

Rogue Access Point Detector in UTAR Campus

By

Kok Ser Leen

A REPORT

SUBMITTED TO

Universiti Tunku Abdul Rahman

in partial fulfillment of the requirements

for the degree of

BACHELOR OF INFORMATION TECHNOLOGY (HONOURS)

COMMUNICATIONS AND NETWORKING

Faculty of Information and Communication Technology

(Kampar Campus)

JANUARY 2024

REPORT STATUS DECLARATION FORM

Title: Rogue Access Point Detector in UTAR Campus

Academic Session: Year 3 Trimester 3

I KOK SER LEEN

(CAPITAL LETTER)

declare that I allow this Final Year Project Report to be kept in

Universiti Tunku Abdul Rahman Library subject to the regulations as follows:

1. The dissertation is a property of the Library.
2. The Library is allowed to make copies of this dissertation for academic purposes.



(Author's signature)

Verified by,



(Supervisor's signature)

Address:

1561, Jalan Seksyen 1/6, _____

Taman Bandar Barat, 31900, __

Kampar, Perak _____

Puan Nor' Afifah Binti Sabri

Supervisor's name

Date: 19/4/2024 _____

Date: 19/4/2024 _____

Universiti Tunku Abdul Rahman			
Form Title : Submission Sheet for FYP			
Form Number: FM-IAD-004	Rev No.: 0	Effective Date: 21 JUNE 2011	Page No.: 1 of 1

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

UNIVERSITI TUNKU ABDUL RAHMAN

Date: 19 April 2024

SUBMISSION OF FINAL YEAR PROJECT

It is hereby certified that **Kok Ser Leen** (ID No: **20ACB01907**) has completed this final year project entitled "**Rogue Access Point Detector in UTAR Campus**" under the supervision of **Puan.Nor 'Afifah Binti Sabri** (Supervisor) from the Department of **Computer and Communication Technology**, Faculty of **Information and Communication Technology**, and **Dr. Adeb Ali Mohammed Ahmed Al-Samet** (Co-Supervisor) from the Department of **Computer and Communication Technology**, Faculty of **Information and Communication Technology**.

I understand that University will upload softcopy of my final year project in pdf format into UTAR Institutional Repository, which may be made accessible to UTAR community and public.

Yours truly,



(*Kok Ser Leen*)

DECLARATION OF ORIGINALITY

I declare that this report entitled “**ROGUE ACCESS POINT DETECTOR IN UTAR CAMPUS**” is my own work except as cited in the references. The report has not been accepted for any degree and is not being submitted concurrently in candidature for any degree or other award.

Signature :  _____

Name : _____ Kok Ser Leen _____

Date : _____ 19/04/2024 _____

ACKNOWLEDGEMENTS

I would like to show my appreciation to my supervisor, Puan Nor 'Afifah Binti Sabri and my moderator, Dr Adeb Ali Mohammed Ahmed Al-Samet for evaluating this project of mine. I want to thank sincerely to my supervisor for helping me and provide guidance throughout the period of my final year project in order to complete this particular report.

I would also like to thank my coursemate and friend Lee Chiew Min for sharing the required hardware with me in order to do this particular project and also providing me transport to travel from my hostel to the campus.

ABSTRACT

In the current digital era, network security is an essential concern, especially given the growing usage of wireless networks. In contrast, network security may be vulnerable to rogue access points and unauthorised wireless access points that provide security threats. As wireless network technology constantly grows and evolves at a rapid pace, the use of this technology in various sectors including tertiary institutions is notably inevitable. The rapid growth and evolution of wireless network technology has improved the quality of life of delivering data and the flexibility of using such technology, however, it has indefinitely also introduced new security challenges in particular the threat of Rogue Access Points (RAP). In addition, this project introduces an intelligent algorithm for RAP detection and an additional isolation feature, if implemented, it is expected to safeguard the internal network of the institutions from unauthorised intruders to gain private insights of the network. Additionally, a preliminary analysis of potential network security vulnerabilities will be carried out and the most recent research on RAP will be analysed and compared with the suggested method in a literature review. As a result, while creating a framework to reduce the threat of rogue access points in tertiary institutions, the idea of employing the proposed technique to do so may be taken into account.

TABLE OF CONTENTS

TITLE PAGE	i
REPORT STATUS DECLARATION FORM	ii
FYP THESIS SUBMISSION FORM	iii
DECLARATION OF ORIGINALITY	iv
ACKNOWLEDGEMENTS	v
ABSTRACT	vi
TABLE OF CONTENTS	vii
LIST OF FIGURES	x
LIST OF TABLES	xii
LIST OF ABBREVIATIONS	xiii
CHAPTER 1 INTRODUCTION	1
1.1 Problem Statement and Motivation	1
1.2 Project Scope	2
1.3 Project Objectives	3
1.4 Contributions	4
1.5 Background Information	5
CHAPTER 2 LITERATURE REVIEW	7
2.1 Access Point	7
2.1.1 Access point vs Router	8
2.2 Scanning	8
2.3 Previous work on hidden RAP detection technique for WLAN	8
2.3.1 Strengths and Weaknesses	10
2.4 Previous work on a novel approach for rogue access point detection on the client-side	10
2.4.1 Strengths and Weaknesses	12
2.5 Previous work on detection and isolation of rogue access point	13

2.5.1 Strengths and Weaknesses	14
2.6 Previous study on detection of fake wireless access points	15
2.6.1 Strengths and Weaknesses	17
2.7 Previous study on rogue access point detection by using ARP failure under the MAC address duplication	18
2.7.1 Strengths and Weaknesses	19
2.8 Previous study on Rogue Access Point Detection by Analysing Network Traffic Characteristics	20
2.8.1 Strengths and Weaknesses	21
2.9 Comparison the proposed method with the previous studies	22
CHAPTER 3 SYSTEM METHODOLOGY/APPROACH	24
3.1 Software Development Life Cycle	24
3.2 System Design	25
3.2.1 System Architecture Diagram	25
3.2.2 Use Case Diagram	26
CHAPTER 4 SYSTEM DESIGN	27
4.1 System Flowchart	27
4.2 Sequence Diagram	28
CHAPTER 5 SYSTEM IMPLEMENTATION	30
5.1 Hardware	30
5.2 Software	31
5.3 Setting and Configuration	31
5.3.1 Setting up the virtual box for the virtual machine at Oracle VM VirtualBox	32
5.3.2 Installing the Kali-Linux virtual machine	35
5.4 System Operation	44
5.4.1 Interface	44
5.4.2 Scenario without RAPs	44

5.4.3	Scenario with RAP	46
5.5	Implementation Issues and Challenges	48
CHAPTER 6 SYSTEM EVALUATION AND DISCUSSION		50
6.1	System Evaluation	50
6.1.1	Detection Accuracy	51
6.1.2	Response Time	51
6.1.3	Scalability	51
6.1.4	Resource Utilisation	52
6.1.5	Incident Handling	52
6.2	Project Challenges	52
6.3	Objectives Evaluation	53
CHAPTER 7 CONCLUSION & RECOMMENDATIONS		55
7.1	Conclusion	55
7.2	Recommendations	56
REFERENCES		58
APPENDIX A		61
1.	Interface	A-1
2.	Output file (Scan)	A-3
3.	Output file (Detect)	A-3
4.	Whitelist	A-3
5.	Screenshot (JiiCAS Award)	A-3
6.	Certificate (JiiCAS Award)	A-4
POSTER		
FINAL YEAR PROJECT WEEKLY REPORT		
PLAGIARISM CHECK RESULT		
CHECK LISTS		

