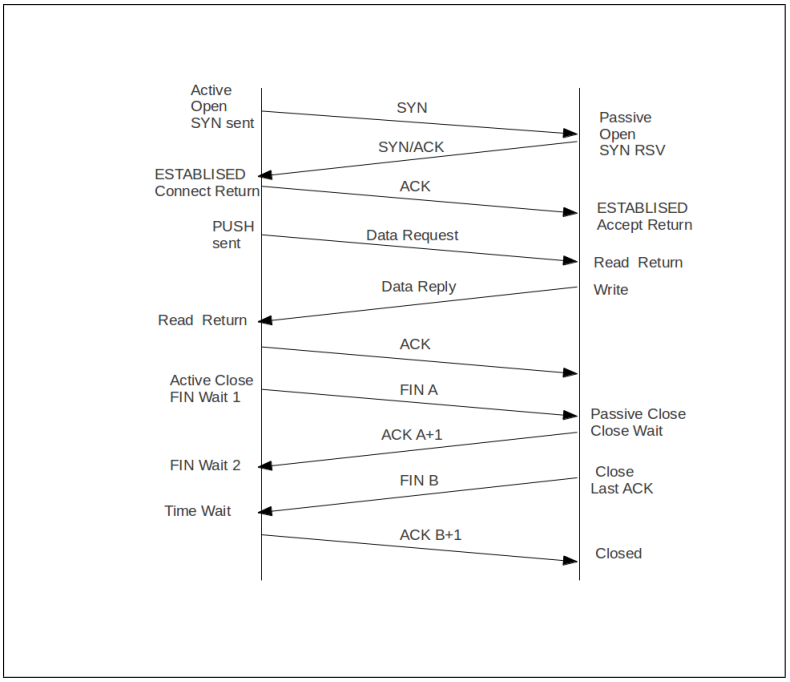



*Figure 2.4.* TCP Packet Exchange (adopted from [88])

TCP connection starts by invoking a three-way handshake consisting of SYN, responding back with SYN-ACK (destination), and finalising with ACK (source). Sustainability between source and destination depends on how frequent they ACK each other. If not, sometimes the connection terminates with passive close when a certain time period expires. A successful collaboration between both sender and receiver refers to whatever the request should follow with the ACK response. As a result this matter has become a rubric for packet capturing. The most frequent and very active TCP flag is ACK.

## 2.7 Packet Filtering

Packet filtering is a process in which a flow of network traffic packets is checked in order for it to be allowed to or denied from flowing through, while referring to a specific rule being specified in the configuration list. A popular packet capturing like *tcpdump* is ready with this feature where users can specify which parameters are to

be implemented in the filtering process [78, 92]. Without a filter parameter, packet capturing operates in default mode where all packets are captured. As a result, a lot of unwanted packets are grabbed in a large footprint file or in computer memory. It is important to have a suitable filter parameter to feed into this research work [93, 94].

Previously, many studies had revealed a method of securing the network from vulnerabilities, like Denial-of-Service attacks, using packet filtering approaches [95, 96, 97, 98, 99, 91, 100]. Each packet is screened for any unauthorised patterns for identifying these attacks. Meanwhile RAP which is no different from other devices that produce packets to be sent and received, when compared to DoS. However, RAP also needs packet filtering to filter TCP flags that specifies the differences between wired and wireless APs.

The allowing and denying of specific parameters can be achieved in two consecutive methods [78]; within packet capturing execution or outside the capture itself. The first method assumes that the filtering is part of the capturing. Before the capturing runs, users must clearly state the filtering parameters for the *tcpdump* execution commands. The process of capturing and filtering occurs concurrently. This affects the performance of a router while performing both sequences.

The second method works opposite to the first method, and separates packet capturing and packet filtering into different events. The capturing result is stored into a flat file, then the filtering is performed afterward using third party tools or users create their own tools. This separation is more practical where the capturing and filtering are running on their own specific space, while not interrupting each other.

For fulfilling the objective of this research project, the *libpcap* library and open

source code provided could be used to completely run the packet capturing and packet filtering simultaneously. This is similar to the first method, as mentioned above. From various parameters of filtering [78], only several were chosen like *tcp-fin*, *tcp-syn, tcp-push*, *tcp-ack* handle by tcpdump (see Table 2.2) and more specific respond flags (FIN/ACK, PSH/ACK, SYN/ACK and PAYLOAD) were filtered through the filtering structure.

Table 2.2
*Packet Capturing and Filtering Parameters*

| Parameters | Usage |
|---|---|
| *proto* | Qualifiers restrict the match to a particular protocol. Possible protos are: *ether*, *fddi*, *tr*, *ip*, *ip6*, *arp*, *rarp*, *decnet*, *tcp* and *udp* |
| *TCP flags* | *tcp-fin*, *tcp-syn*, *tcp-rst*, *tcp-push*, *tcp-ack*, *tcp-urg* |

These two parameters (proto and TCP flags) are injected differently, while packet capturing and filtering are executed. A TCP protocol is provided before the capture is executed. Meanwhile the flag parameters are logically checked after the packet is grabbed and held, either to log into a flat file or dropped. Both parameters are implemented in packet capturing and filtering codes, and they are going to be discussed further in Chapters 3 and 4.

## 2.8 Equal Grouping

In general, equal groups can be defined as the number of groups having the same number of equivalent items. Normally, the items are similar in terms of their characteristics. It is also used to compare specific features among generated groups.

In Mathematics, Kim (2007) in [101] emphasised that this model helps teachers to train their pupils to understand how to interpret multiplication problems. Sometimes, it also

sharpens the abilities of school children to see a relationship between multiplication and division, because at certain stages, division can be used to find specific variables in equal groups' group generated. The teacher draws equal group models to help students get an overall picture of how multiplication and division works [102].

Equal groups can be formulated into number of groups multiplied by group sizes, which is then equivalent to the product [103]. Figure 2.5[1] shows an Equal Groups Model for describing the formula in graphical order, following the equal groups' formula.

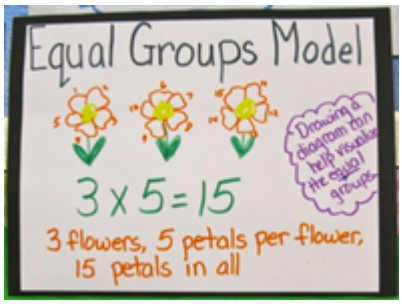



*Figure 2.5.* Equal Groups Model

The items are similar, and the focal point is to count the number of petals (product). Number three represents flowers (number of groups) and five shows number of petals at each flower (size of groups). Equal groups can be classified into three, as shown in the following characteristic of the model.

i. Unknown product/whole unknown (multiplication)

   The total is unknown but the group numbers and sizes are defined. Multiplication will solve this problem.

   Example: 3 flowers x 5 petals per flower = 15 (unknown).

ii. Group size unknown (partition division)

[1] Adapted from www.scholastic.com

Only groups' number and total are specified. This problem needs division between the total (product) to number of groups to find groups' size.

Example: 3 flowers x (unknown) = 15 petals in all. 15 ÷ 3 = 5. Five is a partition in each flower (group).

iii. Number of group unknown (measurement division)

This third type emphasises on an unknown groups' number, whereas size and product are known. Again, division is needed to conclude what number of groups will be in this category, which is called measurement section or division.

Example: (unknown) x 5 = 15. 15 ÷ 5 = 3 (groups' number)

According to the three equal group types, it can be modelled as Measurement x Partition = Multiplication [104]. Equal groups also can be used in quantitative research involving statistical analysis, for example to divide a population into quartiles. Each quartile is measured by 25%, 50%, 75%, and 100%. The percentage is a rank given to individual data that falls into different quartile ranges after it is arranged in ascending or descending order in their population. In this situation, there are four equal groups involved to measure quantitative data. The number of groups depends on the needs and sometimes can be up to hundreds [105].

In this thesis, equal grouping is part of the Traffic Characterisation Mechanism and will follow the Equal Groups Model that is already discussed previously. Product and groups' size are known but number of groups has to be drilled from the number of packets being captured and filtered. Chapters 3 and 4 will elaborate these issues.

## 2.9 Network Management Issues

As discussed before, RAP is a network security phenomenon that should be eliminated before it can interrupt and open more vulnerabilities to the LAN [106, 107, 108]. As

a network security issue, RAP must be solved through proper network management structure which is used to plan, design, execute network task, and monitor network traffic. Moreover, a broader use of wireless as a network expander and ease of mobility use have placed a greater responsibility on network management to solve these potentially problematic RAP issues [109, 31, 110].

Network management issues can be solved through five functional areas, like FCAPS (Fault, Configuration, Accounting, Performance, and Security management) [111, 112]. RAP can be classified under the network security functional area. Network management has three main components, namely management entities, agent, and management database. These three components will be elaborated upon in the Simple Network Management Protocol (SNMP) sub-section below, where SNMP itself is an established tool for supporting network management.

### 2.9.1 Simple Network Management Protocol (SNMP)

SNMP exposes management data in the form of variables on managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications. In typical SNMP usage, there are a number of systems to be managed, and one or more systems managing them. A software component called an agent runs on each managed system and reports information via SNMP to the managing systems. [27, 32, 113]

Essentially, SNMP agents expose management data on the managed systems as variables (such as "free memory", "system name", "number of running processes", "default route"). The managing system can retrieve information through the GET, GETNEXT, and GETBULK protocol operations or the agent will send data without being asked using TRAP or INFORM protocol operations. Management systems can

also send configuration updates or control requests through the SET protocol operation to actively manage the system. Configuration and control operations are used only when changes are needed to the network infrastructure. The monitoring operations are usually performed on a regular basis [114, 115, 116, 117].

The variables accessible via SNMP are organised in hierarchies. These hierarchies, and other metadata (such as type and description of the variable), are described by Management Information Bases (MIBs). An SNMP-managed network consists of three key components (see Figure 2.6):

- managed device,
- agent, and
- network management systems (NMS).

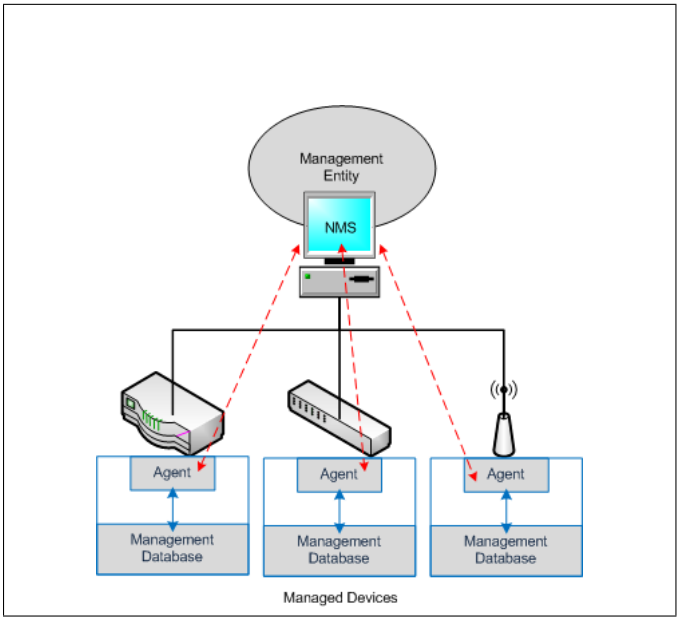



*Figure 2.6.* SNMP Basic Component (adopted from [27])

A managed device is a network node that contains an SNMP agent and resides on a managed network. Managed devices collect and store management information and

make this information available to NMSs using SNMP. Managed devices, sometimes called network elements, can be any type of device including but not limited to, routers, access servers, switches, bridges, hubs, IP telephones, computer hosts, and printers.

An agent is a network management software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP.

A network management system (NMS) executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs may exist on any managed network.

SNMP itself does not define which information (variables) a managed system should offer. Rather, SNMP uses an extensible design, where the available information is defined by management information bases (MIBs). MIBs describe the structure of the management data of a device subsystem; they use a hierarchical name space containing object identifiers (OID). Roughly speaking, each OID identifies a variable that can be read or set via SNMP. MIBs use the notation defined by ASN.1 [118].

In telecommunications and computer networking, Abstract Syntax Notation One (ASN.1) is a standard and flexible notation that describes data structures for representing, encoding, transmitting, and decoding data. It provides a set of formal rules for describing the structure of objects that are independent of machine-specific encoding techniques and is a precise, formal notation that removes ambiguities.

ASN.1 is a joint ISO and ITU-T standard, originally defined in 1984 as part of

CCITT X.409:1984. ASN.1 moved to its own standard, X.208, in 1988 due to its characteristically wide applicability. The substantially revised 1995 version is covered by the X.680 series. An adapted subset of ASN.1, Structure of Management Information (SMI), is specified in SNMP to define sets of related MIB objects; these sets are termed MIB modules [32].

The MIB hierarchy can be depicted as a tree with a nameless root, the levels of which are assigned by different organisations. The top-level MIB OIDs belong to different standards organisations, while lower level object IDs are allocated by associated organisations. This model permits management across all layers of the OSI reference model, extending into applications such as databases, email, and the Java Enterprise Edition reference model, since MIBs can be defined for all such area-specific information and operations.

A managed object (sometimes called the MIB object, an object, or MIB) is one of any number of specific characteristics of a managed device. Managed objects comprise one or more object instances (identified by their OIDs), which are essentially variables.

## 2.10 Related Works

Adya (2004) in [119] suggested that detecting RAP can be achieved through detecting a fault in wireless LAN. They list out four faults that can be detected, which are wireless network fault, connectivity problem, performance problem, and network security problem. However, all these four faults are not easy to be solved, which is probably because there was no intelligent mechanism that can be used during that time. They proposed Conduit for enabling bootstrapping and fault diagnostic of any disconnected client. With Conduit, there was also a mechanism for detecting RAP. However, the details of this part was not described further on how the RAP is detected

and eliminated. They did mention about SNMP, but it was not being used for detecting RAPs as part of their solution. It was just for data collecting diagnostic purposes.

Yeo (2004) in [120] stated that using wireless monitoring can reveal more information about PHY/MAC. In addition, such information is more important than such provided by SNMP or wired monitoring. Their implementation produced a different characterisation between WLAN traffic captured at a different departments. That characterisation consisted of PHY/MAC layers, traffic mix of different frame types, and temporal characteristics. Their approach produced a result that consists of legal and rogue activities. RAPs also can easily be discovered. However, using a wireless client *sniffer* for capturing traffic is not the best approach. It can support within a specific time frame only. Nevertheless, RAPs may appear outside that time frame. Doing the tasks ceaselessly for 24 hours non-stop will consume more manpower and efforts. Wired monitoring is more reliable for overcoming such problem. They agreed that SNMP can support in solving the existence of RAPs, but it was not as good as wireless monitoring. However, the combination of SNMP to wireless or wired will produce more tangible outputs and will be easier to be managed elsewhere. Nowadays, SNMP technologies have been brought forward with many enhancements that allow more functional tasks to be included, especially related to this particular issue.

Many organisations are looking into low cost RAP detectors to minimise their overall operational cost. Bahl (2006) proposed DAIR (Dense Array of Inexpensive Radios) in [121], who used a normal desktop PC with wireless client adapter to become the RAP detector. They connected it to the wired LAN. It is low in cost, but the question is how many PCs needed to be installed to cover the whole network. As far as this research is concerned, the wireless client has small coverage when compared to a normal AP or wireless sensor, and only applicable to small-scale networks.

Wei (2006) in [122] classified wireless and wired LANs using Iterative Bayesian Inference. It is a classification scheme to differentiate Ethernet and WLAN TCP flows based on measurements collected passively at the edge of a large network. It is believed that a TCP flow will traverse a WLAN inside the network. As a result, it is easier to rectify the availability of APs and also RAPs. Consequently, it is not practical for campus network, especially since it is only involved in collecting traffic at the edge of the network.

Another approach is using a verifier to send a test packet from inside the LAN to the outside through a wireless structure and reach a wireless sniffer [46]. This sniffer will try to identify whether there is an appearance of RAP or otherwise. The verifier uses a greedy algorithm to eliminate RAPs, whereas the sniffer uses a probabilistic algorithm to scan encrypted AP traffic that relies on observed packet size. This mechanism is suitable for small LANs with several hosts but it is not like the campus network, since it is impossible to be implemented, especially after implementing the verifier. The questions that arise include where to put the verifier, and also how many verifiers can cater for the whole campus size. An internally detecting mechanism is suitable for detecting RAPs and finally eliminating it.

Deshpande (2006) in [123] said using a wireless sniffer for a huge LAN is not suitable and it is also not easy to monitor various channels at one time within a specific amount of time. They used a comparison method to compare different sampling channels for comparing each signals from APs to rectify any RAPs. They also felt that this technique had a challenge, especially to differentiate between active and non-active channels. They did mention about the weakness of using a wireless sniffer on a huge network, which perhaps is not relevant, but research still continue to enhance it. Detecting from wire is more relevant for huge campus network and the existing

protocol like SNMP can benefit much from detecting RAPs. SNMP agent can stand at a point very near to the suspected AP. As a result, the detection of RAPs is faster and easier at that specific location.

So far, most of the current solutions for detecting RAPs are not automated and always depend on a specific wireless technology. There are different variants within 802.11 (a, b, g, and n mode). Shetty (2007) in [124] proposed an automated mechanism that can be installed on any router. In addition, the main premise of their approach was to distinguish between an authorised WLAN host and unauthorised WLAN host which is connected to the RAP by analysing traffic characteristics at the edge of a network. In addition, this research discovered that this solution can be implemented through simulation and just how it is going to be implemented in a real network environment.

TCP pairs between the sender and receiver also can be used for detecting RAPs, as stated by [76]. They proposed a hypothetical analysis in two algorithms, either with training set and without training set. The 802.11b and 802.11g were tested and it was found that there is a difference between Ethernet and wireless TCP pair time. The training set produced higher percentages than the realistic condition, but still there is a difference. The difference still occurred, but the percentage would be small between both Ethernet (802.3) and wireless (802.11) networks.

Hence TCP-pair time plays a specific role for RAP detection. RTT also can do the same in differentiating between wired and wireless LANs. Watkins (2007) brought this RTT forward to track down RAPs by calculating throughput in [125]. This throughput measurement will show a delay between source and destination. A longer delay means there is a problem with data transmission and it could be assumed that there is an involvement of extra wireless medium like APs. This argument is true but

the advancement of the technology like 802.11n will not produce a significant result. Consequently, the gigabit Ethernet, for instance, has increased the gap between wired and wireless networks. Further experiments should be conducted to find a reasonable doubt about the traffic characteristics between 802.3 and 802.11.

Srilasak (2008) in [25] concluded that there is a solution where both RAP detection mechanisms can be combined with SNMP capabilities. The combination considered integrating RAP detection and elimination solutions. Consequently, the detection is done at the sniffer act by AP, whereas the elimination task is executed by SNMP at the switch. The AP will work in two modes, namely normal and sniffer modes. Normal means it works in the same mode as other APs, while a sniffer is performing activities under the promiscuous mode, which will capture all packets arriving at the AP. The modes run at different time frames and should be activated. The packet capture will be compared with authorised APs, like SSID and wireless MAC. If it is not matched, then checking for either connecting to an intranet or other connections should be performed. Otherwise, it is considered as RAP. Moreover, the link where the RAP packet is coming from will be blocked. This can be done by the SNMP agent at the switch. However, a few questions were not answered by them, especially when to changing from normal to sniffer mode. How long does the port blocking work before it is released? What condition allows it to be opened for other link connections?

See Appendix A for a summary of related works which were arranged into their strengths and weaknesses. Next section will highlight on how to choose a detection mechanism, either wireless or wired, active or passive mode based on the previous related works.

## 2.11 Wireless or Wired RAP Detection Mechanism?

Proposing a proper RAP Detection Mechanism should be guided either by wired or wireless link, and active or passive monitoring mode [126, 127]. From observation and reviewed from related works, it can be concluded that the mechanism can be classified into wireless or wired active and passive RAP detection. (see Figure 2.7).

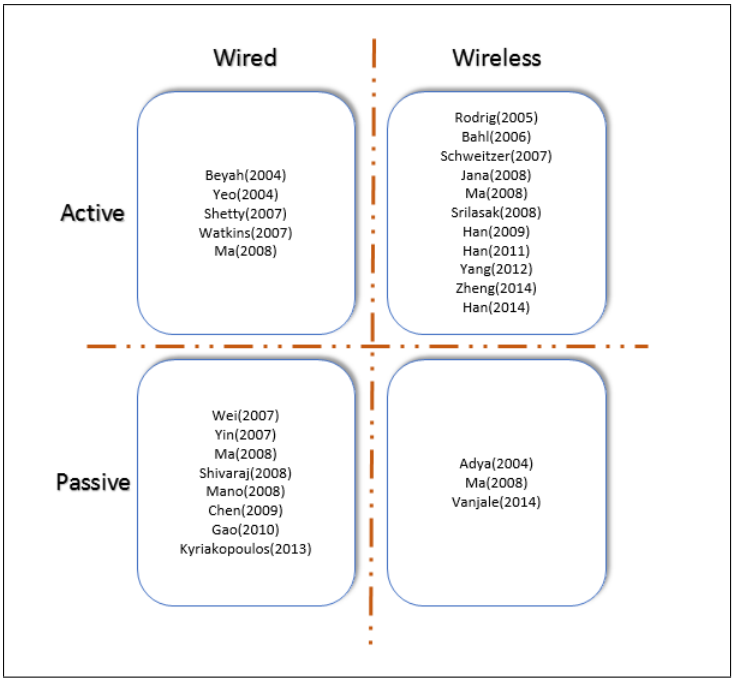



*Figure 2.7.* Link vs Monitoring Mode

As shown by Figure 2.7, many researchers focused on wireless/active mode. Consequently, wired/passive comes on at second place, whereas wireless/passive mode is the last choice. The rank does not indicate whether this is caused by popularity and just coincidence, but rather the ranking is based on researchers' interest.

At this point, the work focused on wired/passive mode because it is more reliable for campus network and has less consumable resources than active mode [76, 46, 21, 128, 17, 129, 130, 54] . In addition, time spent can be more on deploying wireless detectors to very large LAN (campus network). Wireless/active mode is

suitable for a small office network environment [131, 121, 22, 132, 21, 25, 133, 134, 135, 47, 51]. Wired/active is also sufficient for small office RAP monitoring instead of wireless/active, but has less demanding resources [19, 120, 124, 125, 21]. Only [119, 21, 136] looked into wireless/passive mode for detecting RAPs in ad-hoc structures. There is one hybrid mode where all sectors are covered by [21]. For the purpose of achieving the research objectives for this study, the selection was more toward wired/passive mode as the main focus for designing, developing, and evaluating the RAP Detection Mechanism.

## 2.12 RAP Detection Mechanism

After considering wired/passive mode monitoring, more attention was given to a current testbed and algorithm for developing the desired RAP Detection Mechanism. Further discussion is divided into two sub-sections, namely the algorithm and testbed.

### 2.12.1 Algorithm

There are several current algorithms that are being studied that have the potential to assist this research effort, especially in focusing particularly on the RAP detecting segment. In [119], Adya (2004) proposed an algorithm (see Figure 2.8) to detect RAPs based on location. Before that, the MAC address is scanned whether it is registered or otherwise. These two MAC address registration and expected location become key factors to track down RAP on the first hand. In addition, they add another step to check the SSID advertisement either recorded or otherwise. The last step is to check the specified channel for data link connection. If not, it is considered as RAP. So, they try to overcome the RAP detection by proposing four rules, which are MAC, expected location, SSID projection, and checking the expected channel.

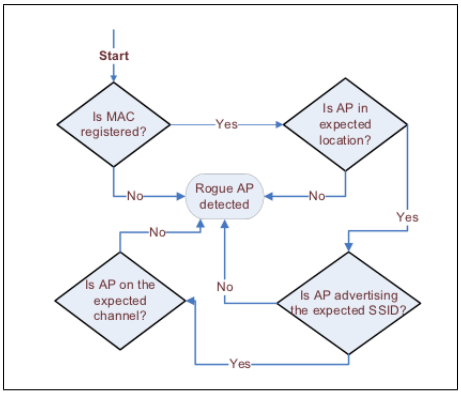



*Figure 2.8.* Flowchart 1 (adopted from [119])

For this work to proceed, only MAC address was chosen to be highlighted in the design. This is because wired and passive RAP monitoring solution factors have been selected. In wired, it is not easy to track the location of APs and scanning SSID broadcasting without support by other devices.

Srilasak (2008) in [25] derived four tracking points in detecting RAPs, consisting of a single major factor and three minor factors (see Figure 2.9). The first checking point is comparing the SSID and MAC address. If it matches then it will go into spoof checker mode until it is proven as a trusted AP, or otherwise RAP. On the other hand, if it does not completely match to the SSID and MAC address, then it is checked to be either connected to intranet or not. If it is connected, it is considered employee's RAP, else it is assumed to be just a normal neighbourhood AP.

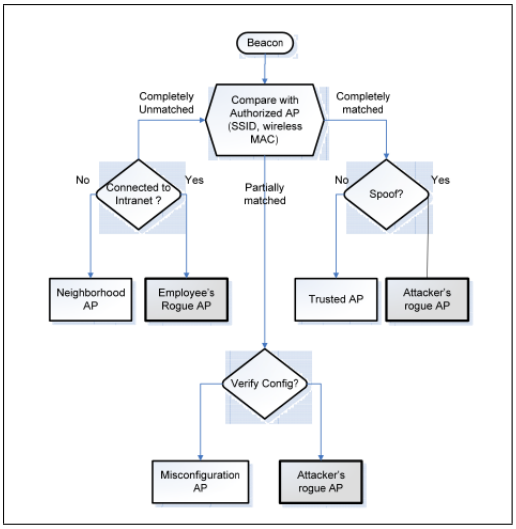



*Figure 2.9.* Flowchart 2 (adopted from [25])

Like Adya, Srilasak also included SSID and MAC address checking. Both solutions are based on wireless detection, but not for the wired side. However MAC can be afforded as the identification of AP at Layer 2. Perhaps, the IP can be used to identify another AP at Layer 3 for detecting it to be RAP or non-RAP.

The next part discusses what was hoped to become a reality, which is a viable solution for RAP detection referring to wired/passing segment monitoring. Mano (2008) in [17] drew a solution to this RAP issue with two processes plus seven rules for checking, which consist of three on the *outbound* and four on *inbound* interface (see Figure 2.10).

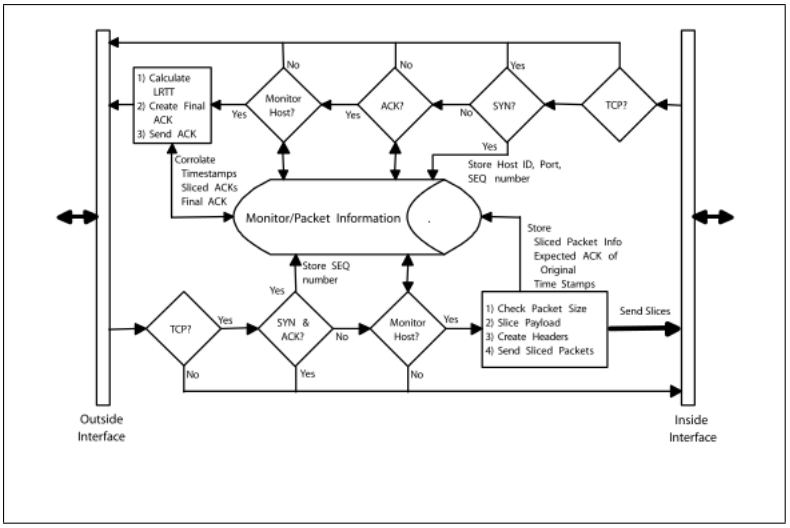



*Figure 2.10.* Flowchart 3 (adopted from [17])

This solution monitors the packet header consisting of SYN and ACK. The checking state happens at the inside and outside interfaces (both inbound and outbound). Moreover, only TCP traffic is monitored with SYN and ACK extraction. Besides that, the host is also monitored from the outside, where only TCP traffic is extracted for SYN and ACK and the sequence number is stored. However, if it is not SYN and ACK, then the host monitor checking is executed. This stage will check for packet size, performs sliced payload, creates headers, and sends sliced packets to the inside interface.

While on the opposite side, when the TCP packet from the inside interface arrives, again TCP checking for SYN or ACK is performed and both are processed at different stages, starting with SYN and followed by ACK. If the ACK packet exists, then the host is checked. The RAP verdict coming from the difference between packet timing is analysed and correlated from the outside and inside interface packet information. In this project, SYN and ACK are highlighted but for more accuracy, a three-way handshake and FIN structure (closing communication) were also injected into the RAP detection mechanism.

Qu (2010) in [137] proposed calculating LRTT to check for RAP by passively monitoring network traffic (see Figure 2.11). The solution is similar to Mano (2008), except it was done on the wireless side.

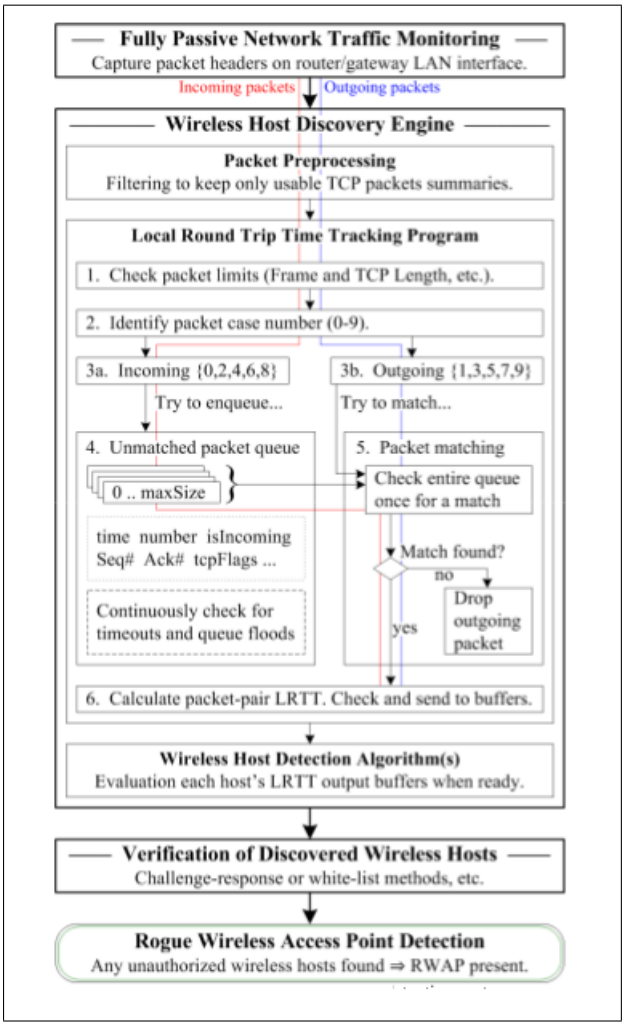



*Figure 2.11.* RAP Detection Framework (adopted from [137])

### 2.12.2 RAP Testbed

This possible future RAP detection mechanism was tested using a real testbed. The infrastructure of the testbed should fulfil the requirements and has the characteristics of a real network environment. A testbed from Watkins (2007) used for analysis of a wired network in [125], had a complete configuration set of a real working network environment (see Figure 2.12).

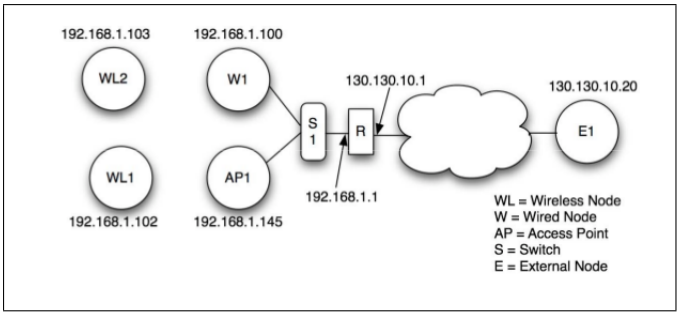



*Figure 2.12.* Testbed 1 (adopted from [125])

Watkins' testbed consisted of a wireless client side connected to the AP through a switch and orchestrated by a router. Additionally, there is an outside node which becomes the server to be accessed by all wireless clients. The RAP detection mechanism is plugged into the router for capturing packets to be analysed for RAP detection. Another similar testbed is shown in Figure 2.13, except there are no routers involved, only switches become the core components of the network.

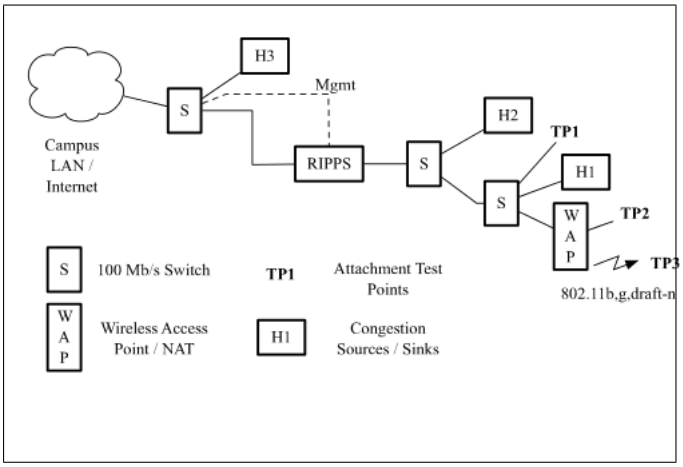



*Figure 2.13.* Testbed 2 (adopted from [17])

## 2.13 Summary

Detecting RAP is not as easy as it might seem. The packet flow could not be viewed inside the network traveling from the source to the destination. As a result, a solution is required to detect RAPs, which utilises packet capturing that solely relies on detecting

RAP at Layer 4, while being filtered with specific TCP flags.

There are many approaches that had been proposed in previous studies, however this thesis had scoped and focused on the wired structure for RAP detection. Moreover, it is a centric solution packet capturing deployed at a router where it is assumed that no packet will skip going through this device. The next chapter will show and describe the steps taken to accomplish the objectives of this research.

# CHAPTER THREE
# DESIGNING AND EXPERIMENTATION OF RAP DETECTION MECHANISM

## 3.1 Introduction

This chapter discusses on designing the RAP detection mechanism in two different parts involving the training and verification models. The training model focused on data gathering for getting a threshold value, whereas the verification model was to clarify the RAP detection mechanism based on a comparison between the threshold with the real-time packet capturing engine. Both models, training and verification are supported by a series of mathematical models while referring to the time stamp, group mean, zone mean, and threshold calculations. This chapter also elaborates about the development of a network testbed as a chronological output of the design phase, which was arranged into three sections. Each section plays a different role and fulfils the research requirement, especially in detecting RAP existence. The RAP detection mechanism was designed and executed on the traffic characteristics in wired LAN (Transport layer).

## 3.2 Training Model

The training part was designed with packet capturing capabilities using PCAP and supported by a filtering structure to filter selected TCP flags that have been chosen. Each packet is stored into a TCP flag flat file (text file) for grouping analysis. At this stage, two threshold values would be discovered for the next section which is the verification stage.

The design phase was divided into four stages, which are packet capturing, packet filtering, time stamping, and grouping. The output shall be two threshold values,

namely the zone threshold and global threshold. Figure 3.1 shows the relationship between each stage and on the right is the output of zone and global thresholds. Each stage will be discussed further in their specific sections below.

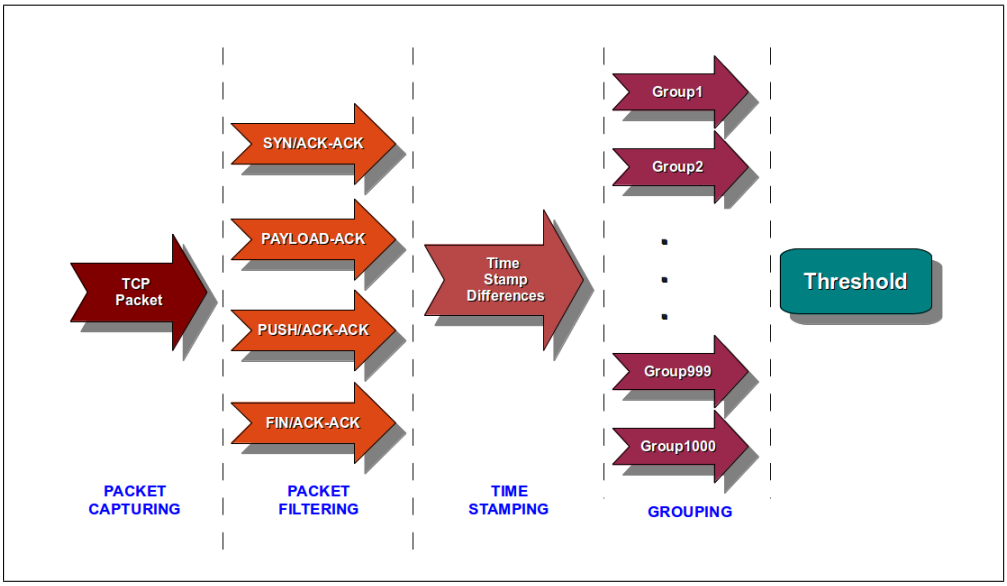



*Figure 3.1.* Training Model

Figure 3.2 shows the relationship between packet capturing and time stamping with three processes, which are packet capturing (3.2.1), packet filtering (3.2.2), and time stamping (3.2.3). These three processes formed the main structure in the overall RAP detection mechanism, whereas the grouping was for secondary purpose after the respective packet had been captured, which would be analysed to produce a result of either the packet was from RAP or non-RAP device.

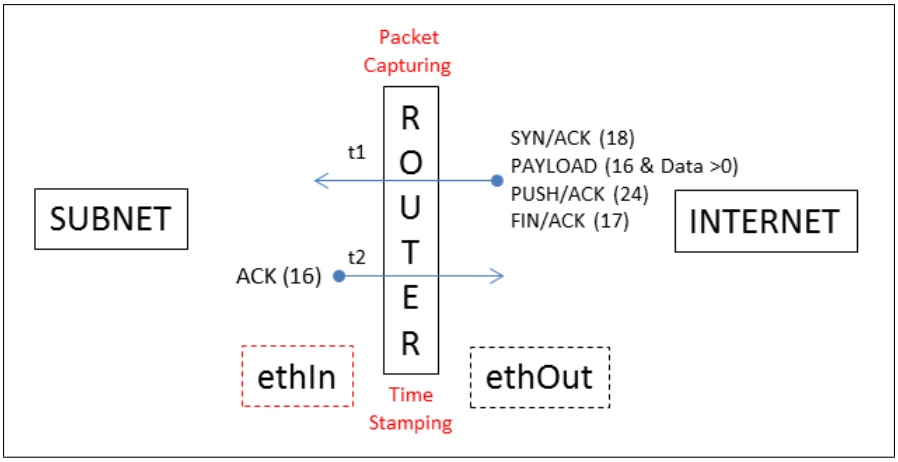



*Figure 3.2.* Packet Capturing and Time Stamping (adopted from [138])

The next few topics shall describe in greater depth on how the RAP detection mechanism was designed.

### 3.2.1 Packet Capturing

Packet capturing that was chosen already has the features that fulfil the needs of this research especially capturing packet that are moved between sender and receiver. It was injected into the overall design to become a frontal structure for capturing the packet flow from the host to router. Packet capturing was handled by the PCAP mechanism by four processes:

i. The interface to capture packets should be divided into two conditions, user specified or system decided what interface is available at the machine and choose the capture. Consequently, other parameters may be optionally provided to make the capture more reliable and accurate in order to come closer towards achieving our objective.

ii. After the interface is stated, then an initialising process begins. It will scope the capture according to specific parameters and a session is created to start the job.

iii. The parameter that was discussed previously is called a rule which is compiled and executed by PCAP, and becomes a filter. This happens in three stages, namely

   a. the rule is kept in a string,
   b. it is converted into PCAP format, and
   c. it is applied to the specific session that is being created just now.

iv. Lastly, the PCAP enter into its execution loop and starts capturing network packets. This ensures that the process is repeated until users interrupt the process with a specific command. While capturing, the packet is filtered according to several chosen TCP flags, like SYN/ACK, PAYLOAD, PUSH/ACK, and FIN/ACK. Each respective flag is paired with its ACK.

The packet capturing engine will execute at the router and waits for TCP segments to arrive and start capturing. The capturing sequence will occur at the subnet interface only where the number of hops is known. Consequently, this study does not focus on the interface at the Internet side because the number of hops is not known and uncontrollable.

### 3.2.2 Packet Filtering

As mentioned earlier, packet capturing is not complete without packet filtering because the promiscuous mode is going to grab all the flowing packets and make data storing and cleansing too large to be managed during traffic analysis [86]. This packet filtering is set up to screen four TCP Flags that works under TCP/IP packets for packet filtering (see Table 3.1).

Table 3.1
*Selected TCP Flags*

| **TCP Flags** | **Flag No.** |
|---|---|
| SYN/ACK | 18 |
| PAYLOAD | 16 & Data size is not 0 |
| PUSH/ACK | 24 |
| FIN/ACK | 17 |
| ACK | 16 & Data size is 0 |

Table 3.1 shows the TCP flags with their flag number. That number is represented by a binary number in the TCP/IP packet. Each flag is discussed below.

i. SYN/ACK-ACK

The normal SYN flag is given two and used to start a three-way-handshake between the host at subnet to server, at the Internet. After receiving a SYN flag, the server will respond by sending a SYN/ACK Flag. The number that is received by the router is 18, which is the addition of SYN(2) and ACK(16). As a result of this flag, the host will send ACK(16) to acknowledge the server.

ii. PAYLOAD-ACK

This flag is a special flag because it shares with the normal ACK flag. Payload is the ACK that has data (data is greater than zero). It is sent by the server to host which is requesting it through the PUSH flag. As usual, the successful payload is acknowledged.

iii. PSH/ACK-ACK

The push flag, which is assigned eight as a flag number, is used to inform the server to send out the data immediately and also there are no further requests being sent by the host. Upon receiving the push flag, the server immediately sends out the PSH/ACK flag (24) and waits for the corresponding ACK from the host, then it sends out the data. PSH/ACK is the summation of Push (8) and

ACK(16).

iv. FIN/ACK-ACK

When there are no further requests by host or no data are to be sent by the server, the fin flag will be indicated by either host or server to finalise the connection. Each party, either the host or server while receiving the fin flag (one), will respond with the FIN/ACK flag (17). FIN/ACK is the combination of FIN(1) and ACK(16).

As shown by Figure 3.2, this research only considered SYN/ACK, PAYLOAD, PUSH/ACK, and FIN/ACK from the server, and ACK from the host for packet filtering purposes in the proposed RAP Detection Mechanism.

### 3.2.3 Time Stamping

This task is to time stamp two different time occurrences between SYN/ACK, PAYLOAD, PUSH/ACK, and FIN/ACK with their corresponding ACK. According to Figure 3.2 the time stamps are indicated by *t1* and *t2*. While *t1* represents SYN/ACK, PAYLOAD, PUSH/ACK, and FIN/ACK, *t2* represents the associated ACK. The *t1* and *t2* is paired through an equality of SEQ number and ACK number, and then a time difference was calculated to measure the time spent from releasing *t1* and *t2*. This difference will be used to detect RAP.

### 3.2.4 Equal Grouping

Even though grouping is the secondary structure in this research, it is nevertheless as important as the main structure. It is used to rectify packets that have already been captured previously by arranging them into groups using the equal group technique. It is used to answer the question of how fast to detect RAP based on the number of packets being grouped together and obtaining the average. In general, a small number

is considered faster than a larger number, but it is needed to be proven before it can be accepted.

Using the same filtered packet capture technique for each different TCP flags, the grouping will be performed from group one to 1000 in order to predict which group is acceptable to be used for tracking down the existence of RAP. As shown in Figure 3.3, for example, it is assumed that the group number is three, then from the beginning, three packets are grouped and the mean to each group of three would then be calculated. For training purposes, the mean from each group is averaged again in order to obtain the zone mean. The collection of group means can be used to generate a new zone mean. Details on zoning is discussed in section 3.2.5.