LIST OF FIGURES

Figure Number	Title	Page
Figure 2.1	First experimental model	9
Figure 2.2	Second experimental model	9
Figure 2.3	The system's algorithm	12
Figure 2.4	Traditional network vs. SDN network	14
Figure 2.5	Scenario setup	16
Figure 2.6	Flowchart of the previous proposed system	18
Figure 3.1	Agile SDLC	24
Figure 3.2	System Architecture Diagram	26
Figure 3.3	Use Case Diagram	26
Figure 4.1	System Flowchart	28
Figure 4.2	Sequence Diagram	29
Figure 5.1	New VirtualBox	32
Figure 5.2	Create Virtual Machine	32
Figure 5.3	Create Virtual Machine (Memory size)	33
Figure 5.4	Create Virtual Machine (Hard disk)	33
Figure 5.5	Create Virtual Hard Disk	34
Figure 5.6	Create Virtual Hard Disk (Storage on physical hard disk)	34
Figure 5.7	Create Virtual Hard Disk (File location and size)	35
Figure 5.8	Installer menu	35
Figure 5.9	Select language	36
Figure 5.10	Select location	36
Figure 5.11	Configure keyboard	37
Figure 5.12	Hostname	37
Figure 5.13	Domain name	38
Figure 5.14	Full name	38
Figure 5.15	Username	39
Figure 5.16	Password	39

Figure 5.17	Configure clock	40
Figure 5.18	Partition disks (method)	40
Figure 5.19	Partition disks (select disk)	41
Figure 5.20	Partition disks (scheme)	41
Figure 5.21	Partition disks (overview)	42
Figure 5.22	Partition disks (Changes)	42
Figure 5.23	Install the GRUB boot loader	43
Figure 5.24	Install the GRUB boot loader (installation)	43
Figure 5.25	Interface	44
Figure 5.26	Setting up the access point	44
Figure 5.27	Start detector result without RAP	45
Figure 5.28	History without RAP	46
Figure 5.29	Setting up the RAP	46
Figure 5.30	Start detector result with RAP	47
Figure 5.31	SMS alert	47
Figure 5.32	History with RAP	48
Figure 6.1	Example of the system testing topology	50

LIST OF TABLES

Table Number	Title	Page
Table 5.1	Specifications of the laptop	30
Table 5.2	Specifications of the wireless USB adapter	31

LIST OF ABBREVIATIONS

<i>RAP</i>	Rogue Access Point
<i>MITM</i>	Man-in-the-Middle
<i>SSID</i>	Service Set Identifier
<i>BSSID</i>	Basic Service Set Identifier
<i>LAN</i>	Local Area Network
<i>SDN</i>	Software-Defined Networking

CHAPTER 1

Introduction

In this chapter, we will delve into the problem statement and motivation of this project, project scope and objectives, the contribution of the project as well as some background information.

1.1 Problem Statement and Motivation

In modern network environments, the proliferation of Rogue Access Points presents a significant security challenge, as unauthorized wireless devices are introduced into the network infrastructure without proper authentication or oversight. These rogue devices not only undermine network integrity but also expose sensitive data to potential breaches, leading to compromised confidentiality, integrity, and availability of critical resources. Addressing this threat requires effective detection, mitigation, and prevention strategies to safeguard organizational assets and maintain network security [27]. Moreover, it is impossible to disregard the damage a rogue AP may cause since it is so enormous. As hacker may carry out a man-in-the-middle attack via rogue APs, the attackers can give victims the impression of them speaking privately with one another but in reality, the attackers have already established a separate connection with the victims' transmitting messages between them and having complete control of the conversation. Moreover, rogue APs send bogus SSIDs that promote alluring extras like unrestricted Internet access. The false SSID is added to the client's wireless configurations after a user connects, and the client starts broadcasting the phoney SSID, infecting additional clients and also provides a channel for data theft to compromise company information [13]. A rogue AP isn't usually the result of an employee with good intentions and it may be set up by a malicious party who is aware that this router has the potential to serve as an access point in the future. However, the security risk is the same regardless of the intention. In short, with the increasing prevalence of wireless access points in various settings, the potential for rogue access points cannot be ignored as it can cause significant damage such as man-in-the-middle attacks, data theft and the spreading of false SSIDs. Whether the rogue APs are set up by well-intentioned employees or other malicious parties, the requirement for a diligent monitoring and

detection system is necessary as the security risks posed by rogue APs are significant and could cause significant damage to and potential breaches of company information and network security [14].

This provokes the motive to solve the issues that are posed by rogue APs to safeguard and minimise the presence and potential growing scale of rogue APs in the future. In the real world, rogue access points may be disguised or in an awkward location which makes it difficult for network administrators to identify or minimise the security concerns they pose. Like any other network environment, tertiary institutions have a fundamental requirement for an efficient and smart detection algorithm developed particularly for the institution's network. The suggested technique tries to address this issue by creating a unique detection algorithm that can quickly and accurately find rogue access points that are concealed or inconveniently placed or those that have their SSID broadcast turned off. Moreover, the motivation to improve network security at tertiary institutions by put out a brand new intelligent rogue access point detection with isolation as an extra feature method, this algorithm is expected to help network administrators to increase their detection skills, protect against possible data breaches and lower the risk of damage that it will cause to the institutions.

1.2 Project Scope

The project scope covers the development of a new smart rogue access point detection with the isolation feature as an extra feature for the algorithm. If such an algorithm is developed and implemented in tertiary institutions specifically for the UTAR campus network, it is expected to enhance its network security and also to unload some tasks for the network administrators and allow them to focus on other more important matters. The development of the system consists of using a combination of hardware and software such as a laptop, Kali-Linux virtual machine, Python etc. Moreover, the scope also includes reviewing the existing research on rogue access point detection features and isolation-related mechanisms. In addition, the process of designing the algorithm including scanning and detecting potential rogue access points as well as an extra feature of isolation mechanism will be carried out. Finally, carry out performance testing and making adjustments to make sure the algorithm is bug-free by evaluating

the accuracy and efficiency. Additionally, the overall project's findings will be documented in a report to provide readers with a structured and easily understandable way for future referencing. On top of that, the focus is on the UTAR campus network and does not cover legal investigation or prosecution. The project does not address any legitimate scenarios and assumes that rogue access points are not set up by any proper authorisation and will pose security risks to an overall network.

1.3 Project Objectives

The project's objectives include creating a new, intelligent detection algorithm for rogue access point that includes an isolation function as a bonus. If such an algorithm is developed and implemented in tertiary institutions specifically for the UTAR campus network, it is expected to efficiently and effectively identify rogue access points that may be hidden, obscurely positioned, or have disabled SSID broadcasts.

The main objectives of the project include developing the 2 main features of the system which are scanning the network to find potential rogue access points and detecting and identifying the hidden rogue access points on the network. Moreover, the objective also includes developing an extra feature which is after detecting and identifying the rogue access point, the system can isolate the rogue access point by utilising an isolation mechanism. The proposed objectives and features are expected to be completed by using a combination of hardware and software such as a laptop that is capable and compatible with running the Kali-Linux virtual machine and the algorithm will be coded by using the programming language of Python.

Other miscellaneous features will also be developed such as looking at the past detected network(s) and rogue access point(s). Nevertheless, performing testing to test the effectiveness of the algorithm and the accuracy of detecting rogue access points to minimise the potential bugs in the algorithm is also part of the project objective. In short, to strengthen rogue access point detection skills and protect against potential network security and data confidentiality breaches, network administrators in tertiary institutions are encouraged to take advantage of the project's key findings and practical suggestions. In short, this project aims to achieve the objective as below simplified:

- Develop a detection algorithm for rogue access points (RAPs) targeting the UTAR campus network.
- Implement scanning mechanism to scan the available access points within the network.
- Creating a detection mechanism that implement a whitelist to identify potential rogue access points.
- Incorporate an isolation function as an additional feature to isolate detected RAPs from the network.
- Utilize a combination of hardware and software, such as a laptop running Kali-Linux virtual machine for algorithm development.
- Implement additional features, including reviewing past detected networks and RAPs.

1.4 Contributions

The main contribution of this project is no other than the development of a rogue access point smart detection system that has an isolation feature as a bonus to comprehend the inevitable and rising use of wireless networks has introduced many new security threats one of which is rogue access points if such an algorithm is developed and implemented in tertiary institutions specifically for the UTAR campus network, it is expected to efficiently and effectively identify rogue access points that may be hidden, obscurely positioned, or have disabled SSID broadcasts. Moreover, a rogue access point can serve as an entry point for other threats like malware distribution, man-in-the-middle attacks and phishing attacks if it successfully intrudes into the internal network of an organisation by implementing this system, it can halt the snowball effect that a rogue access point can impose. Furthermore, this system also aims to contribute to data protection where rogue access points often appear as authorised and legitimate access points which can fool many innocent employees and even other systems within an organisation to provide certain private and confidential data to the attackers. Additionally, this system can also help organisations and network administrators improve their overall security measures to proactively mitigate against threats that are hard to identify, minimising the potential of security incidents from happening.

The importance of this proposed system cannot be underestimated as it helps organisations to maintain network security posture by the advanced rogue access point detection capabilities it has to ensure network administrators do not overlook covert threats like a rogue access point. Moreover, preventing any escalating damage at the earliest stage of an attack attempt is game-changing as the financial impact of a network attack can reach an absurd level which will be out of control by the time of spotting and realising the threat. In addition, this system also can consolidate the overall network security reputation of an organisation such as UTAR. In contrast, when rogue access points successfully compromise security, the institution's position with students, employees, partners and stakeholders may suffer. This is where the proposed system can also contribute to maintaining a good reputation for institutions and organisations as an accountable guardian of private data and digital assets by preventing such breaches.

1.5 Background Information

The rogue access point is a wireless access point that has been installed on a network's wired infrastructure without the permission of network administrators or owners, allowing unauthorized wireless access and appearing to be legitimate to the network's wired infrastructure. Moreover, it has been used together with several attacks including malware distribution, man-in-the-middle attacks and phishing attacks, which can have a significant impact on victims like data breaches, monetary losses and damage to reputation. However, many more rogue APs—known as soft access points—are set up by employees who seek unrestricted wireless access [21]. There are other rogues accessing the network for free access in the vicinity. These access points are frequently low-cost and consumer-grade, and they can only be found in the air. They frequently do not broadcast their presence over the wire. Authentication and encryption are not enabled since they are frequently deployed in their default state, posing a security risk. A wireless LAN access point that is connected to the network is the ideal target for war driving since wireless LAN signals may pass through building barriers. Because it circumvents the authorised security measures, each client that connects to a rogue access point must be regarded as a rogue client.

CHAPTER 1

Let's reconsolidate the field of the project which revolves around network security and the increasingly complex difficulties that organisations like UTAR confront. As the number of users of wireless networks rapidly evolves in today's world, wireless networks have already become an essential aspect of daily operations due to the fact that they allow convenient and flexible communication and data transfer. However, the convenience that wireless networks provide also imposes a rising threat which is rogue access points. Unauthorised network intruders can expose a network to a variety of cybersecurity vulnerabilities, ranging from data theft to sophisticated attacks as a result [22].

Before diving further into this piece of document, let's clarify some fundamental terms. Firstly, rogue access points (RAPs) are unauthorised wireless access points that can jeopardise network security. These rogue APs are typically set up by malicious persons to broadcast either a fake network name or MAC address, making them difficult to identify. Moreover, the 'SSID' or 'Service Set Identifier' is the network's name and a critical wireless network component this is because when a device joins a wireless network, it uses the SSID to identify itself. Furthermore, a Man-in-the-Middle attack refers to an attack that happens between the communication of two victims where the attacker intercepts the communication [23].

CHAPTER 2

Literature Reviews

2.1 Access Point

In today's ever-evolving technological environment, we need to appreciate the creation of access points that can provide us with the ability to surf the internet wirelessly by acting as intermediate devices to bridge wireless devices like smartphones, laptops or tablets to connect to the internet and access the resources that are in the wired infrastructure of the network. Moreover, access points create the possibility for clients to connect to the internet and share data wirelessly by facilitating wireless communications by transmitting and receiving data between the wireless client and the wired network. Access points are usually used in a specific area or location to provide wireless connectivity like offices, airports or public spaces [12].

Furthermore, referring to [11], the components in access points contain one or more radios which are onboard computer and one or more wired network port that can help the device to provide connected devices with wireless connection by receiving and transmitting radio waves depending on the specific wireless standards and the radio frequencies. The onboard computer in the access point is the main component that serve as a bridge for facilitating the communication between the wireless network created by the AP and the connected wired network. Data that are transmitted by the connected devices in the wireless network is relayed through the access point to the wired network and vice versa.

2.1.1 Access Point vs Router

Let's understand the difference between the router and the access point. Starting off, routers are network devices that serve as a central hub in a network and can provide routing functions that help connect devices to the internet with the most efficient path but the connected devices are limited and usually small in number compared to access points. In contrast, access points are another network device although, without any routing functions, they can help extend the wireless coverage of the existing network

to provide internet access for a larger number of users in an area through Wi-Fi converting the wired signal into a wireless one [4].

2.2 Scanning

Prior to this project, various network scanning tools have been developed in the wireless network management and security field to help network administrators make a better effort to monitor the network like nearby access points and connected devices. One of the methods is the command-line tool which is Airodump-ng. This tool actively scans the available channels or packets within the vicinity preferably while it is in monitor mode [1]. Moreover, this tool can provide useful information like the SSID, BSSID, signal and type of encryption during or after the scan. Similarly, Wireshark is another network scanner that is proficient and also has the ability to provide network administrators with the critical information needed such as SSIDs, MAC addresses, signal strengths, encryption methods and some potential hidden networks by scanning and capturing packets in the network from various network interfaces [5]. In order to provide similar efforts that these existing methods offer, this project looks forward to also develop a comprehensible scanning function.

2.3 Previous work on hidden RAP detection technique for WLAN

[2] proposed a study on the detection technique for WLAN particularly for the hidden rogue access points. In this previous study, the researcher considers the importance of the beacon frames similar to [7] as it is the frame that is broadcasted by an access point at regular intervals. Beacon frames consist of the information of the access point including the important items such as the SSID and BSSID which is the unique layer 2 MAC address. Moreover, the research focuses on detecting the hidden rogue access points instead of the usual rogue access points where the hidden ones usually have their SSID remain stealth and not broadcasted. The proposed technique of this research using the information obtained from the beacon frame the BSSID which is the MAC address of the access points can be used to differentiate the legitimate and rogue access points. Furthermore, to investigate the SSID of the hidden RAP, the technique relies on the probe request frame where the key insight is that both rogue and legitimate access

points have the same tag length size in their frames despite the hidden SSID. On top of that, the study also proposed two scenarios where the first is both legitimate and rogue APs having the same BSSID but different SSIDs and the second is both APs having the same SSID but different BSSIDs. The figures below show the experimental model for each scenario.