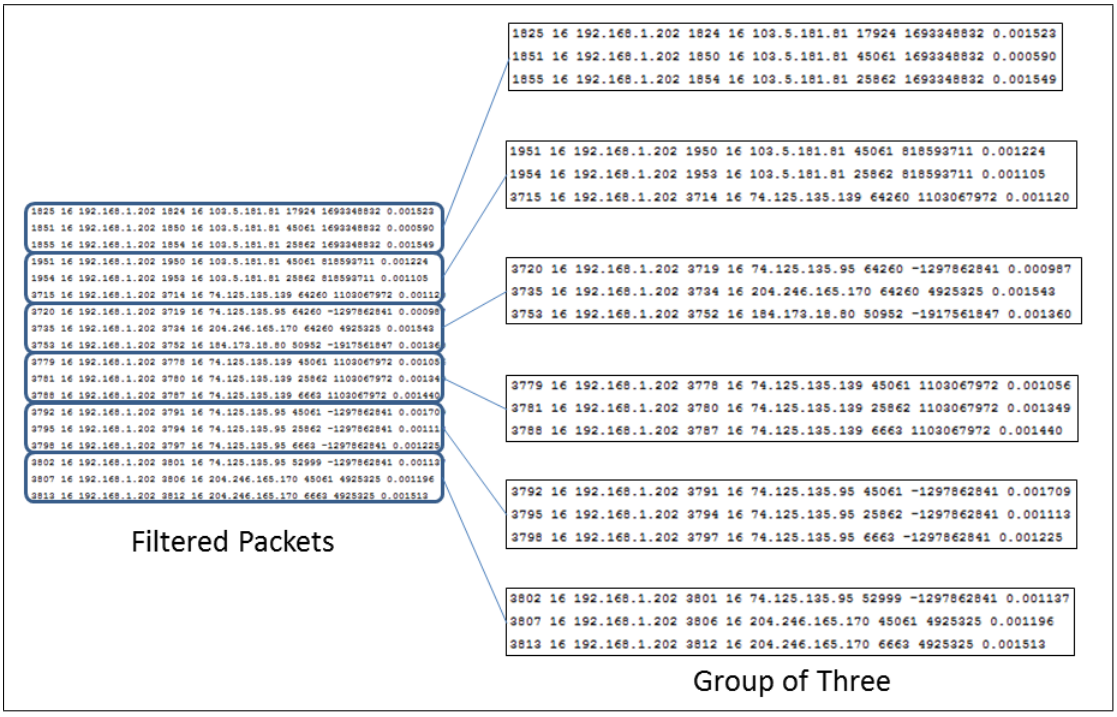



*Figure 3.3.* Group Example

The result from this part shall be used to verify how well the mechanism performs to detect RAPs.

### 3.2.5 Zoning

Zoning is a virtual group being set up to clearly define the border between one training set of data to another. There are specific rules being adhered to for zoning. However, this research shall equally set the range of time for gathering zone mean to represent each group set that has already been described before. The zoning also can help in predicting a global mean from several zone means that shall be clearly discussed in the next few sections for furthering the development of the RAP Detection Mechanism.

### 3.2.6 Threshold

There are three expected results from this research, which are group mean, zone mean, and global mean. The aim is the global mean, a single threshold value that can help to discover RAPs in LAN. That is why this proposed model that has been deliberated upon and designed, has firmly organised all structures to proceed toward the direction of finding a global training threshold. Moreover, the global mean or threshold is not an independent value, it requires support from group mean (grouping process from group 1 until 1000) that forms the zone mean. The zone mean must comply with the zoning rule which is equality; the same amount of allocated time is adhered to in order to ensure there are no differences. Figure 3.4 shows the correlation between all means that were highlighted previously. The average or mean formulation was used to formulate the required global threshold. The details on mathematical modelling will be discussed further in section 3.4.

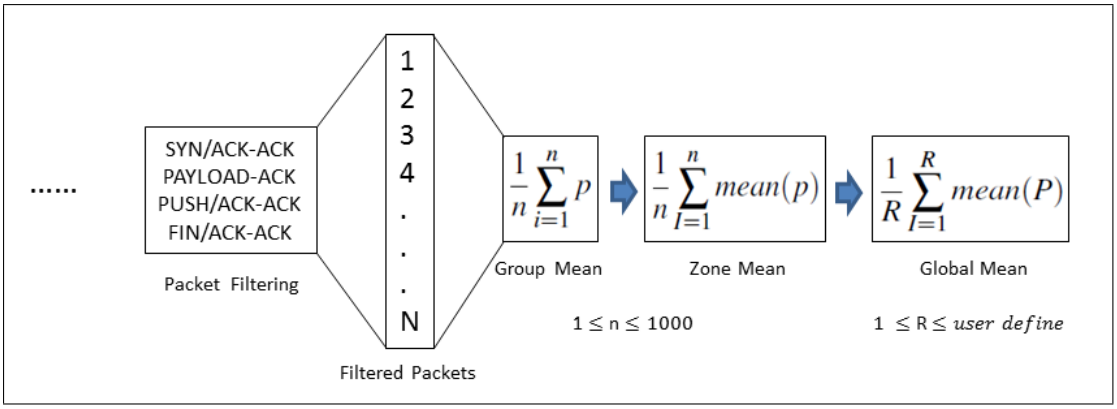



*Figure 3.4.* Training Thresholds

The training model is used to extract the threshold, group, zone, and global means. Our key structure is started by packet capturing, followed by packet filtering which is set to accept SYN/ACK, PAYLOAD, PUSH/ACK, FIN/ACK, and the associated ACK to pair with. Then, time stamping shall stamp two important times, namely the time for SYN/ACK, PAYLOAD, PUSH/ACK, FIN/ACK, and time for ACK pair. These two times are subtracted and the time difference is obtained. This is the main structure and it should work online according to whatever network traffic that flows from the host to the server.

The second structure is grouping and zoning. These two processes have a very close relationship for obtaining the global threshold. They themselves also produce group and zone thresholds. Our next stage is to design a verification model which is used to validate and evaluate another set of data that shall be collected later. The next section shall explain some details on designing the verification model.

## 3.3 Verification Model

The verification part is used to verify another set of packet capturing, packet filtering, time stamping, selected grouping, and a new structure, which is the threshold

checking. Threshold checking will compare the time difference average or means (group, zone, and global) for finding which mean is the best in terms of the number of packets captured, degrees of differences, and grouping effectiveness. This verification model that has been designed is inherited from the training model, except for the threshold checking part.

This section will now discuss the grouping and threshold checking only, while the other parts like packet capturing, packet filtering, and time stamping is not deliberated upon. This is because the way they work is similar to their counterparts in the training structure.

The first four structures are similar to the initial training model, whereas threshold checking is the continuity of the threshold output from the training model. As shown in Figure 3.5, the verification model is similar to the training model except for the last part, which is threshold checking.

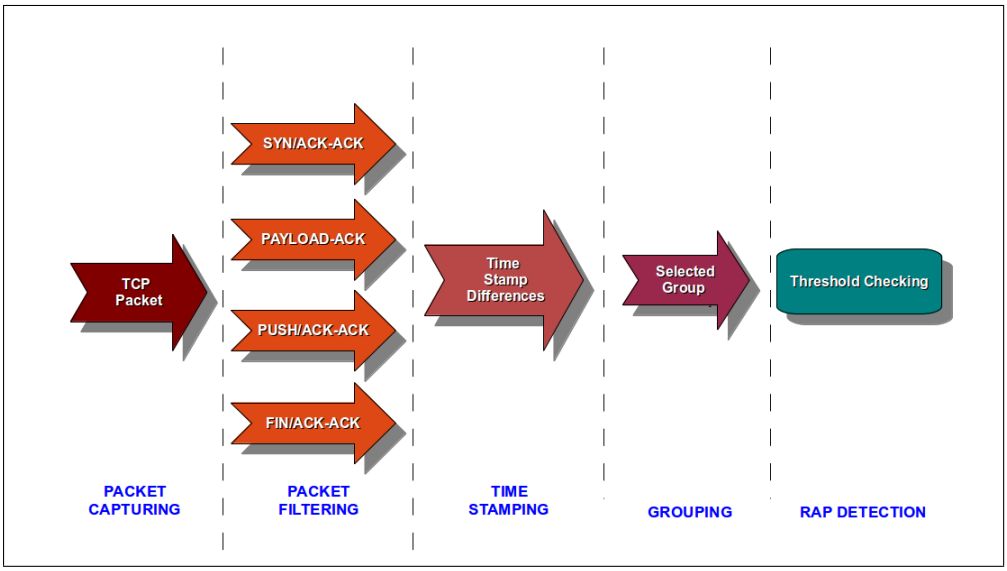



*Figure 3.5.* Verification Model

### 3.3.1 Selected Grouping

The chosen group depends on the analysis that is performed on the training set based on the training model. The way the number of packets in a group is set depends on the result extracted from the training set. When that result concretely shows which packet group is suitable, then that number shall be set in the verification process. However, the non-selected groups are also considered for testing together to rectify the differences between training and verification result differences.

In this verification step, the zoning shall be skipped and packet capturing is done randomly. One third of the packet capturing number of training sets shall be collected. Even though zone separation is not performed, the collecting still proceeds similarly to the zone deviation.

### 3.3.2 Threshold Checking

Threshold checking is the main objective in detecting RAPs. The threshold value comes from the training set, which are zone and global thresholds. At this verification section, this research shall look into group threshold, to observe whether it can support the proposed mechanism for detecting RAPs or otherwise. To accomplish this mission, a mathematical equation that shall be used in this stage will be explained, in section 3.4.

## 3.4 Mathematical Model

In designing the mathematical modelling, this research focused on time stamping and three other equations, which are group, zone, and global mean finders. Each equation shall be discussed in their own topic sections below.

### 3.4.1 Time Stamping

Time stamping equation can stamp five differences involving TCP flags like SYN/ACK, FIN/ACK, PAYLOAD, PUSH/ACK, and ACK. From the five only ACK is stamped separately after the first four have been stamped. This only happens when both sequences and acknowledged numbers are matched. Equation 3.1 shows the time stamp mathematical modelling that consists of $X_{t2}$and $A_{t1}$use to represent two time stamp events.

$$TS = X_{t2} - A_{t1} \tag{3.1}$$

The $X_{t2}$is ACK time stamp whereas $A_{t1}$is other TCP flags (SYN/ACK, FIN/ACK, PAYLOAD, and PUSH/ACK) that have been stated before, while $TS$ is the difference between the two time stamps where $X_{t2} - A_{t1}$.

### 3.4.2 Group Mean

The Group mean is actually a group threshold that is extracted from the training event. As shown in equation 3.2, it is a cumulative summation of time stamp activities that comes from equation 3.1. However that process is controlled with the number of packets in a group ($n$). The initial group packet number is $i = 1$.

$$G = \frac{1}{n}\sum_{i=1}^{n} TS \tag{3.2}$$

The group mean ($G$) is extracted from the division of the cumulative summation into the number of packets in the group, which is $n$. Technically, this $G$ will contribute to

the next section, which is zone mean discovery.

### 3.4.3 Zone Mean

This third equation is used to retrieve a second threshold, which is zone mean. The previous group threshold will be injected into this zone formulation. Equation 3.3 demonstrates the role of commutation addition of $G$ being controlled by $m$, which represents the number of groups in the zone.

$$Z = \frac{1}{m} \sum_{i=1}^{m} G \tag{3.3}$$

Similar to the group mean calculation, the zone mean is concluded at the end by dividing the cumulative summation of $G$ by $m$. This zone mean is important in finding a suitable global mean.

### 3.4.4 Global Mean

The direction of this section is to produce a global threshold. To accomplish this objective, the previous zone threshold will be input and accumulated by dividing with the number of zones that have been set up. Equation 3.4 shows the chronological order occurring in deriving this global mean.

$$O = \frac{1}{r} \sum_{i=1}^{r} Z \tag{3.4}$$

All the zone means are accumulated based on $r$, which is the number of zones being processed in section 3.4.3. The mean is finalised by dividing the cumulative $Z$ into $r$.

Finally the $O$ for global mean, or known as global threshold, is produced and used for detecting RAP.

## 3.5 RAP Detection Testbed

The previous topic discussed the design of the RAP Detection Mechanism from several scopes, which are training model, verification model, and mathematical equation used in both training and verification processes. In addition to these matters, this section is going to discuss an experimental set up of RAP Detection Mechanism, highlighting the RAP Detection Testbed where all the discussed models in the design section are inserted and executed through this testbed.

This topic is organised into several subtopics, which are testbed requirements and the two engines; packet capturing and packet analysis.

### 3.5.1 Testbed Requirement

The requirement of our RAP detection testbed is divided into two; hardware and software. The hardware requirements are listed below.

i. Router - This is our main subject where the engine of packet capturing, traffic filtering, and traffic analysis will be deployed. Most of the time, our work focuses on this part, especially in configuring, executing capturing engine, processing results, and etc.
ii. Hosts - This is the end point and easy to plug into the network testbed. There are no specific specifications that have been set and the most important thing that it is connected and can start requesting information from any destination (Internet). We consider both OS platforms, which are Linux and Windows.
iii. Access Point - The observation is pointing to both wireless g and n modes for

finding the differences between both wireless mode to the wired connection.

Instead of just the hardware above, a list of software to compliment the hardware is required. The software list is shown below:

i. Linux OS Server - The router supported by the OS. Using Ubuntu 11.04 Server Edition, it would be easy to configure the DHCP server, firewall, and Network Address Translation (NAT) for hosting our RAP Detection Mechanism.
ii. C language - The packet capturing, packet filtering, and packet analysis are enhanced and developed based on this language.

Knowing the requirements can lead to the construction of two engines (packet capturing and traffic analysis engines), based on the two models that have already been discussed (refer to sections 3.2 and 3.3).

### 3.5.2 Packet Capturing Engine

The latest libpcap version is 1.2.1 was release on 1 January 2012. As usual, this library needs to be configured, compiled, and installed using Linux native gcc, like *./configure, make, and make install.* The libpcap itself has a flow that must be followed if the development of whatever packet capturing tool is to be materialised. The following is the flow of the libpcap code [139](see Figure 3.6).

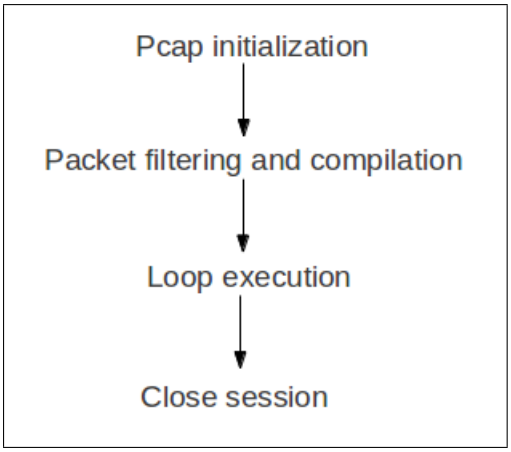



*Figure 3.6.* Pcap Requirement

i. Pcap initialisation

At this stage, an interface may be provided to capture either automatically detected or manually, entered through inside the code. Without it, libpcap could not work.

Pcap can capture many devices at once, however each device should be separated into different sessions. At this point, each session is named according to the device that is going to capture a packet. This stage will answer the question of where and what device is to be captured.

ii. Packet filtering and compilation

There are many layers that packet capturing can occur, for example layer 2, 3, and etc., of the OSI model. This part needs to clarify what are the rules used for capturing. It can be a specific layer like layer 2 (ARP), layer 3 (IP), layer 4 (TCP), and so on. After the filter or rule has been specified, it must then be compiled and applied to a specific session.

iii. Loop execution

This is the final step for entering into the execution loop. When it receives a packet, another function will be called to process the packet. Moreover, own code may be inserted or written in order to manipulate the captured packet.

iv. Close session

After a certain target is achieved (specific packet number), the packet capturing will stop and close the session.

### 3.5.3 Traffic Analysis Engine

Libpcap has four stages which will be used for packet capturing. The focus is on loop execution, which consists of the *got_packet* function where the proposed code is inserted. This code communicates directly to and from traffic analysis procedure, which is also part of the RAP detection mechanism (see Figure 3.7).

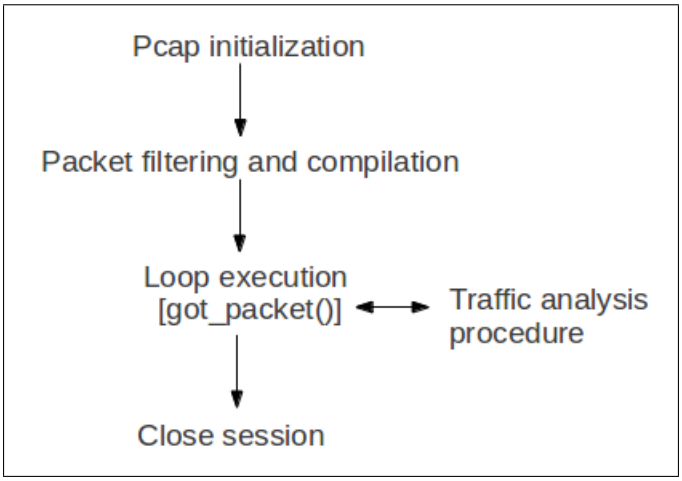



*Figure 3.7.* Pcap and Traffic Analysis Flow

At this point, the discussion shall proceed to the point of capturing for identifying where is the suitable place to time stamp the captured packet. This will produce an accurate result for identifying RAP. The discussion also continues to the file structure, which is important for extracting the captured packet into meaningful information with specific time stamps that will be used for traffic characteristic calculation. The overall detail of how the engine works shall be elaborated in detail in the RAP detection mechanism framework.

#### 3.5.3.1 Point of Timestamps

Figure 3.8 shows the point of timestamps for each type of TCP flags, namely SYN, FIN, PUSH, and Payload. Each timestamp is represented by *t1* and *t2*, where *t1* is the arriving packet from the Internet being ACKed by either SYN/ACK, FIN/ACK, PUSH/ACK, or Payload/ACK whereas *t2* is an ACK from the host back to the server (Internet).

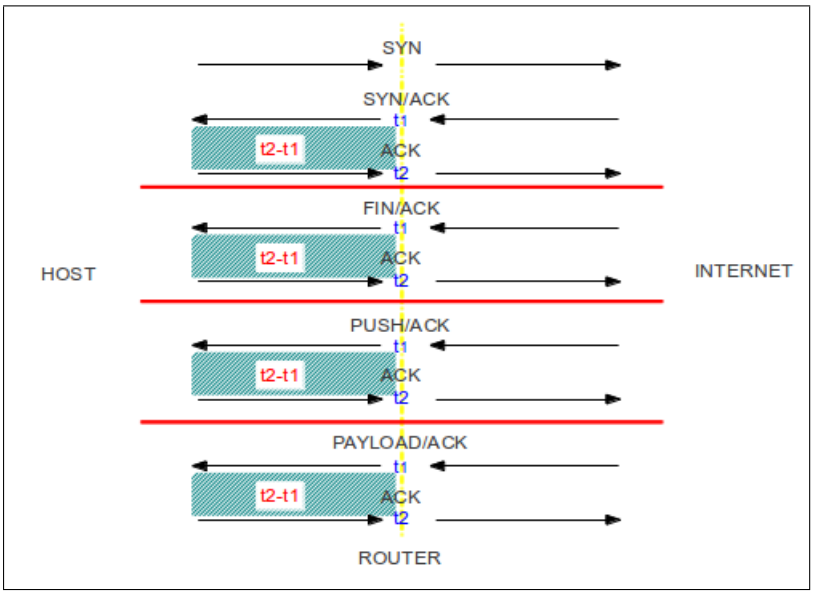



*Figure 3.8.* Point of Timestamps

The time stamp takes place at the internal interface only. Consequently, it is not suitable for each host in the subnet to compare to the external interface, where the number of hops is various and influenced by many factors like availability of the server, the reliability of the intermediate router, and so on. Because of unpredictability, the timestamps should only be taken at the internal interface which is nearest to the subnet being monitored. The difference of time between *t1* and *t2* is *t2-t1*, measured in milliseconds (ms).

#### 3.5.3.2 Record Structure

After the packet is captured, it will be extracted into a series of meaningful information as shown by Figure 3.9. There are four record structures created and used to support this research like *temp*, *ffilter*, *fprepost* and *f16* where *temp* used to store all packets being captured, *fprepost* stored a request and their respective respond packets, *f16* kept an ACK packets and *ffilter* used for further specific filtering action for SYN, FIN, PUSH, and Payload.

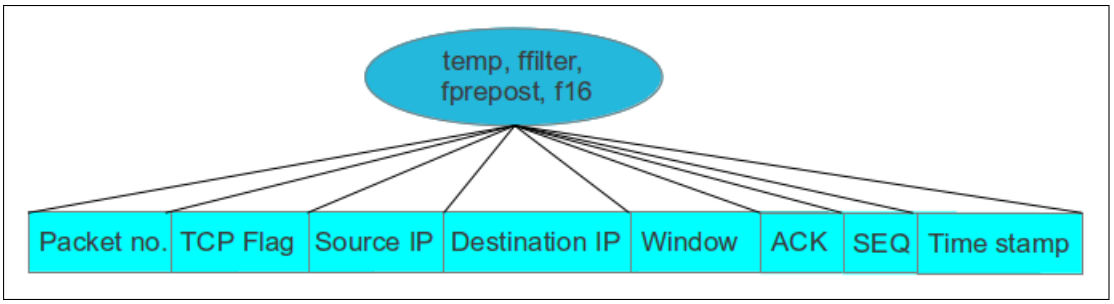



*Figure 3.9.* Record Structure: temp, ffilter, fprepost and f16

Only packet number, TCP flag, source and destination IP, window size, acknowledgment, sequence number, and time stamp are recorded. From the list, TCP Flag, acknowledgement, and sequence number are used for pairing with the next equal packet according to the mentioned fields. The equivalent is brought forward to the traffic analysis segment.

Instead of capturing the stated TCP flags, other host data are also recorded, like IP used and MAC address. The record structure of host is shown in Figure 3.10. The purpose of capturing host info will enable the investigator to monitor the recorded and managed devices by looking up the IP and MAC addresses of each device that bypass the router which is deployed with the proposed RAP detection mechanism.

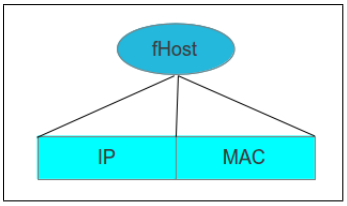



*Figure 3.10.* Record Structure: Host

As we already highlighted previously, *ffilter* will hold a list of packets being captured for the next traffic analysis section which is slicing into different and specific TCP flags basket; SYN, FIN, PUSH and Payload(data) when there are match with the next ACK packet. The matching is check by comparing the previous acknowledge number to the current sequence number. Each matched is stored into each TCP flags record structure (see Figure 3.11)

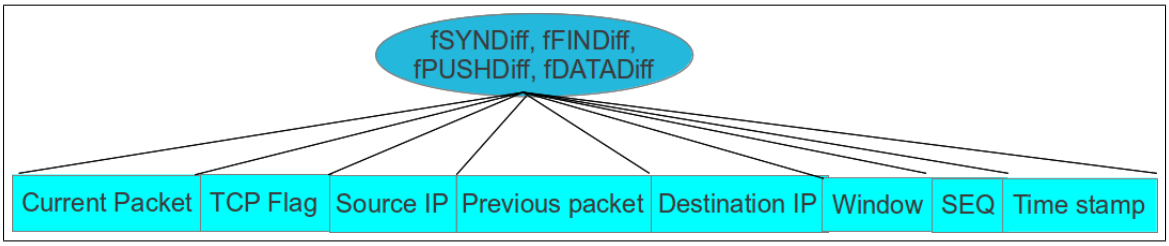



*Figure 3.11.* Record Structure: fSYNDiff, fFINDiff, fPUSHDiff and fDATADiff

For management and inventory purposes, the record is stored to the following fields; current and previous packets, TCP flag, source and destination IPs, window size, sequence number, and time stamp. The fields like current and previous packets, and TCP flag are used for verification only, whereas source and destination IPs, sequence number, and time stamp will be part of the next traffic analysis process. The previous acknowledge number is excluded because of the included sequence number which also represents the acknowledge number.

### 3.5.4 Developing RAP Detection Mechanism

The deployment of the network testbed is divided into three different sections, A, B, and C. This separation has reduced the development process where the investigator can focus on sections at different times, and it would be easier to carry out a test. Among all sections, section B is the toughest whereby it consists of both engine, which are packet capturing and traffic analysis. Section C is not discussed because Internet is already available and can be connected instantly. Figure 3.12 shows the sections which are discussed below.

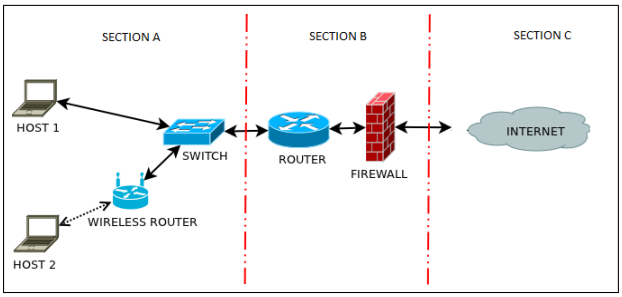



*Figure 3.12.* Network Testbed Deployment

i. Section A

This section is a subnet of LAN that has been set up and consists of several computers connected to the network in two access modes, i.e., wired and wireless. Both access modes are tied-up to the router through a layer 2 switch. The switch is used as a repeater only to the router and also to the end-users.

Two end-users are created where each connection comprises of wired or wireless structures. On the wireless side is the plug-in wireless router where Host 2 will associate later. For configuration purposes, Host 1 gets the IP from the router through DHCP server whereas Host 2 IP is given by wireless router. In addition, the wireless router also get its IP from the DHCP service.

ii. Section B

As stated by Xiaohui (2009) in [140], low cost router can be developed using

a normal desktop computer, supported by an open source operating system like Linux. This Linux Server version comprises router and firewall services which are very easy and practical to be configured and executed. A few steps were taken to prepare this section, as listed below.

a. Ubuntu Server installation

   Since many of the resources employed in this research originates from open source, Linux is the most suitable OS for servicing the network testbed. The Ubuntu server was chosen as the main network provider for its stability and reliability. The Ubuntu server *iso installer* can be downloaded at this link: `http://www.ubuntu.com/download/server`. Installing Ubuntu server is not so difficult and the steps taken is similar to many other popular OS installations like Windows 7.

b. Configuring Network Connection

   i. Network Interface Card (NIC)

      To support packet capturing, the NIC is configured in promiscuous mode and a specific port is selected and set to be in passive mode. This mode grabs whatever packets flow in and out of the NIC.

   ii. DHCP

      Even though packet capture occurs at the transport layer, it is necessary to acknowledge an existence of host and server by their Internet Address (IP). The installed Ubuntu fully supports this functionality.

### 3.5.5 Training Process

The implementation of training process is divided into packet capturing, packet filtering, time stamping, grouping, and obtaining threshold value. Figure 3.13 shows all the stated process.

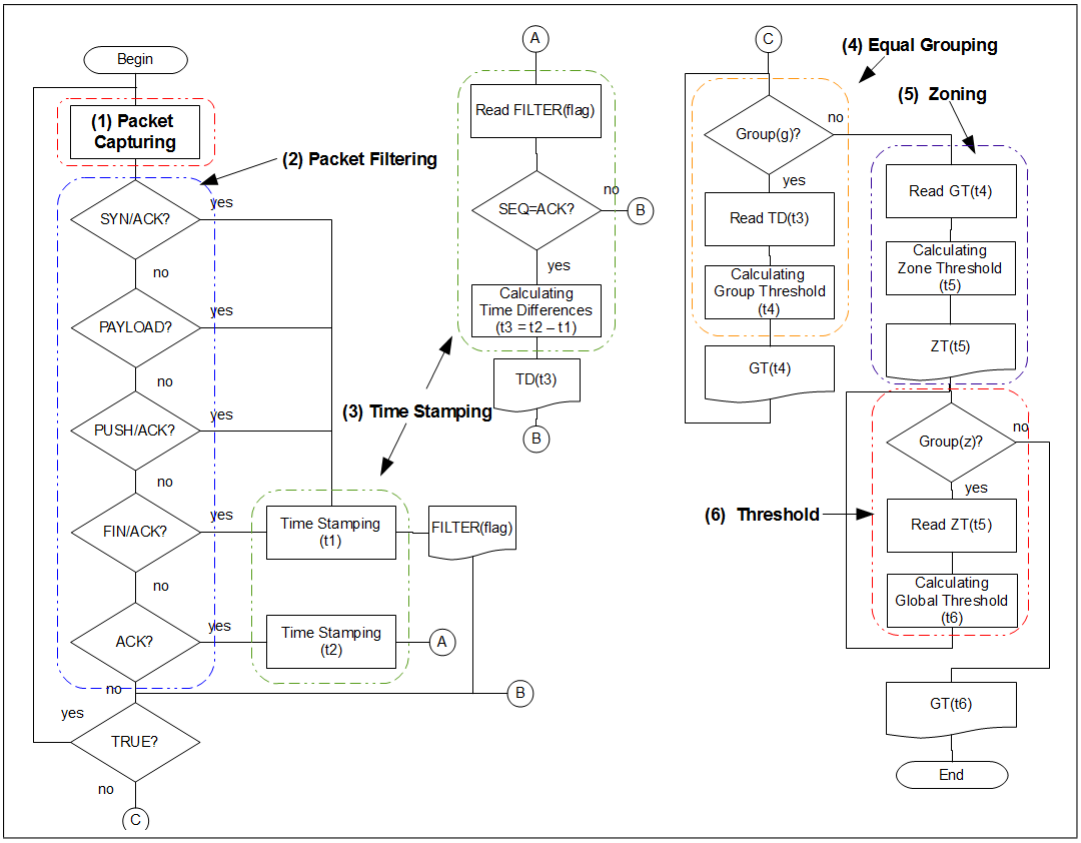



*Figure 3.13.* Training Process

As shown in figure 3.13, the training process can be classified into six and described below.

i. Packet capturing – In promiscuous mode, all the packets flowing through a monitored port are captured.

ii. Packet filtering – The packet captured then are filtered for SYN/ACK, PAYLOAD, PUSH/ACK, FIN/ACK and ACK.

iii. Time Stamping – The respective filtered packets except ACK are time stamped (*t1*) and stored into FILTER (flag) with their own flag labels. Whereas ACK is time stamped (*t2*) differently. However, after the ACK is time stamped, the FILTER (flag) is read and each reading flag Sequence number is compared to ACK number for matching. If it is matching then calculating a time differences

(*t3=t2-t1*) and stored to TD (*t3*). And return back to packet capturing for repeating the process.

iv. Equal Grouping – After the previous three process end, the time differences need to be analyse for finding group, zone and global means. This means also assume to be a threshold. The equal grouping start by generating a group from 1 until 1000 and each group consisting of reading a TD (*t3*) source and calculating a group mean or threshold for group 1 until 1000. Each group means are stored into GT (*t4*).

v. Zoning – This research use zoning or different time zone to make a comparison and verify the finding later on. There are three zones and each zone going through a previous four processes. The zoning process is targeting for finding a zone mean and each three zones are read separately (GT (*t4*)A, GT (*t4*)B , GT (*t4*)C). Then calculating zone mean are executed. Each zone have their own zone mean. The result is stored into ZT (*t5*) at each zone.

vi. RAP Threshold – Getting RAP threshold can be achieved by reading all the three means source separately (ZT (*t4*)A, ZT (*t4*)B , ZT (*t4*)C) and then calculating the global mean. This mean is RAP threshold to be used in verification process later.

The packet capturing and packet filtering have already been discussed in sections 3.5.2 and 3.5.3, respectively. However, only the framework for both engines used in this research is laid out. Here, the mathematical formulation will be highlighted, which was already formulated especially for time stamping, group threshold and overall threshold.

#### 3.5.5.1 Time Stamping

The success of detecting RAP depends on the time stamp on two points at the inner inbound of the subnet at the point where the time stamping mechanism is set up [138] (refer to section 3.5.3.1). From general time stamping formula (refer 3.1), it is divided into four which are showed by $TSs$, $TSp$, $TSps$, and $TSf$ in Table 3.2 below

Table 3.2
*Time Stamping*

| Equation | Descriptions |
|---|---|
| $TSs = Xs_{t2} - As_{t1}$ | $TSs$ is time stamping differences SYN/ACK Packet $Xs_{t2}$ and its SYN $As_{t1}$ |
| $TSp = Xp_{t2} - Ap_{t1}$ | $TSp$ is time stamping differences on PUSH/ACK Packet $Xp_{t2}$ and its PUSH $Ap_{t1}$ |
| $TSps = Xps_{t2} - Aps_{t1}$ | $TSps$ is time stamping differences on PAYLOAD/ACK Packet $Xps_{t2}$ and its PAYLOAD $Aps_{t1}$ |
| $TSf = Xf_{t2} - Af_{t1}$ | $TSf$ is time stamping differences on FIN/ACK Packet $Xf_{t2}$ and its FIN $Af_{t1}$ |

Each operation is handled differently at different points of captured and filtered packets (see Figure 3.8). The similarity between each packet, for example $Xs_{t2}$ (SYN/ACK) to its SYN $As_{t1}$ for subtraction, is compared through the acknowledge and sequence numbers. If both numbers are equal to its pair ($Xs_{t2}$ (SYN/ACK) subtract by its SYN $As_{t1}$), the subtraction will take place where the latest time for that packet will be subtracted by the previous packet. The total is recorded in the result database for the proceeding stage, which is analysis.

One of the feature in our research is the implementation of grouping for threshold determination. A decision was made to get various results from the captured packets and also in finding a specific and reliable threshold. To achieve this target, the next section will discuss this part on getting a group threshold through calculating a group mean. Finding a group mean would not happen if it is not supported by the time

stamping difference equation that was already discussed here in this section.

#### 3.5.5.2 Group Mean

Grouping is a process of dividing or segmenting time stamp differences between different packets into different group. The result is collected from the first until the end, will go through this grouping process. The group begins from 1 until 1000, whereby each result is grouped into sets. Consequently, each set (group) is processed for group mean discoveries using the formula or equation that was constructed previously, as shown in Table 3.3.

Table 3.3
*Group Threshold*

| Equations | Descriptions |
|---|---|
| $Gs = \frac{1}{n}\sum_{i=1}^{n} TSs$ | Accumulative of time stamped differences of SYN/ACK and SYN ($TSs$) then divide by number of group ($n$) |
| $Gp = \frac{1}{n}\sum_{i=1}^{n} TSp$ | Accumulative of time stamped differences of PUSH/ACK and PUSH ($TSp$) then divide by number of group ($n$) |
| $Gps = \frac{1}{n}\sum_{i=1}^{n} TSps$ | Accumulative of time stamped differences of PAYLOAD/ACK and PAYLOAD ($TSps$) then divide by number of group ($n$) |
| $Gf = \frac{1}{n}\sum_{i=1}^{n} TSf$ | Accumulative of time stamped differences of FIN/ACK and FIN ($TSf$) then divide by number of group ($n$) |

Group mean is calculated through the accumulative or summation of different time stamped TCP flag types as a collective, depending on the grouping number. Moreover, this group number becomes the divisor from that collective summation processes. A result of four different time stamps were collected, and formulated into four group means according to the same TCP flag type.

As shown in 3.3, *Gs* is accumulative of time stamped differences of SYN/ACK and

SYN ($TSs$), $Gp$ is accumulative of time stamped differences of PUSH/ACK and PUSH ($TSp$), $Gps$ is accumulative of time stamped differences of PAYLOAD/ACK and PAYLOAD ($TSps$), and $Gf$ is accumulative of time stamped differences of FIN/ACK and FIN ($TSf$). Then all the cumulative results are divided by number of groups ($n$).

The group mean that we received from this topic is useable for finding another threshold; the zone threshold. In conjunction to RAP detection, another approach that is proposed is to divide the detection into different zones (refer to Chapter 4). For completing this target, this research also formulated four zone means that were inherited from the grouping process. The next section will elaborate more on this matter.

#### 3.5.5.3 Zone Mean

In formulating or generating equation for zone mean, this research referred to the grouping process that produced a group mean. However, at this point, it is divided into 1000 ($m$) which is the maximum number of groups in the grouping process. Table 3.4 shows the list of zone mean formulas.

Table 3.4
*Zone Threshold*

| Equations | Descriptions |
|---|---|
| $Zs = \frac{1}{m}\sum_{i=1}^{m} Gs$ | Accumulative of group of SYN threshold ($Gs$) then divide by number of ($m$) |
| $Zp = \frac{1}{m}\sum_{i=1}^{m} Gp$ | Accumulative of group of PUSH threshold ($Gp$) then divide by number of ($m$) |
| $Zps = \frac{1}{m}\sum_{i=1}^{m} Gps$ | Accumulative of group of PAYLOAD threshold ($Gps$) then divide by number of ($m$) |
| $Zf = \frac{1}{m}\sum_{i=1}^{m} Gf$ | Accumulative of group of FIN threshold ($Gf$) then divide by number of ($m$) |

Accumulative group of SYN threshold ($Gs$) then divided by number ($m$), accumulative group of PUSH threshold ($Gp$) then divided by number ($m$), accumulative group of

PAYLOAD threshold ($Gps$) then divide by number ($m$), and accumulative group of FIN threshold ($Gf$) then divide by number ($m$). As a result we have zone thresholds that can be used to detect RAP in different areas.

The obtained zone threshold is important for calculating the last and final threshold, which is the global threshold. It is done through finding a global mean based on the zone means discussed in this section. The next section will highlight the global mean process in more detail.

#### 3.5.5.4 Global Mean

Our last and final process is to calculate a global mean which is also a global threshold that will be used as a whole comparative number between wired and wireless while not being limited to group or zone. As shown in Table 3.5, there are four global mean processes that will produce four differences of global threshold for each TCP flags (SYN, PUSH, PAYLOAD, and FIN), represented by $Zs$, $Zp$, $Zps$, and $Zf$.

Table 3.5
*Global Threshold*

| Equations | Description |
|---|---|
| $Os = \frac{1}{r}\sum_{i=1}^{r} Zs$ | Accumulative of zone of SYN threshold ($Zs$) then divide by number of ($r$) |
| $Op = \frac{1}{r}\sum_{i=1}^{r} Zp$ | Accumulative of zone of PUSH threshold ($Zs$) then divide by number of ($r$) |
| $Ops = \frac{1}{r}\sum_{i=1}^{r} Zps$ | Accumulative of zone of PAYLOAD threshold ($Zs$) then divide by number of ($r$) |
| $Of = \frac{1}{r}\sum_{i=1}^{r} Zf$ | Accumulative of zone of FIN threshold ($Zs$) then divide by number of ($r$) |

Each zone mean is accumulative and the summation is divided into $r$ which represents the number of zone. In our case, the $r$ is three. Moreover, the previous processes will produce the four global thresholds presented by $Os$(SYN global threshold), $Op$(PUSH global threshold), $Ops$(PAYLOAD global threshold), and $Of$(FIN global threshold).

These global thresholds form the main threshold value, instead of group and zone thresholds. This global value with group and zone thresholds can also be used to validate the mechanism that was developed in detecting RAPs in the LAN.

This current discussion has covered the overall picture of how the training process was produced, which results in the construction of three threshold values, namely group, zone, and global thresholds. The result from this training process will be injected into the testbed again for verification. A few other equations will be proposed which will benefit from the training process result already gathered from training the testbed. These process will be discussed in the next section.

### 3.5.6 Verification Process

As mentioned in the training process section, this verification section also has three sets, namely group, zone, and global verification process. Everything is similar to training steps except threshold checking that will produce a result of RAP detection or non-RAP, and Potential RAP.

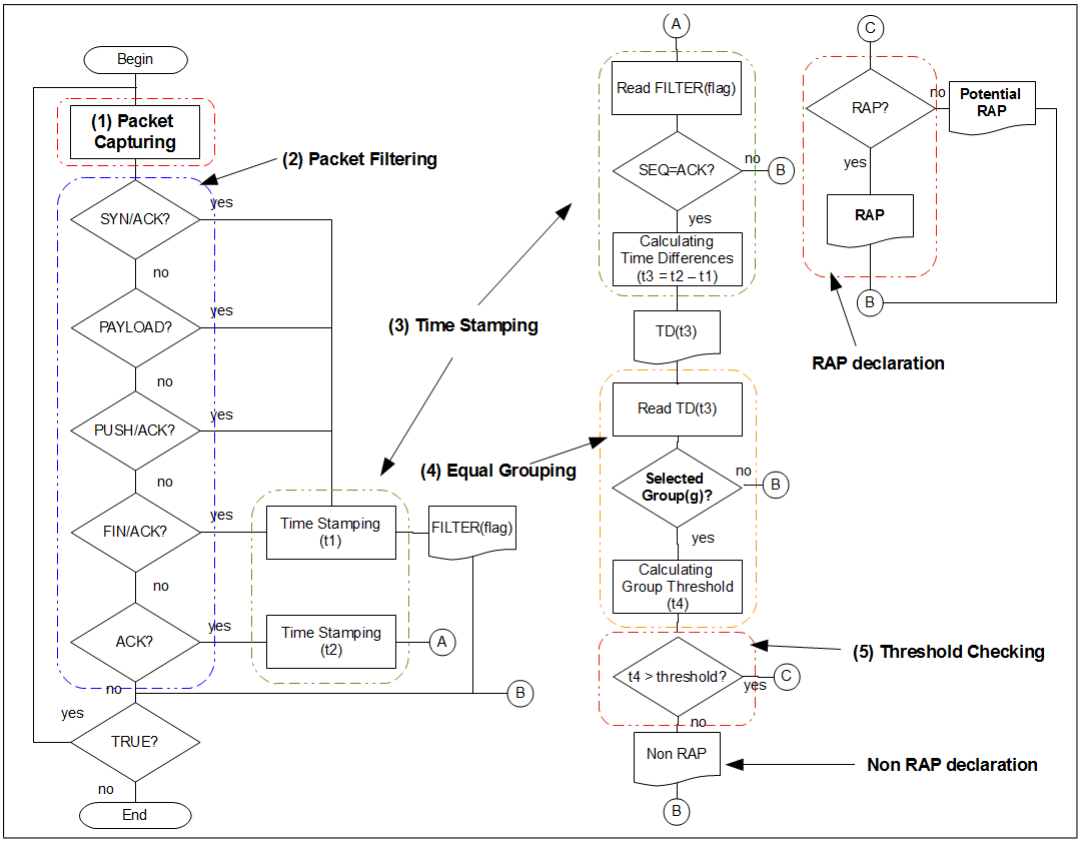



*Figure 3.14.* Verification Process

As stated in Figure 3.14, the highlighted points are the verification stages which focus on two different things; comparing time stamped differences to the setting threshold, and the second point is the RAP verdict of either it is RAP or non-RAP. If it is RAP, then there is another point to be outlined, either that RAP is absolutely discovered or still can be argued, which is labelled as Potential RAP.

## 3.6 Summary

There are two main important things discussed in this chapter, namely the design and experimentation of traffic characterisation mechanism consisting of training and verification processes. Both training and verification processes have similarity in the first few steps, like packet capturing, packet filtering, time stamping, and grouping, however the verification process has one more extra step which is threshold extracting.

This threshold is produced through group threshold and an average of all group thresholds is calculated to yield a global threshold. The outcome to this chapter (training and verification processes) is going to be detailed out further in Chapters 4 and 5.

# CHAPTER FOUR
# THRESHOLD DISCOVERIES

## 4.1 Introduction

The packet capturing was conducted in two separate slots covering two different wireless modes (g and n). Each slot was divided into three different zones (A, B, and C). Each zone is allocated with two hours for packet capturing. The discussion begins with the overall data captured, consisting of two tables (4.1 and 4.2), which describe two different slots used in packet capturing. Both tables were observed in two dimensions, which consists of vertical and horizontal comparisons on columns and rows of TCP flags and network type data. The vertical represents wired network whereas the horizontal represents TCP flags. The main discussion is divided into three distinct sections, namely packet captured analysis, ACK packet analysis, and time stamp analysis. An output to these analyses are a prediction of numbers of packets in their respective group (from group one to 1000), measured in minutes, and a threshold which will become an indicator to the next verification chapter.