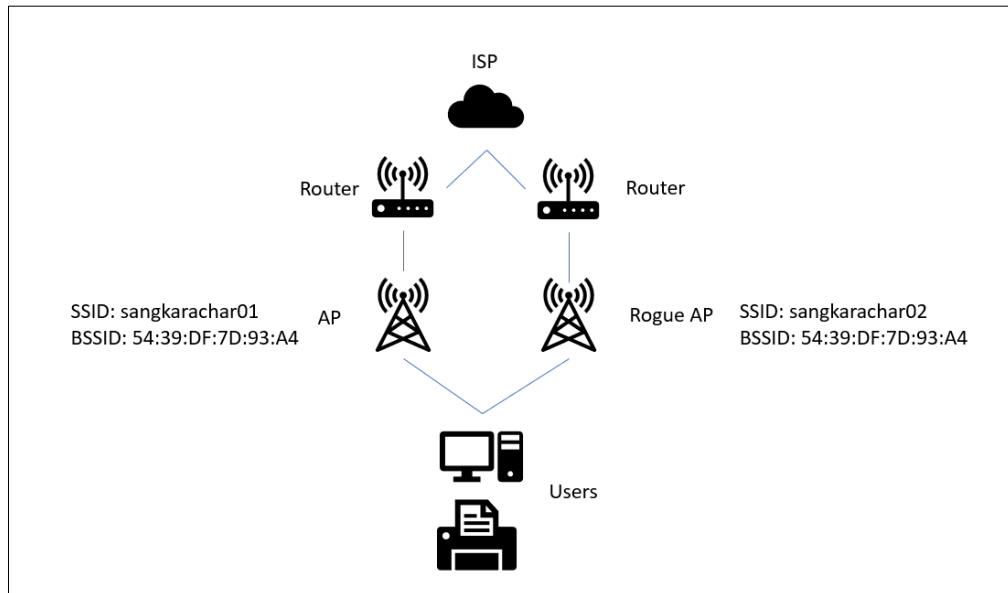


Figure 2.1 First experimental model

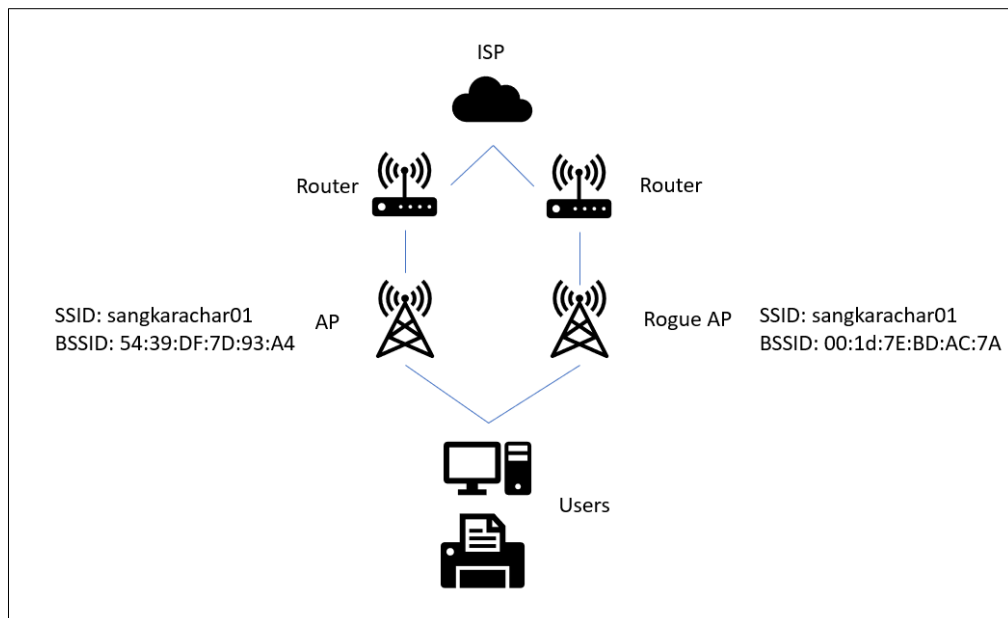


Figure 2.2 Second experimental model

2.3.1 Strengths and Weakness

This proposed technique from the previous research has its strength in its ability to detect concealed rogue access points even when the SSID is not published. This can be supported by the fact that the technique compares the information of the legitimate AP's beacon frame with the probe request information sent from the client as it checks for discrepancies or patterns that lead to the presence of rogue access points. It detects hidden rogue access points that have the same tag length as authorised access points but missing the SSID information. Moreover, the researcher also focuses on referencing the MAC address or BSSID for both legitimate and rogue APs where MAC addresses are globally unique for all access points. The approach is able to detect the presence of disguised rogue access points even if the SSID is not broadcast by actively comparing MAC addresses in beacon frames and probe request frames. As hidden rogue points are more dangerous and pose a serious security threat by their stealthy ability to conceal themselves to better compromise network security, this research specifically addressing this issue can play a crucial role in improving modern network security.

While this proposed technique has its strengths, it also has some potential weaknesses. This technique relies on the beacon and probe request frames which can be a problem sometimes when there are network congestions, interference or other network problems that can cause these frames to not be present. Other than that, the technique relies on MAC address-based detection where it could be a problem if a skilful attacker is aware of it and could potentially evade the detection. Nonetheless, every detection technique has its own unique strengths and inevitable flaws. By studying and referencing this previous research the strengths and weaknesses are carefully noted down in which to help improve this current piece of research and future studies.

2.4 Previous work on a novel approach for rogue access point detection on the client-side

[8] proposed another study on the detection of the rogue access point on the client with a novel approach. In this piece of literature, the researcher implements an approach that

CHAPTER 2

uses IP addresses as a technique to differentiate legitimate access points from potential rogue access points. The technique first begins with the comparison of both access points' IP addresses that are broadcasting the same SSID and MAC address. This is important where it is to access the similarity of the access points when both IP addresses are equal but the trace routes are different this could mean that it can potentially be an evil twin attack. Moreover, the proposed technique also compares the network IDs by calculating the network ID based on the IP classes, this serves as another factor to determine the legitimate access point from the rogue one as the same network IDs indicate that it is set up from the same network commonly for load balancing purpose. Nonetheless, the researcher also proposed that a traceroute comparison will be conducted to identify if there are any extra hops in the network path if both IP addresses and network IDs are different. This is because the presence of an extra hop could indicate that there is a Man-in-the-Middle attack going on where the unauthorised device intercepted the network traffic. The figure below shows the algorithm that is proposed by the researcher.