## 4.2 Packet Captured Analysis

In this section the focus is on the overall captured packets which is handled by two different slots. Each slot captures at different times and supported by two different tables. One table for 802.3 versus 802.11g, and another table for 802.3 versus 802.11n.

As shown in Table 4.1, the total number of packets captured was 1,472,548 from both networks; 802.3 and 802.11g. From that amount, the highest captured packets referred by TCP flag category was ACK, which accounted for 96.18%. The second highest was by PSH/ACK with 2.26%. The following flags FIN/ACK and SYN/ACK came third and fourth, respectively, where FIN/ACK contributed with 0.63% and SYN/ACK with

0.30%.

Table 4.1
*Total No. of Packets Captured 1*

| | 802.3 | | 802.11g | | Total |
|---|---|---|---|---|---|
| **ACK** | 718,139 | 50.71% | 698,099 | 49.29% | 1,416,238 |
| | 96.27% | | 96.07% | | 96.18% |
| **SYN/ACK** | 2,328 | 46.86% | 2,629 | 53.14% | 4,957 |
| | 0.31% | | 0.36% | | 0.30% |
| **PSH/ACK** | 16,878 | 50.77% | 16,368 | 49.23% | 33,246 |
| | 2.27% | | 2.25% | | 2.26% |
| **FIN/ACK** | 4,303 | 46.68% | 4,916 | 53.32% | 9,219 |
| | 0.58% | | 0.68% | | 0.63% |
| **Others** | 4,276 | 48.11% | 4,612 | 51.89% | 8,888 |
| | 0.57% | | 0.64% | | 0.63% |
| **Total** | 745,924 | 50.66% | 726,624 | 49.34% | 1,472,548 |

From the perspective of networks, 802.3 contributed 50.66% and 802.11g contributed 49.34%. In addition, 802.3 had more packets of ACK and PSH/ACK, whereas 802.11g had more packets of SYN/ACK, FIN/ACK, and others. However, a TCP flag types Others were not considered in this research.

Even though ACK made up a large numbers of packets, it consists of other types of flags, like PAYLOAD and also the ACK of SYN/ACK, PSH/ACK, FIN/ACK, and others flags. As a result, it was selected as the focus in finding Rogue Access Points through this TCP flag. Moreover this ACK covers or compliments other flags, like already highlighted at the beginning sections.

The second slot covered the packet capturing between 802.3 and 802.11n (Table 4.2). The total number of captured packets was 1,395,208. Again, ACK had the largest number of packets, which was 97.02%, while PSH/ACK contributed about 1.92%. FIN/ACK came third with 0.45%, and 0.23% went to SYN/ACK. Consequently, other TCP flag constituted 0.38%, but that does not count because there were more than one

flag being referred.

Table 4.2
*Total No. of Packets Captured 2*

| | 802.3 | | 802.11n | | Total |
|---|---|---|---|---|---|
| **ACK** | 811,696 | 59.96% | 541,990 | 40.04% | 1,353,686 |
| | 97.47% | | 96.37% | | 97.02% |
| **SYN/ACK** | 1,624 | 50.47% | 1,594 | 49.53% | 3,218 |
| | 0.20% | | 0.28% | | 0.23% |
| **PSH/ACK** | 13,577 | 50.65% | 13,190 | 49.35% | 26,767 |
| | 1.63% | | 2.35% | | 1.92% |
| **FIN/ACK** | 3,094 | 49.62% | 3,141 | 50.38% | 6,235 |
| | 0.37% | | 0.56% | | 0.45% |
| **Others** | 2,783 | 52.49% | 2,519 | 47.51% | 5,302 |
| | 0.33% | | 0.44% | | 0.38% |
| **Total** | 832,774 | 59.69% | 562,434 | 40.31% | 1,395,208 |

Perhaps the network compared in this second slot had given similar result as the first slot, which comprised 59.69% of 802.3, whereas 40.31% was 802.11n. Comparing 802.3 with 802.11n, only ACK of 802.3 had higher percentage than 802.11n, which was 97.47%, however other TCP flags like SYN/ACK (0.28%), PSH/ACK (1.63%), and others (0.44%) was for 802.11n.

Although 802.3 had more packets than 802.11n or g from both slots, it does not mean that the method to eliminate RAP has been discovered. More precise and reliable ways should be investigated. However from this point, it is agreed that ACK can be selected as the TCP flag used in tracking RAP. In addition, this ACK also pairs up with SYN/ACK, PSH/ACK, FIN/ACK, and PAYLOAD. Thus, the next step was to drill down in depth into ACK for finding a way to rectify RAP through comparing 802.3 to 802.11g and 802.11n.

## 4.3 ACKNOWLEDGMENT Packet Analysis

In this section, an in depth discussion into ACK, comprising the ACK of PAYLOAD (PAYLOAD-ACK), SYN/ACK (SYN/ACK-ACK), PSH/ACK (PSH/ACK-ACK), and FIN/ACK (FIN/ACK-ACK) from both slots (802.3 versus 802.11g and 802.3 versus 802.11n). In addition, the flags were divided into zones (Zone A, Zone B, and Zone C). As stated previously, each zone had been given the same amount of time, which was two hours, during packet capturing. Table 4.3 and 4.4 have two dimensional structures; vertical and horizontal comparison between types of network in different zones and TCP flags.

Table 4.3 has a total of 636,786 for both zoning and TCP flags. From this number, 602,040 came from PAYLOAD-ACK, 25,710 came from PSH/ACK-ACK, 4,951 came from SYN/ACK-ACK, and 4,085 came from FIN/ACK-ACK. In percentage values, PAYLOAD/ACK-ACK contributed 94.54% of the overall and become the largest number of packets, next 4.04% of PSH/ACK-ACK, 0.78% of SYN/ACK-ACK, and last but not least, is FIN/ACK-ACK contributing about 0.64%.

Another point of view is the vertical, where it shows the differences between 802.3 and 802.11g by zone. From the three zones, Zone B had more number of packets compared to others, of which 802.3 had 118,393 (18.59%) and 802.11g had 116,782 (18.34%). Moreover, the Zones A and C did not have much difference from each other, where Zone A's 802.3 contributed about 15.85% and 802.11g contributed about 16.06%, whereas Zone C's 802.3 produced 16.23% and 802.11g gave 14.93%. The vertical view shows that they are between 1 to 3% difference between wired and wireless networks at each zone.

The next Table 4.4 shows the total packets to be 598,000. On the one hand, the

Table 4.3
*Zone based Packet Captured between 802.3 vs. 802.11g*

| | Zone A | | | | Zone B | | | | Zone C | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 802.3 | | 802.11g | | 802.3 | | 802.11g | | 802.3 | | 802.11g | | Total |
| **PAYLOAD-ACK** | 95,462 | **15.86%** | 96,547 | **16.04%** | 112,419 | **18.67%** | 110,349 | **18.33%** | 97,538 | **16.20%** | 89,725 | **14.90%** | 602,040 |
| | **94.58%** | | **94.39%** | | **94.95%** | | **94.49%** | | **94.36%** | | **94.41%** | | **94.54%** |
| **SYN/ACK-ACK** | 799 | **16.14%** | 921 | **18.60%** | 846 | **17.09%** | 902 | **18.22%** | 682 | **13.77%** | 801 | **16.18%** | 4,951 |
| | **0.79%** | | **0.90%** | | **0.71%** | | **0.77%** | | **0.66%** | | **0.84%** | | **0.78%** |
| **PSH/ACK-ACK** | 4,001 | **15.56%** | 4,033 | **15.69%** | 4,456 | **17.33%** | 4,778 | **18.58%** | 4,605 | **17.91%** | 3,837 | **14.93%** | 25,710 |
| | **3.96%** | | **3.94%** | | **3.76%** | | **4.09%** | | **4.46%** | | **4.04%** | | **4.04%** |
| **FIN/ACK-ACK** | 667 | **16.33%** | 780 | **19.09%** | 672 | **16.45%** | 753 | **18.43%** | 542 | **13.27%** | 671 | **16.43%** | 4,085 |
| | **0.67%** | | **0.77%** | | **0.58%** | | **0.65%** | | **0.52%** | | **0.71%** | | **0.64%** |
| **Total** | 100,929 | **15.85%** | 102,281 | **16.06%** | 118,393 | **18.59%** | 116,782 | **18.34%** | 103,367 | **16.23%** | 95,034 | **14.93%** | 636,786 |

horizontal line of view comprises PAYLOAD/ACK-ACK (95.46%), PSH/ACK-ACK (3.53%), SYN/ACK-ACK (0.54%), and FIN/ACK-ACK (0.47%). On the other hand, the vertical line of view shows the zones and its 802.3 and 802.11n in various combinations. The range between 802.3 and 802.11n is from 4% and up to 8%. Zone C has the largest range, which is 8%, Zone B with 6%, and Zone A with 4%.

From the description above, it can be concluded that the largest number of packets can be found to be PAYLOAD/ACK-ACK, as compared to others on both 802.3, and to their comparators 802.11g and 802.11n. In terms of zones, the differences is large between 802.3 to 802.11g and 802.11n, where 802.11g is observed to be starting from 1 and up to 3%, while 802.11n has between 4% and 8%. This is because the way both network modes have different sizes when sending and receiving packets. As a result, because 802.11n carries larger sizes than 802.11g, it has less packets compared to 802.11g. However the time between each TCP flag varies and shall be discussed in Section 4.4

### 4.4 Time-Stamped Analysis

The time stamping process is done concurrently to the packet capturing phase at the transport layer. This time stamped procedure occurs at the inbound side of the router at LAN or Subnet [138]. As a result, the time differences between incoming packets ((FIN/ACK, PAYLOAD, PSH/ACK and SYN/ACK) was obtained from the provider and then the client sends back the outgoing packet (ACK) to the responder. Moreover, the grouping procedure was applied from as small as 1 and up to 1000 group collections. As stated before, it is called the equal group technique. Furthermore, averaging was done to derive the mean for group collection from captured packet data.

Hence, the time stamped analysis was performed for different wireless modes, which

Table 4.4
*Zone based Packet Captured between 802.3 vs. 802.11n*

| | Zone A | | | | Zone B | | | | Zone C | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 802.3 | | 802.11n | | 802.3 | | 802.11n | | 802.3 | | 802.11n | | Total |
| **PAYLOAD-ACK** | 96,407 | **16.89%** | 70,392 | **12.33%** | 121,245 | **21.24%** | 84,124 | **14.74%** | 123,008 | **21.55%** | 75,681 | **13.25%** | 570,857 |
| | **95.37%** | | **93.78%** | | **97.00%** | | **95.93%** | | **95.36%** | | **94.39%** | | **95.46%** |
| **SYN/ACK-ACK** | 714 | **22.24%** | 818 | **25.48%** | 445 | **13.86%** | 368 | **11.46%** | 465 | **14.49%** | 400 | **12.46%** | 3,210 |
| | **0.71%** | | **1.09%** | | **0.36%** | | **0.42%** | | **0.36%** | | **0.50%** | | **0.54%** |
| **PSH/ACK-ACK** | 3,343 | **15.82%** | 3,144 | **14.87%** | 2,903 | **13.74%** | 2,872 | **13.59%** | 5,124 | **24.24%** | 3,751 | **17.74%** | 21,137 |
| | **3.31%** | | **4.19%** | | **2.32%** | | **3.28%** | | **3.98%** | | **4.68%** | | **3.53%** |
| **FIN/ACK-ACK** | 619 | **22.14%** | 704 | **25.18%** | 400 | **14.31%** | 329 | **11.77%** | 396 | **14.16%** | 348 | **12.44%** | 2,796 |
| | **0.61%** | | **0.94%** | | **0.32%** | | **0.37%** | | **0.30%** | | **0.43%** | | **0.47%** |
| **Total** | 101,083 | **16.83%** | 75,058 | **12.49%** | 124,993 | **20.80%** | 87,693 | **14.60%** | 128,993 | **21.47%** | 80,180 | **13.35%** | 598,000 |

were 802.11g and 802.11n. Both modes were compared to their 802.3 network using four TCP flags (FIN/ACK, PAYLOAD, PSH/ACK, and SYN/ACK) with their respective ACK. As stated earlier, FIN/ACK, PAYLOAD, PSH/ACK, and SYN/ACK was time stamped one and ACK was time stamped two. The time differences was calculated using time stamped two and time stamped one. The term time differences is used throughout this section to refer to the TCP flag, as FIN/ACK-ACK, PAYLOAD-ACK, PSH/ACK-ACK, and SYN/ACK-ACK.

Next sections 4.4.1 and 4.4.2 will exclusively reveal the time stamped analysis between 802.3 to 802.11g and 802.11n, in two separate sections. The discussion occurs as follows. Each zone is separately discussed with their respective graph side-by-side 802.3 and 802.11g or 802.11n. Consequently, the graph is strengthened by next table showing the summary of minimum, average, median, and maximum. These measurements are projecting the number of times differences from wired to wireless. The table also highlights the number of groups over average line and also below an equal to average lines with three indicators; zero if wired and wireless have an equal number of groups, positive if wireless have more number of groups than wired and negative if wired have more number of groups than wireless. Next, another table which displays the percentage of increase and decrease that helps the investigator to observe the gap between adjacent groups, between wired and wireless networks. The next sections 4.4.1 and 4.4.2 will look into all these matters.

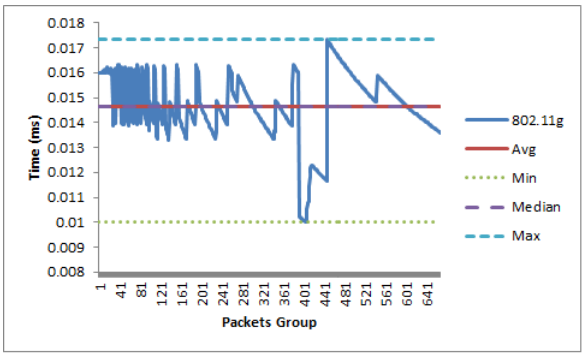
### 4.4.1 802.11g vs 802.3 Time-stamped Differences

This section describes the differences between 802.11g and 802.3 networks. It is segmented into FIN/ACK-ACK, PAYLOAD-ACK, PSH/ACK-ACK, and SYN/ACK-ACK in three different zones, namely Zones A, B, and C. The graphs and tables demonstrate the result from packet capturing process including inbound time

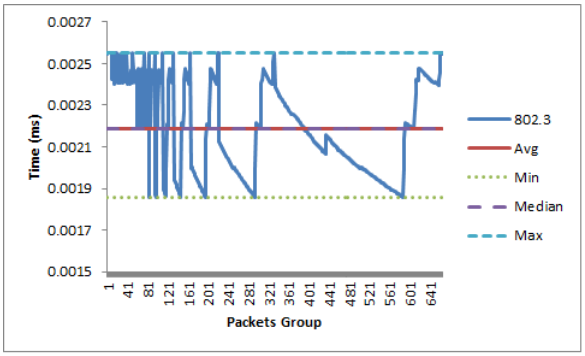
stamped, equal grouping, and averaging. As a result, the differences could be clearly observed between wired and wireless networks for rectifying the existence of RAP.

i. FIN/ACK-ACK

The nature of FIN/ACK function is to disconnect the connection between client and provider (server). It is a response from server to client which is agreed upon to finish the transmission and acknowledged again by the client.




(a) 802.11g




(b) 802.3

*Figure 4.1.* 802.11g vs 802.3 FIN/ACK-ACK Zone A

According to Figure 4.1 there are groups contributing to minimum and maximum values for 802.11g, which are group 405 (minimum value) and 446 (maximum value). However, 802.3 has six minimum groups and seven maximum groups. Group 85 with the minimum and group 11 with the maximum were pinned out, where both are the smallest group in each segment. Table 4.5 shows the differences of Minimum, Average, median, and Maximum between

the two networks.

Table 4.5
*FIN/ACK-ACK of 802.11g vs 802.3 for Zone A*

| | **minimum** | **average** | **median** | **maximum** | **Group > average** | **Group <= average** |
|---|---|---|---|---|---|---|
| **802.11g** | 0.010001 | 0.014626 | 0.014652 | 0.017331 | 337 | 330 |
| **802.3** | 0.001857 | 0.002189 | 0.002188 | 0.002554 | 327 | 340 |
| **Different** | **5.39** | **6.68** | **6.7** | **6.79** | **10** | **-10** |

The table above shows the differences in minimum, average, median, and maximum between 802.11g and 802.3. There are 5.39 time differences between 802.3 and 802.11g in minimum, 6.68 times in average, 6.7 times in median, and 6.79 times showed by maximum. The numbers do not vary much between the others and only minimum has fewer differences. However others are nearly the same. Both 802.11g and 802.3 have plus and minus 10 differences measured in the number of groups that falls over or under the average. 802.11g has more than 10 groups over the average line, whereas 802.3 also has 10 more groups equal or less than average line. Table 4.6 shows the percentage increase or decrease between groups for both 802.11g and 802.3.

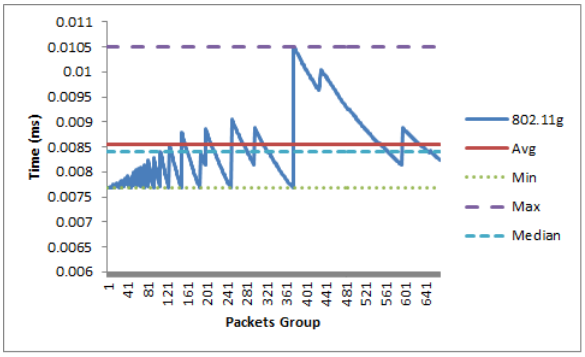
Table 4.6
*FIN/ACK-ACK of 802.11g vs 802.3 Group Percentage Increment and Decrement for Zone A*

| **% changes** | **802.11g** | | **802.3** | |
|---|---|---|---|---|
| | **No. of group** | | **No. of group** | |
| | **increase** | **decrease** | **increase** | **decrease** |
| **0** | 7 | null | 29 | null |
| **0.01-5.00** | 37 | 563 | 65 | 525 |
| **5.01-10.00** | 22 | 8 | 23 | 7 |
| **10.01-15.00** | 7 | 11 | 6 | 1 |
| **15.01-20.00** | 8 | 1 | 4 (19.39) | 1 |
| **20.01-25.00** | 0 | 0 | 0 | 2 |
| **25.01-30.00** | 0 | 0 | 0 | 3 (-27.26) |
| **35.01-40.00** | 0 | 1 (-35.94) | 0 | 0 |
| **45.01-50.00** | 1 (48.56) | 0 | 0 | 0 |
| **Total** | **82** | **584** | **95** | **576** |

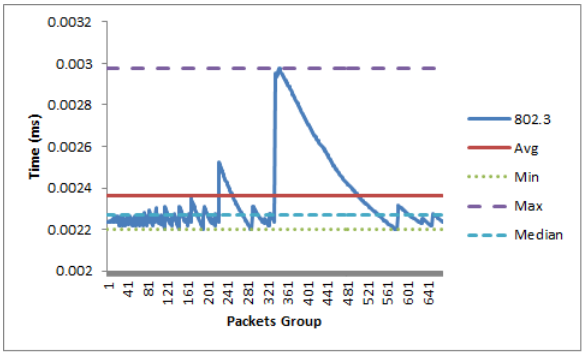
The total number of percentage increase and decrease between 802.11g and

802.3 are 82 and 584, and 95 and 576 respectively. While 802.11g had an extreme change of 48.56%, the rest was less than 20%. Consequently, 802.11g percentage decrement showed about -35.94%. Meanwhile, 802.3 did not have any extreme increment and it showed about 19.39% for the maximum, while the percentage decrement was only recorded at -27.26%. The largest number of percentage increment was shown at 0.01 until 5% where 803.11g had about 37 and 65 of 802.3. Moreover, the largest percentage decrement had the biggest number, which were 563 for 802.11g and 525 for 802.3. Lastly, 0% changes went to 802.3 of about 29, while 802.11g recorded 7.

The Figure 4.2 below shows 802.11g and 802.3 for Zone B. From the 802.11g graph, it was recorded as the minimum showed by group 1 whereas the maximum showed by group 337. On the other hand, 802.3 had minimum at group 116 and maximum at group 345. There was no specific pattern showed by both structures.




(a) 802.11g




(b) 802.3

*Figure 4.2.* 802.11g vs 802.3 FIN/ACK-ACK Zone B

In addition to the above two graphs, Table 4.7 lists all the differences between wired and wireless in the scope of minimum, average, median, and maximum. The differences look equal where minimum was 3.49, average was 3.62, median was 3.7, and maximum was 3.53 times from 802.3 to 802.11g.

Table 4.7
*FIN/ACK-ACK of 802.11g vs 802.3 for Zone B*

| | **minimum** | **average** | **median** | **maximum** | **Group > average** | **Group <= average** |
|---|---|---|---|---|---|---|
| **802.11g** | 0.007673 | 0.008548 | 0.008407 | 0.010509 | 270 | 402 |
| **802.3** | 0.002199 | 0.002364 | 0.002272 | 0.002979 | 193 | 479 |
| **Different** | **3.49** | **3.62** | **3.70** | **3.53** | **77** | **-77** |

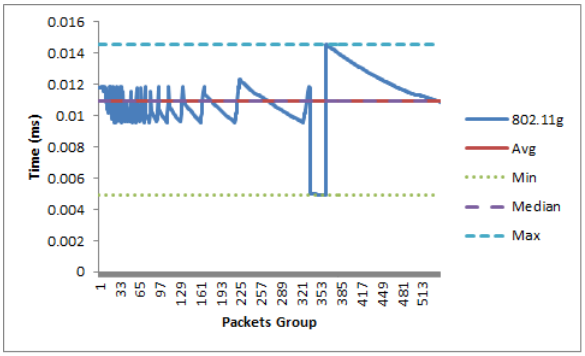
The number of groups that falls above and below average line showed more gaps between these two structures. As stated in Zone A, more 802.11g group numbers (77) were over average line, whereas more 802.3 group numbers were on the line and below average line (-77).

The percentage increase or decrease between groups is shown in Table 4.8. The maximum percentage increase by 802.11g was 36.82%, while 802.3 had only 32.04%. The measure was not different between both wireless and wired networks. However, both shared the same maximum numbers that have percentage increment from 0.01 to 5%, which were 802.11g with 39 and 802.3 with 68. At this percentage, the largest group number comprised percentage decrement, which were 802.11g with 619 and 802.3 with 576. In terms of no changes, 802.3 had about 22 groups, whereas only one from 802.11g.

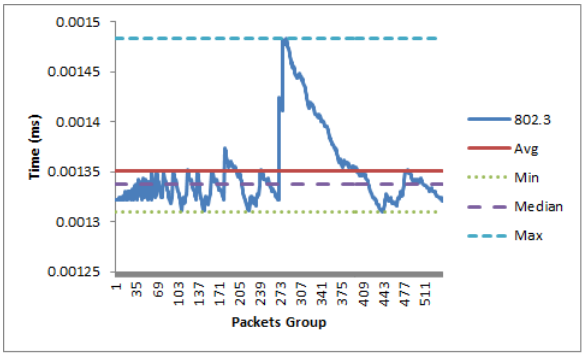
Table 4.8
*FIN/ACK-ACK of 802.11g vs 802.3 Group Percentage Increment and Decrement for Zone B*

| % changes | 802.11g | | 802.3 | |
|---|---|---|---|---|
| | No. of group | | No. of group | |
| | increase | decrease | increase | decrease |
| **0** | 1 | null | 22 | null |
| **0.01-5.00** | 39 | 619 (-1.80) | 68 | 576 (-2.08) |
| **5.01-10.00** | 8 | 0 | 3 | 0 |
| **10.01-15.00** | 2 | 0 | 1 | 0 |
| **15.01-20.00** | 1 | 0 | 0 | 0 |
| **30.01-35.00** | 0 | 0 | 1 (32.04) | 0 |
| **35.01-40.00** | 1 (36.82) | 0 | 0 | 0 |
| **Total** | **52** | **619** | **95** | **576** |

Last but not least, FIN/ACK-ACK for Zone C is shown in Figure 4.3. 802.11g minimum was represented by group 359 and group 361 for maximum, and then 802.3 minimum went to group 443 and maximum was recorded by group 284.




(a) 802.11g




(b) 802.3

*Figure 4.3.* 802.11g vs 802.3 FIN/ACK-ACK Zone C

The median and average of 802.11g was nearly equal, however in 802.3 the

average line was on the top of the median line. Table 4.9 shows the different values where minimum (3.76) displayed low differences, compared to average with 8.08, median with 8.19, and maximum with 9.83. This is because the 802.3 minimum was recorded very low as compared to Zones A and B.

Table 4.9
*FIN/ACK-ACK of 802.11g vs 802.3 for Zone C*

| | **minimum** | **average** | **median** | **maximum** | **Group > average** | **Group < average** |
|---|---|---|---|---|---|---|
| **802.11g** | 0.004924 | 0.010915 | 0.010954 | 0.014580 | 275 | 267 |
| **802.3** | 0.00131 | 0.001351 | 0.001338 | 0.001483 | 163 | 379 |
| **Different** | **3.76** | **8.08** | **8.19** | **9.83** | **112** | **-112** |

The next step regarding FIN/ACK-ACK in Zone C is to look into percentage increase and decrease, which is shown by Table 4.10. The total of percentages was shown as 78 increase and 461 decrease for 802.11g. In addition, there are about 227 increase and 314 decrease for 802.3. The maximum percentage increase was contributed by 802.11g, which was about 195.98 where the value is almost extreme compared to the previous values for FIN/ACK-ACK. The percentage decrease for 802.11g was -57.49. On the other hand, 802.3 had low percentages for both increase with 7.72% and decrease with -0.83%. As a whole, it is still from 0.01 up to 5% covered for the overall group numbers.

Table 4.10
*FIN/ACK-ACK of 802.11g vs 802.3 Group Percentage Increment and Decrement for Zone C*

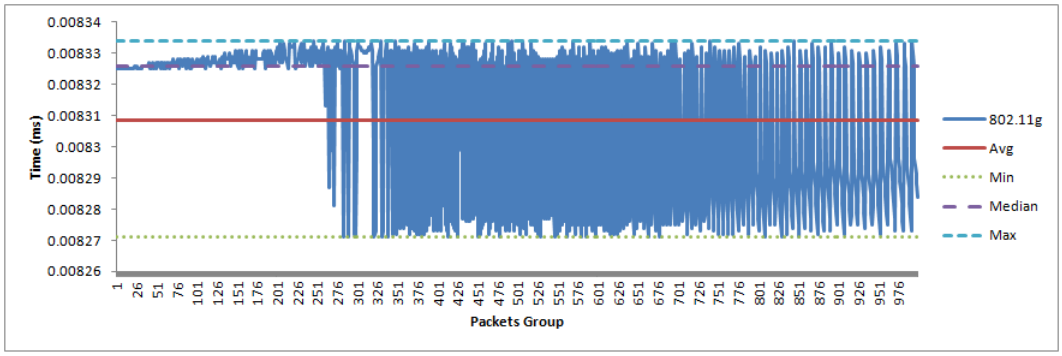
| **% changes** | **802.11g** | | **802.3** | |
|---|---|---|---|---|
| | **No. of group** | | **No. of group** | |
| | **increase** | **decrease** | **increase** | **decrease** |
| **0** | 4 | null | 71 | null |
| **0.01-5.00** | 40 | 438 | 154 | 314 (-0.83) |
| **5.01-10.00** | 19 | 10 | 2 (7.72) | 0 |
| **10.01-15.00** | 9 | 7 | 0 | 0 |
| **15.01-20.00** | 1 | 6 | 0 | 0 |
| **20.01-25.00** | 5 | 0 | 0 | 0 |
| **55.01-60.00** | 1 | 1 (-57.49) | 0 | 0 |
| **195.01-200.00** | 1 (195.98) | 0 | 0 | 0 |
| **Total** | **78** | **461** | **227** | **314** |

In terms of no change, 802.3 had more numbers which is 71, compared to 4 for 802.11g and this shows 802.3 is more stable than 802.11g.

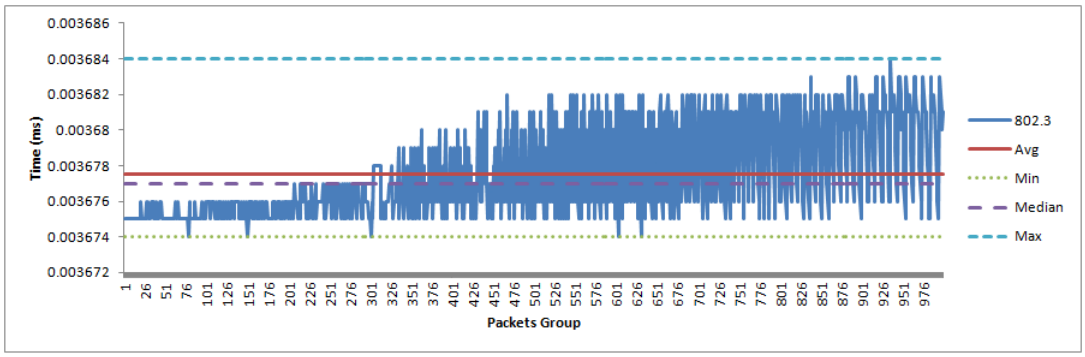
ii. PAYLOAD-ACK

The nature of PAYLOAD is sharing the same code with ACK, however, the payload field is not empty. Normally it is sent by provider (server) after PSH/ACK-ACK is sent by the user machine. Therefore, it is actually data being downloaded into the client machine. As stated earlier, more than 95% of the packet capturing process was contributed by PAYLOAD. As a result, it is easy to meet with our equal group process of up to 1000 groups.

Figure 4.4 shows the PAYLOAD-ACK for Zone A. 802.11g median line was at the top of average line, otherwise it was below 802.3 average line. The group minimum of 802.11g was 284 and maximum 287, while 802.3 minimum was 79 and maximum was 936. This shows some patterns between these two structures.




(a) 802.11g




(b) 802.3

*Figure 4.4.* 802.11g vs 802.3 PAYLOAD-ACK Zone A

The differences between minimum, average, median, and maximum did not much differ and were nearly equal, as shown in Table 4.11. This is because PAYLOAD has huge packets and it is easy to build the equal groups. The number of groups that fall either over the average, equal or below average line also showed a specific characteristic. 802.11g contained 578 groups above average line, while 802.3 showed about 629 groups equal or below the average line. The difference was recorded at 207 between wireless and wired networks.

Table 4.11
*PAYLOAD-ACK of 802.11g vs 802.3 for Zone A*

| | **minimum** | **average** | **median** | **maximum** | **Group > average** | **Group < average** |
|---|---|---|---|---|---|---|
| **802.11g** | 0.008271 | 0.008308 | 0.008326 | 0.008334 | 578 | 422 |
| **802.3** | 0.003674 | 0.003678 | 0.003677 | 0.003684 | 371 | 629 |
| **Different** | **2.25** | **2.26** | **2.26** | **2.26** | **207** | **-207** |

In terms of percentage increment and decrement, Table 4.12 shows the balance between 802.11g and 802.3. All groups had equal range, which was 0.01 to 5%, either increment or decrement. Both had the same characteristics, where more group categories fell under percentage decrement, namely 577 for 802.11g and 464 for 802.3. However, no changes were shown in 240 for 802.3 and 89 for 802.11g. 802.3 was more stable than 802.11g and 2.26 average less time stamped while in real action.

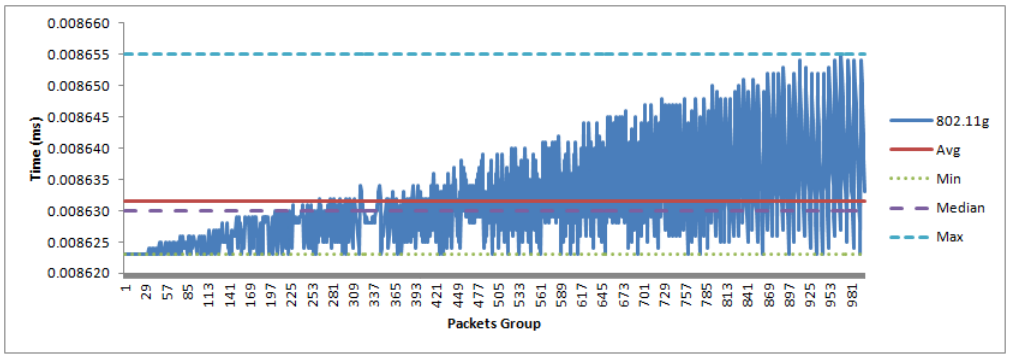
Table 4.12
*PAYLOAD-ACK of 802.11g vs 802.3 Group Percentage Increment and Decrement for Zone A*

| **% changes** | **802.11g** | | **802.3** | |
|---|---|---|---|---|
| | **No. of group** | | **No. of group** | |
| | **increase** | **decrease** | **increase** | **decrease** |
| **0** | 89 | null | 240 | null |
| **0.01-5.00** | 333 (0.76) | 577 (-0.76) | 295 (0.22) | 464 (-0.14) |
| **Total** | **422** | **577** | **535** | **464** |

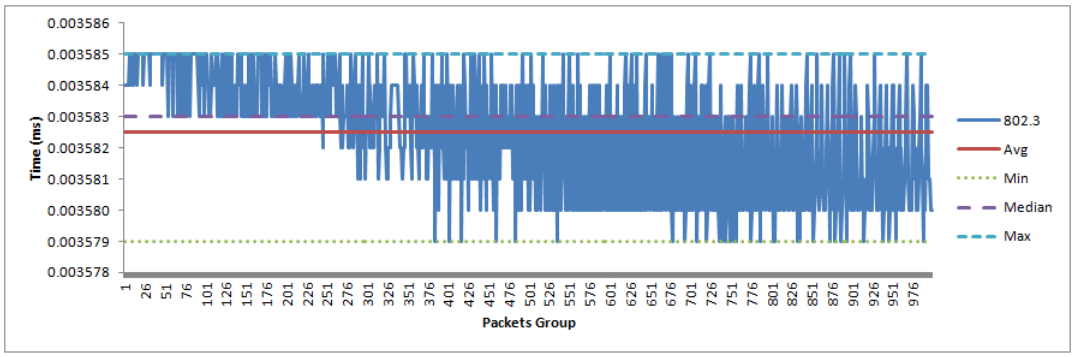
The Zone B graph pattern was observed to be a reverse of Zone A, where 802.11g started at the bottom line which was nearly at the minimum line,

whereas 802.3 started at the opposite (see Figure 4.5). This phenomenon affected the 802.11g minimum where group 1 was its minimum. Furthermore the maximum of 802.11g, which was 968, was nearly at the end of groups (1000). Because of this reverse pattern, the median line is below the average line.

Besides that, 802.3 minimum stated that at group 385 and maximum is 7, thus fills the pattern being shown by the graph. This 802.3 characteristic put the median line above the average line.




(a) 802.11g




(b) 802.3

*Figure 4.5.* 802.11g vs 802.3 PAYLOAD-ACK Zone B

This Payload for Zone B was equally recorded with 2.41 differences for each measurement (see Figure 4.13). Because of the reverse pattern from Zone A to Zone B, the number of groups being analysed for above or equal and below average lines were also influenced, where 802.11g groups were located more at the equal or below average line (611 groups), and while 802.3 had more groups

above the average line, which was 558. The difference is about 169 groups either above average line or equal and below the average line. Even though Zones A and B have different group patterns, 802.3 is still the fastest to respond compared to 802.11g. This is true when the network traffic is unpredictable, even though sometimes it is in a controlled situation.

Table 4.13
*PAYLOAD-ACK of 802.11g vs 802.3 for Zone B*

| | **minimum** | **average** | **median** | **maximum** | **Group > average** | **Group < average** |
|---|---|---|---|---|---|---|
| **802.11g** | 0.008623 | 0.008632 | 0.008630 | 0.008655 | 389 | 611 |
| **802.3** | 0.003579 | 0.003583 | 0.003583 | 0.003585 | 558 | 442 |
| **Different** | **2.41** | **2.41** | **2.41** | **2.41** | **-169** | **169** |

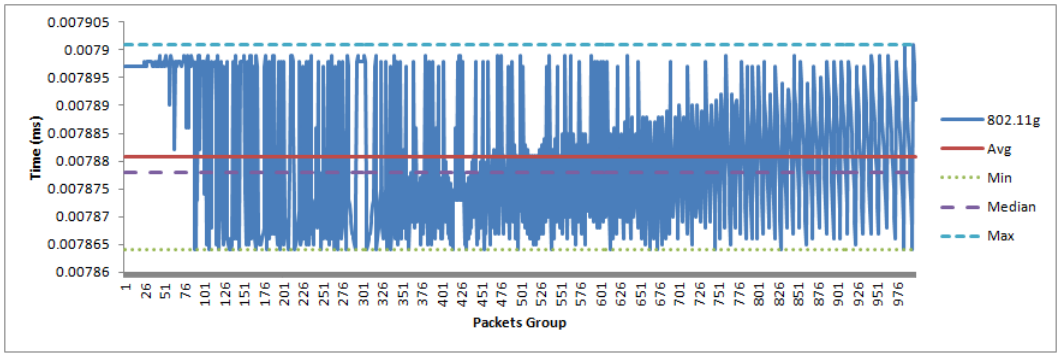
The percentage increase and decrease showed similarity to Zone A, where almost all changes occurred from 0.01 up to 5% (see Table 4.14). However for 802.3, the number of group percentage increase had more numbers (431). In terms of percentage changes, 802.11g recorded 0.36%. 802.3 still had more numbers of groups with no changes, numbering 236, whereas 802.11g had only 82.

Table 4.14
*PAYLOAD-ACK of 802.11g vs 802.3 Group Percentage Increment and Decrement for Zone B*

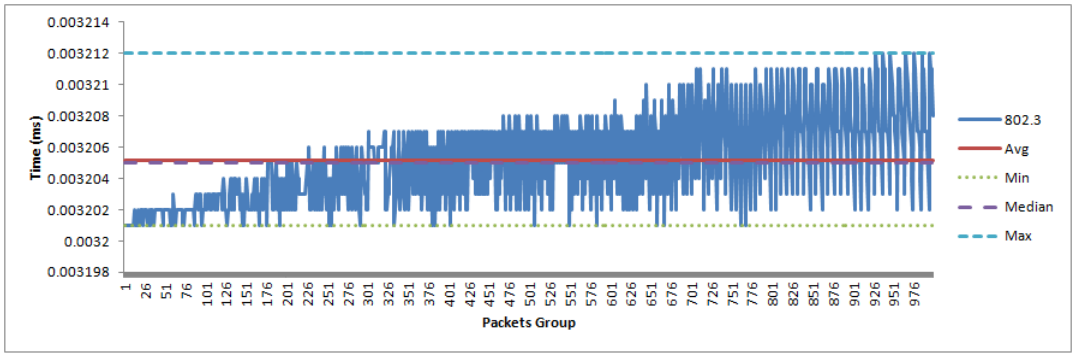
| **% changes** | **802.11g** | | **802.3** | |
|---|---|---|---|---|
| | **No. of group** | | **No. of group** | |
| | **increase** | **decrease** | **increase** | **decrease** |
| **0** | 82 | null | 236 | null |
| **0.01-5.00** | 333 (0.36) | 584 (-0.12) | 431 (0.14) | 332 (-0.17) |
| **Total** | **415** | **584** | **667** | **332** |

The Zone C Payload-ACK had similar pattern to Zone A (see Figure 4.6). 802.11g started at the high point, while 802.3 started at the low point. 802.11g minimum was represented by group 90 and maximum by group 986, while 802.3 minimum was stated by group 1 and maximum by group 929. Both structures had the same pattern where the minimum was represented by low group and

maximum pinpoint by the group near to group 1000. Differently from Zone A and B, this Zone C highlighted the median line to be below average line for both 802.11g and 802.3.




(a) 802.11g




(b) 802.3

*Figure 4.6.* 802.11g vs 802.3 PAYLOAD-ACK Zone C

The differences between 802.11g and 802.3, for all the measurements, are shown in Table 4.15, which have the same values, namely 2.46 times between each wireless and wired networks. There is not much difference between Zone A and B. However the number of differences, between both structures to be above average line and equal or below the average line, produced only 10, where each had nearly equal above or below average line, while 802.11g had 460 groups and 802.3 had 470 above the average line. However for the equal or below average line, 802.11g had 540 groups and 802.3 had 530 groups.

Table 4.15
*PAYLOAD-ACK of 802.11g vs 802.3 for Zone C*

| | **minimum** | **average** | **median** | **maximum** | **Group > average** | **Group < average** |
|---|---|---|---|---|---|---|
| **802.11g** | 0.007864 | 0.007881 | 0.007878 | 0.007901 | 460 | 540 |
| **802.3** | 0.003201 | 0.003205 | 0.003205 | 0.003212 | 470 | 530 |
| **Different** | **2.46** | **2.46** | **2.46** | **2.46** | **-10** | **10** |

Regarding to percentage of increment and decrement, like Zones A and B, Zone C changes was logged beginning from 0.01 up to 5%. 802.11g had 317 groups increasing and 605 groups decreasing, while 802.3 had 292 groups increasing and 501 decreasing. Both structures showed more decreasing than increasing. In the scope of no changes, still 802.3 had 206 groups, while 802.11g had 77 groups only.

Table 4.16
*PAYLOAD-ACK of 802.11g vs 802.3 Group Percentage Increment and Decrement for Zone C*

| **% changes** | **802.11g** | | **802.3** | |
|---|---|---|---|---|
| | **No. of group** | | **No. of group** | |
| | **increase** | **decrease** | **increase** | **decrease** |
| **0** | 77 | null | 206 | null |
| **0.01-5.00** | 317 (0.47) | 605 (-0.44) | 292 (0.31) | 501 (-0.19) |
| **Total** | **394** | **605** | **498** | **501** |

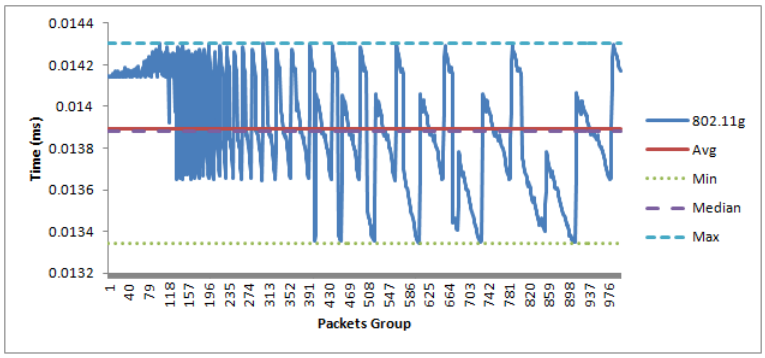
From Zones A, B, and C the amount of differences is between 2.25 and 2.46. This is very stable in both structures, while there are difference in actions where wired is 2.25 times less time stamped than 802.11g. The number of groups involved in between groups percentage was also at the same range, which was 0.01% to 5%. The number of groups that fell above and equal or below average line also had a different number, where Zone A was the highest with 207 and the lowest was from Zone C, with 10.

iii. PSH/ACK-ACK

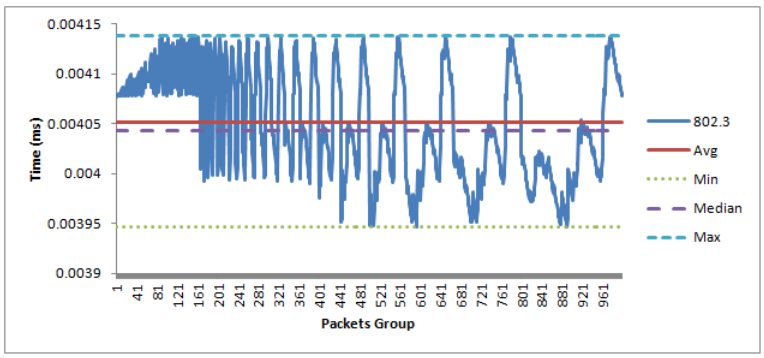
The nature of PSH is to play a role of telling the server what information is requested by sender which must be PSH/ACK by provider and again ACK by

sender or client. This is the second largest packet being captured, however it is not more than 4% of the overall and behind Payload but in front of FIN and SYN. In the case of this research, this PSH flag is also easier to handle for performing the equal group process, because the number of packets being captured is enough to form the 1000 grouping.