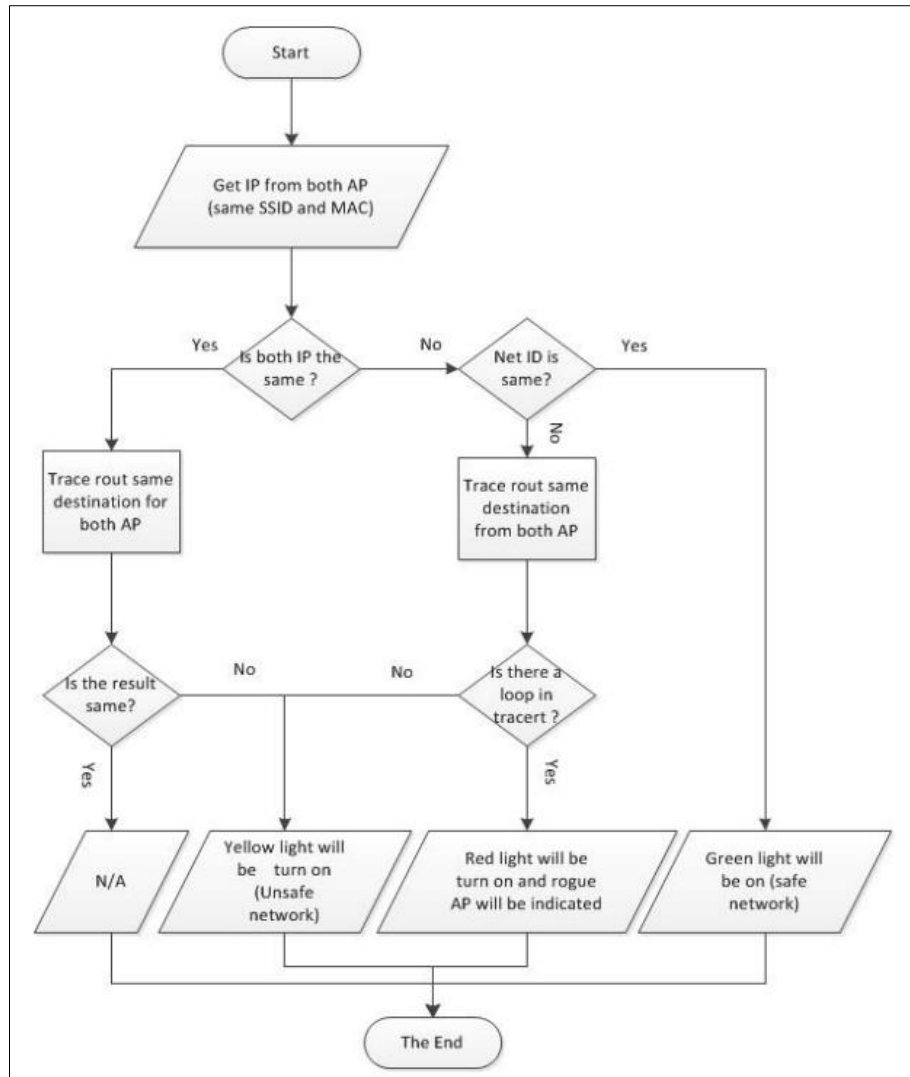


Figure 2.3 The system's algorithm

2.4.1 Strengths and Weakness

The strength of this proposed technique lies in the utilisation of traceroute comparison as the crucial component in differentiating legitimate access points from rogue ones. The traceroute comparison is particularly useful for scenarios that involve Man-in-the-Middle (MITM) attacks and evil twin attacks. In addition, MITM attacks usually occur when the attacker intercepts the communication between two parties with an unauthorised device resulting in an extra hop in the network path when compared to the legitimate access point. Moreover, it is very difficult to fake a network path even for a very skilled attacker therefore, complementing the IP address and network ID comparisons could provide a comprehensive approach to detecting RAPs and

significantly improve the detection process. Other than that, the technique's approach to traceroute comparison is fairly consistent as it is adaptive to many network configurations and changes, even if IP addresses are dynamically configured.

On the other hand, there are also some weaknesses present in this previous research where if the attacker were able to successfully spoof the IP address of a legitimate network device, it can very likely bypass the system detection. Additionally, the technique initially compares the IP addresses can cause the system to falsely identify the rogue access point as legitimate if the attacker were able to spoof the IP address of the legitimate one, thus, if this technique has also incorporated the proposed technique in [], the system might be able to overcome this issue. With that being said, this technique still provides some valuable insights by looking at its various strengths and weaknesses that hope to improve the current research on RAP detection.

2.5 Previous work on detection and isolation of rogue access point

In recent years, increasing attention has been gained to creating technologies that can efficiently identify and remove rogue devices from networks. However, the inability of traditional networks to swiftly adapt to shifting security requirements has prompted researchers in [3] to consider the adoption of Software-Defined Networking (SDN)-based networks for this purpose. SDN networks are a desirable option for applying security measures since they have benefits like simple software configuration and reconfiguration. The SDN technology consists of an SDN controller that controls and manages the traffic flow of devices on a network and one or more switches that are responsible for receiving, processing, and forwarding the packets to their destination. In previous studies, the detection and isolation of attackers have been simulated in network environments and investigated from networks using SDN networks in conjunction with emulator tools such as the Mininet-WiFi platform which is a well-liked emulator tool for simulating SDN networks, enabling researchers to build and test virtual SDN networks. Researchers have a flexible and scalable environment for evaluating security solutions in SDN-based networks via the usage of Mininet-WiFi. The research suggests building an SDN network on the Mininet-WiFi platform, concentrating on developing tools and enforcing policies to identify and remove rogue

devices from the network. By utilising the benefits of SDN technology, the study attempts to provide an efficient system for identifying and isolating rogue devices from an SDN-based network particularly its flexibility and agility, in combination with emulation tools like Mininet-WiFi. Figure 2.4 shows the difference between an SDN network and a traditional network.

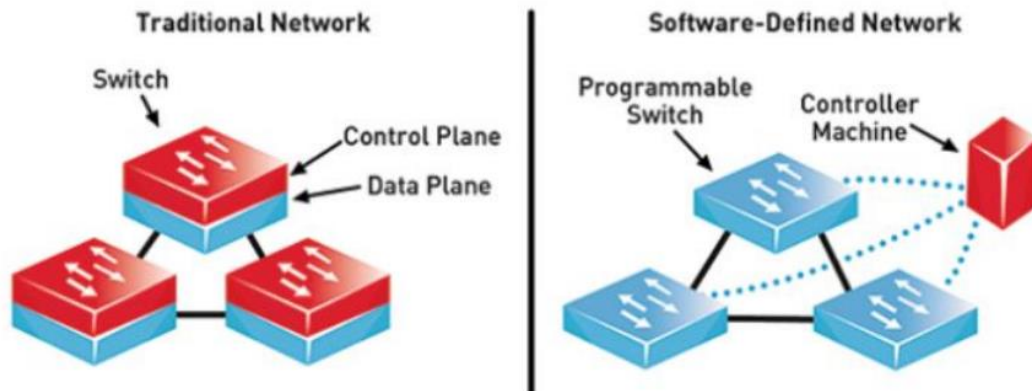


Figure 2.4 Traditional network vs. SDN network

2.5.1 Strength and Weakness

A convincing strategy for increasing network security, an SDN-based solution for identifying and isolating rogue devices from a network provides a number of advantages. First, SDN networks are more flexible compared to traditional networks since the network administrator can quickly modify the software and adjust network policies to suit the requirements of the organisation. As threats change, security measures may be updated and adjusted quickly as a result. SDN networks may also be heavily programmed, allowing the creation of unique software programs and rules to carry out certain security measures. This enables the development of sophisticated security methods and offers fine-grained control over network behaviour [6]. Additionally, a central controller is used to administer SDN networks that serve as a single point of control for network setup and management. This lowers the possibility of incorrect setups and inconsistencies by enabling the enforcement of coordinated and uniform security policies throughout the whole network. As centralised monitoring and recording enable real-time analysis of network data, making it simpler to identify aberrant behaviour and possible security concerns, SDN networks' greater visibility into

network traffic and events also helps in the identification of rogue devices [10]. Moreover, SDN networks are also very scalable, making them appropriate for huge networks with a lot of devices and complicated topologies. Due to this, the solution may be used in a range of network contexts [9].

Although there are several benefits of SDN-based solutions, there are also a number of possible drawbacks to take into consideration. First of all, the complexity of setting up and maintaining an SDN-based system. This is because it demands a high level of skill and a specialised understanding of SDN concepts, protocols and technologies. Organisations that lack the resources or knowledge necessary to properly implement and manage SDN networks may find this to be a difficulty [10]. Second, different organisations with different restricted budgets may find it difficult to implement and maintain SDN-based solutions since they may demand a sizable upfront investment in terms of hardware, software and training. SDN networks may also cost more to install and maintain than conventional networks, especially if specialised hardware or proprietary software is needed. Thirdly, because SDN technology is still in its early stages of development, there may be restrictions on the level of standardisation, stability and maturity of SDN protocols and tools. Due to this, the interoperability, compatibility and dependability of SDN-based systems may introduce other problems, particularly in workplaces [9]. Finally, network administrators and IT personnel may have a learning curve while using SDN ideas and technology, demanding further detailed training [3]. Despite the strengths that SDN offers, the weaknesses mentioned above might not be practical to implement in the current proposed method but certain concepts such as the flexibility and scalability of the study can be referenced and noted down.

2.6 Previous study on detection of fake wireless access points

Moreover, researchers in [17] have proposed another method for the detection of rogue access points by combining the abilities of two well-known tools such as Suricata and Kismet which are a comprehensive log in system and monitoring and analysing the wireless network at link layer. In order to fulfill the proposed method, the researchers have created 6 independent modules to meet the requirements. Modules including

CHAPTER 2

wireless interface management which is responsible for controlling connected wireless interface like switching between monitor mode or managed mode for the wireless network card and to handle regular frequency change. Next is a module for scanning the wireless network which is responsible for capturing transmitted frames that are within the range. Furthermore, a frame analysis module is also implemented for filtering captured frames into beacon frames, probe frames and deauthentication frames to create signatures for future analysis and processing. A create signature and fingerprints module is also used to store unique fingerprints based on the created signature. Nevertheless, a signature processing and attack detection module which is a detection algorithm for comparing captured frames and create an alert based on the results obtained in real-time. Finally, a logging information module is used to store and present important information in a log file.

The researchers set up a scenario as shown in figure 2.5 which consists of a legitimate AP, detector, a legitimate user and an attacker. The legitimate AP first broadcasts standard beacon frames to the legitimate user where these beacon frames will be captured by the detector and the unique signatures and fingerprints that consists of the SSID, BSSID, broadcast channel and security setting will be stored into the database for future analysis. Meanwhile, the attacker utilises a network scanning tool to get the signatures of the legitimate AP and store the signatures into its own database. The attacker then creates a rogue access point and starts broadcasting beacon frames with the same signatures and fingerprint of the legitimate AP. After that, the detector was able to detect the same beacon frames with the same signatures as the legitimate AP from the attacker. Finally, an alert is created as a result of the algorithm realised the transmitted signatures do match with the ones in the database.

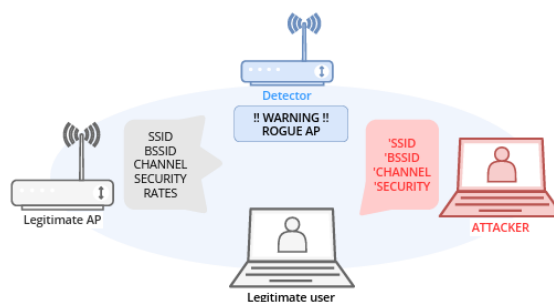


Figure 2.5 Scenario setup

2.6.1 Strength and Weakness

The strength of this previously researched method can be seen by the utilisation of signature-based detection. Similar to other previous research, this research method captures and analyse specific frame like the beacon frame to get information about the SSID and BSSID of the legitimate and comparing it to enhance the accuracy of the detection for any potential rogue access points. Moreover, real-time analysis is implemented in the detection algorithm that allows the capturing of signatures in real-time and immediate response and detection if a potential rogue AP is detected. Furthermore, the consideration of using multiple parameters like SSID, BSSID, Channel, Security, Country and bit rates for creating signatures provides a more comprehensive approach and increases the robustness for the detection of rogue APs. In addition, the proposed method also includes a logging system which is a very useful function that will track important information into a log file for post-incident analysis and forensics examinations.

Despite the strengths that has been mentioned, there are also some weaknesses present in this proposed method. First, the method makes the assumption that legitimate access points always operate consistently where false positives or false negatives could result from any departure from these presumptions. In addition, false positive and false negative rates are not covered in great detail in the study. A more thorough examination of the method's accuracy taking these elements into account would definitely improve the reliability evaluation. Moreover, the single-platform implementation is also one of the drawbacks of this proposed method as the implementation of the function is customised for the Raspberry Pi's ARM architecture. Although useful, it also restricts the flexibility for other platforms' deployment, which might limit its adoption in some settings. Furthermore, the method has a limited discussion on the system's load where low processing requirements are mentioned in passing in the study, but it doesn't go into great length on how the suggested detection method affects the general functionality and available resources of the Raspberry Pi. Although the Raspberry Pi is renowned for its adaptability, its memory and processing capacity are limited. The possible effects of executing the detection system on the Raspberry Pi's overall

performance including any potential effects on other services or apps that may be operating on the device which are not included in the research.

2.7 Previous study on rogue access point detection by using ARP failure under the MAC address duplication

[15] proposed a study on the detection of Rogue Access Points (RAPs) in WiFi networks, with an emphasis on the risk of an Evil Twin Attack. An attacker establishes a Rogue Access Point in a targeted Wi-Fi network using the same Service Set Identifier (SSID) as a Legitimate Access Point (LAP) in an Evil Twin Attack. As part of a Man-in-the-Middle (MITM) attack, the Rogue Access Point can relay traffic through a Legitimate Access Point to intercept confidential client information. Moreover, the proposed approach makes use of Address Resolution Protocol (ARP) failure under MAC address duplication to identify rogue access points. It is predicated on the idea that if duplicate MAC addresses are present on the path from the gateway to the client, the client will not be able to receive ARP reply packets.