The Zone A PSH/ACK-ACK graphs shows the same pattern for 802.11g and 802.3 (see Figure 4.7). However they are not the same in terms of time stamped. Both structures showed median line below the average line. The 802.11g minimum was exhibited by group 607 and maximum shown by group 303, whereas 802.3 minimum was found in group 594 and maximum in group 326.




(a) 802.11g




(b) 802.3

*Figure 4.7.* 802.11g vs 802.3 PSH/ACK-ACK Zone A

The differences between main measurements like minimum, average, median, and maximum were more than three times between 802.3 and 802.11g. The minimum was 3.38, average and median 3.43, and maximum 3.46. Not much

different between both structures in specifying the group numbers that fell over, equal, or less than average line. For this PSH/ACK-ACK Zone A, 802.11g had more numbers falling over average line, which was 480, whereas 802.3 had about 537 groups recorded equal or below average line. Total differences on this matter was 17.

Table 4.17
*PSH/ACK-ACK of 802.11g vs 802.3 for Zone A*

| | **minimum** | **average** | **median** | **maximum** | **Group > average** | **Group < average** |
|---|---|---|---|---|---|---|
| **802.11g** | 0.013346 | 0.013892 | 0.013879 | 0.014302 | 480 | 520 |
| **802.3** | 0.003947 | 0.004051 | 0.004043 | 0.004138 | 463 | 537 |
| **Different** | **3.38** | **3.43** | **3.43** | **3.46** | **17** | **-17** |

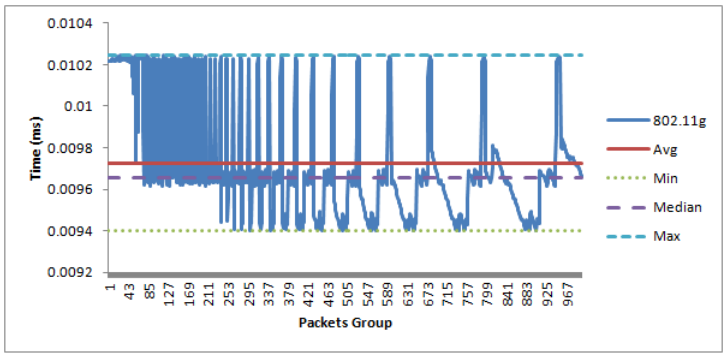
In percentage increase and decrease terms, the majority were from 0.01 up to 5%, either 802.11g or 802.3. However, 802.11g had one group increasing and two groups decreasing from 5.01 up to 10%. Previous report showed no change in 802.3, but at this point, changes occurred in 802.11g with 22, and 802.3 with 15 groups. However these numbers were not as large as previous 0% or no changes.

Table 4.18
*PSH/ACK-ACK of 802.11g vs 802.3 Group Percentage Increment and Decrement for Zone A*

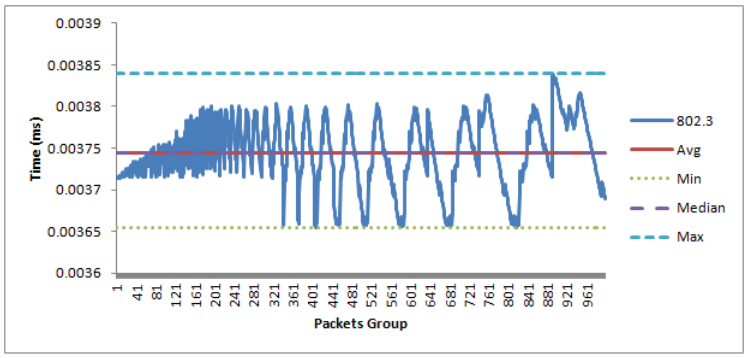
| **% changes** | **802.11g** | | **802.3** | |
|---|---|---|---|---|
| | **No. of group** | | **No. of group** | |
| | **increase** | **decrease** | **increase** | **decrease** |
| **0** | 22 | null | 15 | null |
| **0.01-5.00** | 225 | 749 | 346(2.81) | 638 (-3.19) |
| **5.01-10.00** | 1 (5.09) | 2 (-5.61) | 0 | 0 |
| **Total** | **248** | **751** | **361** | **638** |

At Zone B, the graph in Figure 4.8 exhibited a new trend from the starting point, especially 802.3 where it started neither at the top nor bottom. It seemed to be starting at or nearly to the average line. As usual 802.11g started nearly at the top and the median line was below the average line. Consequently, 802.3 median line was nearly equal to average line. The minimum of 802.11g was recorded by

group 556 and maximum was pointed out by group 29, while 802.3 minimum was shown by group 409 and maximum by group 892.




(a) 802.11g




(b) 802.3

*Figure 4.8.* 802.11g vs 802.3 PSH/ACK-ACK Zone B

On the other hand, the differences between both wireless and wired networks showed as minimum and median to be given 2.57 and 2.58 times, respectively, while the average and maximum pointed to 2.60 and 2.67, respectively. It was quite stable between these two structures. Meanwhile the number of groups either over or below the average line had some abnormal values, where 802.3 had 488 groups more or over average line, while 720 groups were equal or below the average line in 802.11g. The total group number differences toward the average line was 208.

Table 4.19
*PSH/ACK-ACK of 802.11g vs 802.3 for Zone B*

| | **minimum** | **average** | **median** | **maximum** | **Group > average** | **Group < average** |
|---|---|---|---|---|---|---|
| **802.11g** | 0.009401 | 0.009723 | 0.009659 | 0.010246 | 280 | 720 |
| **802.3** | 0.003655 | 0.003744 | 0.003744 | 0.003840 | 488 | 512 |
| **Different** | **2.57** | **2.60** | **2.58** | **2.67** | **-208** | **208** |

The percentage changes also showed the same result as Zone A, where 802.11g had more numbers of no changes than 802.3. It was stated as 19 compared to 15 for 802.3. However 802.3 only changed in between 0.01% up to 5%, compared to 802.11g that had one extra level between 5.01% and 10%. The number of changes also showed that many groups had changes which were 27 groups that increased and 46 groups that decreased toward that amount.

Table 4.20
*PSH/ACK-ACK of 802.11g vs 802.3 Group Percentage Increment and Decrement for Zone B*

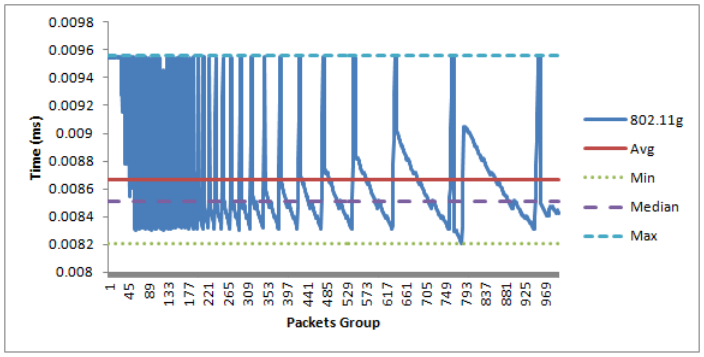
| **% changes** | **802.11g** | | **802.3** | |
|---|---|---|---|---|
| | **No. of group** | | **No. of group** | |
| | **increase** | **decrease** | **increase** | **decrease** |
| **0** | 19 | null | 15 | null |
| **0.01-5.00** | 289 | 609 | 305 (3.36) | 679 (-1.72) |
| **5.01-10.00** | 27 (6.56) | 46 (-8.01) | 0 | 0 |
| **Total** | **344** | **655** | **320** | **679** |

At this point, the differences between times stamping always showed 802.3 to have less time taken compared to 802.11g. The percentage changes also recorded that 802.11g had extra level or had more percentage changes than 802.3. This showed 802.3 to be so stable while it is in action. Because of this stability it is hoped to be used as a mechanism for identifying RAP that is represented by 802.11g.

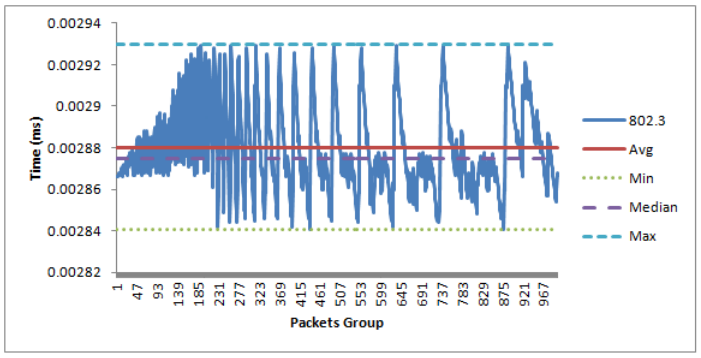
The graph pattern of Zone C does not differ from Zone B where 802.11g was observed at the top and the median line was below the average line. The 802.11g minimum was represented by group 785 and the maximum was pointed out by group 35. There was a cross line between minimum and maximum in presenting

the group, where the minimum was represented by a big group, otherwise the maximum was represented by a small group.

On the other hand, 802.3 started the movement nearly to the average line. The maximum was pinned by group 439 and the maximum pointed out by group 887. The result looked more normal than 802.11g. The median line was drawn below the average line, similarly for 802.11g.




(a) 802.11g




(b) 802.3

*Figure 4.9.* 802.11g vs 802.3 PSH/ACK-ACK Zone C

The average and maximum themselves were more than three times comparing between 802.3 to 802.11g. Meanwhile, minimum and maximum were less than and approaching to three (see Figure 4.21). As stated for Zone B, the number of groups was either above or below average line that had the same pattern where 425 groups exceeded the average line came from 802.3, while 667 groups were equal or below the average line reported from 802.11g. Only Zone A had a different pattern other than Zones B and C.

Table 4.21
*PSH/ACK-ACK of 802.11g vs 802.3 for Zone C*

| | minimum | average | median | maximum | Group > average | Group < average |
|---|---|---|---|---|---|---|
| **802.11g** | 0.008207 | 0.008664 | 0.008511 | 0.009556 | 333 | 667 |
| **802.3** | 0.002841 | 0.002880 | 0.002875 | 0.002930 | 425 | 575 |
| **Different** | **2.89** | **3.01** | **2.96** | **3.25** | **-92** | **92** |

Comparing Zones A and B, Zone C especially 802.11g, had bigger percentage changes than 802.3. It recorded about 15.01% by one group and 34 groups with -13.05%, the highest. Otherwise 802.3 was placed at the normal change rates of between 0.01% and 5%. The highest increment recorded for 802.3 was 2.14% and decrement was -0.91%. As far as this research is concerned, the no changes is still the same as Zone A and B where it is recorded as 14 by 802.11g and 13 by 802.3.

Table 4.22
*PSH/ACK-ACK of 802.11g vs 802.3 Group Percentage Increment and Decrement for Zone B*

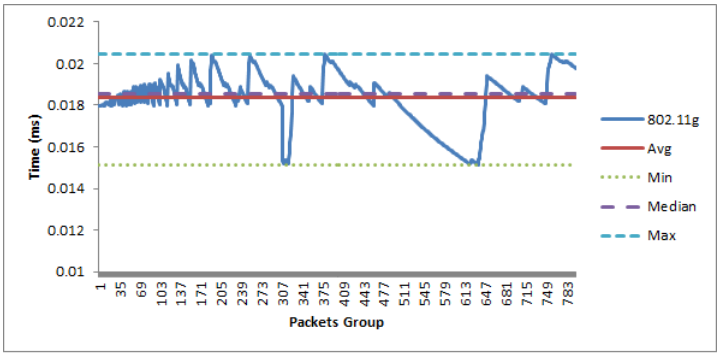
| % changes | 802.11g | | 802.3 | |
|---|---|---|---|---|
| | No. of group | | No. of group | |
| | increase | decrease | increase | decrease |
| **0** | 14 | null | 13 | null |
| **0.01-5.00** | 187 | 688 | 259 (2.14) | 725 (-0.91) |
| **5.01-10.00** | 32 | 20 | 0 | 0 |
| **10.01-15.00** | 23 | 34 (-13.05) | 0 | 0 |
| **15.01-20.00** | 1 (15.01) | 0 | 0 | 0 |
| **Total** | **257** | **742** | **274** | **725** |

As a second contributor after Payload, the Push TCP flag showed some pattern differences between wireless and wired networks.

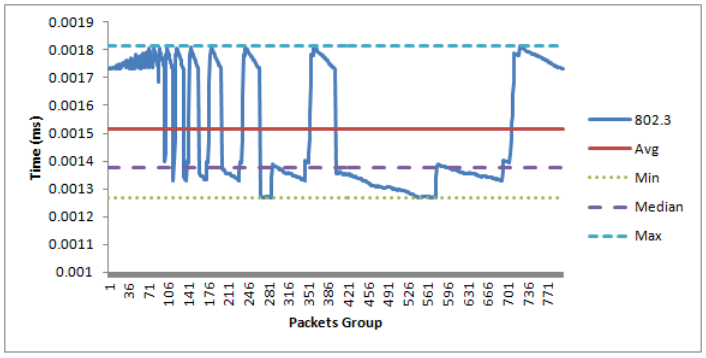
iv. SYN/ACK-ACK

In establishing a connection between client and server, the TCP flag being sent is SYN. Synchronisation is very important between both parties to start handshaking and then ready to proceed to the next level. The time stamped occurs when the provider responds to the SYN that was sent by the sender. The

provider responds with SYN/ACK flag and then the ACK is sent by the client. As shown in Figure 4.10, both started the graph at different points. 802.11g started nearly from the bottom of average line whereas 802.3 started at the top of its average line. The 802.11g median was above the average line, while 802.3 median line was at the bottom of its average line. Meanwhile, 802.11g group minimum was pinned at 635 and maximum at 379. In addition, 802.3 minimum was recorded for group 547 and maximum at group 361. Both structures showed the groups to be above 350, but not more than 700. This is in the middle of Equal Group (1-1000).




(a) 802.11g




(b) 802.3

*Figure 4.10.* 802.11g vs 802.3 SYN/ACK-ACK Zone A

There were about 146 group differences between wireless and wired networks to be above and equal or below the average line. From these numbers, 479 groups were above 802.11g average line, while 466 groups were equal or below the 802.3 average line. Comparing to the previous analysis, this SYN/ACK-ACK

Zone A showed more in between 11.96 to 13.45 times from 802.3 to 802.11g than all the other measurements (see Table 4.23).

Table 4.23
*SYN/ACK-ACK of 802.11g vs 802.3 for Zone A*

| | **minimum** | **average** | **median** | **maximum** | **Group > average** | **Group < average** |
|---|---|---|---|---|---|---|
| **802.11g** | 0.015159 | 0.018378 | 0.018539 | 0.020442 | 479 | 320 |
| **802.3** | 0.001267 | 0.001515 | 0.001378 | 0.001813 | 333 | 466 |
| **Different** | **11.96** | **12.13** | **13.45** | **11.28** | **146** | **-146** |

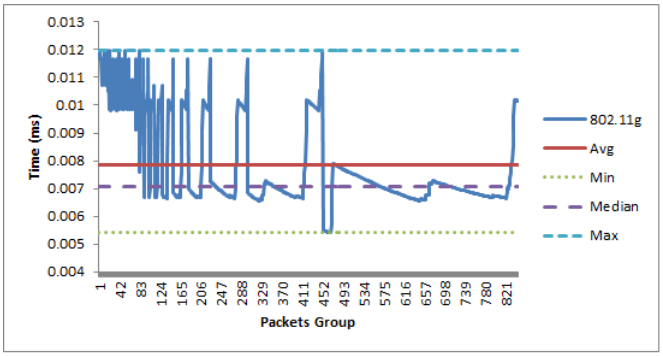
The total number of changes showed in Table 4.48 were 134 groups increasing and 664 groups decreasing for 802.11g. Otherwise 802.3 had a total of 294 groups increasing and 504 groups decreasing. In terms of percentages, 802.3 showed higher level of increase or decrease, where 25% was the highest percentage increase and -26.02% was the highest percentage decrease. Consequently 802.11g percentage increase was less than 802.3 increment. The percentage increase by 802.11g was shown at 11.95%, and percentage decrease was pointed out at -15.03%.

Table 4.24
*SYN/ACK-ACK of 802.11g vs 802.3 Group Percentage Increment and Decrement for Zone B*

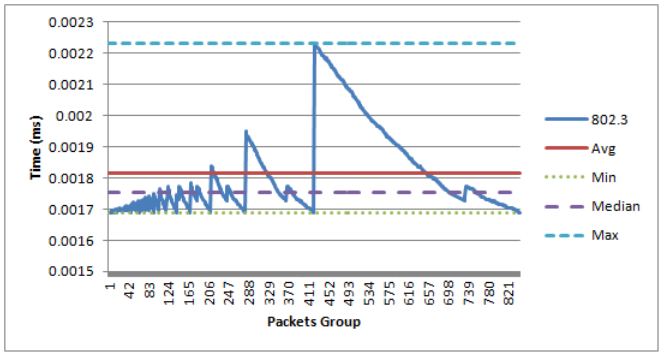
| **% changes** | **802.11g** | | **802.3** | |
|---|---|---|---|---|
| | **No. of group** | | **No. of group** | |
| | **increase** | **decrease** | **increase** | **decrease** |
| **0** | 3 | null | 129 | null |
| **0.01-5.00** | 120 | 663 | 143 | 497 |
| **5.01-10.00** | 9 | 0 | 16 | 0 |
| **10.01-15.00** | 2 (11.95) | 0 | 4 | 0 |
| **15.01-20.00** | 0 | 1 (-15.03) | 0 | 1 |
| **20.01-25.00** | 0 | 0 | 1 (25.00) | 5 |
| **25.01-30.00** | 0 | 0 | 0 | 1 (-26.02) |
| **Total** | **134** | **664** | **294** | **504** |

From the previous descriptions, only this Zone A SYN/ACK-ACK showed difference in percentage changes. In the no changes situation, 802.3 had about 129 groups with 0% changes, whereas 802.11g only had three groups.

Next, Zone B started the graphs at different points (see Figure 4.11). The 802.11g started at the top of average line while 802.3 started at below of the average line. Both structures had the same median line which was below the average line. Meanwhile, the minimum group for 802.11g was logged at 468, which was near to the middle of the equal group. The maximum of 802.11g was recorded in group 17. In addition, 802.3 minimum was group 2 and maximum was recorded in group 424. There are differences between how the graphs were plotted and their starting and ending were also at different points.




(a) 802.11g




(b) 802.3

*Figure 4.11.* 802.11g vs 802.3 SYN/ACK-ACK Zone B

In terms of the number of differences, it was about from 3.21 to 5.38 for 802.3 and 802.11g (see Table 4.25). Comparing to Zone A, this zone had standard differences between 802.3 to 802.11g, as was previously observed with other TCP flags. The differences were also logged between these two structures in the scope of number of groups located above and equal or below the average line,

which was 38. 802.11g revealed that the biggest number of groups fell equal and below the average line. Meanwhile 802.3 had more groups sitting above the average line, which was 605 groups.

Table 4.25
*SYN/ACK-ACK of 802.11g vs 802.3 for Zone B*

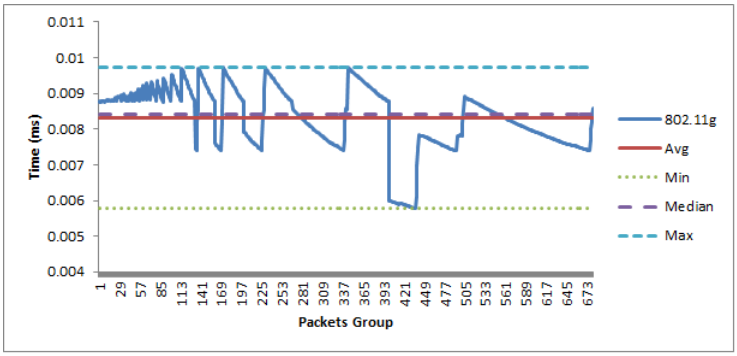
| | **minimum** | **average** | **median** | **maximum** | **Group > average** | **Group < average** |
|---|---|---|---|---|---|---|
| **802.11g** | 0.005411 | 0.007837 | 0.007071 | 0.011993 | 241 | 605 |
| **802.3** | 0.001688 | 0.001817 | 0.001756 | 0.002230 | 279 | 567 |
| **Different** | **3.21** | **4.31** | **4.03** | **5.38** | **-38** | **38** |

Besides that, the percentage changes also showed the extreme level of changes and the number of groups that feed into this level. 802.11g showed about 35.94% increment and -54.21% decrement, while 802.3 logged 32.11% increment and -0.88% decrement (see Table 4.26). Even though this does not usually happen to this flag and in this zone, however the changes majority occurred from 0.01 up to 5% for both wireless and wired networks. Though there are some strange measurements to have observed happened here, the no changes was still led by 802.3, which recorded 93 groups compared to seven groups from 802.11g.

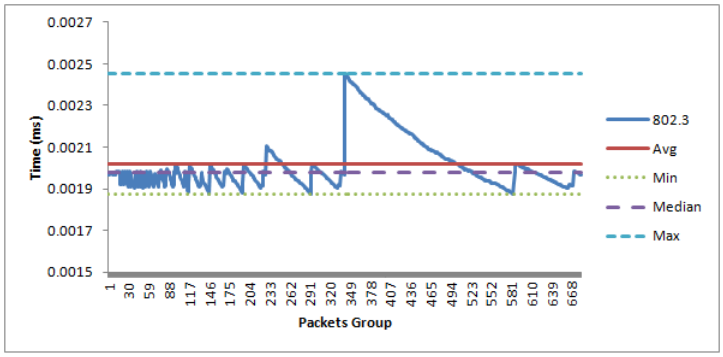
Table 4.26
*SYN/ACK-ACK of 802.11g vs 802.3 Group Percentage Increment and Decrement for Zone B*

| **% changes** | **802.11g** | | **802.3** | |
|---|---|---|---|---|
| | **No. of group** | | **No. of group** | |
| | **increase** | **decrease** | **increase** | **decrease** |
| **0** | 7 | null | 93 | null |
| **0.01-5.00** | 56 | 675 | 80 | 668 (-0.88) |
| **5.01-10.00** | 39 | 11 | 2 | 0 |
| **10.01-15.00** | 19 | 4 | 0 | 0 |
| **15.01-20.00** | 9 | 5 | 1 | 0 |
| **20.01-25.00** | 4 | 1 | 0 | 0 |
| **25.01-30.00** | 3 | 0 | 0 | 0 |
| **30.01-35.00** | 1 | 0 | 1 (32.11) | 0 |
| **35.01-40.00** | 1 (35.94) | 4 | 0 | 0 |
| **40.01-45.00** | 0 | 5 (-54.21) | 0 | 0 |
| **Total** | **139** | **705** | **177** | **668** |

Figure 4.12 showed two graphs with their different patterns. The wired network shows a median line below the average line however the wireless network showed the opposite, where the median was over the average line. The minimum and maximum for 802.3 were shown by groups 292 and 342, respectively. Meanwhile 802.11g group minimum was 437 and group maximum was 172. Consequently, both started at different points, 802.11g was the first group starting above average line, whereas 802.3 started below the average line.




(a) 802.11g




(b) 802.3

*Figure 4.12.* 802.11g vs 802.3 SYN/ACK-ACK Zone C

The time differences related to this SYN/ACK-ACK are shown in Table 4.27. From the table, the minimum was 3.08, average was 4.12, median was reported at 4.26, and maximum logged in at 3.96. The result for 802.3 was 4.12 times slower than 802.11g. In addition, the number of groups nearing the average line also showed 802.11g to have more numbers above the average line, otherwise 802.3 was highlighted to be equal or less than the average line. The number of

differences between the group numbers to the average line was 160.

Table 4.27
*SYN/ACK-ACK of 802.11g vs 802.3 for Zone C*

| | **minimum** | **average** | **median** | **maximum** | **Groups > average** | **Groups < average** |
|---|---|---|---|---|---|---|
| **802.11g** | 0.005773 | 0.008301 | 0.008424 | 0.009726 | 361 | 321 |
| **802.3** | 0.001876 | 0.002017 | 0.001979 | 0.002455 | 201 | 481 |
| **Different** | **3.08** | **4.12** | **4.26** | **3.96** | **160** | **-160** |

Percentage differences in Table 4.28 projected that the majority of groups for both structures changed at the rate of 0.01 to 5%. However 802.11g had less percentage increment, which was 14.07 as compared to 24.87% for 802.3. A percentage decrease for 802.3 was normal at -3.88% as compared to -31.61% for 802.11g. Moreover, 802.3 had 24 groups with no changes, while 802.11g had four groups only.

Table 4.28
*SYN/ACK-ACK of 802.11g vs 802.3 Group Percentage Increment and Decrement for Zone B*

| **% changes** | **802.11g** | | **802.3** | |
|---|---|---|---|---|
| | **No. of group** | | **No. of group** | |
| | **increase** | **decrease** | **increase** | **decrease** |
| **0** | 4 | null | 24 | null |
| **0.01-5.00** | 54 | 600 | 81 | 572 (-3.88) |
| **5.01-10.00** | 12 | 1 | 3 | 0 |
| **10.01-15.00** | 7 (14.07) | 1 | 0 | 0 |
| **15.01-20.00** | 0 | 1 | 0 | 0 |
| **20.01-25.00** | 0 | 0 | 1 (24.87) | 0 |
| **25.01-30.00** | 0 | 0 | 0 | 0 |
| **30.01-35.00** | 0 | 1 (-31.61) | 0 | 0 |
| **Total** | **77** | **604** | **109** | **572** |

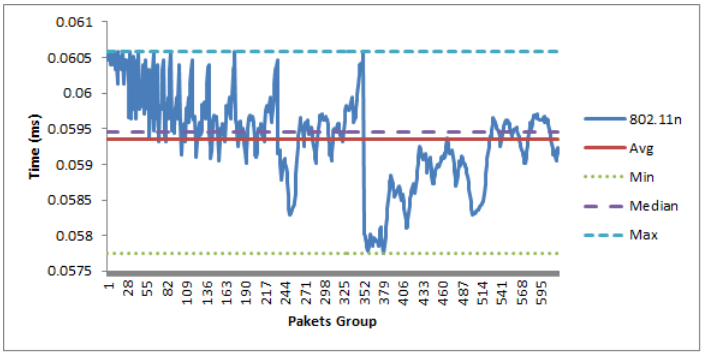
The typifying of 802.3 and 802.11g had some characterisations, especially since they were analysed by different TCP indicators. The next section is going to highlight the comparison between 802.11n and 802.3 networks. The layout of both structures is still similar to these section.

### 4.4.2 802.11n vs 802.3 Time-stamped Differences

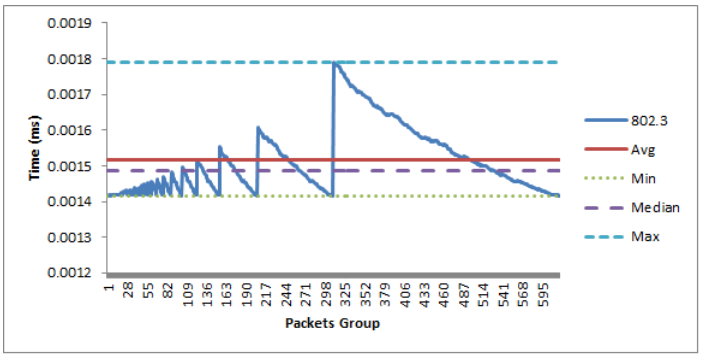
This section shall have similar discussion structure for 802.11g versus 802.3. However the result will vary because there are differences between 802.11g and 802.11n. The number of data that can be carried would vary from both modes where g can carry up to 54 mbps, while n can carry between 150 up to 300 mbps.

i. FIN/ACK-ACK

We start our observation by looking into two FIN/ACK-ACK graphs representing 802.11n and 802.3, as shown in Figure 4.13. The two graphs started at different angles, with 802.11n starting at the top of average line whereas 802.3 at the bottom of the average line. A group minimum for 802.11n was observed in group 380 and maximum with group 1. On the other hand, 802.3 minimum was represented by group 1, maximum by group 310. From the description it can be observed that there are a huge variety of differences between these two structures; the group minimum for 802.3 is the group maximum for 802.11n




(a) 802.11n




(b) 802.3

*Figure 4.13.* 802.11n vs 802.3 FIN/ACK-ACK Zone A

Instead of graph pattern differences, both networks also have time stamped differences. Compared to the discussion of 802.11g versus 802.3, the result showed huge differences. Table 4.29 shows the differences where the average differences between 802.3 and 802.11n was 39.17. The minimum was stated at 40.84, median at 40.01, and maximum at 33.86. From this result, it showed that it is easier to detect RAP if it is in the n mode. The group number toward the average line difference between wired and wireless network n is about 109. Meanwhile, 802.3 had more groups equal or below the average line, and 802.11n showed more groups placed above the average.

Table 4.29
*FIN/ACK-ACK of 802.11n vs 802.3 for Zone A*

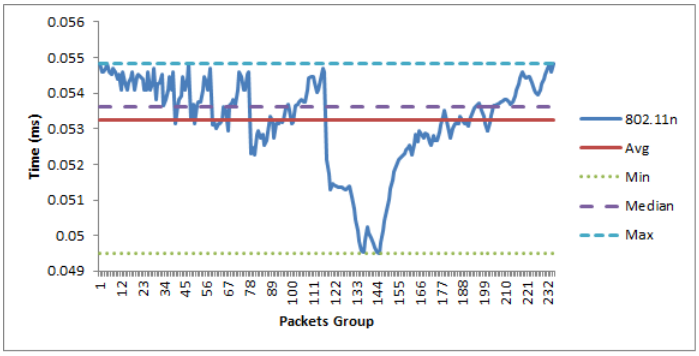
| | **minimum** | **average** | **median** | **maximum** | **Group > average** | **Group < average** |
|---|---|---|---|---|---|---|
| **802.11n** | 0.057743 | 0.05774 | 0.059460 | 0.060577 | 354 | 265 |
| **802.3** | 0.001414 | 0.001515 | 0.001486 | 0.001789 | 245 | 374 |
| **Different** | **40.84** | **39.17** | **40.01** | **33.86** | **109** | **-109** |

In addition to the big values of time differences between 802.11n and 802.3, Table 4.30 shows some differences from previous percentage changes. At this point, 802.3 recorded 26.34% increment, whereas 802.11n increment is normal, from 0.01 to 5%. Even though 802.3 showed some high increment, it also had more groups with normal decrement changes. No change is still maintained by 802.3 compared to 802.11n.

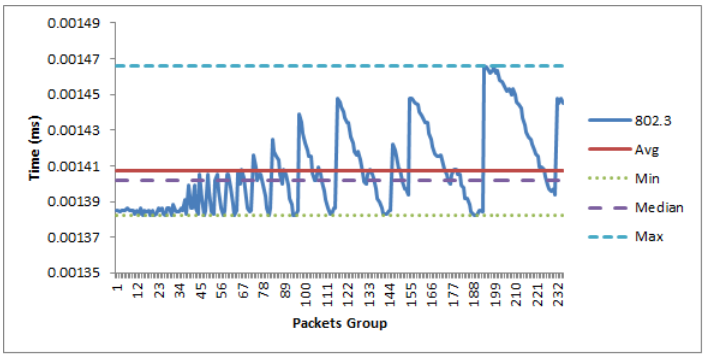
Table 4.30
*FIN/ACK-ACK of 802.11n vs 802.3 Group Percentage Increment and Decrement for Zone A*

| **% changes** | **802.11n** | | **802.3** | |
|---|---|---|---|---|
| | **No. of group** | | **No. of group** | |
| | **increase** | **decrease** | **increase** | **decrease** |
| **0** | 3 | null | 81 | null |
| **0.01-5.00** | 331 (1.55) | 284(-4.23) | 84 | 448 (-0.91) |
| **5.01-10.00** | 0 | 0 | 3 | 0 |
| **10.01-15.00** | 0 | 0 | 1 | 0 |
| **15.01-20.00** | 0 | 0 | 0 | 0 |
| **20.01-25.00** | 0 | 0 | 0 | 0 |
| **25.01-30.00** | 0 | 0 | 1 (26.34) | 0 |
| **Total** | **334** | **284** | **170** | **448** |

The Zone B FIN/ACK-ACK between 802.11n and 802.3 had a different pattern. 802.11n started at the top of the average line, while 802.3 below it. The median of 802.11n is over the average, whereas 802.3 had the opposite. A minimum group for 802.11n was 145 and maximum in group 233. Otherwise 802.3 minimum was group 15 and maximum to be group 194. It was concluded that the pattern of these two structures showed an opposite trend, however the time differences will reflect other assumptions.




(a) 802.11n




(b) 802.3

*Figure 4.14.* 802.11n vs 802.3 FIN/ACK-ACK Zone B

As shown in Zone A, Zone B was similar where the average was recorded at 37.83 times between 802.3 and 802.11n. Other values like minimum was shown to be 35.81, median of at 38.25, and maximum at 37.40. The number of groups placed around the average had small differences between wired and wireless networks. It was about 45, which is about half of Zone A. In the case of number of groups placed to or near the average line, 802.11n had more numbers above the average line whereas 802.3 had more equal or below the average line. This is similar to Zone A.

Table 4.31
*FIN/ACK-ACK of 802.11n vs 802.3 for Zone B*

| | **minimum** | **average** | **median** | **maximum** | **Group > average** | **Group < average** |
|---|---|---|---|---|---|---|
| **802.11n** | 0.049487 | 0.053234 | 0.053623 | 0.054834 | 137 | 98 |
| **802.3** | 0.001382 | 0.001407 | 0.001402 | 0.001466 | 92 | 143 |
| **Different** | **35.81** | **37.83** | **38.25** | **37.40** | **45** | **-45** |

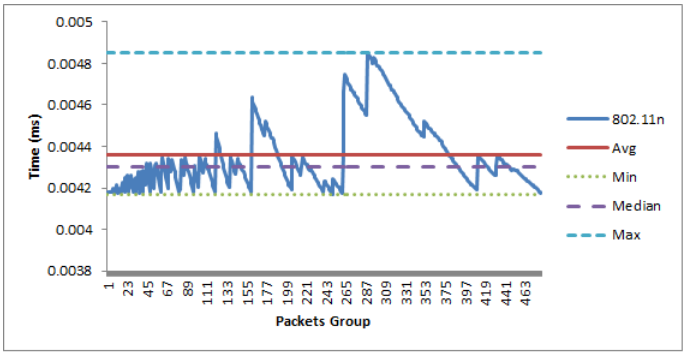
In the sense of percentage changes, it was also similar to Zone A where this Zone

B increment was conquered by 802.3, with 5.92% (see Table 4.32). However this value was low compared to Zone A. The normal changes were reported from 0.01 to 5%, where all previous Zones were highlighted.

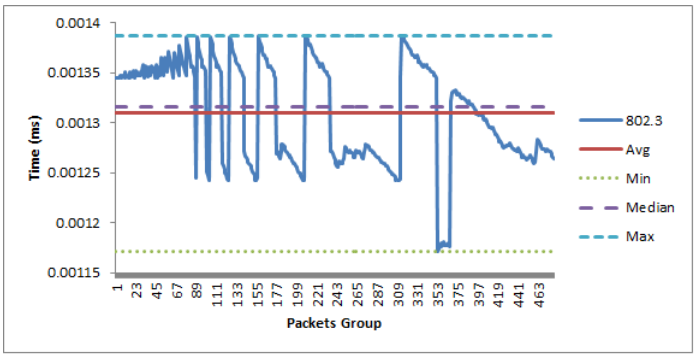
Table 4.32
*FIN/ACK-ACK of 802.11g vs 802.3 Group Percentage Increment and Decrement for Zone B*

| **% changes** | **802.11n** | | **802.3** | |
|---|---|---|---|---|
| | **No. of group** | | **No. of group** | % decrease |
| | **increase** | **decrease** | **increase** | **decrease** |
| **0** | 1 | null | 30 | null |
| **0.01-5.00** | 139 (1.28) | 94 (-4.51) | 55 | 148 (-0.93) |
| **5.01-10.00** | 0 | 0 | 1 (5.92) | 0 |
| **Total** | **140** | **94** | **86** | **148** |

The last Zone C had different graph patterns, compared to the other two Zones A and B. 802.11n started at the above average and the median is also in the same condition. As shown in Figure 4.15, 802.3 started at the top and above the average, with the median also at the top of the line. A group minimum and maximum for 802.11n was observed in groups 250 and 289, respectively, while on the other side, 802.3 minimum and maximum were in groups 353 and 157, respectively. This Zone C showed a different pattern compared to Zone A and Zone B.




(a) 802.11n




(b) 802.3

*Figure 4.15.* 802.11n vs 802.3 FIN/ACK-ACK Zone C

Table 4.33 shows low time differences between 802.3 to 802.11n. The 802.11n produces similar average time differences for 802.11g, with an average of 3.33, minimum of 3.56, median of 3.27, and maximum of 3.50. The number of groups located above, equal, or below average was at 92. Due to the differences between this zone with Zones A and B, 802.11n had more groups equal and below the average as compared to 802.3 that had more above the average.

Table 4.33
*FIN/ACK-ACK of 802.11n vs 802.3 for Zone C*

| | **minimum** | **average** | **median** | **maximum** | **Group > average** | **Group < average** |
|---|---|---|---|---|---|---|
| **802.11n** | 0.004169 | 0.004360 | 0.004304 | 0.004850 | 153 | 328 |
| **802.3** | 0.001171 | 0.001310 | 0.001316 | 0.001387 | 245 | 236 |
| **Different** | **3.56** | **3.33** | **3.27** | **3.50** | **-92** | **92** |

The differences also showed 802.3 to be aligned with 802.11n in the sense of both were increasing. Even 802.3 decrement was also at the same level. However 802.11n decrement was located at the normal level from 0.01 to 5%.

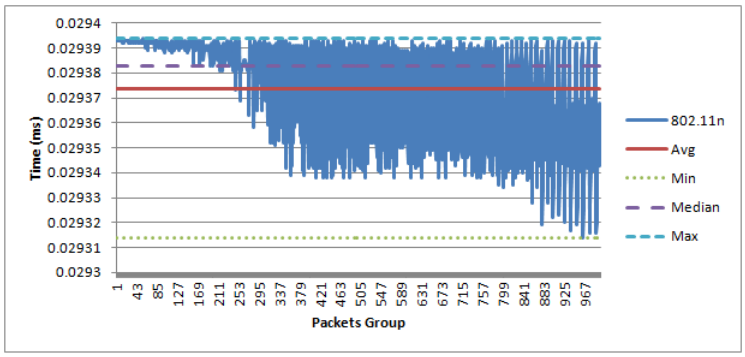
As usual 802.3, still dominated the no changes category with 85 groups, as compared to 11 groups for 802.11n.

Table 4.34
*FIN/ACK-ACK of 802.11n vs 802.3 Group Percentage Increment and Decrement for Zone C*

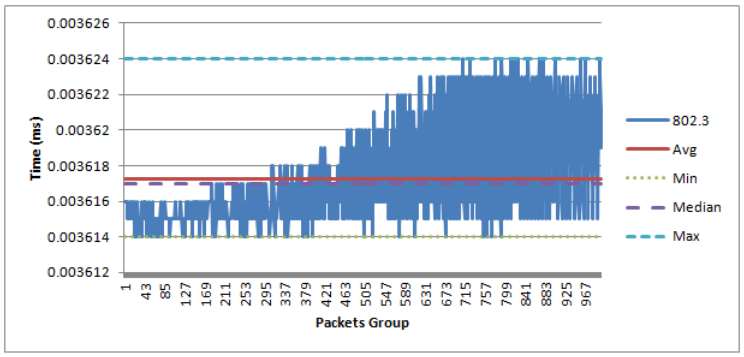
| % changes | 802.11n | | 802.3 | |
|---|---|---|---|---|
| | No. of group | | No. of group | |
| | increase | decrease | increase | decrease |
| **0** | 11 | null | 65 | null |
| **0.01-5.00** | 56 | 409 (-1.88) | 100 | 301 |
| **5.01-10.00** | 3 | 0 | 1 | 6 |
| **10.01-15.00** | 1 (10.93) | 0 | 6 (12.41) | 1 (-12.94) |
| **Total** | **71** | **409** | **172** | **308** |

ii. PAYLOAD-ACK

The second analysis started by looking at Figure 4.16 that showed two graph patterns starting at different points, where 802.11n started at the top of the average, whereas 802.3 began at the bottom. The graphs show the same pattern with no difference between 802.3 and 802.11g. The minimum group for 802.11n was found in 965 and maximum was in group 5, while 802.3 minimum was in group 23 and maximum in group 709.




(a) 802.11n




(b) 802.3

*Figure 4.16.* 802.11n vs 802.3 PAYLOAD-ACK Zone A

Consequently, the Zone A time differences showed to be not as high as FIN/ACK-ACK in Zones A and B where an average was logged at 8.12. Additionally, other items were not much different and nearly equal to the average. The median was similar to the average, but minimum and maximum themselves had value of 8.11. Like 802.11g versus 802.3, these values showed the stability of PAYLOAD-ACK. See Table 4.35 for more details regarding the time differences and number of groups located to be surrounding the average line.

Table 4.35
*PAYLOAD-ACK of 802.11n vs 802.3 for Zone A*

| | **minimum** | **average** | **median** | **maximum** | **Group > average** | **Group < average** |
|---|---|---|---|---|---|---|
| **802.11n** | 0.029314 | 0.029374 | 0.029383 | 0.029394 | 583 | 417 |
| **802.3** | 0.003614 | 0.003617 | 0.003617 | 0.003624 | 341 | 659 |
| **Different** | **8.11** | **8.12** | **8.12** | **8.11** | **242** | **-242** |

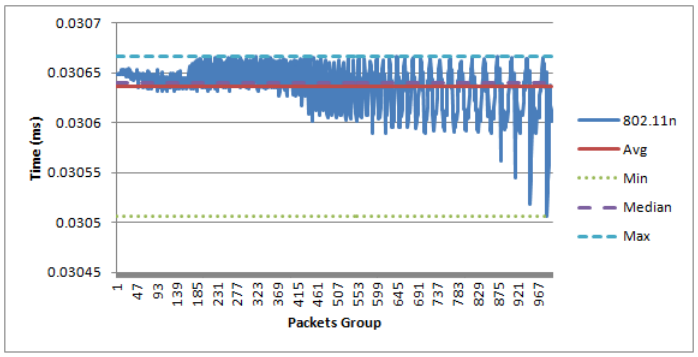
As was expected, the percentage changes did not differ from other PAYLOAD

that was presented before, where it was dotted around the 0.001 to 5% (see Figure 4.36). However, the no changes was still conquered by 802.3 with 166 groups, while 802.11n was observed with 74 groups.