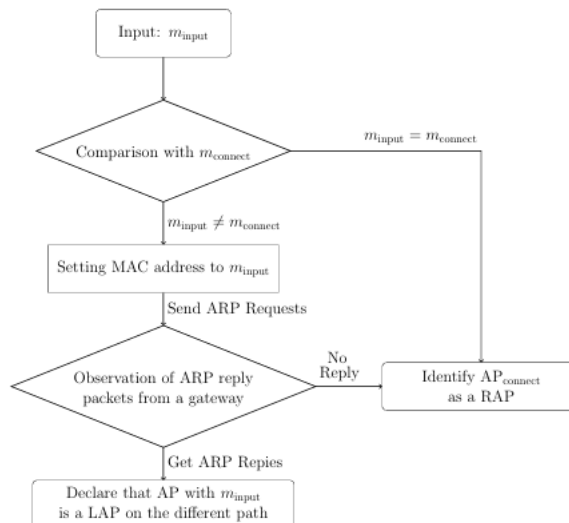


Figure 2.6 Flowchart of the previous proposed system

The algorithm proposed by the researchers in this previous study consists of 2 main sections where the first is MAC address collection to collect MAC addresses of access points with the same SSID as the connected access point. The second section is about the ARP reply based detection which is divided into 3 procedures. In the first procedure, the comparison between the MAC address of the connected AP and the collected MAC

address take place, if it's the same, it indicates that the connected AP can be a potential RAP as it is using the cloned MAC address but if the MAC addresses are different it may suggest that the RAP did not clone the MAC address and proceed to the next procedure. In the second procedure, the system will disconnect the client temporarily and set its MAC address as one of the collected MAC addresses. The client will then try to reconnect by using ARP by sending an automatic request and proceed to the third procedure. The third procedure which is the observation procedure, observe the ARP reply to packets that are destined for the set MAC address will reach the client or not. If the client did not receive any ARP reply, it means that there could be a potential rogue AP in between the legitimate AP and the client associated the MAC address. On the other hand, if client do receive a reply, it implies that there is no potential RAP is presence and repeat the process again with other collected MAC address until there is a potential RAP is detected or declare the connected AP as a legitimate AP if there is none.

2.7.1 Strength and Weakness

This method proposed by previous researchers is a promising approach that however do come with a few strengths and weaknesses. One of the strengths of this approach is that it utilises two-channel approach where in order to reduce channel interference and boost the dependability of the detection technique, two separate channels for communication are used which is the Legitimate Access Point (LAP) and the Rogue Access Point (RAP). Moreover, the detection strategy is based on purposefully disrupting the channel that is used between the LAP and the RAP in order to reduce throughput. It also proposes that the channel be saturated by disrupting extra equipment in the client, which will further lower throughput. If there is a decline, the throughput is used to determine whether a rogue access point is present. Other than that, the study also mentioned that a hardware-based AP was introduced in the previous research, emphasising that the suggested detection system makes use of or takes into consideration the deployment of such specialised hardware. This implies that the hardware-based AP might have some benefits or features that increase the detection scheme's resilience and ability to adjust to various performance levels where the detection system is made to be more applicable by being able to adjust to various

hardware setups. Furthermore, the proposed method also has a focus on the open Wi-Fi networks that is referring to Wi-Fi networks that do not have security in place like WPA2. By concentrating on open Wi-Fi networks, the attack model for detecting rogue access points is made simpler. Since encryption and authentication methods might not be present in open networks, the network is more vulnerable to some kinds of attacks.

On the other hand, there are some weaknesses that are present in the study one of which is real-life limitations where the researchers admit that in practical situations, the technique finds it difficult to identify Rogue Access Points. Variations in network traffic, collisions, changes in network architecture and unwanted interference are some of the elements that impact it. Moreover, although the utilisation of throughput is one of strengths to detect RAPs it can also serve as a double-edged sword this is because the accuracy of detection in dynamic and complex environments can be limited by a variety of network environment characteristics that have a substantial impact on throughput. Furthermore, the proposed method is sensitive to network changes where this weakness shows that a number of variables, such as traffic flow and modifications to the network topology can affect how accurate the detection technique is. The study indicates that several factors, such as modifications to the network environment, influence the scheme's performance significantly in addition to the existence of rogue access points. Changes in the locations of active devices are referred to as traffic mobility, they can have an impact on the throughput and communication pathways that the detection method observes. In addition, changes in the configuration of network components might also result in changes to the topology of the network which could cause irregularities in the detection process.

2.8 Previous study on Rogue Access Point Detection by Analysing Network Traffic Characteristics

In this previous study [16], the researchers proposed a method that uses the characteristics of the network traffic to analyse the presence of potential rogue access points. This proposed approach has two stages where the first stage is the ethernet and WLAN traffic classification and the second stage is the RAP detection phase for the detection of Rogue Access Points (RAPs) and they are both carried out by using a

Network Traffic Analyzer (NTA) at the gateway router to analyse traffic. The objective is to locate possible RAPs in a heterogeneous network with wired and wireless subnets and notify the network administrator about them. In order to determine the difference between hosts connected to Ethernet and WLAN, the NTA examines both incoming and outgoing traffic at the gateway router during the first phase, it is assumed that the gateway router's majority of ports are linked to Ethernet subnets. The number of hops between the end host and the gateway router affects the traffic characteristics meanwhile wireless links involve capacity changes and random delays owing to channel circumstances, Ethernet links are thought to be reliable. Moreover, taking into consideration the contention-based MAC protocol used in wireless networks, the analysis compares the inter-packet spacing for traffic from Ethernet and wireless links. After the classification of traffic in the first phase, the second phase begins with traffic classification and then it concentrates on identifying rogue access points. The process of detection requires distinguishing between communication created by authorised and unauthorised WLAN hosts. Unauthorised WLAN hosts frequently engage in port scanning, which is identified by counting how often straight-access and crossing-access attempts above a threshold. Crossing-access happens when an access point is reached on a port to which it is not physically connected, whereas straight-access happens when an access point is physically connected to a port on the gateway router. Increases in straight-access and crossing-access frequencies are used by the NTA to identify unauthorised WLAN hosts connected to a RAP through monitoring application layer client request packets. The detection thresholds are established using empirical means.

2.8.1 Strength and Weakness

One of the strengths for this approach is that it works with both wired and wireless subnets in a heterogeneous network. Because current networks frequently include a combination of wired and wireless connections, this makes it suitable to real-world settings. Moreover, using network traffic characteristics this previous proposed method can distinguish between Ethernet and WLAN hosts by depending on traffic analysis at the gateway router. When compared to approaches that only take into account network topology or signatures, this method can offer a more precise and sophisticated detection. Furthermore, the technique focuses on detecting Rogue Access Points by

keeping an eye on behaviours like port scanning that are frequently linked to unauthorised WLAN hosts which can improve the security posture by identifying particular behaviours that may be signs of future security vulnerabilities. In addition, a degree of adaptability to various network environments is added by using alert levels for detection parameters that are empirically derived. Rather than depending on predetermined cutoff points, the approach enables modifications according to the unique attributes and trends detected in the flow of data within a given network.

Despite the number of strengths in this proposed method, there are also a few weaknesses present in this approach where it makes assumptions on network architecture. The approach runs under the assumption that the gateway router's ports are mostly connected to Ethernet subnets. This presumption may not hold true in a particular network context, which could jeopardise the classification and detection phases' accuracy. For instance, the assumption might not hold true in a network with a sizable number of wireless connections. Moreover, the dependencies on traffic characteristics where the method's accuracy is largely dependent on the differences in traffic characteristics between Ethernet and wireless networks. Consequently, the dependability of these features may be impacted by modifications to protocols, network conditions or the introduction of new technologies, which could result in incorrect classifications or false detections. Furthermore, it is limited to specific attack scenarios where it is designed to use particular actions such as port scanning to find the Rogue Access Points. Even while it works well against some kinds of attacks, it might not be able to stop all possible threats or attack routes and it's possible that new and advanced attack techniques could go unnoticed. Furthermore, it only has a single point of analysis which could lead to a single point of failure if traffic analysis is done only through the gateway router. The network may be open to unwanted access points and the detection system as a whole may be rendered useless if the gateway router is compromised.