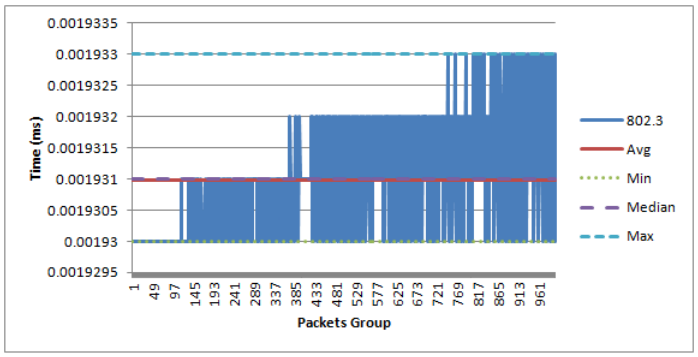
Table 4.36
*PAYLOAD-ACK of 802.11n vs 802.3 Group Percentage Increment and Decrement for Zone A*

| **% changes** | **802.11n** | | **802.3** | |
|---|---|---|---|---|
| | **No. of group** | | **No. of group** | |
| | **increase** | **decrease** | **increase** | **decrease** |
| **0** | 74 | null | 166 | null |
| **0.01-5.00** | 532 (0.16) | 393 (-0.27) | 312 (0.28) | 521 (-0.11) |
| **Total** | **606** | **393** | **478** | **521** |

Figure 4.17 also showed more graphs with similar patterns to Zone A above, where 802.11n was initially located above the average, whereas 802.3 began at the bottom of the average. Like Zone A, the minimum and maximum of both structures were opposite, where minimum of 802.11n was in group 989, while for 802.3, it was in group 2. On the other hand, the maximum for 802.11n was in group 266, and 802.3 was in group 746.




(a) 802.11n




(b) 802.3

*Figure 4.17.* 802.11n 802.3 PAYLOAD-ACK Zone B

The next step was to observe the time differences in this zone (see Table 4.37). An average of 15.87 times was observed between 802.3 and 802.11n. The minimum is logged at 15.81, median was similar to average, while maximum was recorded at 15.86. As with the previous zone, Zone B also had no differences between those values. In terms of a relationship between group to average, it showed that 802.11n had more groups equal or below average than 802.3, which showed more groups over the average.

Table 4.37
*PAYLOAD-ACK of 802.11n vs 802.3 for Zone B*

| | **minimum** | **average** | **median** | **maximum** | **Group > average** | **Group < average** |
|---|---|---|---|---|---|---|
| **802.11n** | 0.030507 | 0.030636 | 0.030640 | 0.030667 | 604 | 396 |
| **802.3** | 0.001930 | 0.001931 | 0.001931 | 0.001933 | 655 | 345 |
| **Different** | **15.81** | **15.87** | **15.87** | **15.86** | **-51** | **51** |

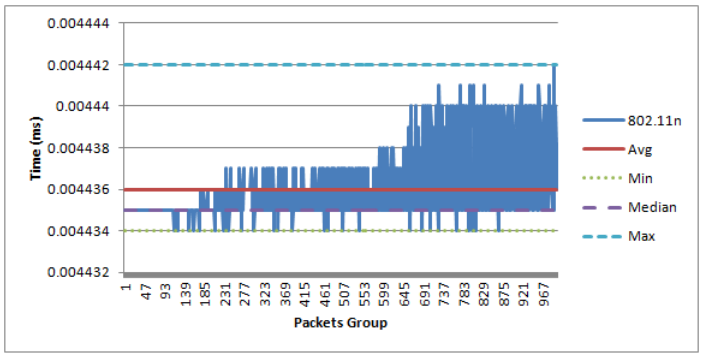
Perhaps percentage changes was reported as a normal changes for both, but there were differences in terms of no changes, where 802.3 showed 405 groups,

as compared to 48 groups for 802.11n. It was concluded that the percentage changes for this zone was normal.

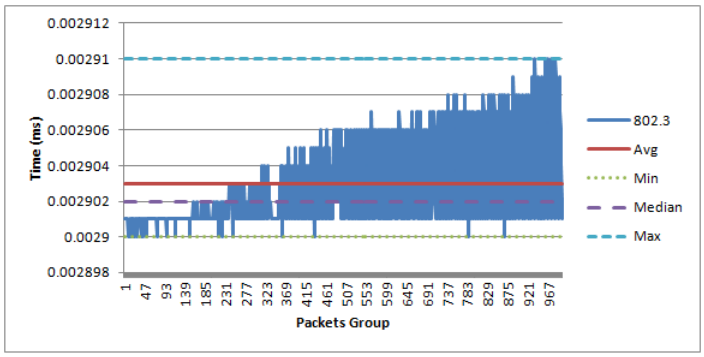
Table 4.38
*PAYLOAD-ACK of 802.11n vs 802.3 Group Percentage Increment and Decrement for Zone B*

| **% changes** | **802.11n** | | **802.3** | |
|---|---|---|---|---|
| | **No. of group** | | **No. of group** | |
| | **increase** | **decrease** | **increase** | **decrease** |
| **0** | 48 | null | 405 | null |
| **0.01-5.00** | 533 (0.14) | 418 (-0.47) | 264 (0.16) | 330 (-0.10) |
| **Total** | **581** | **418** | **669** | **330** |

The next Zone C showed differences from other zones, where the pattern for both wired and wireless were the same (see Figure 4.18). Both started at below average, with the median for both also being below average. Group minimum and maximum indicated a similar pattern also, with 802.11n minimum and maximum showing in groups 115 and 993, respectively, whereas for 802.3, they were in groups 9 and 937, respectively.




(a) 802.11n




(b) 802.3

*Figure 4.18.* 802.11n vs 802.3 PAYLOAD-ACK Zone C

The next indicator also showed some differences compared to the previous two. Figure 4.39 showed about 1.53 times between 802.3 and 802.11n in all the measurements. This value was low compared to Zones A and B. The number of group differences toward the average line was also low, at only 3. At the same time, 802.3 had more groups over the average than 802.11n, which conquered the equal or below average area.

Table 4.39
*PAYLOAD-ACK of 802.11n vs 802.3 for Zone C*

| | **minimum** | **average** | **median** | **maximum** | **Group > average** | **Group < average** |
|---|---|---|---|---|---|---|
| **802.11n** | 0.004434 | 0.004436 | 0.004435 | 0.004442 | 451 | 549 |
| **802.3** | 0.002900 | 0.002903 | 0.002902 | 0.002910 | 448 | 552 |
| **Different** | **1.53** | **1.53** | **1.53** | **1.53** | **3** | **-3** |

Not much difference from the past with this flag of PAYLOAD 802.11n versus 802.3. The percentage changes was viewed as normal, which was between 0.01

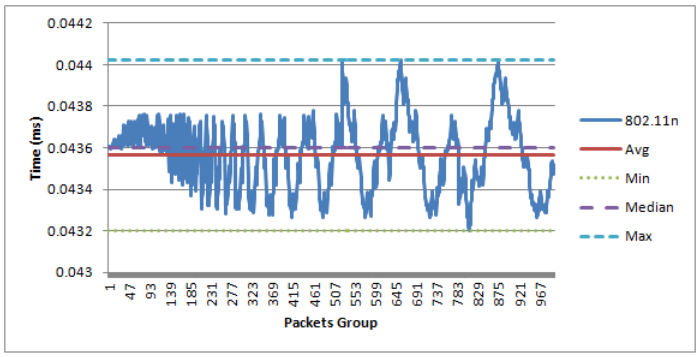
and 5%. Otherwise in this zone, 802.3 was overtaken by 802.11n in the no changes category, showing 802.11n to have more groups than 802.3.

Table 4.40
*PAYLOAD-ACK of 802.11n vs 802.3 Group Percentage Increment and Decrement for Zone C*

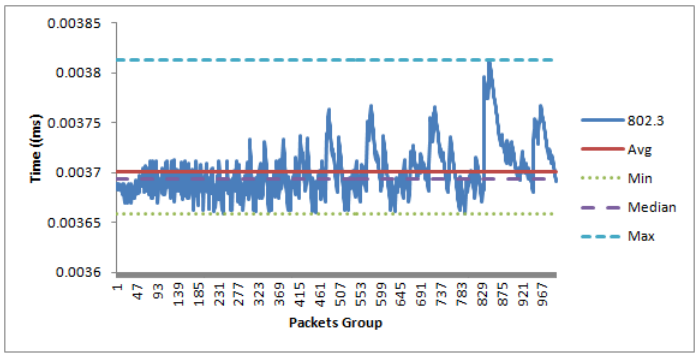
| **% changes** | **802.11n** | | **802.3** | |
|---|---|---|---|---|
| | **No. of group** | | **No. of group** | |
| | **increase** | **decrease** | **increase** | **decrease** |
| **0** | 346 | null | 269 | null |
| **0.01-5.00** | 282 (0.16) | 371 (-0.07) | 259 (0.31) | 471 (-0.14) |
| **Total** | **628** | **371** | **528** | **471** |

iii. PSH/ACK-ACK

Figure 4.19 shows the two graph patterns of 802.11n versus 802.3. As can be observed, it started at different points, where 802.11n began above the average and stood on the median line, while 802.3 somehow was in the opposite position. The minimum group position for 802.11n was in group 810. This value was quite high compare to group 244 for 802.3. The maximum value for 802.11n was lower than the respective minimum (group 656), while 802.3 was recorded by group 848.




(a) 802.11n




(b) 802.3

*Figure 4.19.* 802.11n vs 802.3 PSH/ACK-ACK Zone A

The time difference between this zone to 802.11g zone had more range, where the average was logged at 11.77, minimum stated as 11.81, with the median was recorded as 11.80, and finally maximum was shown as 11.55. The number of group close to the average line was 186 differences, where 802.11n stated more groups above the average and the reverse result for 802.3. See Figure 4.17 for more details.

Table 4.41
*PSH/ACK-ACK of 802.11n vs 802.3 for Zone A*

| | **minimum** | **average** | **median** | **maximum** | **Group > average** | **Group < average** |
|---|---|---|---|---|---|---|
| **802.11n** | 0.043202 | 0.043567 | 0.043599 | 0.044025 | 565 | 435 |
| **802.3** | 0.003659 | 0.003701 | 0.003694 | 0.003813 | 379 | 621 |
| **Different** | **11.81** | **11.77** | **11.80** | **11.55** | **186** | **-186** |

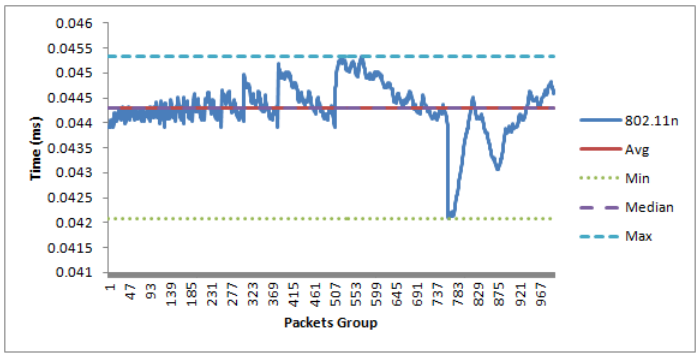
Even though 802.3 had less delay from 802.11n (11.77 times), their percentage changes was at a normal level, which was 0.01 to 5% (see Figure 4.42). Both

wired and wireless networks had nearly the same number of groups that did not change.

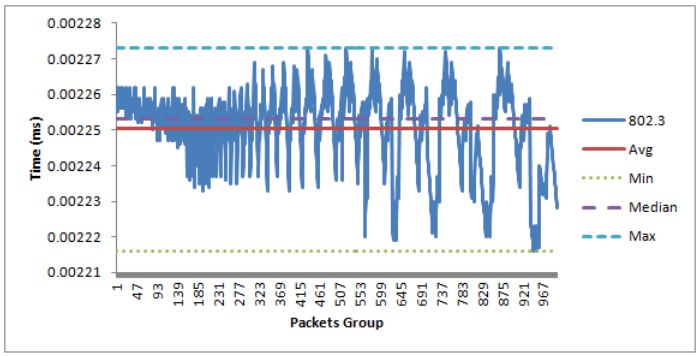
Table 4.42
*PSH/ACK-ACK of 802.11n vs 802.3 Group Percentage Increment and Decrement for Zone A*

| **% changes** | **802.11n** | | **802.3** | |
|---|---|---|---|---|
| | **No. of group** | | **No. of group** | |
| | **increase** | **decrease** | **increase** | **decrease** |
| **0** | 14 | null | 13 | null |
| **0.01-5.00** | 485 (0.94) | 500 (-0.75) | 317 (3.07) | 669 (-0.94) |
| **Total** | **499** | **500** | **330** | **669** |

The Zone B graphs showed a different plot (see Figure 4.20), with 802.11n starting below and 802.3 started above the average line. The group for minimum and maximum of 802.11n were in groups 764 and 568 respectively. Meanwhile 802.3 minimum and maximum were observed in the respective groups of 946 and 435. The median over the average for both showed a different pattern, with 802.11n median below the average, even though it looked like a stack in the graph, while 802.3 median was above the average.




(a) 802.11n




(b) 802.3

*Figure 4.20.* 802.11n vs 802.3 PSH/ACK-ACK Zone B

The Zone B time differences was higher than the previous Zone A. An average showed 802.3 to be 19.68 times as compared to 802.11n. The other values were as follows, minimum 18.99, median 19.66, and maximum 19.94. However, the number of groups positioned close to the average line varied. The 802.11n groups were positioned more on equal or below the average line and 802.3 had a reverse result. Table 4.43 also highlighted about 135 number of groups differing between 802.11n and 802.3

Table 4.43
*PSH/ACK-ACK of 802.11n vs 802.3 for Zone B*

| | **minimum** | **average** | **median** | **maximum** | **Group > average** | **Group < average** |
|---|---|---|---|---|---|---|
| **802.11n** | 0.042085 | 0.044298 | 0.044292 | 0.045326 | 477 | 523 |
| **802.3** | 0.002216 | 0.002251 | 0.002253 | 0.002273 | 612 | 388 |
| **Different** | **18.99** | **19.68** | **19.66** | **19.94** | **-135** | **135** |

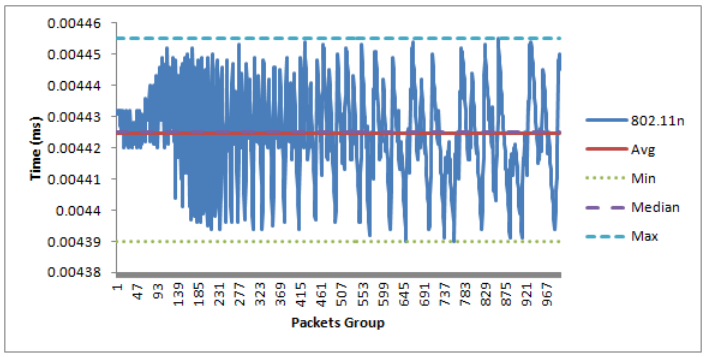
Table 4.44 points out that both structures had the level of percentage changes of between 0.01 and 5%. In terms of numbers, 802.11n had more increasing

groups as otherwise compared to 802.3, which had more on decreasing groups. Apart from this result, the no changes was managed by 802.3 with 34 groups, as compared to 802.11n with 11 groups.

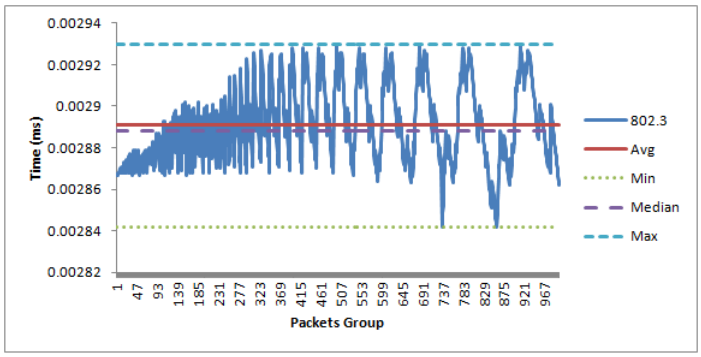
Table 4.44
*PSH/ACK-ACK of 802.11n vs 802.3 Group Percentage Increment and Decrement for Zone B*

| **% changes** | **802.11n** | | **802.3** | |
|---|---|---|---|---|
| | **No. of group** | | **No. of group** | |
| | **increase** | **decrease** | **increase** | **decrease** |
| **0** | 11 | null | 34 | null |
| **0.01-5.00** | 463 (2.93) | 525 (-4.10) | 343 (1.07) | 622 (-1.60) |
| **Total** | **474** | **525** | **377** | **622** |

The Zone C is as shown in Figure 4.21, being a little bit different, with 802.11n spreading slightly equally to the bottom and to the top, while starting above the average line, while conversely 802.3 started below the average. The median and average for 802.11n had the same value, while the 802.3 median was below the average. The minimum and maximum for 802.11n were shown in group 170 and 861 respectively. On the other hand, 802.3 minimum and maximum were in the respective groups 736 and 913.




(a) 802.11n




(b) 802.3

*Figure 4.21.* 802.11n vs 802.3 PSH/ACK-ACK Zone C

There were large differences between this Zone C to Zones A and B, where the time differences showed small times values between 802.3 and 802.11n (see Figure 4.45). The value also looked the same at 1.53 average and median, 1.54 minimum, and 1.52 maximum. The number of groups to the average also differed where 802.11n had more numbers above the average, however, 802.3 showed more group numbers equalling or being below the average. Their differences was about 63.

Table 4.45
*PSH/ACK-ACK of 802.11n vs 802.3 for Zone C*

| | **minimum** | **average** | **median** | **maximum** | **Group > average** | **Group < average** |
|---|---|---|---|---|---|---|
| **802.11n** | 0.004390 | 0.004425 | 0.004425 | 0.004455 | 518 | 482 |
| **802.3** | 0.002842 | 0.002891 | 0.002888 | 0.002930 | 455 | 545 |
| **Different** | **1.54** | **1.53** | **1.53** | **1.52** | **63** | **-63** |

Like Zones A and B, Zone C also had normal percentage changes between 0.01 and 5%. The no changes was nearly equal between both wired and wireless

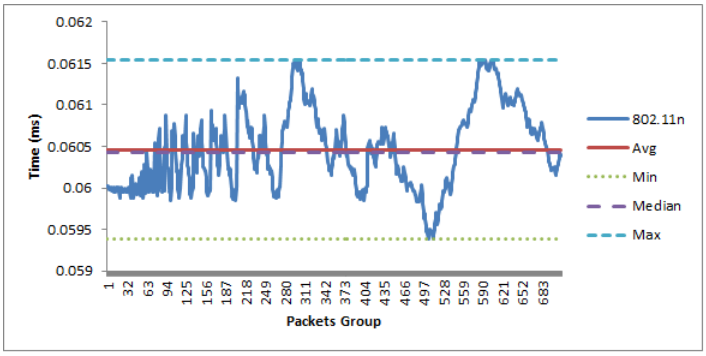
structures.

Table 4.46
*PSH/ACK-ACK of 802.11n vs 802.3 Group Percentage Increment and Decrement for Zone C*

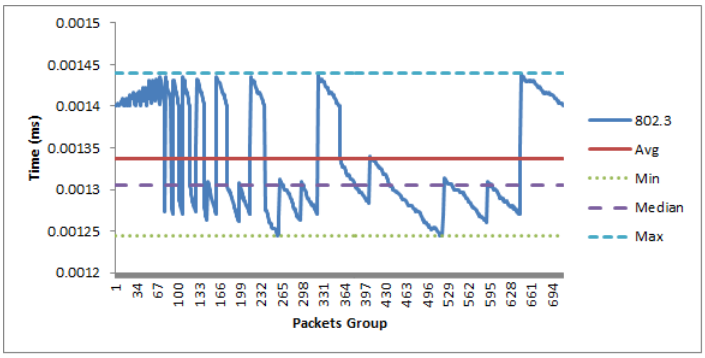
| **% changes** | **802.11n** | | **802.3** | |
|---|---|---|---|---|
| | **No. of group** | | **No. of group** | |
| | **increase** | **decrease** | **increase** | **decrease** |
| **0** | 22 | null | 24 | null |
| **0.01-5.00** | 332 (1.07) | 645 (-0.61) | 213 (2.09) | 663 (-0.91) |
| **Total** | **354** | **645** | **336** | **663** |

iv. SYN/ACK-ACK

As usual, Figure 4.22 showed two plot of graphs having different starting points, with 802.11n starting below the average, whereas 802.3 started above the average. Meanwhile, both had medians below the average. The minimum and maximum for 802.11n showed up in group 505 and group 593, respectively, where both indicators sat in groups greater than 500. On the other hand, 802.3 had low groups representing the minimum and maximum, both of which were recorded by group 259 and 323, respectively.




(a) 802.11n




(b) 802.3

*Figure 4.22.* 802.11n vs 802.3 SYN/ACK-ACK Zone A

Table 4.47 exhibits extreme time differences between 802.3 to 802.11n, with the average recorded at 45.24 times, minimum logged at 47.74, median of 46.31, and maximum of 42.76. There were 63 group differences placed toward the average line, with 802.11n having more group numbers above the average while 802.3 was the opposite.

Table 4.47
*SYN/ACK-ACK of 802.11n vs 802.3 for Zone A*

| | **minimum** | **average** | **median** | **maximum** | **Group > average** | **Group < average** |
|---|---|---|---|---|---|---|
| **802.11n** | 0.059386 | 0.060463 | 0.060431 | 0.061537 | 336 | 377 |
| **802.3** | 0.001244 | 0.001337 | 0.001306 | 0.001439 | 273 | 440 |
| **Different** | **47.74** | **45.24** | **46.31** | **42.76** | **63** | **-63** |

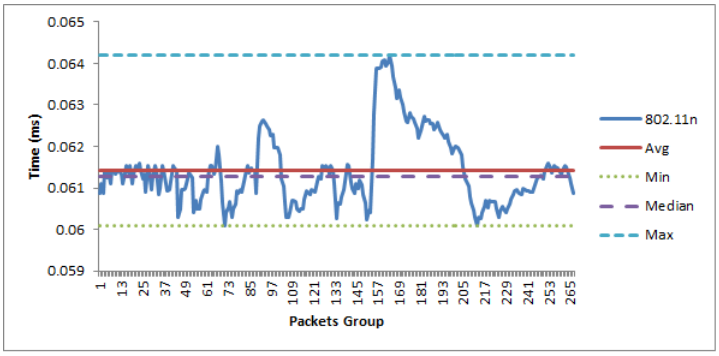
Even though there is an extreme time difference condition, the percentage changes showed its own independent trend, with 802.11 sitting at the normal level, and even 802.3 also had more groups in the same level. Meanwhile, 802.3 had more percentage increment and decrement, which were 13.22% and -9.20%

respectively. Though this was unexpected, the no changes was still conquered by 802.3 with 153 groups as compared to seven groups for 802.11n.

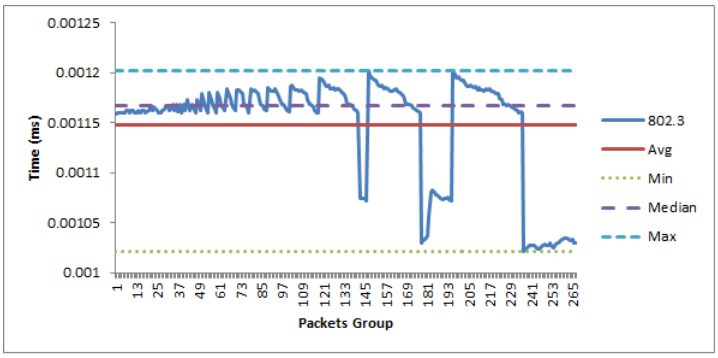
Table 4.48
*SYN/ACK-ACK of 802.11n vs 802.3 Group Percentage Increment and Decrement for Zone A*

| **% changes** | **802.11n** | | **802.3** | |
|---|---|---|---|---|
| | **No. of group** | | **No. of group** | |
| | **increase** | **decrease** | **increase** | **decrease** |
| **0** | 7 | null | 153 | null |
| **0.01-5.00** | 335 (2.21) | 370 (-0.73) | 90 | 451 |
| **5.01-10.00** | 0 | 0 | 6 | 7 (-9.20) |
| **10.01-15.00** | 0 | 0 | 5 (13.22) | 0 |
| **Total** | **342** | **370** | **254** | **458** |

As usual Figure 4.23 shows two plots of graphs that had different starting points, with 802.11n starting from below the average, whereas 802.3 started above the average. Both had a different median to average. The 802.11n median was above the average, and 802.3 was observed the opposite. Meanwhile, the minimum and maximum of 802.11n showed up in group 71 and group 164, respectively. On the other hand, 802.3 minimum and maximum were recorded by groups 237 and 147, respectively.




(a) 802.11n




(b) 802.3

*Figure 4.23.* 802.11n vs 802.3 SYN/ACK-ACK Zone B

Table 4.49 shows more extreme time differences than Zone A between 802.3 and 802.11n, with the average recorded at 53.51 times, minimum logged at 58.81, median was 52.51, and maximum was 53.41. Meanwhile, there were 122 group differences placed toward the average line, with 802.11n having more group numbers being equal or below the average, while 802.3 was the opposite.

Table 4.49
*SYN/ACK-ACK of 802.11n vs 802.3 for Zone B*

| | **minimum** | **average** | **median** | **maximum** | **Group > average** | **Group < average** |
|---|---|---|---|---|---|---|
| **802.11n** | 0.060103 | 0.061422 | 0.061279 | 0.064202 | 101 | 166 |
| **802.3** | 0.001022 | 0.001148 | 0.001167 | 0.001202 | 213 | 54 |
| **Different** | **58.81** | **53.51** | **52.51** | **53.41** | **-122** | **122** |

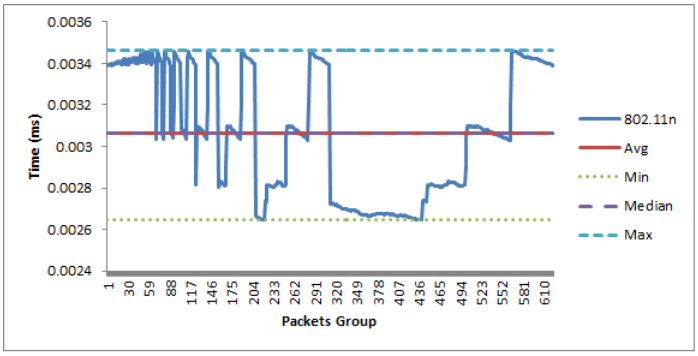
The percentage changes shown in Table 4.50 was also similar to Zone A, where 802.3 had more degree of change than 802.11n, which was at the normal level. It was observed that 802.3 had the highest increment logged at 12.13%, and

decrement was -11.90%. The no changes category specified that 802.3 had more group numbers (34) than 802.11n (one).

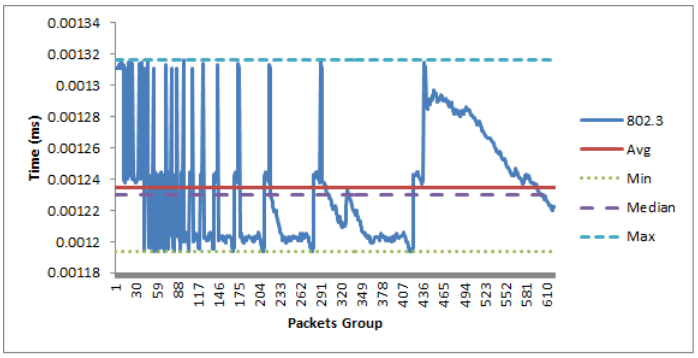
Table 4.50
*SYN/ACK-ACK of 802.11n vs 802.3 Group Percentage Increment and Decrement for Zone B*

| % changes | 802.11n | | 802.3 | |
|---|---|---|---|---|
| | No. of group | | No. of group | |
| | increase | decrease | increase | decrease |
| **0** | 1 | null | 34 | null |
| **0.01-5.00** | 120 (2.17) | 145 (-1.81) | 72 | 155 |
| **5.01-10.00** | 0 | 0 | 0 | 1 |
| **10.01-15.00** | 0 | 0 | 2 (12.13) | 2 (-11.90) |
| **Total** | **121** | **145** | **108** | **158** |

Last but not least is Zone C, in which the two graphs started at the above average. Both plotted a median below the average. Meanwhile, the minimum and maximum for 802.11n showed up in group 220 and group 283, respectively. On the other hand, 802.3 minimum and maximum were recorded by the respective groups 42 and 9. See Figure 4.24 for more precise details.




(a) 802.11n




(b) 802.3

*Figure 4.24.* 802.11n vs 802.3 SYN/ACK-ACK Zone C

As can be observed in Figure 4.51, Zone C had some differences with other zones, in which the time differences were spotted to be low between 802.3 to 802.11n. From the results, the average was 2.48, minimum 2.22, median 2.49, and maximum 2.63. As can be observed, there are still differences between wired and wireless networks. In real RAP detection, a mechanism is not going to differentiate between wireless g or n, since it will typify wired and wireless networks only. The next measurement showed 14 groups differing between both wired and wireless n, in terms of number of groups to the average line, with 802.11n having more numbers on and over the average, whereas 802.3 had more groups equal and below the average.

Table 4.51
*SYN/ACK-ACK of 802.11n vs 802.3 for Zone C*

| | minimum | average | median | maximum | Group > average | Group < average |
|---|---|---|---|---|---|---|
| **802.11n** | 0.002645 | 0.003066 | 0.003065 | 0.003461 | 311 | 312 |
| **802.3** | 0.001194 | 0.001235 | 0.001230 | 0.001316 | 297 | 326 |
| **Different** | **2.22** | **2.48** | **2.49** | **2.63** | **14** | **-14** |

At this moment, the percentage changes indicated 802.11n and 802.3 to have an abnormal result from previous situations, where 802.11n showed about 14.01% increment and -21.36% decrement, while 802.3 denoted an increment of 6.30% and decrement of -8.92%. Meanwhile 802.11n had more percentage changes for both increasing and decreasing. However, the majority of group numbers showed to be in the 0.01 and 5% range. In addition, no changes pointed that 802.3 had more groups (127) than the 71 for 802.11n

Table 4.52
*SYN/ACK-ACK of 802.11n vs 802.3 Group Percentage Increment and Decrement for Zone C*

| % changes | 802.11n | | 802.3 | |
|---|---|---|---|---|
| | No. of group | | No. of group | |
| | increase | decrease | increase | decrease |
| **0** | 71 | null | 127 | null |
| **0.01-5.00** | 134 | 393 | 162 | 291 |
| **5.01-10.00** | 12 | 2 | 21 (6.30) | 21 (-8.92) |
| **10.01-15.00** | 4 (14.01) | 2 | 0 | 0 |
| **15.01-20.00** | 0 | 3 | 0 | 0 |
| **20.01-25.00** | 0 | 1 (-21.36) | 0 | 0 |
| **Total** | **221** | **401** | **310** | **312** |

Thus, the TCP flags discussion is now complete, with the focus being on the group representation regarding their characteristics. Previously, the focus was on group mean deriving from the equal group technique that was embedded into the traffic analysis after being collected through packet capturing. Some TCP indicators, like PAYLOAD and PUSH, can accommodate a group of up to 1000. Other flags did not reach 1000 because they lacked the volume of packets. The

next section will highlight again all group zones to be used for acquiring the global threshold.

## 4.5 Number of Groups in a Minute

The implementation of equal group was to extract the group mean, zone mean, and finally the global mean or threshold. At the same time, it was also used to measure a time for each group accomplishment. For example, how much time is needed to form group 1000. Tables 4.53 and 4.54 show the number of packets in a minute produced by each flag for both 802.3 versus 802.11g, and 802.11n. SYN/ACK-ACK and FIN/ACK-ACK had the same amount in all zones. The highest number of packets was observed in PAYLOAD-ACK, and second goes to PSH/ACK-ACK, while the PAYLOAD for 802.11n had less numbers as compared to 802.11g.

Table 4.53
*802.3 vs. 802.11g Number of Groups in a Minute*

| | **ZONE A** | | **ZONE B** | | **ZONE C** | | **AVERAGE** | |
|---|---|---|---|---|---|---|---|---|
| | **802.3** | **802.11g** | **802.3** | **802.11g** | **802.3** | **802.11g** | **802.3** | **802.11g** |
| **PAYLOAD-ACK** | 796 | 805 | 937 | 920 | 813 | 748 | 848 | 824 |
| **SYN/ACK-ACK** | 7 | 8 | 7 | 8 | 6 | 7 | 6 | 7 |
| **PSH/ACK-ACK** | 33 | 34 | 37 | 40 | 38 | 32 | 36 | 35 |
| **FIN/ACK-ACK** | 6 | 7 | 6 | 6 | 5 | 6 | 5 | 6 |
| **TOTAL** | **841** | **852** | **987** | **973** | **861** | **792** | **896** | **872** |

Table 4.54
*802.3 vs. 802.11n Number of Groups in a Minute*

| | **ZONE A** | | **ZONE B** | | **ZONE C** | | **AVERAGE** | |
|---|---|---|---|---|---|---|---|---|
| | **802.3** | **802.11n** | **802.3** | **802.11n** | **802.3** | **802.11n** | **802.3** | **802.11n** |
| **PAYLOAD-ACK** | 803 | 587 | 1010 | 701 | 1025 | 631 | 946 | 639 |
| **SYN/ACK-ACK** | 6 | 7 | 4 | 3 | 4 | 3 | 5 | 4 |
| **PSH/ACK-ACK** | 28 | 26 | 24 | 24 | 43 | 31 | 32 | 27 |
| **FIN/ACK-ACK** | 5 | 6 | 3 | 3 | 3 | 3 | 4 | 4 |
| **TOTAL** | **842** | **625** | **1042** | **731** | **1075** | **668** | **986** | **675** |

Based on the two tables, a graph was generated to project the number of minutes each

group can be formed. Each graph has different plots and patterns due to the figures that were obtained from the previous table.

Figure 4.25 showed some variations of graphs in terms of minutes taken to generate a group (1 to 1000). However they had a common trait, which is the plot was observed to be linear. From the figure, it was concluded that it took less than two minutes to have a group 1000 for the PAYLOAD-ACK. The time consumption coming from FIN/ACK-ACK and SYN/ACK-ACK in attempting to achieve group 1000 was approximately between 250 and 300 minutes, whereas for PSH/ACK-ACK, it was less than 40 minutes to get the first group 1000. This will contribute toward the user selecting the most appropriate flag for fast detection of RAP, and otherwise. While taking all into consideration, PAYLOAD-ACK was proposed as the flag or indicator for detecting RAP. However, other flags will become value added and it was not encouraged to go for setting them up in the higher groups. This information were then used for selecting specific groups within a minute for verification purposes.

## 4.6 Zone Mean and Global Mean (Threshold)

The main purpose for this section is to propose a global threshold value for detecting RAP. Tables 4.55 and 4.56 give some variations between zones in the same class, for example 802.11g where the majority of means started two digits after the floating point (Zones A and B), whereas 802.3 started at digit three after the floating point. In addition, 802.11g and 802.11n at Zone C started similarly to 802.3. However, this is not the same as 802.3 values, and there is still a gap, as was clarified in the previous discussion. Consequently, the tables also show 802.3 to be more stable than 802.11, and because of this, the zone mean was proposed to overcome this situation.

As can be observed from the above table, a zone for each flag was produced from

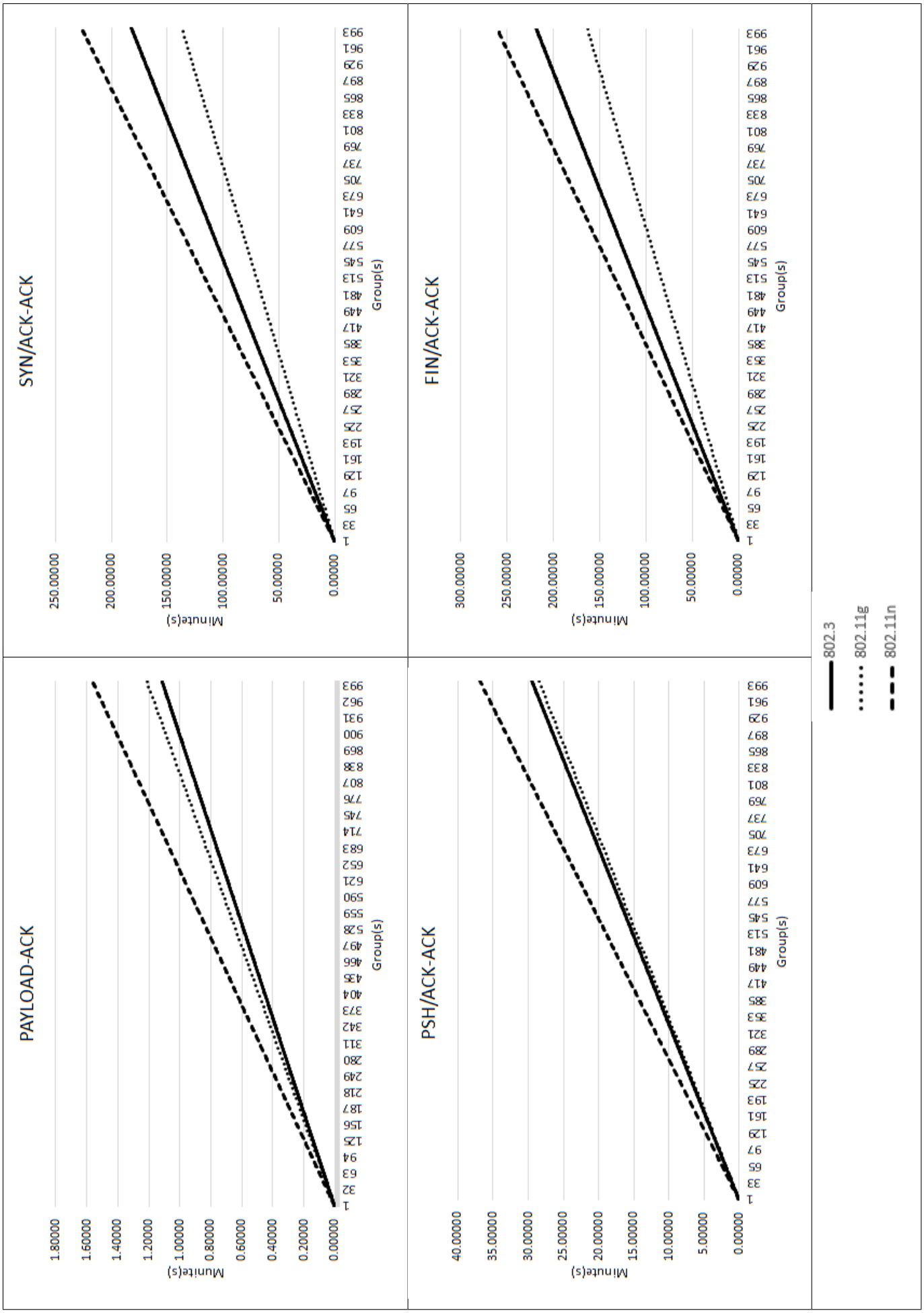



*Figure 4.25.* Groups and Minutes

Table 4.55
*82.11g vs. 802.3: Zone Mean and Global Threshold*

| | FIN/ACK-ACK | | PAYLOAD-ACK | | PSH/ACK-ACK | | SYN/ACK-ACK | | GLOBAL MEAN | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **802.11g** | **802.3** | **802.11g** | **802.3** | **802.11g** | **802.3** | **802.11g** | **802.3** | **802.11g** | **802.3** |
| **ZONE A** | 0.014626 | 0.002189 | 0.008308 | 0.003678 | 0.013892 | 0.004051 | 0.018378 | 0.001515 | | |
| **ZONE B** | 0.008548 | 0.002364 | 0.008632 | 0.003583 | 0.009723 | 0.003744 | 0.007837 | 0.001817 | | |
| **ZONE C** | 0.010915 | 0.001351 | 0.007881 | 0.003205 | 0.008664 | 0.002880 | 0.008301 | 0.002017 | | |
| **ZONE MEAN** | **0.011363** | **0.001968** | **0.008274** | **0.003489** | **0.010760** | **0.003558** | **0.011505** | **0.001783** | | |
| | | | | | | | | | **0.010475** | **0.002700** |

the zone's mean. The actual zone mean was inherited from the group mean. On the rightmost of the table, there are two indicators showing as 0.010475 and 0.002700, respectively representing the global mean for 802.11g and 802.3. By comparing both values, it shows that 802.3 is 3.88 times less than 802.11g.

Meanwhile, 802.11n compared to 802.11g had zone means showing that there is a gap, even though both were wireless networks. From the global mean, 802.11g was 0.32 times less than 802.11n. As a result, 802.11n can easily be detected as wireless if it is compared to wired. However the wireless g is not going to overtake 802.3 in terms of time differences. From the above table, 802.11n and 802.3 themselves were recorded at 0.033085 and 0.02104, respectively, while it is 15.73 times between 802.3 and 803.11n.

One of the contributions of this research was to propose a global threshold for the traffic characterisation mechanism that can detect RAP easily. The result showed 802.3 to be more stable and have less delay compared to the 802.11 network. The global threshold was nominated by 802.3 where it was derived from the first digit after 0, beginning from the leftmost, with the result 0.002 from both 802.3 (Table 4.55 and 4.56). Instead of bringing out the 802.3 as the indicator for detecting RAP, the 802.11 global mean also can be used as a wireless indicator for rectifying wireless packets.

## 4.7 Summary

The main objective of this chapter was to find an indicator from the 802.3 structure and then use it for clarification against wireless structures. This indicator was extracted from the process of equal grouping and averaging, which aimed at producing a zone mean to be averaged again for obtaining all zone means to eventually produce the global mean. This is a threshold value that is important in the verification stage to

Table 4.56
*82.11n vs. 802.3: Zone Mean and Global Threshold*

| | FIN/ACK-ACK | | PAYLOAD-ACK | | PSH/ACK-ACK | | SYN/ACK-ACK | | GLOBAL MEAN | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **802.11n** | **802.3** | **802.11n** | **802.3** | **802.11n** | **802.3** | **802.11n** | **802.3** | **802.11n** | **802.3** |
| **ZONE A** | 0.057740 | 0.001515 | 0.029374 | 0.003617 | 0.043567 | 0.003701 | 0.060463 | 0.001337 | | |
| **ZONE B** | 0.053234 | 0.001407 | 0.030636 | 0.001931 | 0.044298 | 0.002251 | 0.061422 | 0.001148 | | |
| **ZONE C** | 0.004360 | 0.001310 | 0.004436 | 0.002903 | 0.004425 | 0.002891 | 0.003066 | 0.001235 | | |
| **ZONE MEAN** | **0.038445** | **0.001411** | **0.021482** | **0.002817** | **0.030763** | **0.002948** | **0.041650** | **0.001240** | | |
| | | | | | | | | | **0.033085** | **0.002104** |

clarify, verify, and confirm a proposed traffic characterisation mechanism that can successfully meet the ultimate objective of finding and detecting RAPs in LANs.

# CHAPTER FIVE
# VERIFICATION OF RAP DETECTION MECHANISM

## 5.1 Introduction

This chapter is the most important part in this dissertation which attempts to verify whether the traffic characterisation mechanism is actually capable of detecting RAPs within LANs. As mentioned before, a specific group at each flag was used, based on average values showed in Table 4.53 and 4.54 to verify differences between wireless and wired networks. A second packet capturing process was done for this purpose and an average of zones was backed up by selected groups, all of which were already discussed in Section 1.6 that follows the verification algorithm. Then RAPs can be discovered and thus this characterisation can be verified to be working. Like training, this verification process was also classified into 802.11g and 802.11n. However, 802.3 represents the global mean or threshold value that was discovered during the training phase. The direct differences was used to find a percentage difference between 802.11 g or n to the 802.3 threshold.

Each graph shows a wireless time stamp difference in the chosen group within the five minute range starting from a minute up to an hour, while the associated table shows a list of time stamp difference means within five minutes up to an hour. At the same time, an average of time stamped differences, min, max, and median were also highlighted. Finally, there is a percentage field showing percentage differences between wireless and wired thresholds. The next sections 5.2 and 5.3 will deeply elaborate on the outcome of this research.

At the end of the chapter, this report shall highlight either RAP can be discovered or it can be argued by using equal 50-50 percentage, where if it is 50% and above, then it

is labelled as RAP, or if it is less than 50%, it is assumed as a Potential RAP. However, if it is 0% and less, it will be classed as non-RAP.

## 5.2 Verification of 802.11g

The wireless g verification stage were classified into the respective TCP flags, as stated in the learning phase. Each indicator was sub-divided into Zones A, B, and C and discussed separately. These zones are described using a graph comprising a five minute range up to an hour between wireless times stamped differences and wired threshold. Additionally, a table will show the significant wireless time stamped differences, 802.3 threshold, and other suitable figures, such as the average of 802.11 time stamped differences, min, max, and median. These figures can also be used to strengthen the outcome, instead of just the mean and threshold. On the rightmost of the tables, there are percentages showing the percentage difference between wireless and wired thresholds. These shall become the indicators to prove that the proposed traffic characterisation mechanism is verified and proven for detecting RAPs in LANs.

i. SYN/ACK-ACK

   In TCP/IP, the first flag to be sent for establishing a connection is SYN from the client to server. The server responds by sending SYN/ACK back to the client. Then, the client again sends back the ACK and thus completing the connection. Within this three way handshake, this research invokes a time stamp at SYN/ACK and ACK in order to find time differences. Hopefully, RAP discovery can be easily performed and thus verified as illegal AP. This SYN/ACK-ACK used group 7 as the selective group within a minute for verification purposes.

   First and foremost, Figure 5.1 shows two indicators between the 802.11g and 802.3 thresholds where Group 7 was the group selective of 802.11g. From the

figure, there are no points pointing below the threshold and based on Table 5.1, a minimum was logged at five minutes, which is 49.11% different, while the maximum was focused on 30 minutes with 74.95%.

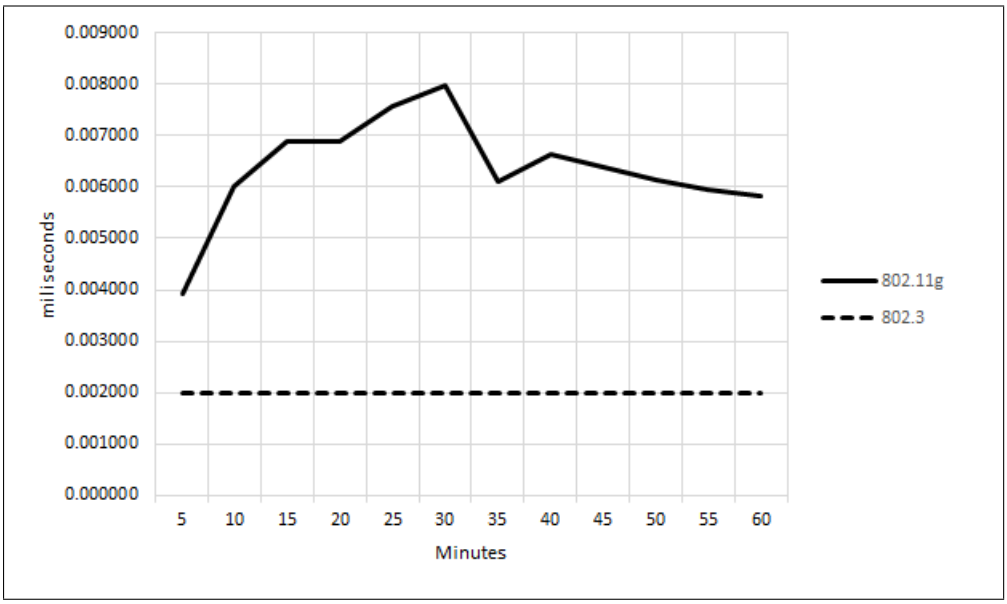



*Figure 5.1.* 802.11g vs Threshold: SYN/ACK-ACK Zone A

This flag also showed an average at 0.006355 ms, minimum of 0.003930 ms, maximum of 0.007985 ms, and median of 0.006251 ms. As compare to threshold (0.002000), all the mentioned values were over of the line.

Table 5.1
*802.11g vs Threshold: SYN/ACK-ACK Zone A*

| **Minutes** | **802.11g** | **% Differ** |
|---|---|---|
| 5 | 0.003930 | 49.11% |
| 10 | 0.006006 | 66.70% |
| 15 | 0.006877 | 70.92% |
| 20 | 0.006877 | 70.92% |
| 25 | 0.007575 | 73.60% |
| 30 | 0.007985 | 74.95% |
| 35 | 0.006119 | 67.32% |
| 40 | 0.006629 | 69.83% |
| 45 | 0.006377 | 68.64% |
| 50 | 0.006125 | 67.35% |
| 55 | 0.005938 | 66.32% |
| 60 | 0.005821 | 65.64% |

Zone B has a reversed shape of Zone A above, however, there are no crossing

over the threshold line, as shown in Figure 5.2. A minimum was identified at 30 minutes and maximum was focused in 5 minutes. In terms of percentage differences, each minimum and maximum had values of 38.29% and 71.8%, respectively (see Figure 5.2).

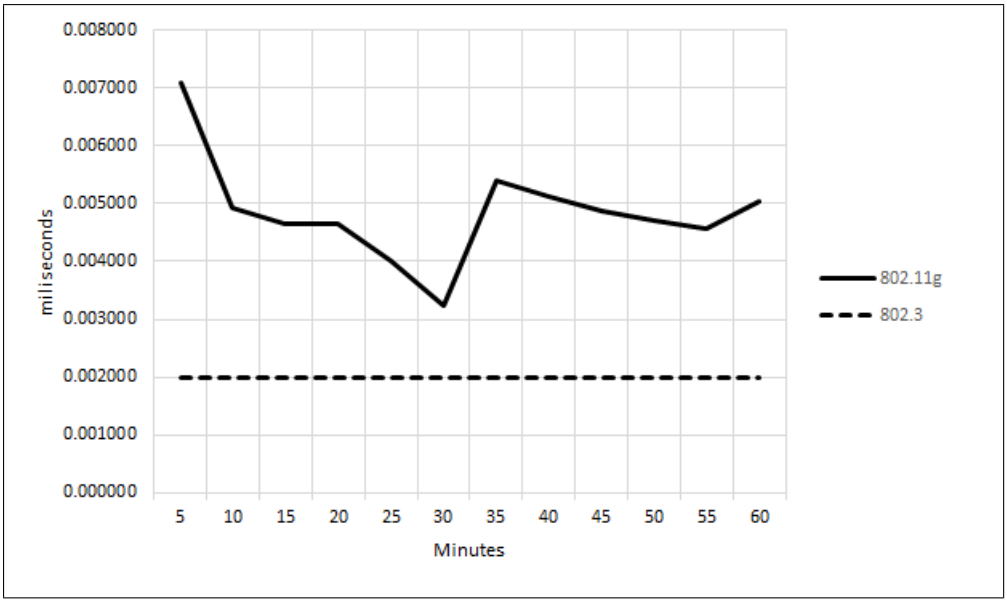



*Figure 5.2.* 802.11g vs Threshold: SYN/ACK-ACK Zone B

The threshold was below the line as compared to the average, which was stated at 0.004859 ms, minimum at 0.003241 ms, maximum at 0.007091 ms, and median at 0.004793 ms.

Table 5.2
*802.11g vs Threshold: SYN/ACK-ACK Zone B*

| **Minutes** | **802.11g** | **% Differ** |
|---|---|---|
| 5 | 0.007091 | 71.80% |
| 10 | 0.004940 | 59.52% |
| 15 | 0.004643 | 56.92% |
| 20 | 0.004643 | 56.92% |
| 25 | 0.004017 | 50.22% |
| 30 | 0.003241 | 38.29% |
| 35 | 0.005387 | 62.87% |
| 40 | 0.005129 | 61.01% |
| 45 | 0.004880 | 59.02% |
| 50 | 0.004705 | 57.49% |
| 55 | 0.004580 | 56.33% |
| 60 | 0.005053 | 60.42% |

The last SYN/ACK-ACK trend also did not differ from the previous two zones. The graph shows a threshold to be at the bottom and lower than 802.11g lines (see Figure 5.3). A minimum was logged at between 15 and 20 minutes with 56.08% differences, and maximum showed at minute 35 with 68.68% differences between wireless g and 802.3 threshold.

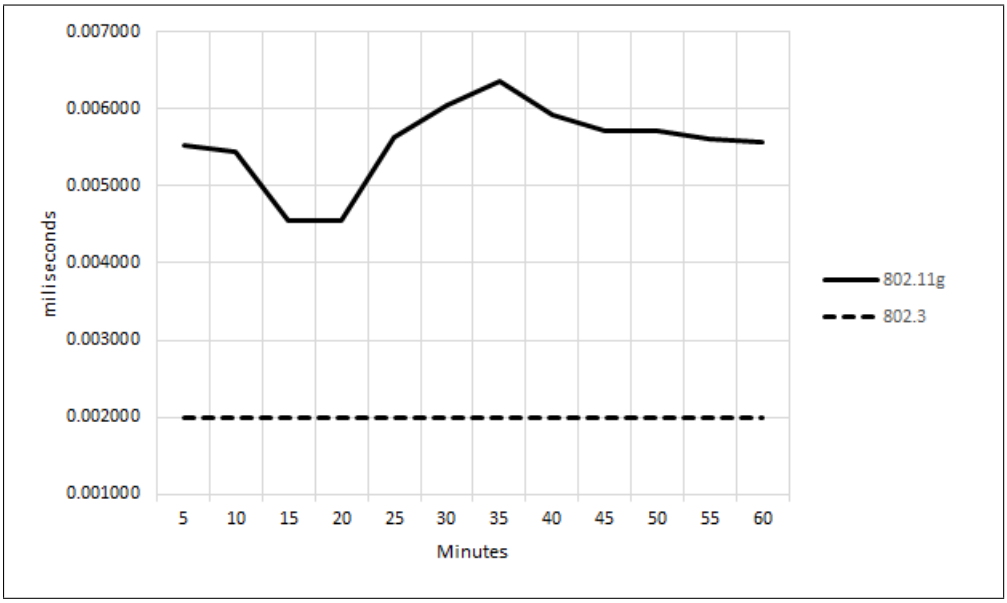



*Figure 5.3.* 802.11g vs Threshold: SYN/ACK-ACK Zone C

At this point, the average (0.005555 ms), minimum (0.004554 ms), maximum (0.006360 ms), and median (0.005619 ms) were still over the threshold value.

Table 5.3
*802.11g vs Threshold: SYN/ACK-ACK Zone C*

| Minutes | 802.11g | % Differ |
|---|---|---|
| 5 | 0.005528 | 63.82% |
| 10 | 0.005450 | 63.31% |
| 15 | 0.004554 | 56.08% |
| 20 | 0.004554 | 56.08% |
| 25 | 0.005622 | 64.43% |
| 30 | 0.006057 | 66.98% |
| 35 | 0.006360 | 68.55% |
| 40 | 0.005923 | 66.23% |
| 45 | 0.005722 | 65.05% |
| 50 | 0.005709 | 64.97% |
| 55 | 0.005615 | 64.38% |
| 60 | 0.005570 | 64.09% |

There were not much differences between all the zones. The majority of a values were more than 50% different between 802.11g in this TCP flag, and this strongly suspects that there is a wireless network existing within the wired structure, and it is RAP. However, this not yet confirmed nor proven until all the flags have been discussed, which are in the proceeding sections.

ii. FIN/ACK-ACK

In a normal situation, each network connection must be closed through FIN. Similar to SYN, FIN also occurs in three phases, namely FIN, FIN/ACK, and ACK. In this verification stage, FIN/ACK-ACK was twice time stamped and differentiated to find RAPs, and shall be discussed in three different Zones, namely A, B, and C. The zones are supported by a graph and table with their respective values to scan for the existence of RAPs. The overall selective group used was group 6.

Figure 5.4 and Table 5.4 show the verification of FIN/ACK-ACK Zone A between 802.11g and 802.3 threshold, which was 0.002 milliseconds.

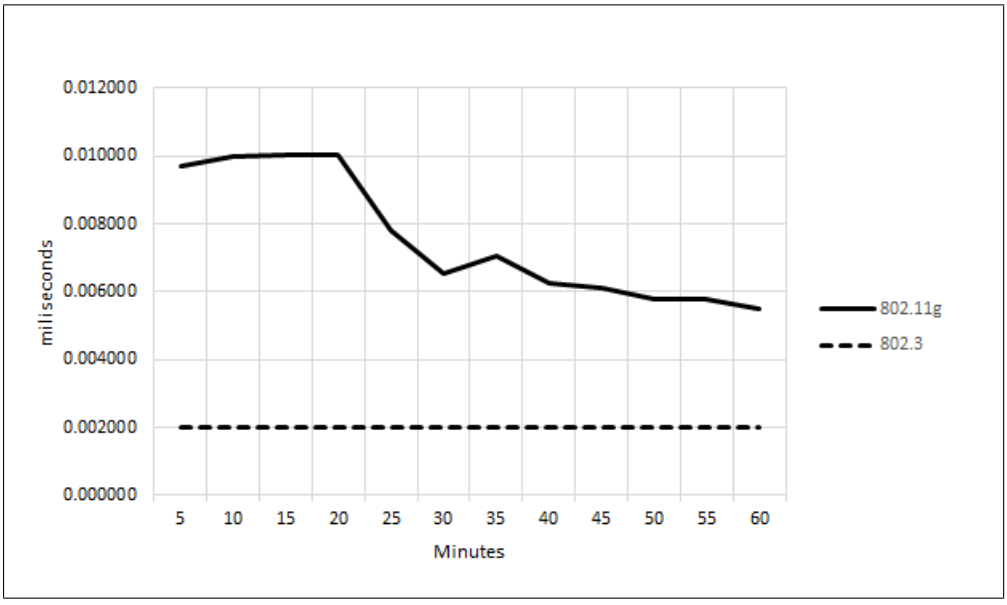



*Figure 5.4.* 802.11g vs Threshold: FIN/ACK-ACK Zone A

A minimum value was reported to be at 60 minutes or an hour, whereas the maximum was at 15 and 20 minutes. Both minimum and maximum percentage

differences were 63.65% and 79.38%, respectively. No values were recorded below 50%. In the comparison of average, minimum, maximum, and median to the threshold value, it was observed that the threshold was below the stated measures. At this point, the average was at 0.007546 ms, minimum at 0.005502 ms, maximum was 0.010046 ms, and median logged at 0.006794 ms.

Table 5.4
*802.11g vs Threshold: FIN/ACK-ACK Zone A*

| **Minutes** | **802.11g** | **% Differ** |
|---|---|---|
| 5 | 0.009700 | 79.38% |
| 10 | 0.009972 | 79.94% |
| 15 | 0.010046 | 80.09% |
| 20 | 0.010046 | 80.09% |
| 25 | 0.007791 | 74.33% |
| 30 | 0.006541 | 69.42% |
| 35 | 0.007048 | 71.62% |
| 40 | 0.006270 | 68.10% |
| 45 | 0.006095 | 67.18% |
| 50 | 0.005785 | 65.43% |
| 55 | 0.005761 | 65.28% |
| 60 | 0.005502 | 63.65% |

Zone B, as shown in Figure 5.5 and Table 5.5, exhibits some increment in terms of percentage, where the minimum was at 25 minutes with 72.31%, while maximum was at 5 minutes with 90.39% differences between 802.11g and 802.3 thresholds. All values were over 50% similar to Zone A, however it was more than 70% and up to 90%.

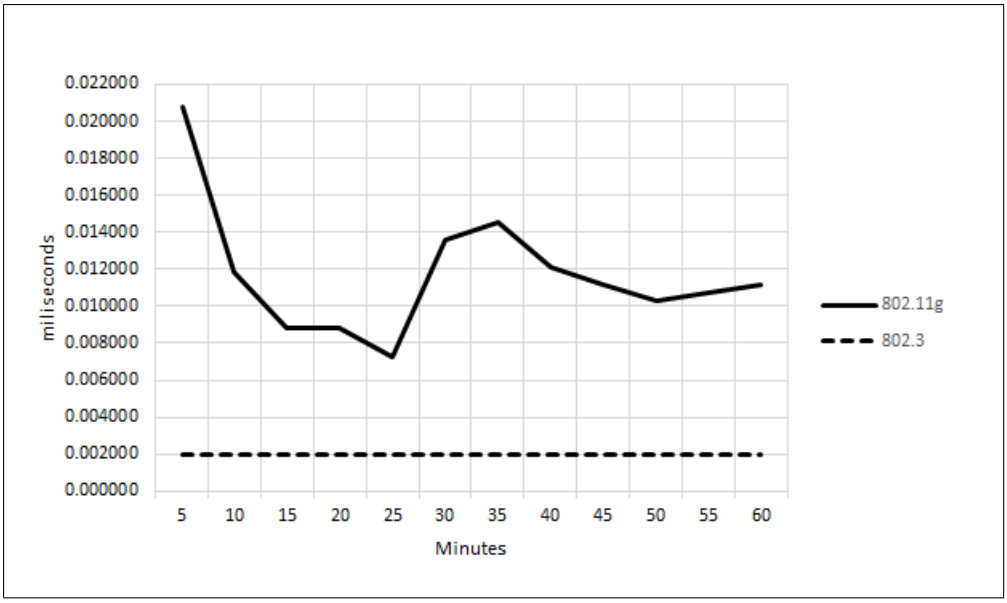



*Figure 5.5.* 802.11g vs Threshold: FIN/ACK-ACK Zone B

This Zone B produced similar results where the threshold was below the average (0.011766 ms), minimum (0.007222 ms), maximum (0.020819 ms), and median (0.011151 ms).

Table 5.5
*802.11g vs Threshold: FIN/ACK-ACK Zone B*

| **Minutes** | **802.11g** | **% Differ** |
|---|---|---|
| 5 | 0.020819 | 90.39% |
| 10 | 0.011827 | 83.09% |
| 15 | 0.008842 | 77.38% |
| 20 | 0.008842 | 77.38% |
| 25 | 0.007222 | 72.31% |
| 30 | 0.013603 | 85.30% |
| 35 | 0.014584 | 86.29% |
| 40 | 0.012147 | 83.53% |
| 45 | 0.011119 | 82.01% |
| 50 | 0.010277 | 80.54% |
| 55 | 0.010733 | 81.37% |
| 60 | 0.011182 | 82.11% |

Meanwhile, Zone C showed a slightly different pattern compared to Zones A and B, and also had extreme differences between wireless and wired networks. As shown in Figure 5.6 and Table 5.6, the minimum point was discovered at 5

minutes with 77.39%, whereas the maximum was logged nearly at 100%, which was 99.88%, at two points, namely 15 and 20 minutes.

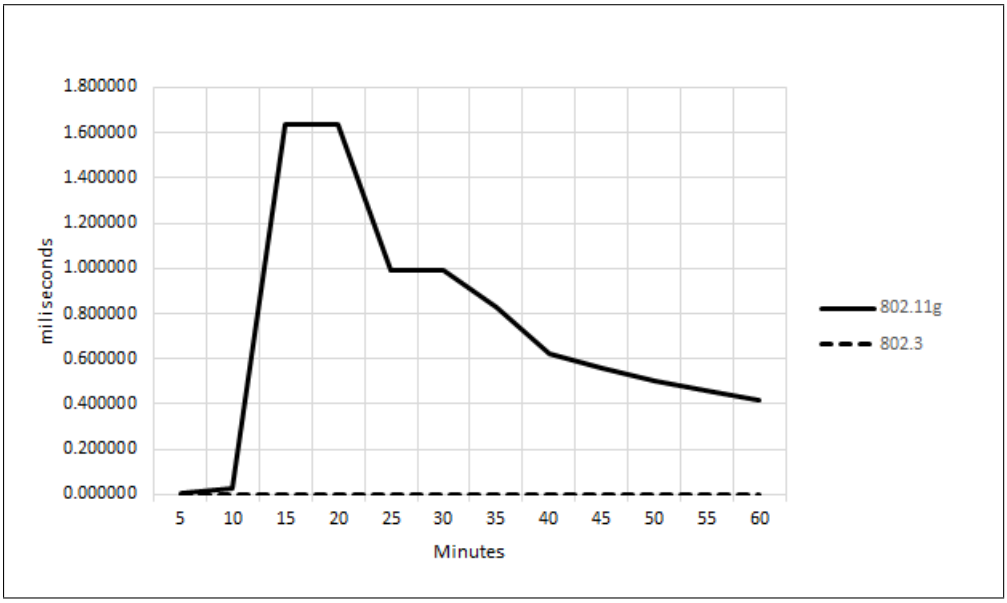



*Figure 5.6.* 802.11g vs Threshold: FIN/ACK-ACK Zone C

The majority of Zone C had more than 90% and this was considered very extreme when compared to both Zones A and B. Furthermore, the differences between threshold was maintained below average (0.722784 ms), minimum (0.008844 ms), maximum (1.634267 ms), and median (0.589947 ms). Even though at 5 and 10 minutes, it was shown that they are nearly redundant (see 5.6), this probably occured due to each measurement having extreme value differences between the maximum and minimum.

Table 5.6
*802.11g vs Threshold: FIN/ACK-ACK Zone C*

| **Minutes** | **802.11g** | **% Differ** |
|---|---|---|
| 5 | 0.008844 | 77.39% |
| 10 | 0.026025 | 92.32% |
| 15 | 1.634267 | 99.88% |
| 20 | 1.634267 | 99.88% |
| 25 | 0.991002 | 99.80% |
| 30 | 0.992070 | 99.80% |
| 35 | 0.828195 | 99.76% |
| 40 | 0.623819 | 99.68% |
| 45 | 0.556075 | 99.64% |
| 50 | 0.501491 | 99.60% |
| 55 | 0.457260 | 99.56% |
| 60 | 0.420094 | 99.52% |

As can be clearly observed, Zone C totally shows that there is the existence of RAPs in the LAN. In addition Zone A and B also showed indicators of the availability of RAPs, but not as strong as Zone C.

iii. PSH/ACK-ACK

In data communication, to let the provider or server send data to the client, the PUSH or PSH flag is used. As mentioned previously and similarly to the previous two flags SYN and FIN, the operation involving this PSH flag also occurs in three distinct phases, namely the generation of PSH, PSH/ACK, and ACK flags. In this verification step, the identified selective group was group 35. As shown in Figure 5.7, the Zone A plot shows some increment from a lower to a higher state. The minimum was shown at 5 minutes, whereas maximum was logged at 30 minutes.

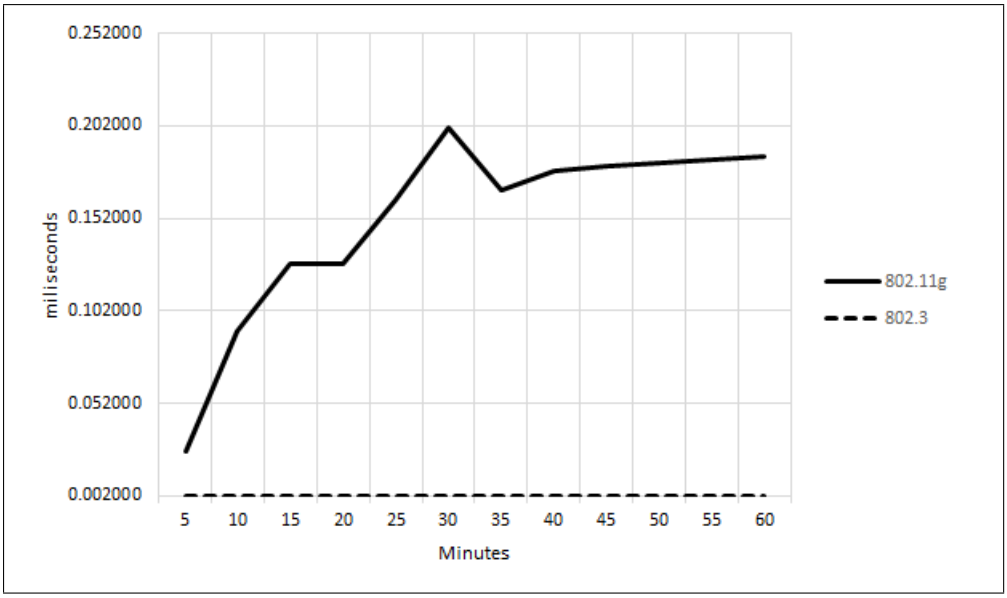



*Figure 5.7.* 802.11g vs Threshold: PSH/ACK-ACK Zone A

Table 5.7 highlights these two values, where the minimum and maximum were both at 92.23% and 99.01%, respectively. All the numbers were above 90%, thus strongly suggesting the existence of RAPs in the network. Comparing to the threshold value, the average (0.150892 ms), minimum (0.025729 ms), maximum (0.201452 ms), and median (0.172345) were observed to have exceeded that value.

Table 5.7
*802.11g vs Threshold: PSH/ACK-ACK Zone A*

| **Minutes** | **802.11g** | **% Differ** |
|---|---|---|
| 5 | 0.025729 | 92.23% |
| 10 | 0.090619 | 97.79% |
| 15 | 0.127504 | 98.43% |
| 20 | 0.127504 | 98.43% |
| 25 | 0.162378 | 98.77% |
| 30 | 0.201452 | 99.01% |
| 35 | 0.167201 | 98.80% |
| 40 | 0.177490 | 98.87% |
| 45 | 0.180061 | 98.89% |
| 50 | 0.181871 | 98.90% |
| 55 | 0.183593 | 98.91% |
| 60 | 0.185299 | 98.92% |

Next, Zone B showed a similar pattern to Zone A, where the first five minutes

became the minimum point, while a maximum was reported at 30 minutes (see Figure 5.8).

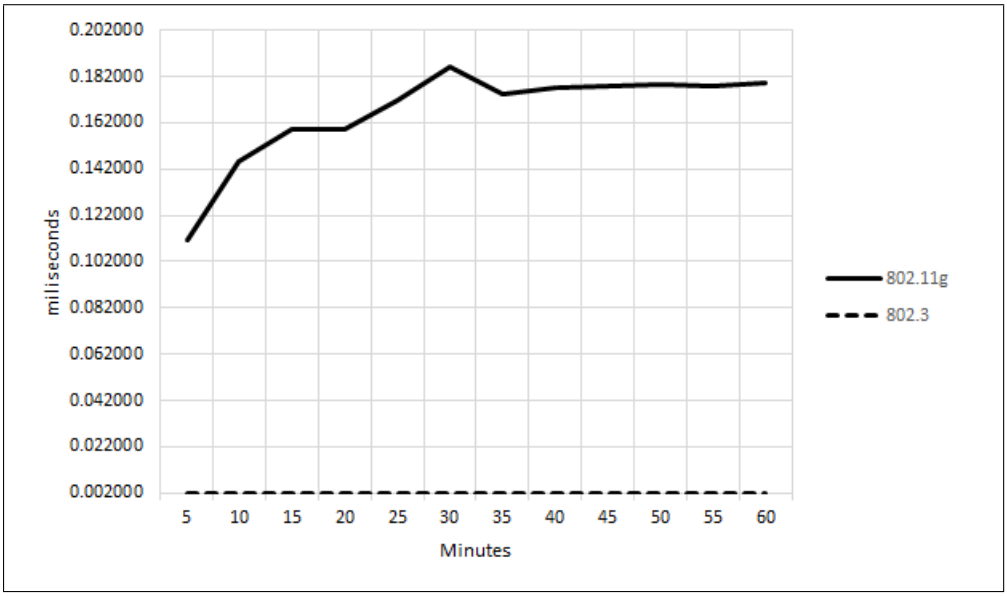



*Figure 5.8.* 802.11g vs Threshold: PSH/ACK-ACK Zone B

In terms of percentage difference, the minimum was about 98.20% and maximum was about 98.93%. The majority of the differences between 802.11g and the threshold value were over 98%. Also, the values for average (0.166493 ms), minimum (0.111374 ms), maximum (0.186475 ms), and median (0.175748 ms) were over the threshold line (0.002000 ms).

Table 5.8
*802.11g vs Threshold: PSH/ACK-ACK Zone B*

| **Minutes** | **802.11g** | **% Differ** |
|---|---|---|
| 5 | 0.111374 | 98.20% |
| 10 | 0.145208 | 98.62% |
| 15 | 0.159223 | 98.74% |
| 20 | 0.159223 | 98.74% |
| 25 | 0.171395 | 98.83% |
| 30 | 0.186475 | 98.93% |
| 35 | 0.174372 | 98.85% |
| 40 | 0.177125 | 98.87% |
| 45 | 0.177941 | 98.88% |
| 50 | 0.178598 | 98.88% |
| 55 | 0.177903 | 98.88% |
| 60 | 0.179073 | 98.88% |

The following Zone C had a different pattern from both Zones A and B. Its minimum was plotted at 30 minutes, while maximum was pinned at 5 minutes.

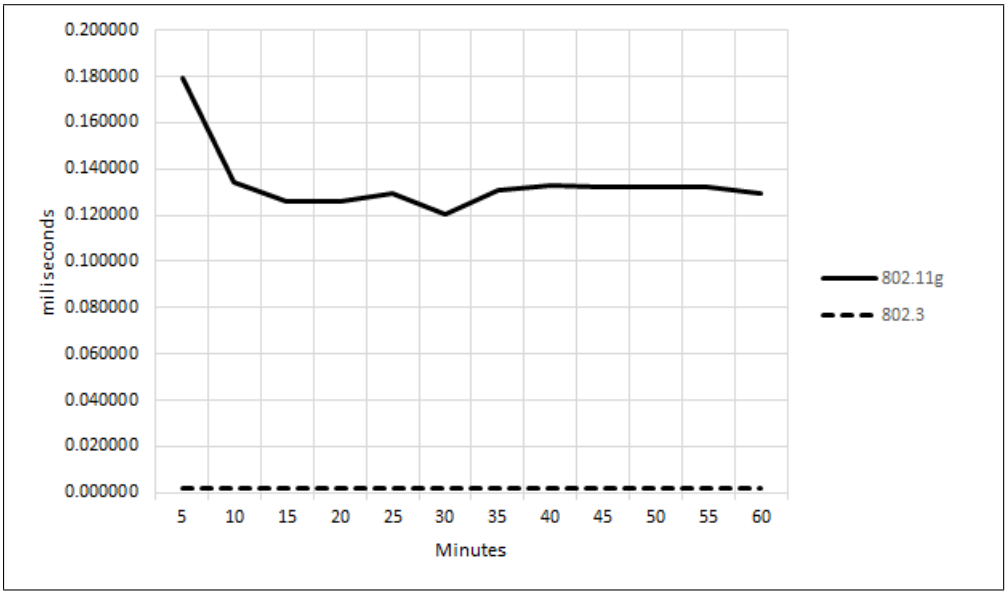



*Figure 5.9.* 802.11g vs Threshold: PSH/ACK-ACK Zone C

However, Zone C has some similarity with Zone B, where the majority of differences were above 98%. The minimum value was 98.33% and maximum value was 98.88%. As a result, it is indicative of the presence of an existing RAP in the tested LAN. In addition, a vis-a-vis comparison between 802.11g and 802.3 thresholds can be seen as over the line of 0.002000 ms, compared to the average of 0.133706 ms, minimum of 0.120106 ms, maximum of 0.179335 ms, and median of 0.131251 ms.

Table 5.9
*802.11g vs Threshold: PSH/ACK-ACK Zone C*

| **Minutes** | **802.11g** | **% Differ** |
|---|---|---|
| 5 | 0.179335 | 98.88% |
| 10 | 0.134372 | 98.51% |
| 15 | 0.125743 | 98.41% |
| 20 | 0.125743 | 98.41% |
| 25 | 0.129318 | 98.45% |
| 30 | 0.120106 | 98.33% |
| 35 | 0.130500 | 98.47% |
| 40 | 0.132827 | 98.49% |
| 45 | 0.132489 | 98.49% |
| 50 | 0.132414 | 98.49% |
| 55 | 0.132002 | 98.48% |
| 60 | 0.129627 | 98.46% |

In this PSH/ACK-ACK verification stage, all Zones identified the existence of RAP, where both Zones B and C showed above 98% differences, while Zone A above 90%. However, the majority of differences of Zone A were above 98% also.

iv. PAYLOAD-ACK

Meanwhile, the PAYLOAD-ACK involves the largest number of packets as compared to the other three flags. As a result, the group selected for this verification process was also large, namely group 824. This flag is useful in downloading data from the server to client host. It is not like the other flags, after PSH/ACK, the ACK occurs, and only then PAYLOAD is sent from provider to receiver. After the client received, then it send another ACK.

Between 802.11g and 802.3 thresholds, the differences showed to be between 75.84% and 77.33%. There were very small differences between minimum and maximum values. Figure 5.10 and Table 5.10 exhibits those values being discussed for Zone A.

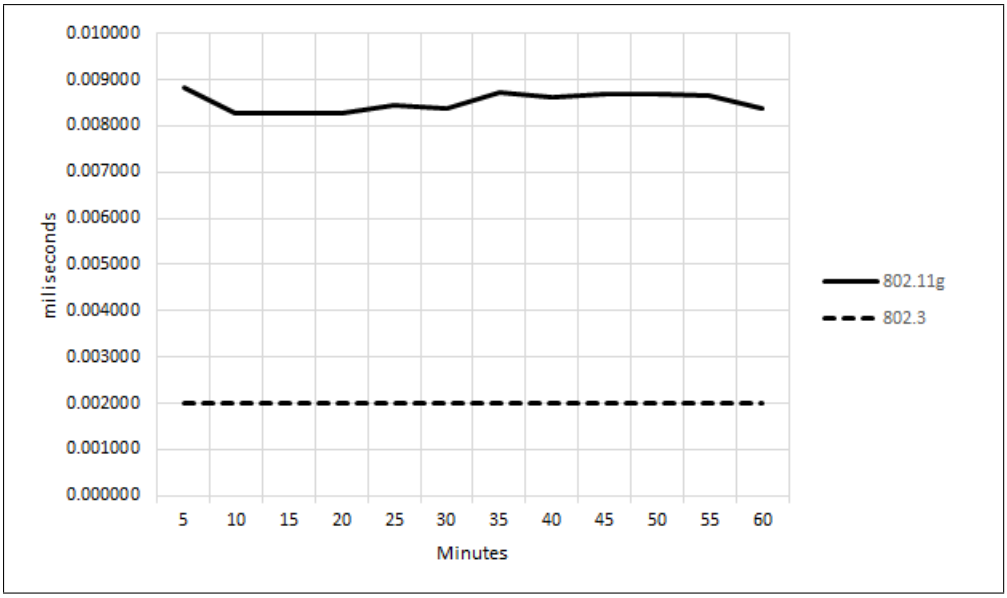



*Figure 5.10.* 802.11g vs Threshold: PAYLOAD-ACK Zone A

The smallest projected value was at 10 minutes, while maximum at 5 minutes. This shows that the two indicators appeared at the very beginning of the process. However overall, RAP can be found to exist in the LAN, as proven by the differences in wireless g and wired thresholds. Meanwhile, as mentioned above, the threshold was below compared to other measurements of average (0.008522 ms), minimum (0.008278 ms), maximum (0.008823 ms), and medium (0.008531 ms).

Table 5.10
*802.11g vs Threshold: PAYLOAD-ACK Zone A*

| **Minutes** | **802.11g** | **% Differ** |
|---|---|---|
| 5 | 0.008823 | 77.33% |
| 10 | 0.008278 | 75.84% |
| 15 | 0.008280 | 75.85% |
| 20 | 0.008280 | 75.85% |
| 25 | 0.008446 | 76.32% |
| 30 | 0.008392 | 76.17% |
| 35 | 0.008733 | 77.10% |
| 40 | 0.008617 | 76.79% |
| 45 | 0.008679 | 76.96% |
| 50 | 0.008677 | 76.95% |
| 55 | 0.008669 | 76.93% |
| 60 | 0.008388 | 76.16% |

Next Zone B is equally similar to Zone A, where the values were in between 0.008 and 0.009 milliseconds. Figure 5.11 highlighted this similarity and Table 5.11 shows a series of numbers showing the differences between 802.11g and 802.3 thresholds.

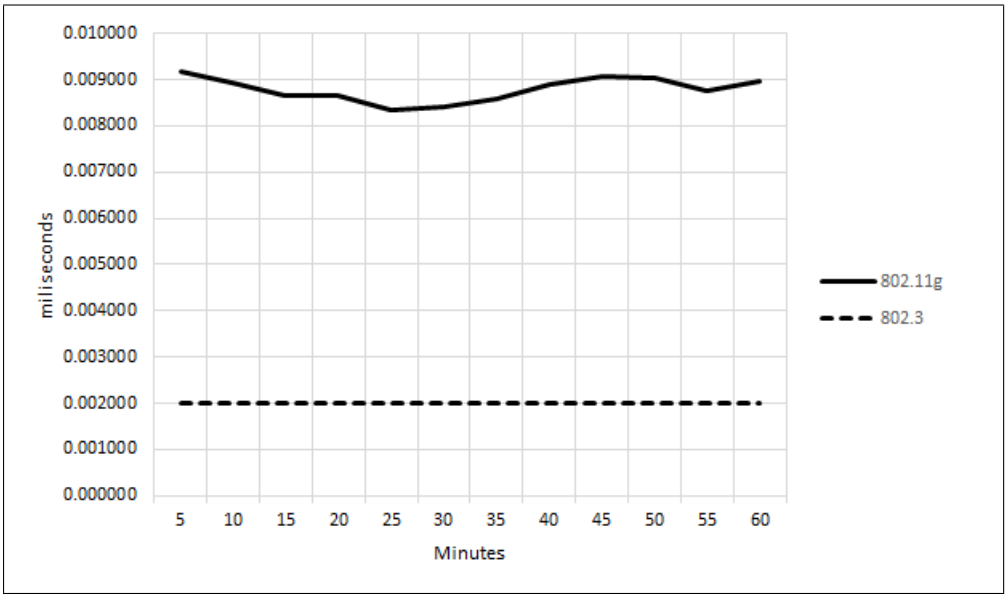



*Figure 5.11.* 802.11g vs Threshold: PAYLOAD-ACK Zone B

The minimum was pinned at 5 minutes with 74.44%, whereas maximum was pointed out at 15 and 20 minutes with 79.80%. Even though Zone B was 2% higher than the Zone A maximum values, it is still considered to be equally verified, when comparing to average (0.009074 ms), minimum (0.007825 ms), maximum (0.009902 ms), and median (0.009073 ms) to the threshold, which is still showing to be over the line.

Table 5.11
*PAYLOAD-ACK Zone B*

| Minutes | 802.11g | % Differ |
|---|---|---|
| 5 | 0.007825 | 74.44% |
| 10 | 0.008254 | 75.77% |
| 15 | 0.009902 | 79.80% |
| 20 | 0.009902 | 79.80% |
| 25 | 0.009571 | 79.10% |
| 30 | 0.009701 | 79.38% |
| 35 | 0.009457 | 78.85% |
| 40 | 0.009280 | 78.45% |
| 45 | 0.008866 | 77.44% |
| 50 | 0.008850 | 77.40% |
| 55 | 0.008703 | 77.02% |
| 60 | 0.008576 | 76.68% |

Like Zone B, Zone C had similar range differences between 802.11g and 802.3. Table 5.12 gives more detail in differentiating 802.11g and 802.3 thresholds, especially minimum and maximum values, and also others like mean and median.

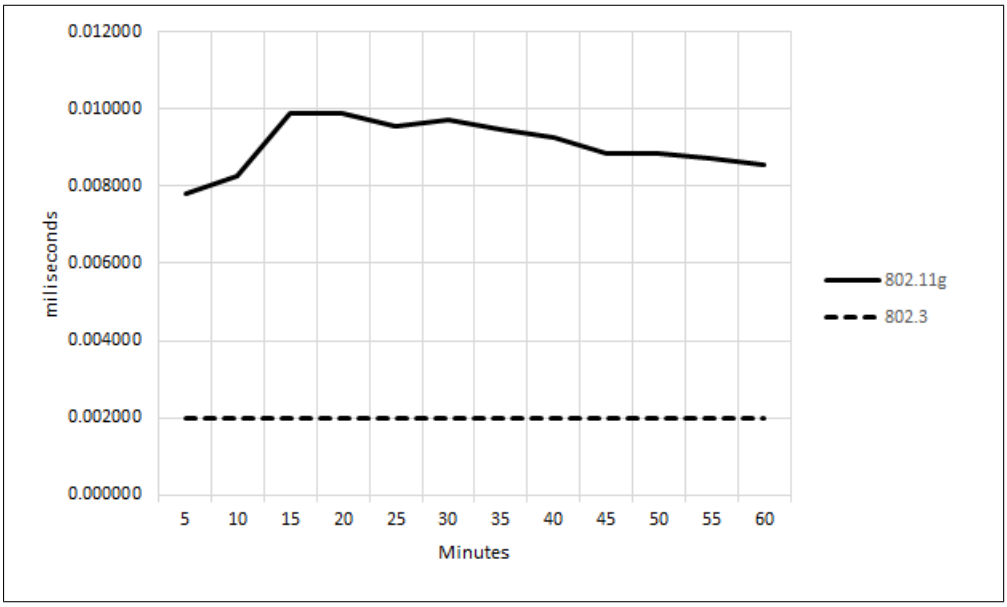



*Figure 5.12.* 802.11g vs Threshold: PAYLOAD/ACK-ACK Zone C

The minimum values recorded was as early as 5 minutes with 74.44%, while maximum was noticed at 15 and 20 minutes with 79.80%. In terms of time,

the threshold was less time taken than the average (0.009074 ms), minimum (0.007825 ms), maximum (0.009902 ms), and median (0.009073 ms).

Table 5.12
*802.11g vs Threshold: PAYLOAD/ACK-ACK Zone C*

| Minutes | 802.11g | % Differ |
|---|---|---|
| 5 | 0.007825 | 74.44% |
| 10 | 0.008254 | 75.77% |
| 15 | 0.009902 | 79.80% |
| 20 | 0.009902 | 79.80% |
| 25 | 0.009571 | 79.10% |
| 30 | 0.009701 | 79.38% |
| 35 | 0.009457 | 78.85% |
| 40 | 0.009280 | 78.45% |
| 45 | 0.008866 | 77.44% |
| 50 | 0.008850 | 77.40% |
| 55 | 0.008703 | 77.02% |
| 60 | 0.008576 | 76.68% |

All zones had a similar pattern of traffic characterisation, where each showed to be as low as 74% and as high as 79% for differences between 802.11g and 802.3 thresholds. The PAYLOAD-ACK was verified to detect RAP in LAN for all zones.

## 5.3 Verification of 802.11n

This section and the following shall discuss the outcome of 802.11n in the verification stage. Like 802.11g, the discussion is divided according to four flags, which were SYN/ACK-ACK, FIN/ACK-ACK, PSH/ACK-ACK, and PAYLOAD-ACK in three Zones A, B, and C. For each zone, there are graphs and tables that support the related discussion.

i. SYN/ACK-ACK

Naturally, SYN will act as an opening to any connection in the TCP/IP three-way handshake. As a starter, SYN needs to complete the three cycles that start with

SYN, then SYN/ACK, and ACK. As was stated previously, two points were time stamped to calculate differences between SYN/ACK and ACK. In this verification process the selective group was group 4.

For Zone A 802.11n, this flag starts at its lowest in the 5 minute mark or close to 802.3 threshold, with 10.65% difference only (see Figure 5.13). Gradually, this climbs to a maximum within the hour with 61.15% (see Table 5.13).

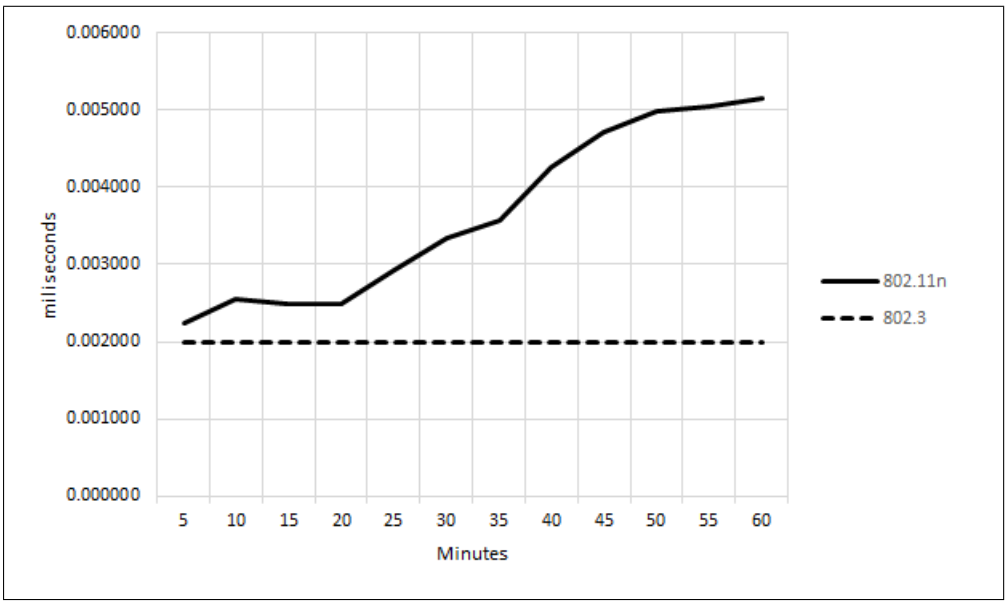



*Figure 5.13.* 802.11n vs Threshold: SYN/ACK-ACK Zone A

Comparing to 802.11g, the same flag showed some contradiction where this 802.11n was nearly but higher than the threshold. However, after 35 minutes, it went up more than 50%. The comparison between threshold to average (0.003647 ms), minimum (0.002238 ms), maximum (0.005148 ms), and median (0.003456 ms) showed the threshold to be below the rest of aforementioned values.

Table 5.13
*802.11n vs Threshold: SYN/ACK-ACK Zone A*

| Minutes | 802.11n | % Differ |
|---|---|---|
| 5 | 0.002238 | 10.65% |
| 10 | 0.002553 | 21.66% |
| 15 | 0.002491 | 19.71% |
| 20 | 0.002491 | 19.71% |
| 25 | 0.002935 | 31.87% |
| 30 | 0.003335 | 40.04% |
| 35 | 0.003578 | 44.10% |
| 40 | 0.004250 | 52.94% |
| 45 | 0.004710 | 57.53% |
| 50 | 0.004989 | 59.91% |
| 55 | 0.005048 | 60.38% |
| 60 | 0.005148 | 61.15% |

Meanwhile, Zone B showed a different pattern to Zone A. Figure 5.14 and Table 5.14 each showed the result of this verification stage for Zone B.

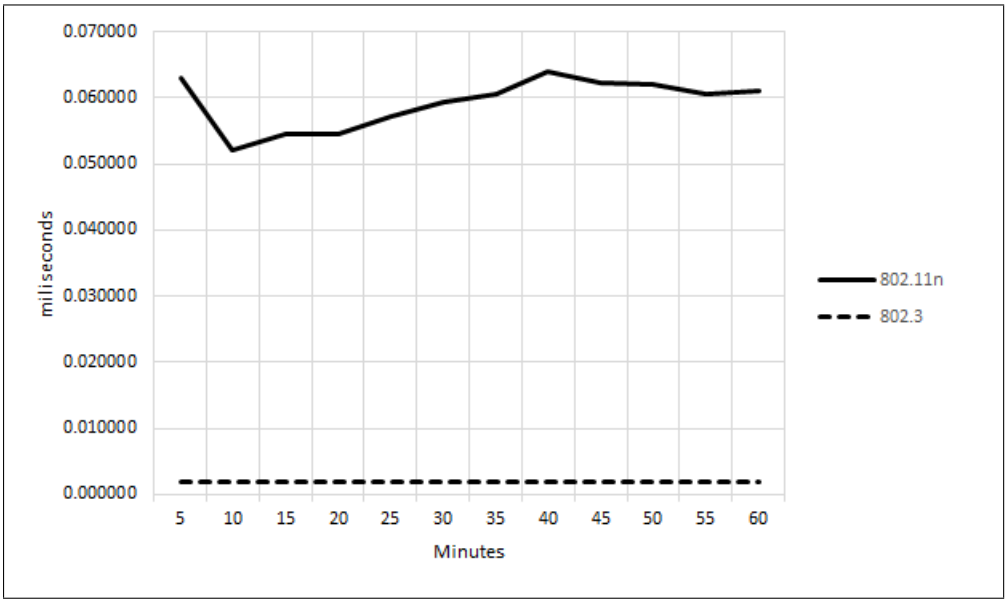



*Figure 5.14.* 802.11n vs Threshold: SYN/ACK-ACK Zone B

The minimum value occurred at minute 10 with 96.16%, whereas the maximum was observed at 40 minutes with 96.88% differences between wireless n to threshold indicators. It was concluded that there is an availability of RAP in the LAN. Meanwhile, average value of 0.059273 ms, minimum value of 0.052021 ms, maximum value of 0.064065 ms, and median value of 0.060682 ms are all

greater than the threshold lines, and with those percentages showed in the table, it can be concluded as being RAP.

Table 5.14
*802.11n vs Threshold: SYN/ACK-ACK Zone B*

| Minutes | 802.11n | % Differ |
|---|---|---|
| 5 | 0.063092 | 96.83% |
| 10 | 0.052021 | 96.16% |
| 15 | 0.054494 | 96.33% |
| 20 | 0.054494 | 96.33% |
| 25 | 0.057174 | 96.50% |
| 30 | 0.059422 | 96.63% |
| 35 | 0.060673 | 96.70% |
| 40 | 0.064065 | 96.88% |
| 45 | 0.062194 | 96.78% |
| 50 | 0.061979 | 96.77% |
| 55 | 0.060691 | 96.70% |
| 60 | 0.060971 | 96.72% |

In terms of similarity of trend, Zone C is located in between Zones A and B. The outcome showed a minimum of 46.22% differences at 5 minutes and the maximum logged at 30 minutes with 74.32% (see Figure 5.15 and Table 5.15).

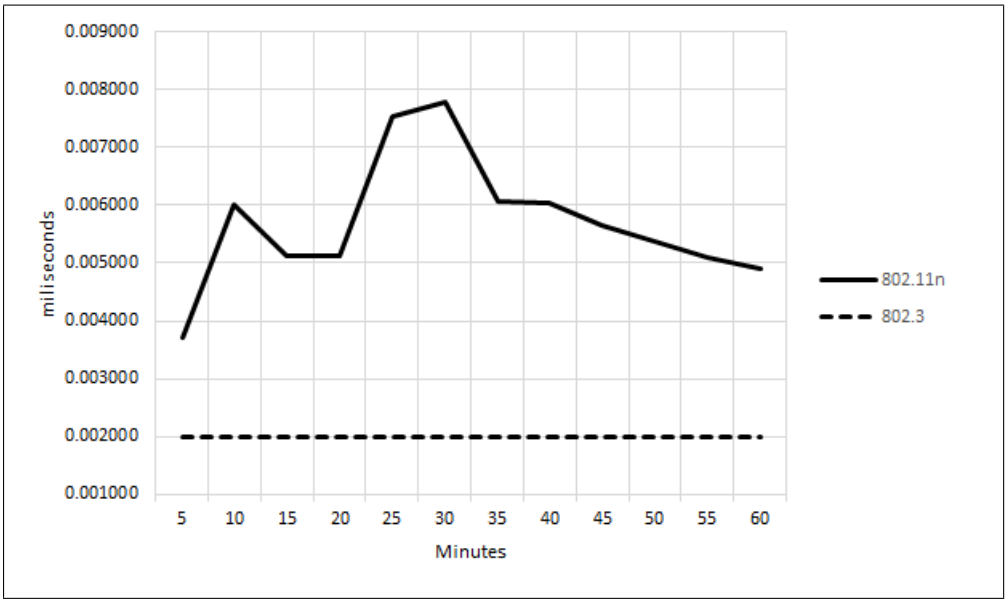



*Figure 5.15.* 802.11n vs Threshold: SYN/ACK-ACK Zone C

The results were in the range of 46% to 74%, and this was considered to be the RAP that exists in the LAN. In addition, with the values of average (0.005705

ms), minimum (0.003719 ms), maximum (0.007789 ms), and median (0.005516 ms) over a certain percentage, as shown in the table of threshold figures, then it is concretely confirmed as RAP.

Table 5.15
*802.11n vs Threshold: SYN/ACK-ACK Zone C*

| **Minutes** | **802.11n** | **% Differ** |
|---|---|---|
| 5 | 0.003719 | 46.22% |
| 10 | 0.006002 | 66.68% |
| 15 | 0.005137 | 61.07% |
| 20 | 0.005137 | 61.07% |
| 25 | 0.007533 | 73.45% |
| 30 | 0.007789 | 74.32% |
| 35 | 0.006079 | 67.10% |
| 40 | 0.006035 | 66.86% |
| 45 | 0.005645 | 64.57% |
| 50 | 0.005387 | 62.88% |
| 55 | 0.005095 | 60.75% |
| 60 | 0.004895 | 59.14% |

In this SYN/ACK-ACK term, all the Zones have their own particular patterns. However, all of them did not cross threshold line. Both Zones B and C were considered to contain RAP, but the first 30 minutes of Zone A can be assumed as having potential RAP; another 30 minutes of Zone A, it would be considered as RAP.

ii. FIN/ACK-ACK

At the opposite end of SYN, FIN is compliments it by closing the connection that SYN opened. Figure 5.16 has the same pattern to SYN/ACK-ACK for Zone A. The lowest was shown at 15 and 20 minutes, while the highest was logged at 50 minutes.

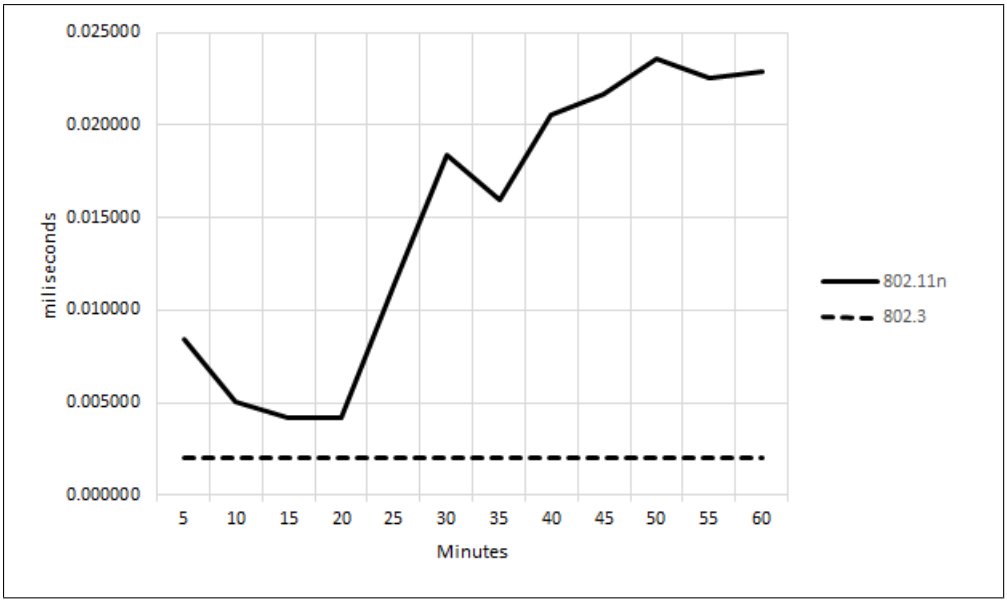



*Figure 5.16.* 802.11n vs Threshold: FIN/ACK-ACK Zone A

In a terms of percentage differences, 52.65% was the smallest and 91.53% was the biggest differences between wireless n and the threshold (see Table 5.16). The table also stated the threshold to be lower than average (0.014907 ms), minimum (0.004224 ms), maximum (0.023621 ms), and median (0.017156 ms).

Table 5.16
*802.11n vs Threshold: FIN/ACK-ACK Zone A*

| **Minutes** | **802.11n** | **% Differ** |
|---|---|---|
| 5 | 0.008412 | 76.22% |
| 10 | 0.005027 | 60.21% |
| 15 | 0.004224 | 52.65% |
| 20 | 0.004224 | 52.65% |
| 25 | 0.011359 | 82.39% |
| 30 | 0.018363 | 89.11% |
| 35 | 0.015948 | 87.46% |
| 40 | 0.020573 | 90.28% |
| 45 | 0.021688 | 90.78% |
| 50 | 0.023621 | 91.53% |
| 55 | 0.022588 | 91.15% |
| 60 | 0.022858 | 91.25% |

In addition, Zone B also did not differ from the results for SYN/ACK-ACK verification in the same zone. They were observed to be synergistic from the

beginning to the end. However, there are differences in some values (see Figure 5.17).

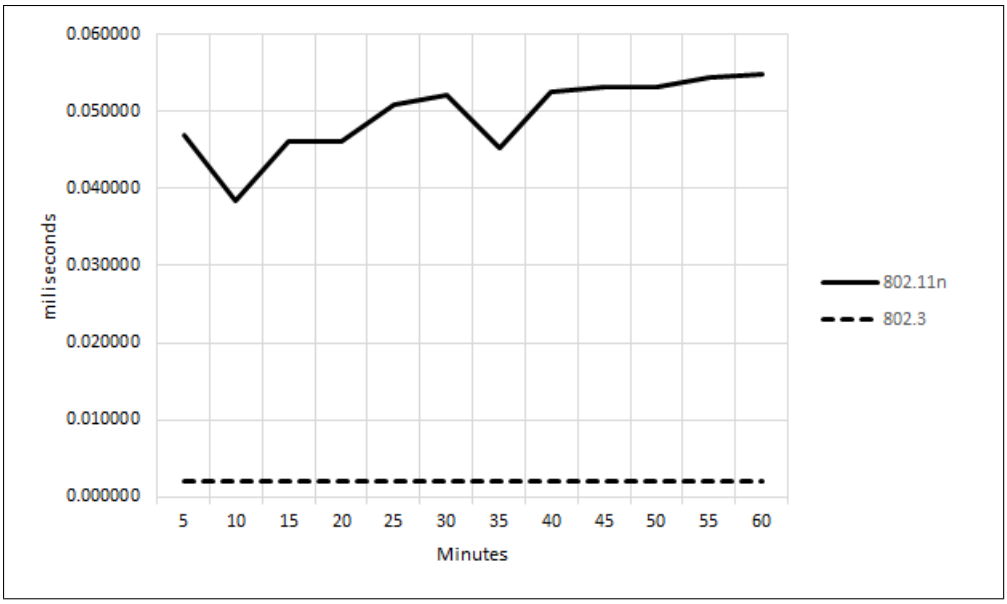



*Figure 5.17.* 802.11n vs Threshold: FIN/ACK-ACK Zone B

The minimum was recorded with 94.81% at 10 minutes whereas the maximum was pinned with 96.35% at 60 minutes (see Figure 5.17). The majority of values were above 90% and this can be considered to be the identification of RAP existence. With the percentages showed in the table and a threshold figures less than average (0.049526 ms), minimum (0.038507 ms), maximum (0.054831 ms), and median (0.051524 ms), this section of verification strongly supports the existence of RAP in the tested LAN.

Table 5.17
*802.11n vs Threshold: FIN/ACK-ACK Zone B5.17*

| Minutes | 802.11n | % Differ |
|---|---|---|
| 5 | 0.047032 | 95.75% |
| 10 | 0.038507 | 94.81% |
| 15 | 0.046150 | 95.67% |
| 20 | 0.046150 | 95.67% |
| 25 | 0.050892 | 96.07% |
| 30 | 0.052157 | 96.17% |
| 35 | 0.045318 | 95.59% |
| 40 | 0.052473 | 96.19% |
| 45 | 0.053214 | 96.24% |
| 50 | 0.053145 | 96.24% |
| 55 | 0.054444 | 96.33% |
| 60 | 0.054831 | 96.35% |

Zone C was in reverse order to Zone B, where it started with a maximum at 5 minutes, with the minimum occurring at 30 minutes (see Figure 5.18).

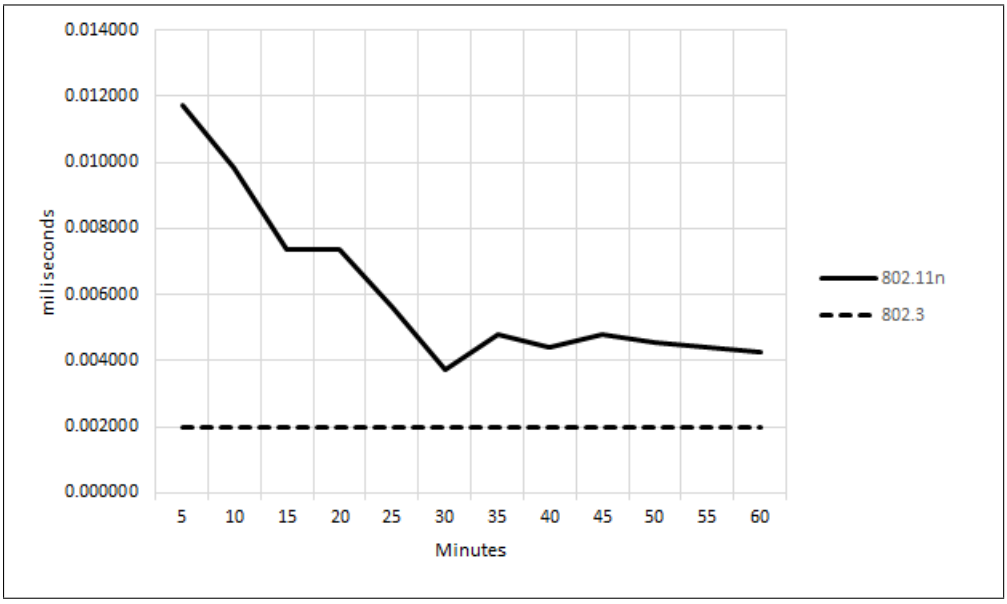



*Figure 5.18.* 802.11n vs Threshold: FIN/ACK-ACK Zone C

In the sense of percentage differences, the minimum point was 46% whereas maximum value was 82.91% (see Table 5.18). Between minimum and maximum values, there are bigger ranges recorded as compare to Zones A and B. At the same time, the average (0.006062 ms), minimum (0.003711 ms),

maximum (0.011706 ms), and median (0.004803 ms) were over the threshold line.

Table 5.18
*802.11n vs Threshold: FIN/ACK-ACK Zone C*

| Minutes | 802.11n | % Differ |
|---|---|---|
| 5 | 0.011706 | 82.91% |
| 10 | 0.009818 | 79.63% |
| 15 | 0.007345 | 72.77% |
| 20 | 0.007345 | 72.77% |
| 25 | 0.005638 | 64.53% |
| 30 | 0.003711 | 46.10% |
| 35 | 0.004814 | 58.45% |
| 40 | 0.004403 | 54.57% |
| 45 | 0.004791 | 58.26% |
| 50 | 0.004529 | 55.84% |
| 55 | 0.004403 | 54.57% |
| 60 | 0.004244 | 52.87% |

This flag had shown the existence of RAP from evidences obtained from all zones. Even though Zone C had the minimum value of less than 50%, but the majority was over that percentage and can be considered to support the condition of RAP being discovered.

iii. PSH/ACK-ACK

As stated previously, PSH supports PAYLOAD to alert the provider to send data to the client. As it functions, the number of packets is less than PAYLOAD, but higher than SYN and FIN. As showed by Figure 5.19, it started the plot at a very high level, then gradually decreased at 30 minutes, then climbed a little up to 40 minutes, and ended going down at 60 minutes.

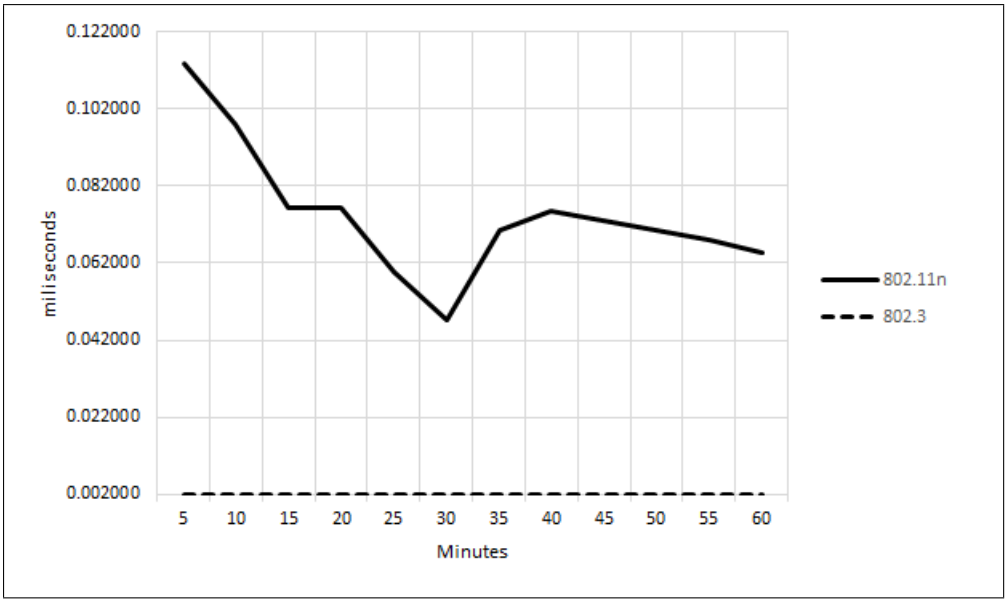



*Figure 5.19.* 802.11n vs Threshold: PSH/ACK-ACK Zone A

Table 5.19 indicates a percentage difference between wireless n and the threshold. The minimum percentage was 95.76%, while maximum was 98.24%. Overall, the table presents values above 90% and this totally supports the presence of RAP. Moreover, this is strengthened with the threshold value being below average (0.074421 ms), minimum (0.047170 ms), maximum (0.113614 ms), and median (0.071736 ms) values.

Table 5.19
*802.11n vs Threshold: PSH/ACK-ACK Zone A*

| **Minutes** | **802.11n** | **% Differ** |
|---|---|---|
| 5 | 0.113614 | 98.24% |
| 10 | 0.097852 | 97.96% |
| 15 | 0.076366 | 97.38% |
| 20 | 0.076366 | 97.38% |
| 25 | 0.059638 | 96.65% |
| 30 | 0.047170 | 95.76% |
| 35 | 0.070434 | 97.16% |
| 40 | 0.075638 | 97.36% |
| 45 | 0.072867 | 97.26% |
| 50 | 0.070604 | 97.17% |
| 55 | 0.067854 | 97.05% |
| 60 | 0.064652 | 96.91% |

Next, Zone B showed some gaps between higher and lower levels. There were

not much difference from 5 minutes until 55 minutes. However at 60 minutes, the trend drastically climbed higher to an extreme value (see Figure 5.20).

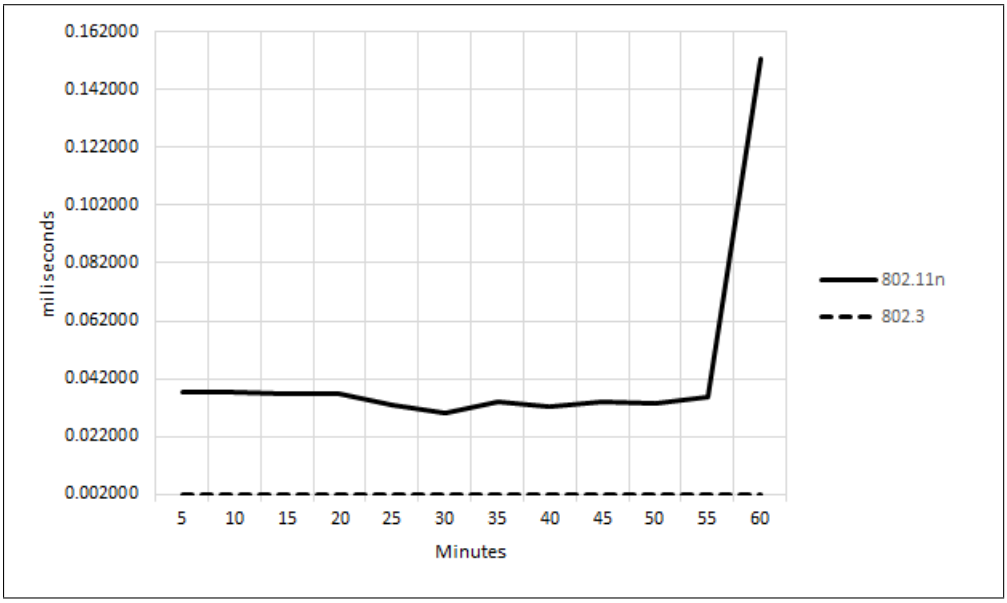



*Figure 5.20.* 802.11n vs Threshold: PSH/ACK-ACK Zone B

In the terms of percentage differences, Table 5.20 highlighted the above situation, with the minimum value indicated at 30 minutes and 93.37%, whereas the maximum was assumed as extreme at 98.69%. The threshold value was also observed to be less than the average (0.044420 ms), minimum (0.030167ms), maximum (0.152630 ms), and median (0.034902 ms) values. An overall value of more than 90% was logged and this is very indicative that RAP was discovered in the LAN.

Table 5.20
*802.11n vs Threshold: PSH/ACK-ACK Zone B*

| Minutes | 802.11n | % Differ |
|---|---|---|
| 5 | 0.037344 | 94.64% |
| 10 | 0.037108 | 94.61% |
| 15 | 0.036728 | 94.55% |
| 20 | 0.036728 | 94.55% |
| 25 | 0.032691 | 93.88% |
| 30 | 0.030167 | 93.37% |
| 35 | 0.033792 | 94.08% |
| 40 | 0.032643 | 93.87% |
| 45 | 0.034106 | 94.14% |
| 50 | 0.033403 | 94.01% |
| 55 | 0.035697 | 94.40% |
| 60 | 0.152630 | 98.69% |

Zone C had a different arrangement, where it was flat and there existed small gaps between each other (see Figure 5.21). A maximum was indicated at as early as 5 minutes, and minimum was located at both 15 and 20 minutes.

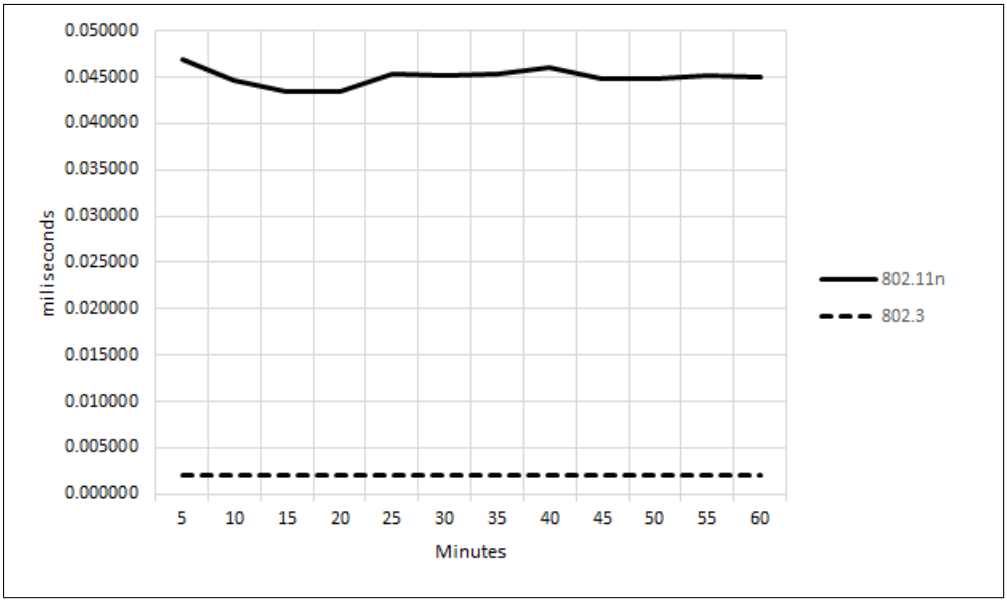



*Figure 5.21.* 802.11n vs Threshold: PSH/ACK-ACK Zone C

In the sense of verification of the wireless condition, the threshold was shown at 95.40% minimum, and 95.73% maximum, and these values were nearly equal and the majority exceeded 90% (see Table 5.21). Additionally, the average (0.045052 ms), minimum (0.043500 ms), maximum (0.046886 ms), and median

(0.045132 ms) were over the threshold line which meets the requirements of RAP discovery in LAN.

Table 5.21
*802.11n vs Threshold: PSH/ACK-ACK Zone C*

| **Minutes** | **802.11n** | **% Differ** |
|---|---|---|
| 5 | 0.046886 | 95.73% |
| 10 | 0.044736 | 95.53% |
| 15 | 0.043500 | 95.40% |
| 20 | 0.043500 | 95.40% |
| 25 | 0.045434 | 95.60% |
| 30 | 0.045208 | 95.58% |
| 35 | 0.045376 | 95.59% |
| 40 | 0.045974 | 95.65% |
| 45 | 0.044918 | 95.55% |
| 50 | 0.044783 | 95.53% |
| 55 | 0.045255 | 95.58% |
| 60 | 0.045056 | 95.56% |

iv. PAYLOAD-ACK

As discussed previously, almost all traffic flows is virtually conquered by ACK and PAYLOAD related processes. Figure 5.22 shows a balanced increment from bottom to the top, even though there was a decrement at 35 minutes that climbed again up until 60 minutes. This showed a minimum plot at 5 minutes and maximum at 60 minutes.

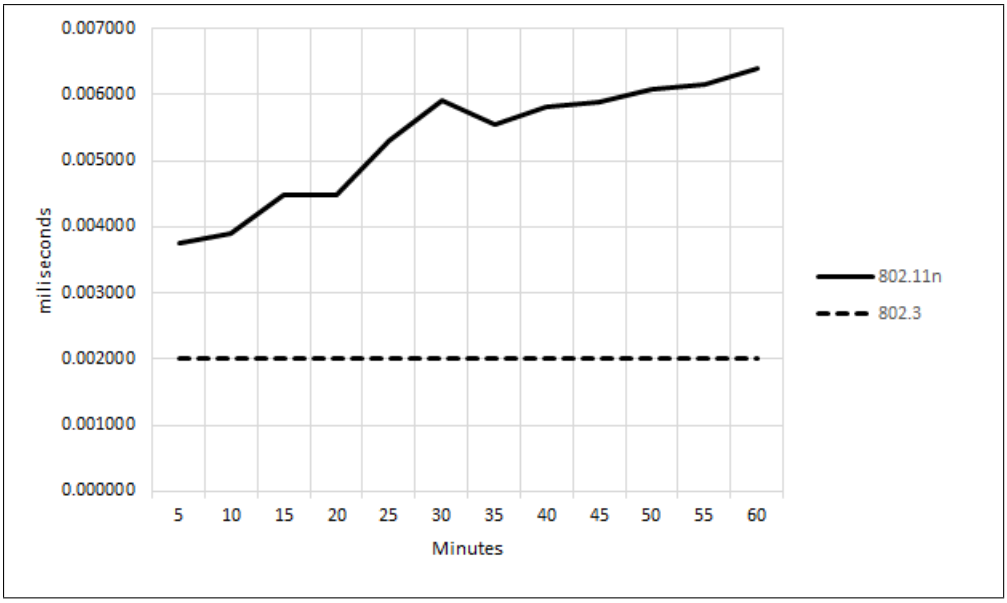



*Figure 5.22.* 802.11n vs Threshold: PAYLOAD-ACK Zone A

Table 5.22 recorded as minimum percentage of 46.83% and maximum of 68.79%. The first 5 and 10 minutes, the percentage was less than 50%, while the rest were above 50%. At the same time, the threshold was shown to be below the average (0.005312 ms), minimum (0.003761 ms), maximum (0.006409 ms), and median (0.005689 ms) values.

Table 5.22
*802.11n vs Threshold: PAYLOAD-ACK Zone A*

| **Minutes** | **802.11n** | **% Differ** |
|---|---|---|
| 5 | 0.003761 | 46.83% |
| 10 | 0.003891 | 48.59% |
| 15 | 0.004486 | 55.42% |
| 20 | 0.004486 | 55.42% |
| 25 | 0.005312 | 62.35% |
| 30 | 0.005901 | 66.11% |
| 35 | 0.005551 | 63.97% |
| 40 | 0.005827 | 65.68% |
| 45 | 0.005879 | 65.98% |
| 50 | 0.006083 | 67.12% |
| 55 | 0.006153 | 67.50% |
| 60 | 0.006409 | 68.79% |

Meanwhile, Zone B showed an opposite result to Zone A, where a longer time difference was recorded. The minimum was shown at 30 minutes, while a

maximum was located at 5 minutes (see Figure 5.23). In terms of percentage variation, all are shown in Table 5.23.

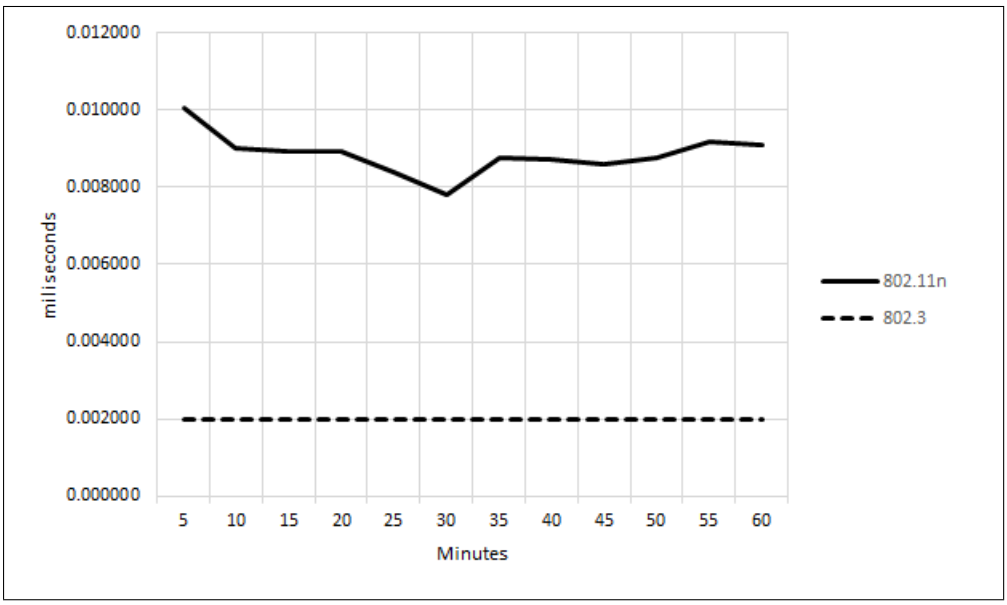



*Figure 5.23.* 802.11n vs Threshold: PAYLOAD-ACK Zone B

A percentage minimum was written as 74.41% and at the same time, maximum was pointed out at 80.12%. As compared to Zone A, Zone B showed more are above 70%. The average (0.008856 ms), minimum (0.007815 ms), maximum (0.010059 ms), and median (0.008852 ms) were all above the threshold value.

Table 5.23
*802.11n vs Threshold: PAYLOAD-ACK Zone B*

| **Minutes** | **802.11n** | **% Differ** |
|---|---|---|
| 5 | 0.010059 | 80.12% |
| 10 | 0.008998 | 77.77% |
| 15 | 0.008923 | 77.59% |
| 20 | 0.008923 | 77.59% |
| 25 | 0.008386 | 76.15% |
| 30 | 0.007815 | 74.41% |
| 35 | 0.008781 | 77.22% |
| 40 | 0.008735 | 77.10% |
| 45 | 0.008586 | 76.71% |
| 50 | 0.008760 | 77.17% |
| 55 | 0.009194 | 78.25% |
| 60 | 0.009109 | 78.04% |

The last but not least was Zone C, as shown in Figure 5.24. This zone has

some similarity to Zone A and against Zone B. The minimum was shown at an early point, which was 5 minutes, and the maximum was at 10 minutes. This is the first and second minute indicators, side-by-side showing minimum and maximum values.

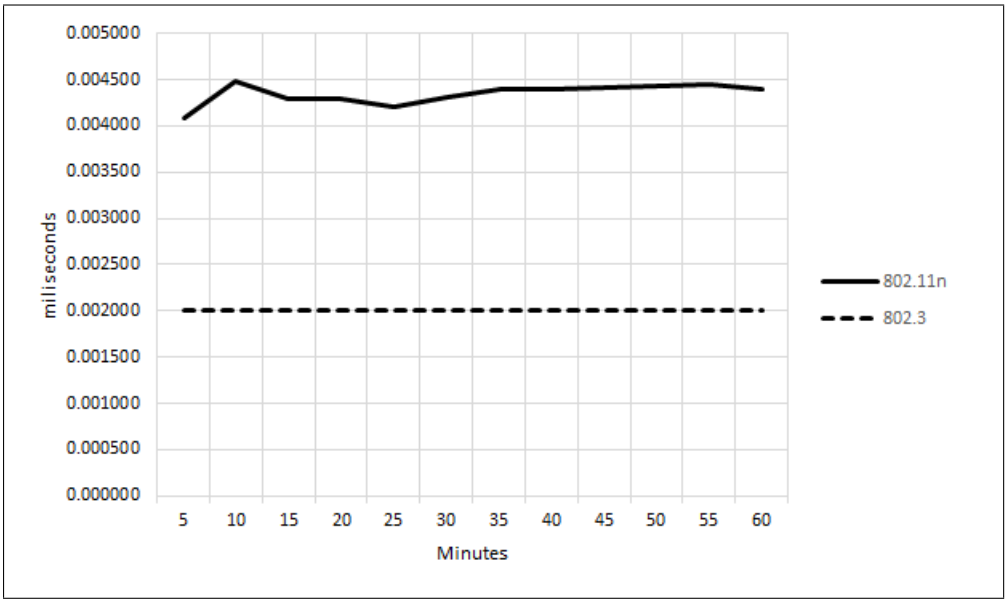



*Figure 5.24.* 802.11n vs Threshold: PAYLOAD/ACK-ACK Zone C

Meanwhile, the percentage differences between wireless and threshold value showed the largest differences between the first and the second (5 and 10 minutes) with values of 51.03% and 55.36% (see Table 5.24). Compared to Zone A which had two indicators below 50%, Zone C had the majority of values above 50%, while the threshold was recorded to be lower than the average (0.004345 ms), minimum (0.004084 ms), maximum (0.004481 ms), and median (0.004394 ms) values.

Table 5.24
*802.11n vs Threshold: PAYLOAD/ACK-ACK Zone C*

| Minutes | 802.11n | % Differ |
|---|---|---|
| 5 | 0.004084 | 51.03% |
| 10 | 0.004481 | 55.36% |
| 15 | 0.004300 | 53.48% |
| 20 | 0.004300 | 53.48% |
| 25 | 0.004209 | 52.48% |
| 30 | 0.004305 | 53.54% |
| 35 | 0.004398 | 54.52% |
| 40 | 0.004391 | 54.45% |
| 45 | 0.004411 | 54.66% |
| 50 | 0.004425 | 54.80% |
| 55 | 0.004447 | 55.02% |
| 60 | 0.004396 | 54.51% |

## 5.4 RAP or Potential RAP

Section 5.2 and 5.3 discussed in detail about the verification of both modes of wireless networks (802.11g and 802.11n). Each verification result can be used to clarify the existence of RAP or Potential RAP. This research proposed that the AP is RAP if it is greater than or equal to 50%, otherwise if it is less than 50%, it is categorised as potential RAP.

As stated in Table 5.25, highlighted figures are less than 50% and labelled as potential RAP. This accounted for 4.51% as compared to 95.49% that concretely identified the existence of RAP. The potential RAP was mostly identified by the SYN/ACK-ACK traffic in 802.11g Zone A at 5 minutes and at 30 minutes in Zone B. Also involving the same flags, 802.11n Zone A recorded from 5 to 35 minutes and at 5 minutes in Zone C were highlighted as potential RAP. Moreover, FIN/ACK-ACK at 30 minutes for 802.11n Zone C was also considered as potential RAP. No figures from PSH/ACK-ACK, mostly over 90%, differed from the threshold. There were two figures from PAYLOAD-ACK at 5 and 10 minutes in 802.11n that were found to be potential RAP. The remaining figures were more than or equal to 50%, which were

Table 5.25
*RAP or Potential RAP*

| Minutes | SYN/ACK-ACK | | | | | | FIN/ACK-ACK | | | | | | PSH/ACK-ACK | | | | | | PAYLOAD-ACK | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 802.11g | | | 802.11n | | | 802.11g | | | 802.11n | | | 802.11g | | | 802.11n | | | 802.11g | | | 802.11n | | |
| | ZA | ZB | ZC | ZA | ZB | ZC | ZA | ZB | ZC | ZA | ZB | ZC | ZA | ZB | ZC | ZA | ZB | ZC | ZA | ZB | ZC | ZA | ZB | ZC |
| 5 | 49.11% | 71.80% | 63.82% | 10.65% | 96.83% | 46.22% | 79.38% | 90.39% | 77.39% | 76.22% | 95.75% | 82.91% | 92.23% | 98.20% | 98.88% | 98.24% | 94.64% | 95.73% | 77.33% | 74.44% | 74.44% | 46.83% | 80.12% | 51.03% |
| 10 | 66.70% | 59.52% | 63.31% | 21.66% | 96.16% | 66.68% | 79.94% | 83.09% | 92.32% | 60.21% | 94.81% | 79.63% | 97.79% | 98.62% | 98.51% | 97.96% | 94.61% | 95.53% | 75.84% | 75.77% | 75.77% | 48.59% | 77.77% | 55.36% |
| 15 | 70.92% | 56.92% | 56.08% | 19.71% | 96.33% | 61.07% | 80.09% | 77.38% | 99.88% | 52.65% | 95.67% | 72.77% | 98.43% | 98.74% | 98.41% | 97.38% | 94.55% | 95.40% | 75.85% | 79.80% | 79.80% | 55.42% | 77.59% | 53.48% |
| 20 | 70.92% | 56.92% | 56.08% | 19.71% | 96.33% | 61.07% | 80.09% | 77.38% | 99.88% | 52.65% | 95.67% | 72.77% | 98.43% | 98.74% | 98.41% | 97.38% | 94.55% | 95.40% | 75.85% | 79.80% | 79.80% | 55.42% | 77.59% | 53.48% |
| 25 | 73.60% | 50.22% | 64.43% | 31.87% | 96.50% | 73.45% | 74.33% | 72.31% | 99.80% | 82.39% | 96.07% | 64.53% | 98.77% | 98.83% | 98.45% | 96.65% | 93.88% | 95.60% | 76.32% | 79.10% | 79.10% | 62.35% | 76.15% | 52.48% |
| 30 | 74.95% | 38.29% | 66.98% | 40.04% | 96.63% | 74.32% | 69.42% | 85.30% | 99.80% | 89.11% | 96.17% | 46.10% | 99.01% | 98.93% | 98.33% | 95.76% | 93.37% | 95.58% | 76.17% | 79.38% | 79.38% | 66.11% | 74.41% | 53.54% |
| 35 | 67.32% | 62.87% | 68.55% | 44.10% | 96.70% | 67.10% | 71.62% | 86.29% | 99.76% | 87.46% | 95.59% | 58.45% | 98.80% | 98.85% | 98.47% | 97.16% | 94.08% | 95.59% | 77.10% | 78.85% | 78.85% | 63.97% | 77.22% | 54.52% |
| 40 | 69.83% | 61.01% | 66.23% | 52.94% | 96.88% | 66.86% | 68.10% | 83.53% | 99.68% | 90.28% | 96.19% | 54.57% | 98.87% | 98.87% | 98.49% | 97.36% | 93.87% | 95.65% | 76.79% | 78.45% | 78.45% | 65.68% | 77.10% | 54.45% |
| 45 | 68.64% | 59.02% | 65.05% | 57.53% | 96.78% | 64.57% | 67.18% | 82.01% | 99.64% | 90.78% | 96.24% | 58.26% | 98.89% | 98.88% | 98.49% | 97.26% | 94.14% | 95.55% | 76.96% | 77.44% | 77.44% | 65.98% | 76.71% | 54.66% |
| 50 | 67.35% | 57.49% | 64.97% | 59.91% | 96.77% | 62.88% | 65.43% | 80.54% | 99.60% | 91.53% | 96.24% | 55.84% | 98.90% | 98.88% | 98.49% | 97.17% | 94.01% | 95.53% | 76.95% | 77.40% | 77.40% | 67.12% | 77.17% | 54.80% |
| 55 | 66.32% | 56.33% | 64.38% | 60.38% | 96.70% | 60.75% | 65.28% | 81.37% | 99.56% | 91.15% | 96.33% | 54.57% | 98.91% | 98.88% | 98.48% | 97.05% | 94.40% | 95.58% | 76.93% | 77.02% | 77.02% | 67.50% | 78.25% | 55.02% |
| 60 | 65.64% | 60.42% | 64.09% | 61.15% | 96.72% | 59.14% | 63.65% | 82.11% | 99.52% | 91.25% | 96.35% | 52.87% | 98.92% | 98.88% | 98.46% | 96.91% | 98.69% | 95.56% | 76.16% | 76.68% | 76.68% | 68.79% | 78.04% | 54.51% |

indicative of RAP. Unfortunately there were no non-RAP being discovered and this shows that this threshold is potentially valid for discovering RAP.

## 5.5 Summary

This verification chapter outlined an evaluation of another process of packet capturing session and packet analysis, as compared to the training phase previously. The previous training threshold indicator value was used to verify and clarify whether the proposed characterisation mechanism can be used for finding RAPs in LANs. The process is similar to the training process, except it focused on capturing 802.11g and n, then using 802.3 threshold (0.00200 ms), to verify the presence of wireless AP in LAN.

The outcome to this stage were the two results, which are RAP and potential RAP. This research proposes a potential RAP result if there is a difference between the threshold value and a test subject, namely a reading of less than 50%. Meanwhile 50% and above was deemed to be indicative of the presence of RAP in the LAN. This proposal took an equal trial between potential RAP and RAP to ensure that the decision being carried out is believable and acceptable to the point of beyond reasonable doubt. To achieve this, this project injected an equal grouping approach where a packet capture filtered through selective flags (SYN/ACK-ACK, FIN/ACK-ACK, PAYLOAD-ACK and PSH/ACK-ACK) can function and assist in finding RAPs in the LAN, even though in the first place, the network is very dynamic, has more uncertainty, and is characteristically unpredictable. The proposed traffic characterisation mechanism was capable of easily predicting the presence of RAP that has been illegally plugged into the LAN.

# CHAPTER SIX
# CONCLUSION AND FUTURE WORK

## 6.1 Introduction

This final chapter summarises and concludes this research project exclusively after going through all the chapters before it. Firstly, the research importance shall be highlighted covering the network testbed, packet capturing process, inbound time stamp, and traffic analysis of wired and wireless networks. The following topic focused on the impact of traffic analysis, which produced three important indicators to detect RAP. The three thresholds were group, zone, and global means. Consequently, these thresholds were used as a measurement indicator that can detect RAP within the LAN environment. Furthermore, the processes involved in this research project concluded in producing two main research contributions, which were RAP detection network testbed and traffic characterisation mechanism. These two findings can assist in discovering RAPs more precisely with the supported of learning and verification structures. Moreover, both structures are backed-up by packet capturing, packet filtering, time stamping, grouping, and getting training threshold, all of which are used to test RAP in the verification stage. In addition to the threshold, the results of this research project can be used in future work projects like SNMP agent and SNMP MIB. SNMP agent needs MIB to function and MIB needs threshold as an indicator for detecting RAP in LANs.

## 6.2 Research Importance

There are three main objectives of the research project which were to summarise as a design of a suitable testbed, to develop a detection mechanism, and to evaluate a new RAP detection mechanism in detecting RAPs in LANs. All the steps were supported by the network testbed for holding all other parts of the mechanism, like

packet capturing to capture selected filtered TCP flags, packet time stamps, arranging time stamped packets into groups through equal group technique, and lastly the result of comparing between wired and wireless network structures which was covered by traffic analysis. The details for these matters are explained in the proceeding sections below.

### 6.2.1 Network Testbed

Even though the main target was for detecting RAPs, a network testbed is needed to hold the mechanism that has been designed, developed, and evaluated. Perhaps network testing was also part of the objective where it was also to design and develop a network testbed. It was used to become the foundation for holding the packet capturing and traffic analysis mechanisms.

Instead of being the foundation base to this research project, it is also useful as a tool for other purposes that involve packet capturing and analysis by other researchers in the future. Other future researchers would expend little effort to adapt the testbed in order to achieve their research targets that involve scanning and analysing traffic, especially in the OSI model transport layer.

### 6.2.2 Packet Capturing

Overall, this research targeted RAP detection through traffic characterisation. As a result, packet capturing was deemed the best process that can thoroughly look into the traffic components which flow in the network. This is very significant for identifying a differences between 802.3 and 802.11 networks. To be more precise, instead of capturing a packet, selective flags were set to meet with traffic characteristic differences between wired and wireless networks. Four flags were chosen among the TCP flags, namely SYN/ACK, PAYLOAD, PSH/ACK, and FIN/ACK. Then, each

respective ACK was paired to the outcome time differences. These time differences had shown big differences between wired and wireless networks as was highlighted in previous discussion. Meanwhile, inbound time stamp played a vital role to this success.

### 6.2.3 Inbound Time Stamp

In differentiating between 802.3 and 802.11, an availability of inbound time stamps was not queried. It works at the inbound port of a subnet in LAN. It waits for a SYN/ACK, PAYLOAD, PSH/ACK, and FIN/ACK from server to arrive and proceeds to time stamp it. When the client receives those packets, it will ACK to the server for concluding the receiving and waits for the next command. This ACK that came from client will get through this inbound time stamp and stamped. The two time stamps are compared to characterise between wired and wireless networks. Without this inbound time stamp, a time differentiation was not going to be gathered and characterised.

### 6.2.4 Equal Group Technique

As stated previously, the concept of inbound time stamp is stamping two different times to produce time differences by two packet differences. Each unit of time differences is equally grouped from one until one thousand using equal group technique. This technique produced a time difference average, where it is used in traffic analysis. This contribution also assists in measuring the time taken for each selected TCP flag to reach a certain group number. As a result in detecting RAPs, some packets are faster that others when this technique is used.

### 6.2.5 Traffic Analysis

Traffic analysis is an important mechanism for differentiating between wired and wireless environments (g and n modes). Two main components of this mechanism

are inbound time stamping and equal grouping. Then it is supported by averaging each group extracted from the equal group technique phase. This mean or average was then compared respectively between wired and wireless environments. There are three average values, namely group, zone, and global mean. This research considered the three means for wired and wireless comparison. Instead of the means outcome, this research also highlighted the time taken for each packet to achieve selected group numbers, which is measured in minutes. The next topic will precisely discuss this matter (6.3).

## 6.3 Conclusion

This research concludes that there is a research gap that was addressed, which was between wired and wireless network, tested through a network testbed supported by packet capturing that filtered SYN/ACK, PAYLOAD, PSH/ACK and FIN/ACK to their ACK pair, while being time stamped at the inbound section in LAN, and being backed up by grouping from 1 until 1000 groups. This series of processes produced three threshold values for finding different characterisations between wired and wireless networks. Moreover, the time for a packet to fill up each group was also measured. Next section will detail out these discoveries.

This research has coined a few outcome terms like Group, Zone, and Global Means. This Global Mean is also known as the Threshold. Furthermore, the work also calculated a packet gathering time which can become a guideline to choose a selected group, while implementing Equal Group technique for RAP discoveries. These stated terms are discussed further in the following subsections.

### 6.3.1 RAP Threshold

As proposed earlier, the main outcome of this research was to find RAP by comparing 802.3 and 802.11 (g and n mode) through getting a 802.3 global mean and using this value as the threshold value. Before the threshold is gathered, it has already gone through another series of calculation work that resulted in the group mean and zone mean. These threshold values are used to verify and clarify the existence of RAPs in LAN.

As stated in 5.4, it showed 4.51% to be categorised as potential RAP, as compared to 95.49% that were classified as RAP. This is a clear evidence which strongly supported this research work in detecting RAP using the proposed Traffic Characterisation Mechanism that was proven to work.

In addition to this, the verification would not be smoothly executed if there is no specific information about what is the selective equal group to be used in the verification process. These are tabled and showed as a prediction of which groups can produce the highest number of packets within a minute. The next section will elaborate further about this matter.

### 6.3.2 Packet Gathering Time

As stated in Figures 4.53 and 4.56, only a selective group is chosen in the verification process. In inheritance, it is very helpful in projecting a verification analysis that occurs within an hour of packet capturing with a five minute range in between those times.

This finding will help in setting a best equal group to be used in the process of comparing both wired and wireless environments through the proposed Traffic

Characterisation Mechanism. The next section describes this research contribution.

## 6.4 Research Contribution

The previous section 6.2 already put five important keys which can be considered as the major contribution of this research work. Without those keys, the process of finding RAP would not be a major success. These five contributions play a vital role and function in a research process, which are mainly the learning and verification processes.

### 6.4.1 Learning and Verification Processes

As shows in section 3.5.5, there are several processes in the learning process, namely packet capturing, packet filtering, time stamping, grouping, and threshold. Whereas section 3.5.6 highlighted the first three similar processes to learning, there are two different processes which are selected grouping and threshold checking.

Learning process is used to find a threshold, and in this research work, 802.3 showed less time response compared to 802.11g and 802.11n. As a result, 0.002 ms was chosen to become the global mean or threshold in the verification process. The result of this event had already been discussed in subsection 6.3.1.

## 6.5 Future Work

At the beginning, this dissertation highlighted SNMP as one of the alternatives for solving this RAP issue. However, before this could be realised, the earlier work that this research performed did not involve SNMP directly. Indirectly after the mechanism was designed, developed, and verified, it was identified as a contribution to network security, especially network management. The two most important network management components benefitting from this research output are network

management agent and management information base (MIB). These two components are discussed further in their respective subsections below.

### 6.5.1 RAP Detection Agent

The verification process can be transformed into a network management agent like SNMP for scanning and detecting RAP at the switch or router at the inbound in LAN. The network functional area (FCAPS), especially security management, can take benefits from this research project in executing RAP detection and thus eliminate the problem. As stated previously, the SNMP agent can follow a series of processes that have already been formulated starting from packet capturing, packet filtering, equal grouping, and comparing between wired and wireless, in order to detect RAP.

Another approach is to cooperate a Traffic Characterisation Mechanism from this research to an existing agent by injecting threshold figures for comparison. The SNMP agent then becomes the feeder and organiser to SNMP manager who will create a trap once the RAP is detected.

A complimentary SNMP Agent is the MIB, where the agent must refer to in order to operate either by detecting or reflecting when the RAP problem is rectified.

### 6.5.2 RAP Management Information Base (MIB)

Another next future works can be forwarded is RAP MIB which is a compulsory mechanism for agent to respond and react from to manager. Traffic Characterization Mechanism which is designed, developed and verified is suitable in the future of developing network management solution for scanning RAP in LAN.

## 6.6 Summary

The importance of this research work is the conclusion of the five key factors, namely packet capturing, packet filtering, time stamping, equal grouping, and traffic analysis. Packet capturing is the first process to fully capture traffic activity from and to, inside and outside the LAN. Meanwhile, specific indicators or flags is chosen through the packet filtering process. The filtered flags like SYN/ACK, FIN/ACK, PSH/ACK, and PAYLOAD with their respective ACK are prioritised to be time stamped at the inbound LAN. As a result, a time differences between those flags and their acknowledgment can be revealed.

With support from the equal grouping process, the dynamic time differences is reduced by finding an average of the selective group that is set up from one to 1000. This equal group also assists in predicting the number of packets produced within a minute and which group is relevant and suitable for feeding the Traffic Characterisation Mechanism that this research has successfully designed, developed, and verified.

An outcome of equal grouping can be forwarded to the traffic analysis part, where the means (group, zone, and global means) are constructed. Finally, the global mean or threshold is proposed as the optimal time differences between SYN/ACK, FIN/ACK, PSH/ACK, and PAYLOAD with their respective ACK for differentiating wired and wireless environments. Because RAP is a wireless structure, it can be easily differentiated from wired structure.

This research went through two cycles for solving RAP issues, namely the training and verification processes. Both processes were already discussed in greater detail in Chapters 3, 4, and 5. The results revealed two RAP criteria where both were given a 50-50 per cent chance in labelling either the AP is a genuine RAP or suspected to be

RAP (potential RAP). As a result, about 4.51% were categorised as potential RAP and the rest 95.49% were classified as RAP. The good news is there was 0% non-RAP.

Traffic Characterisation Mechanism that this work performed was already proven to be able to detect RAP through a wired and wireless environment comparison and can be benefited by the network management environment.

# REFERENCES


[1] CISCO, "Five reasons to go wireless," 2014. [Online]. Available: http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/work_from_anywhere/why_go_wireless/index.html

[2] S. Evans, "Wired vs wireless in the enterprise," 2014. [Online]. Available: http://www.computerweekly.com/feature/Wired-vs-wireless-in-the-enterprise

[3] Bizhelp24, "How can a wireless network benefit your business?" 2010. [Online]. Available: http://www.computerweekly.com/feature/Wired-vs-wireless-in-the-enterprise

[4] S. Plosz, A. Farshad, M. Tauber, C. Lesjak, T. Ruprechter, and N. Pereira, "Security vulnerabilities and risks in industrial usage of wireless communication," in *Emerging Technology and Factory Automation (ETFA), 2014 IEEE*, 2014, pp. 1–8. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7005129

[5] J. Zhang, L. Fu, and X. Wang, "Asymptotic analysis on secrecy capacity in large-scale wireless networks," vol. 22, no. 1, pp. 66–79, 2014. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6470734

[6] E. Mckinney, "Disadvantages of wireless networks," 2014. [Online]. Available: http://www.ehow.com/facts_4809373_disadvantages-wireless-networks.html

[7] G. Francia, III, D. Thornton, and T. Brookshire, "Wireless vulnerability of scada systems," in *Proceedings of the 50th Annual Southeast Regional Conference*, ser. ACM-SE '12. New York, NY, USA: ACM, 2012, pp. 331–332. [Online]. Available: http://doi.acm.org/10.1145/2184512.2184590

[8] P. De, Y. Liu, and S. Das, "An epidemic theoretic framework for vulnerability analysis of broadcast protocols in wireless sensor networks," vol. 8, no. 3, pp. 413–425, 2009. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4591395

[9] T. Stimpson, L. Liu, J. Zhang, R. Hill, W. Liu, and Y. Zhan, "Assessment of security and vulnerability of home wireless networks," in *Fuzzy Systems and Knowledge Discovery (FSKD), 2012 9th International Conference on*, 2012, pp. 2133–2137. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6233783

[10] T. Walker, M. Tummala, and J. McEachen, "Security vulnerabilities in hybrid flow-specific traffic-adaptive medium access control," in *System Science (HICSS), 2012 45th Hawaii International Conference on*, 2012, pp. 5649–5658. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6149581

[11] E. Stavrou and A. Pitsillides, "Vulnerability assessment of intrusion recovery countermeasures in wireless sensor networks," in *Computers and*

*Communications (ISCC), 2011 IEEE Symposium on*, 2011, pp. 706–712. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5983922

[12] P. Tague, D. Slater, J. Rogers, and R. Poovendran, "Evaluating the vulnerability of network traffic using joint security and routing analysis," vol. 6, no. 2, pp. 111–123, 2009. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4668352

[13] S. Anand, K. Hong, R. Chandramouli, S. Sengupta, and K. Subbalakshmi, "Security vulnerability due to channel aggregation/bonding in LTE and HSPA+ network," in *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, 2011, pp. 1–5. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6134063

[14] S. Reddy, K. Sai Ramani, K. Rijutha, S. Ali, and C. Reddy, "Wireless hacking - a WiFi hack by cracking wep," in *Education Technology and Computer (ICETC), 2010 2nd International Conference on*, vol. 1, 2010. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5529269

[15] Airtight, "Conquering the minefield of soft rogue aps in the enterprise," 2014. [Online]. Available: http://airtightnetworks.com/fileadmin/pdf/whitepaper/Conquering-the-Minefield-of-Soft-Rogue-APs.pdf

[16] AirMagnet, "Best practices for rogue detection and annihilation," 2004. [Online]. Available: http://airmagnet.flukenetworks.com/assets/whitepaper/Rogue_Detection_White_Paper.pdf

[17] C. D. Mano, A. Blaich, Q. Liao, Y. Jiang, D. A. Cieslak, D. C. Salyers, and A. Striegel, "Ripps: Rogue identifying packet payload slicer detecting unauthorized wireless hosts through network traffic conditioning," *ACM Trans. Inf. Syst. Secur.*, vol. 11, no. 2, pp. 1–23, 2008.

[18] K. N. Gopinath and H. Chaskar, "All you wanted to know about wifi rogue access points," 2014. [Online]. Available: http://www.rogueap.com/rogue-ap-docs/RogueAP-FAQ.pdf

[19] R. Beyah, S. Kangude, G. Yu, B. Strickland, and J. Copeland, "Rogue access point detection using temporal traffic characteristics," *Global Telecommunications Conference, 2004. GLOBECOM '04. IEEE*, vol. 4, pp. 2271–2275 Vol.4, 2004.

[20] H. Hou, R. Beyah, and C. Corbett, "A passive approach to rogue access point detection," in *Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE*, 26-30 Nov. 2007, pp. 355–360.

[21] L. Ma, A. Teymorian, and X. Cheng, "A hybrid rogue access point protection framework for commodity wi-fi networks," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, 13-18 April 2008, pp. 1220–1228.

[22] D. Schweitzer, W. Brown, and J. Boleng, "Using visualization to locate rogue access points," *J. Comput. Small Coll.*, vol. 23, no. 1, pp. 134–140, 2007.

[23] CISCO, "Cisco wireless lan controller configuration guide," 2014. [Online]. Available: http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED.pdf

[24] C. Liu and J. Yu, "Rogue access point based dos attacks against 802.11 wlans," in *Telecommunications, 2008. AICT '08. Fourth Advanced International Conference on*, 8-13 June 2008, pp. 271–276.

[25] S. Srilasak, K. Wongthavarawat, and A. Phonphoem, "Integrated wireless rogue access point detection and counterattack system," in *Information Security and Assurance, 2008. ISA 2008. International Conference on*, 24-26 April 2008, pp. 326–331.

[26] P. Drake, "Using snmp to manage networks," in *Proc. IEE Colloquium on Designing Resilient Architectures*, Nov. 15, 1991, pp. 2/1–2/4.

[27] J. Case, M. Fedor, M. Schoffstall, and J. Davin, "Rfc 1157: Simple network management system," 2012. [Online]. Available: http://datatracker.ietf.org/doc/rfc1157/

[28] Y.-S. Hwang and E. bae Kim, "An architecture of snmp-based network management of the broadband wireless access system," in *Proc. 9th Asia-Pacific Conference on Communications APCC 2003*, vol. 3, Sep. 21–24, 2003, pp. 1163–1166.

[29] J. Schonwalder, A. Pras, M. Harvan, J. Schippers, and R. van de Meent, "Snmp traffic analysis: Approaches, tools, and first results," in *Proc. 10th IFIP/IEEE International Symposium on Integrated Network Management IM '07*, May 2007, pp. 323–332.

[30] A. Ahmad and S. Hassan, "Detecting rogue access point (rap) using simple network management protocol (snmp)," in *International Conference on Network Applicaitons, Protocols and Services NetApps2008)*, November 21 2008–November 22 2008. [Online]. Available: http://www.internetworks.my/NetApps2008/Proceedings/accepted%20paper/Detecting%20Rogue%20Access%20Point%20%28RAP%29%20using%20SNMP.pdf

[31] X. Wang, L. Wang, B. Yu, and G. Dong, "Studies on network management system framework of campus network," in *Informatics in Control, Automation and Robotics (CAR), 2010 2nd International Asia Conference on*, vol. 2, March 2010, pp. 285–289.

[32] NetSNMP, "Netsnmp," 2011. [Online]. Available: http://www.net-snmp.org

[33] MYCERT, "Malaysian computer emergency response team," 2012. [Online]. Available: http://www.mycert.org.my

[34] CyberSecurity, "Cyber999," 2012. [Online]. Available: http://www.cybersecurity.my

[35] J. Yang, Y. Chen, and W. Trappe, "Detecting spoofing attacks in mobile wireless environments," in *Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON '09. 6th Annual IEEE Communications Society Conference on*, 2009, pp. 1–9. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5168926

[36] A. Ahmad and M. A. Hajer, "Spoofing tracking mechanism for eliminating masquerade users," in *The Fifth Social Economic and Information Technology SEiT 2010 Conference*. UUM, 2010, pp. 50–53.

[37] A. Hadid, "Face biometrics under spoofing attacks: Vulnerabilities, countermeasures, open issues, and research directions," in *Computer Vision and Pattern Recognition Workshops (CVPRW), 2014 IEEE Conference on*, 2014, pp. 113–118. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6909967

[38] D. Reising, M. Temple, and J. Jackson, "Authorized and rogue device discrimination using dimensionally reduced rf-dna fingerprints," *Information Forensics and Security, IEEE Transactions on*, vol. PP, no. 99, pp. 1–1, 2015.

[39] R. Henning, "Vulnerability assessment in wireless networks," in *Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on*, 2003, pp. 358–362. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1210186

[40] V. Agapov and S. Rahman, "Exploring wireless device driver vulnerabilities," in *Computer and Information Technology, 2008. ICCIT 2008. 11th International Conference on*, 2008, pp. 78–84. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4803130

[41] F. Azzali, A. Ahmad, and A. Daud, "Determining wireless local area network (wlan) vulnerabilities on academic network," in *Proc. International Conference on Computing and Informatic (ICOCI09)*, 2009.

[42] A. Amran, D. Ali Yusny, and A. Fazly, "Determining wireless local area network vulnerabilities on academic network," in *PROSIDING SEMINAR HASIL PENYELIDIKAN SEKTOR PENGAJIAN TINGGI KE-3*, July 2 2013–July 3 2013, pp. 516–527.

[43] SANS, "Security vulnerabilities and wireless lan technology," 2014. [Online]. Available: http://www.sans.org/reading-room/whitepapers/wireless/security-vulnerabilities-wireless-lan-technology-1629

[44] A. K. Gupta, "Wifi vulnerabilities: Advances and incidents in 2010," 2014. [Online]. Available: http://www.networkworld.com/article/2197200/wi-fi/wifi-vulnerabilities--advances-and-incidents-in-2010.html

[45] PCMag, "Encyclopedia," 2014. [Online]. Available: http://www.pcmag.com/encyclopedia/term/50596/rogue-access-point

[46] H. Yin, G. Chen, and J. Wang, "Detecting protected layer-3 rogue aps," in *Proc. Fourth International Conference on Broadband Communications, Networks and Systems BROADNETS 2007*, Sep. 10–14, 2007, pp. 449–458.

[47] X. Zheng, C. Wang, Y. Chen, and J. Yang, "Accurate rogue access point localization leveraging fine-grained channel information," in *Communications and Network Security (CNS), 2014 IEEE Conference on*, 2014, pp. 211–219. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6997488

[48] S. Jadhav, S. Vanjale, and P. Mane, "Illegal access point detection using clock skews method in wireless LAN," in *Computing for Sustainable Global Development (INDIACom), 2014 International Conference on*, 2014, pp. 724–729. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6828057

[49] S. Nikbakhsh, A. Manaf, M. Zamani, and M. Janbeglou, "A novel approach for rogue access point detection on the client-side," in *Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on*, 2012, pp. 684–687. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6185342

[50] R. Shrestha and S. Y. Nam, "Access point selection mechanism to circumvent rogue access points using voting-based query procedure," *IET Communications*, vol. 8, no. 16, pp. 2943–2951, 2014.

[51] H. Han, F. Xu, C. Tan, Y. Zhang, and Q. Li, "Vr-defender: Self-defense against vehicular rogue aps for drive-thru internet," vol. 63, no. 8, pp. 3927–3934, 2014. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6762935

[52] K. F. Kao, W. C. Chen, J. C. Chang, and H. T. Chu, "An accurate fake access point detection method based on deviation of beacon time interval," in *Software Security and Reliability-Companion (SERE-C), 2014 IEEE Eighth International Conference on*, 2014, pp. 1–2. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6901631

[53] N. Agrawal, B. Pradeepkumar, and S. Tapaswi, "Preventing arp spoofing in WLAN using sha-512," in *Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on*, 2013, pp. 1–5. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6724145

[54] K. Kyriakopoulos, F. Aparicio-Navarro, and D. Parish, "Detecting misbehaviour in WiFi using multi-layer metric data fusion," in *Measurements and Networking Proceedings (M&N), 2013 IEEE International Workshop on*, 2013, pp. 155–160. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6663795

[55] R. Beyah and A. Venkataraman, "Rogue-access-point detection: Challenges, solutions, and future directions," *IEEE Secur Priv*, vol. 9, no. 5, pp. 56–61, 2011. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5963632

[56] K. Sawicki and Z. Piotrowski, "The proposal of ieee 802.11 network access point authentication mechanism using a covert channel," in *Microwave Radar and Wireless Communications (MIKON), 2012 19th International Conference on*, vol. 2, May 2012, pp. 656–659.

[57] Y. Song, C. Yang, and G. Gu, "Who is peeping at your passwords at starbucks? x2014; to catch an evil twin access point," in *Dependable Systems and Networks (DSN), 2010 IEEE/IFIP International Conference on*, 282010-july1 2010, pp. 323 –332.

[58] M. Wong and A. Clement, *Sharing wireless internet in urban neighbourhoods*. Springer, 2007.

[59] A. Kalbasi, O. Alomar, M. Hajipour, and F. Aloul, "Wireless security in uae: A survey paper," in *Proc. of the IEEE GCC Conference*, 2007.

[60] C.-M. Chuang, C. Tung, H.-L. Lee, and K.-S. Huang, "Distributed wireless security system," Jun. 15 2006, uS Patent App. 11/453,725.

[61] V. Sharma, "Intrusion detection in infrastructure wireless lans," *Bell Labs Technical Journal*, vol. 8, no. 4, pp. 115–119, 2004.

[62] HKGoverment, "Wireless networking security," 2014. [Online]. Available: http://www.infosec.gov.hk/english/technical/files/wireless.pdf

[63] K. Jones and L. Liu, "What where wi: An analysis of millions of wi-fi access points," in *Portable Information Devices, 2007. PORTABLE07. IEEE International Conference on*, 25-29 May 2007, pp. 1–4.

[64] A. Phippen and S. Furnell, "Taking responsibility for online protection–why citizens have their part to play," *Computer Fraud & Security*, vol. 2007, no. 11, pp. 8–13, 2007.

[65] H. Sathu, "Wardriving dilemmas," in *Proceedings of the Nineteenth Annual Conference of the National Advisory Committee on Computing Qualifications, Wellington*, 2006, pp. 237–242.

[66] H. Berghel and J. Uecker, "Wireless infidelity ii: airjacking," *Commun. ACM*, vol. 47, no. 12, pp. 15–20, 2004.

[67] NetStumbler, "The physics of where to put a wi-fi router," 2014. [Online]. Available: http://www.netstumbler.com/2014/09/19/the-physics-of-where-to-put-a-wi-fi-router/

[68] A. Weiss, "Introduction to netstumbler," 2014. [Online]. Available: http://www.wi-fiplanet.com/tutorials/article.php/3589131

[69] A. Sulaiman and M. Hussein, "A modified multi-wall wave propagation model for concrete based building structure," in *Computer and Communication Engineering (ICCCE), 2012 International Conference on*, 2012, pp. 325–330. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6271205

[70] S. Gold, "Hacking on the hoof," *Engineering & Technology*, vol. 7, no. 3, pp. 80–83, 2012. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6210313

[71] E. S. Aimuanmwosa, "Evaluating kismet and netstumbler as network security tools & solutions," Ph.D. dissertation, Blekinge Institute of Technology, 2010.

[72] K. R. Foster, "Radiofrequency exposure from wireless lans utilizing wi-fi technology," *Health Physics*, vol. 92, no. 3, pp. 280–289, 2007.

[73] M. Sajat, S. Hassan, and S. Chit, "An analysis of wi-fi security vulnerabilities in Malaysia: A survey in golden triangle kuala lumpur," in *Computing & Informatics, 2006. ICOCI '06. International Conference on*, 2006, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5276423

[74] K. Y. Park, Y. S. Kim, and J. Kim, "Security enhanced IEEE 802.1x authentication method for WLAN mobile router," in *Advanced Communication Technology (ICACT), 2012 14th International Conference on*, 2012, pp. 549–553. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6174728

[75] E.-K. Ryu, G.-J. Lee, and K.-Y. Yoo, "Unlinkable authentication for roaming user in heterogeneous wireless networks," in *Connected Vehicles and Expo (ICCVE), 2013 International Conference on*, Dec 2013, pp. 629–634.

[76] W. Wei, K. Suh, B. Wang, Y. Gu, J. Kurose, and D. Towsley, "Passive online rogue access point detection using sequential hypothesis testing with tcp ack-pairs," in *IMC '07: Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*. New York, NY, USA: ACM, 2007, pp. 365–378.

[77] T. Le, R. P. Liu, and M. Hedley, "Rogue access point detection and localization," in *Personal Indoor and Mobile Radio Communications (PIMRC), 2012 IEEE 23rd International Symposium on*, 2012, pp. 2489–2493. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6362775

[78] Tcpdump, "Tcpdump and libpcap," 2014. [Online]. Available: http://www.tcpdump.org

[79] M. Qadeer, M. Zahid, A. Iqbal, and M. Siddiqui, "Network traffic analysis and intrusion detection using packet sniffer," in *Communication Software and Networks, 2010. ICCSN '10. Second International Conference on*, Feb 2010, pp. 313–317.

[80] L. Braun, A. Didebulidze, N. Kammenhuber, and G. Carle, "Comparing and improving current packet capturing solutions based on commodity hardware," in *Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement*, ser. IMC '10. New York, NY, USA: ACM, 2010, pp. 206–217. [Online]. Available: http://doi.acm.org/10.1145/1879141.1879168

[81] P. Orosz and T. Skopko, “Software-based packet capturing with high precision timestamping for linux,” in *Systems and Networks Communications (ICSNC), 2010 Fifth International Conference on*, Aug 2010, pp. 381–386.

[82] L. Zabala, A. Ferro, and A. Pineda, “Modelling packet capturing in a traffic monitoring system based on linux,” in *Performance Evaluation of Computer and Telecommunication Systems (SPECTS), 2012 International Symposium on*, July 2012, pp. 1–6.

[83] B. Lee, S. Moon, and Y. Lee, “Application-specific packet capturing using kernel probes,” in *Integrated Network Management, 2009. IM ’09. IFIP/IEEE International Symposium on*, June 2009, pp. 303–306.

[84] J. Therdphapiyanak and K. Piromsopa, “An analysis of suitable parameters for efficiently applying k-means clustering to large tcpdump data set using hadoop framework,” in *Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2013 10th International Conference on*, May 2013, pp. 1–6.

[85] S. Binti Alias, S. Manickam, and M. Kadhum, “A study on packet capture mechanisms in real time network traffic,” in *Advanced Computer Science Applications and Technologies (ACSAT), 2013 International Conference on*, Dec 2013, pp. 456–460.

[86] I. Cerrato, M. Leogrande, and F. Risso, “Filtering network traffic based on protocol encapsulation rules,” in *Computing, Networking and Communications (ICNC), 2013 International Conference on*, Jan 2013, pp. 1058–1063.

[87] W. Wu and P. DeMar, “Wirecap: A novel packet capture engine for commodity nics in high-speed networks,” in *Proceedings of the 2014 Conference on Internet Measurement Conference*, ser. IMC ’14. New York, NY, USA: ACM, 2014, pp. 395–406. [Online]. Available: http://doi.acm.org/10.1145/2663716.2663736

[88] DARPA, “Rfc 793: Transmission control protocol,” 2012. [Online]. Available: http://datatracker.ietf.org/doc/rfc793/

[89] A. Khadimi, M. Lmater, M. Eddabbah, and M. El Kayyali, “Packet classification using the hidden markov model,” in *Multimedia Computing and Systems (ICMCS), 2011 International Conference on*, April 2011, pp. 1–5.

[90] J. Wang, L. Weiwei, Z. Yan, L. Tao, and W. Zilong, “P2p traffic identification based on netflow tcp flag,” in *Future Computer and Communication, 2009. ICFCC 2009. International Conference on*, April 2009, pp. 700–703.

[91] S. Haris, R. Ahmad, and M. Ghani, “Detecting tcp syn flood attack based on anomaly detection,” in *Network Applications Protocols and Services (NETAPPS), 2010 Second International Conference on*, Sept 2010, pp. 240–244.

[92] S. Yan and L. Shuai, "Robust $\mathscr{H}\infty$ filtering in sensor networks with uncertain rates of packet losses," in *Control Conference (CCC), 2014 33rd Chinese*, 2014, pp. 5282–5287. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6895840

[93] S. McCanne and V. Jacobson, "The bsd packet filter: A new architecture for user-level packet capture," in *Proceedings of the USENIX Winter 1993 Conference Proceedings on USENIX Winter 1993 Conference Proceedings*, ser. USENIX'93. Berkeley, CA, USA: USENIX Association, 1993, pp. 2–2. [Online]. Available: http://dl.acm.org/citation.cfm?id=1267303.1267305

[94] L. Abeni, N. Bonelli, and G. Procissi, "Randomized packet filtering through specialized partitioning of rulesets," vol. 17, no. 12, pp. 2380–2383, 2013. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6656077

[95] L. Ning, S. Sen, J. Maohua, and H. Jian, "A router based packet filtering scheme for defending against dos attacks," *China Communications*, vol. 11, no. 10, pp. 136–146, 2014. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6969802

[96] G. Wang, M. Xu, and X. Huan, "Design and implementation of an embedded router with packet filtering," in *Electrical & Electronics Engineering (EEESYM), 2012 IEEE Symposium on*, 2012, pp. 285–288. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6258645

[97] L. Cuizhi, Z. Hui, and W. L. Ping, "The design and research based on the intrusion detection model of packet filtering technology," in *Computer Science & Education (ICCSE), 2011 6th International Conference on*, 2011, pp. 22–23. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6028575

[98] Z. Wu, M. Xie, and H. Wang, "Design and implementation of a fast dynamic packet filter," vol. 19, no. 5, pp. 1405–1419, 2011. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5719540

[99] R. Fantacci, L. Maccari, P. Neira Ayuso, and R. Gasca, "Efficient packet filtering in wireless ad hoc networks," vol. 46, no. 2, pp. 104–110, 2008. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4473091

[100] Q. Chen, W. Lin, W. Dou, and S. Yu, "Cbf: A packet filtering method for DDoS attack defense in cloud environment," in *Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on*, 2011, pp. 427–434. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6118752

[101] Y. Kim, W. Ren, J.-Y. Jo, Y. Jiang, and J. Zheng, "Sfric: A secure fast roaming scheme in wireless lan using id-based cryptography," in *Communications, 2007. ICC '07. IEEE International Conference on*, 24-28 June 2007, pp. 1570–1575.

[102] E. Linda Dacey, *Operations and Algebraic Thinking Leveled Problems: Division and Equal Groups*, ser. 50 Leveled Math Problems, 2014. [Online]. Available: https://books.google.com.my/books?id=3X5TBAAAQBAJ

[103] Y. Xin, *Conceptual Model-Based Problem Solving: Teach Students with Learning Difficulties to Solve Math Problems*, ser. SpringerLink : Bücher. SensePublishers, 2013. [Online]. Available: https://books.google.com.my/books?id=7c5JAAAAQBAJ

[104] Types of multiplication and division problems. Www.math.ccsu.edu/mitchell/multiplicationanddivision.pptx, Jan 14 2015.

[105] R. Antonius, *Interpreting Quantitative Data with SPSS*. SAGE Publications, 2003. [Online]. Available: https://books.google.com.my/books?id=H1_mH0glk0IC

[106] C.-M. Bao, "Intrusion detection based on one-class svm and snmp mib data," in *Proc. Fifth International Conference on Information Assurance and Security IAS '09*, vol. 2, Aug. 18–20, 2009, pp. 346–349.

[107] M. Amezziane, E. Al-Shaer, and M. Ali, "On stochastic risk ordering of network services for proactive security management," in *Network Operations and Management Symposium (NOMS), 2012 IEEE*, April 2012, pp. 994–1000.

[108] Z.-Y. Li, C.-H. Xie, R. Tao, H. Zhang, and N. Shi, "A network security analysis method using vulnerability correlation," in *Natural Computation, 2009. ICNC '09. Fifth International Conference on*, vol. 1, Aug 2009, pp. 17–21.

[109] L. Bhebhe, "Mobility management issues in heterogeneous mobile wireless networks," in *Globecom Workshops (GC Wkshps), 2012 IEEE*, Dec 2012, pp. 787–791.

[110] E. Wonghirunsombat, T. Asawaniwed, V. Hanchana, N. Wattanapongsakorn, S. Srakaew, and C. Charnsripinyo, "A centralized management framework of network-based intrusion detection and prevention system," in *Computer Science and Software Engineering (JCSSE), 2013 10th International Joint Conference on*, May 2013, pp. 183–188.

[111] P. Goyal, R. Mikkilineni, and M. Ganti, "Fcaps in the business services fabric model," in *Enabling Technologies: Infrastructures for Collaborative Enterprises, 2009. WETICE '09. 18th IEEE International Workshops on*, 2009, pp. 45–51. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5159212

[112] S. Jacobs, "Introduction," in *Security Management of Next Generation Telecommunications Networks and Services*. Wiley-IEEE Press, 2014.

[113] D. C. Lee, B. Park, K. E. Kim, and J. J. Lee, "Fast traffic anomalies detection using snmp mib correlation analysis," in *Proc. 11th International Conference on Advanced Communication Technology ICACT 2009*, vol. 01, Feb. 15–18, 2009, pp. 166–170.

[114] E. Harahap, J. Wijekoon, R. Tennekoon, F. Yamaguchi, S. Ishida, and H. Nishi, "A router-based management system for prediction of network congestion," in *Advanced Motion Control (AMC),2014 IEEE 13th International Workshop on*, 2014, pp. 398–403. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6823315

[115] G. Xilouris, G. Gardikis, K. Sarsembagieva, and A. Kourtis, "Snmp-driven active measurements in diffserv networks," in *Communications (ICC), 2013 IEEE International Conference on*, 2013, pp. 2545–2549. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6654917

[116] G. Gardikis, K. Sarsembagieva, G. Xilouris, and A. Kourtis, "An snmp agent for active in-network measurements," in *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2012 4th International Congress on*, 2012, pp. 302–307. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6459684

[117] T. Kazaz, M. Kulin, E. Kaljic, and T. Carsimanovic, "One approach to the development of custom snmp agents and integration with management systems," in *MIPRO, 2012 Proceedings of the 35th International Convention*, 2012, pp. 557–561. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6240708

[118] E. Barka, F. Sallabi, and A. Hosani, "Managing access and usage controls in snmp," in *Computing, Communications and Applications Conference (ComComAp), 2012*, 2012, pp. 41–47. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6154000

[119] A. Adya, P. Bahl, R. Chandra, and L. Qiu, "Architecture and techniques for diagnosing faults in ieee 802.11 infrastructure networks," in *MobiCom '04: Proceedings of the 10th annual international conference on Mobile computing and networking*. New York, NY, USA: ACM, 2004, pp. 30–44.

[120] J. Yeo, M. Youssef, and A. Agrawala, "A framework for wireless lan monitoring and its applications," in *WiSe '04: Proceedings of the 3rd ACM workshop on Wireless security*. New York, NY, USA: ACM, 2004, pp. 70–79.

[121] P. Bahl, R. Chandra, J. Padhye, L. Ravindranath, M. Singh, A. Wolman, and B. Zill, "Enhancing the security of corporate wi-fi networks using dair," in *MobiSys '06: Proceedings of the 4th international conference on Mobile systems, applications and services*. New York, NY, USA: ACM, 2006, pp. 1–14.

[122] W. Wei, S. Jaiswal, J. Kurose, and D. Towsley, "Identifying 802.11 traffic from passive measurements using iterative bayesian inference," in *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*, April 2006, pp. 1–12.

[123] U. Deshpande, T. Henderson, and D. Kotz, "Channel sampling strategies for monitoring wireless networks," in *Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, 2006 4th International Symposium on*, April 2006, pp. 1–7.

[124] S. Shetty, M. Song, and L. Ma, "Rogue access point detection by analyzing network traffic characteristics," in *Military Communications Conference, 2007. MILCOM 2007. IEEE*, 29-31 Oct. 2007, pp. 1–7.

[125] L. Watkins, R. Beyah, and C. Corbett, "A passive approach to rogue access point detection," in *Proc. IEEE Global Telecommunications Conference GLOBECOM '07*, Nov. 26–30, 2007, pp. 355–360.

[126] P. Asadoorian, "Using nessus to discover rogue access points," 2014. [Online]. Available: http://www.tenable.com/blog/using-nessus-to-discover-rogue-access-points

[127] R. Pacchiano, "How to track down rogue wireless access points," 2006. [Online]. Available: http://www.smallbusinesscomputing.com/webmaster/article.php/3590656/How-to-Track-Down-Rogue-Wireless-Access-Points.htm

[128] G. Shivaraj, M. Song, and S. Shetty, "A hidden markov model based approach to detect rogue access points," in *Proc. IEEE Military Communications Conference MILCOM 2008*, 16–19 Nov. 2008, pp. 1–7.

[129] E. Chen and M. Ito, "Using end-to-middle security to protect against evil twin access points," in *World of Wireless, Mobile and Multimedia Networks Workshops, 2009. WoWMoM 2009. IEEE International Symposium on a*, 2009, pp. 1 –6.

[130] K. Gao, C. Corbett, and R. Beyah, "A passive approach to wireless device fingerprinting," in *Dependable Systems and Networks (DSN), 2010 IEEE/IFIP International Conference on*, 282010-july1 2010, pp. 383 –392.

[131] M. Rodrig, C. Reis, R. Mahajan, D. Wetherall, and J. Zahorjan, "Measurement-based characterization of 802.11 in a hotspot setting," in *E-WIND '05: Proceedings of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis*. New York, NY, USA: ACM, 2005, pp. 5–10.

[132] S. Jana and S. K. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," in *MobiCom '08: Proceedings of the 14th ACM international conference on Mobile computing and networking*. New York, NY, USA: ACM, 2008, pp. 104–115.

[133] H. Han, B. Sheng, C. C. Tan, Q. Li, and S. Lu, "A timing-based scheme for rogue ap detection," vol. 22, no. 11, pp. 1912–1925, 2011.

[134] H. Han, F. Xu, C. C. Tan, Y. Zhang, and Q. Li, "Defending against vehicular rogue aps," in *Proc. IEEE INFOCOM*, 2011, pp. 1665–1673.

[135] C. Yang, Y. Song, and G. Gu, "Active user-side evil twin access point detection using statistical techniques," vol. 7, no. 5, pp. 1638–1651, 2012. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6236067

[136] S. Vanjale and P. Mane, "A novel approach for elimination of rogue access point in wireless network," in *India Conference (INDICON), 2014 Annual IEEE*, 2014, pp. 1–4. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7030418

[137] G. Qu and M. Nefcy, "Rapid: An indirect rogue access points detection system," in *Performance Computing and Communications Conference (IPCCC), 2010 IEEE 29th International*, 2010, pp. 9 –16.

[138] A. Ahmad, S. Hassan, and M. H. Omar, "Inbound time stamping for detecting rogue access point," in *Proc. International Conference on Computing and Informatic (ICOCI13)*, 2013. [Online]. Available: http://www.icoci.cms.net.my/proceedings/2013/PDF/PID113.pdf

[139] T. CarstensZola and G. Harris, "Programming with pcap," 2014. [Online]. Available: http://www.tcpdump.org/pcap.html

[140] Z. Xiaohui, C. Shuqiao, and L. Ping, "On traffic characteristics and low-cost router design," in *Multimedia Information Networking and Security, 2009. MINES '09. International Conference on*, vol. 1, Nov 2009, pp. 268–272.