2.9 Comparison the proposed method with the previous studies

By comparing in general of the proposed method with the previous proposed method in [2-3], [7-8], [15-17], the proposed system relies on scanning the network and comparing SSIDs and BSSIDs against a whitelist to identify potential RAPs which is effective for detecting unauthorized access points that may be hidden or broadcasting

false SSIDs. Although these previous studies may offer more advanced detection capabilities by utilising various detection techniques, including signal strength analysis, anomaly detection algorithms and many others which could require more computational resources and training data. Moreover, the proposed system includes an isolation mechanism that blocks the MAC address of detected which can prevent unauthorized devices from accessing the network and mitigates security risks. In comparison, some previous studies may have proposed similar isolation mechanisms, while others have focused more on the detection and alerting capabilities without providing any explicit isolation functionalities. Furthermore, the proposed system has an alerting system where it can send SMS alerts to network administrators upon detecting potential RAPs, providing the ability for swift response and actions. Although some of the previous studies have implemented an alert mechanism like email notification and SNMP traps, but SMS alert provide direct and immediate notification which is beneficial for time-sensitive incidents. Finally, the proposed system's detection accuracy relies on the accuracy of the whitelist and the effectiveness of the comparison algorithm which means that False positives may occur if legitimate access points are not properly included in the whitelist or if there are inconsistencies in signal strength or environmental factors.

CHAPTER 3

System Methodology/Approach

The process of development of the project involves conducting pre-development research by reviewing existing literatures, collect information about the legitimate access points, system planning and algorithm designing and developing a prototype.

3.1 Software Development Life Cycle

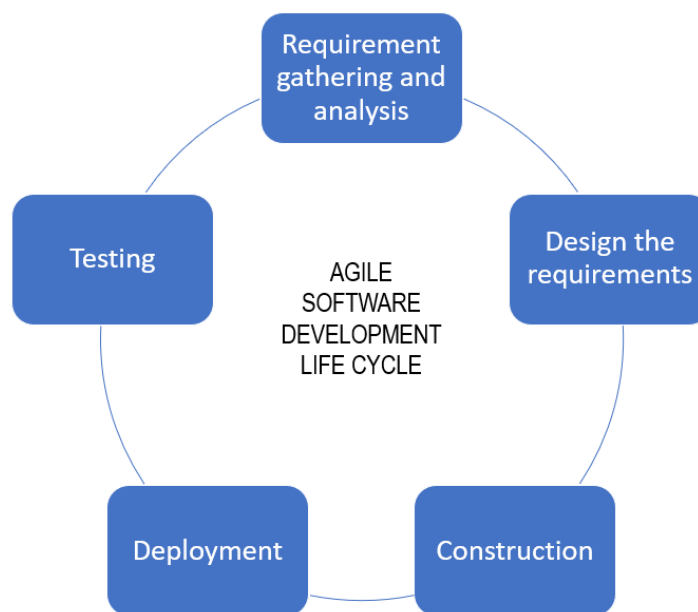


Figure 3.1 Agile SDLC

The system methodology involves using an agile approach where the 5 development stages are shown in the Figure 3.1 above. The 5 stages involved are requirement gathering and analysis, design the requirements, construction, deployment and testing.

1. In the first stage, the key requirements are identified and prioritised, including the need for a whitelist that contains the signatures of the authorised access points and the required functions involved in the system.
2. In the second stage, the requirements from the first stage must be designed and a blueprint must be drawn for the system before proceeding. In contrast, the

system architecture diagram and use case diagram must be constructed to visualise the overall flow of the system.

3. In the construction stage, development work begins on implementing the features and functionalities defined in the requirements and design phases. To ensure the development work goes smoothly, the system flowchart and sequence diagram are drawn to help.
4. In the deployment stage, the system is deployed to the target environment, such as a house local area network which may involve configuring the system to work within the network environment, ensuring compatibility with the existing infrastructure.
5. In the testing stage, continuous testing is performed to ensure the quality and reliability of the system as well as to minimise the potential bugs and errors that are present in the system.

3.2 System Design Diagram

In this section, the system architecture diagram and use case diagram will be presented to provide the overall concept and flow of the proposed system.

3.2.1 System Architecture Diagram

In this section, the figure below is the system architecture diagram to represent the functionalities of the system. The command-line interface is the interface where the users can interact with the system by typing the arguments such as `-sd` and `-his`. The main Python scripts in this system are `scan.py`, `detect.py`, `isolate.py` and `history.py` to handle the functionalities and user input of the system. `Scan.py` is used to handle the scanning for rogue access points and collect network information, `detect.py` contains functions that help to detect potential rogue access points by using a whitelist. Moreover, `isolate.py` is used to isolate and block the detected potential rogue access points from the network and `history.py` is used to manage the history of past scans, detections and isolated rogue access points for analysis. Figure 3.2 below presented the system architecture diagram.

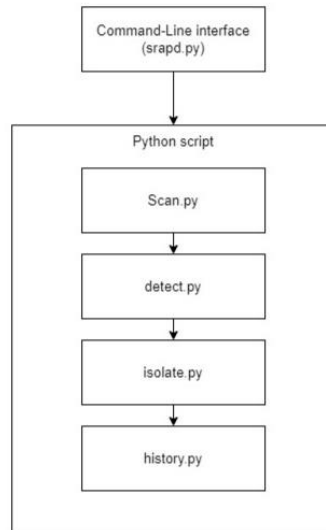


Figure 3.2 System architecture diagram

3.2.2 Use Case Diagram

In this section, a use case diagram is used to show the details of the system’s user. The main user of this system is the network administrator. The network administrator can use the system by typing the argument -sd into the command-line. The system will then scan the network, detect if there are any potential rogue access points and isolate any potential rogue access points from the network. Moreover, the user can also use the system by typing the argument -his to use the history function to see the past scans, detections and isolation results. Figure 3.3 below presented the use case diagram.

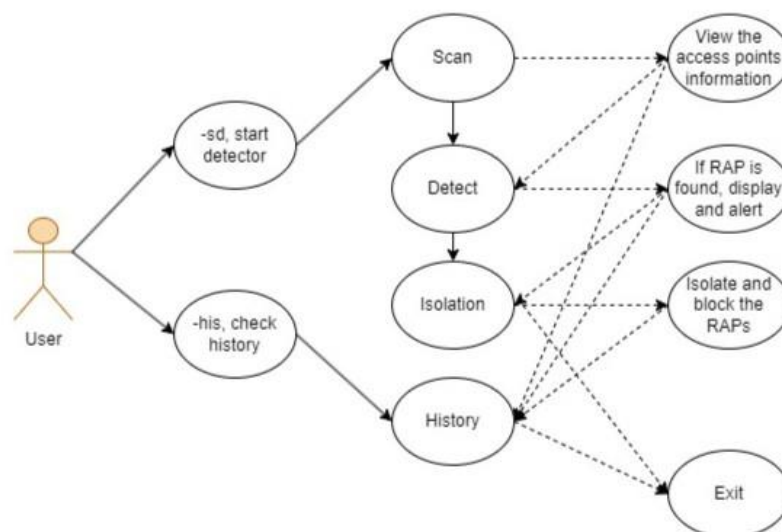


Figure 3.3 Use Case Diagram

CHAPTER 4

System Design

In this section, it showcases the overview of the system's flow to give a brief concept on the flow of the system by using a flowchart and the detail of the system's sequence with a sequence diagram.

4.1 System Flowchart

In this section, the figure below is a flowchart that shows the overview of the flow of the system. The system will prompt for user input and see which function the user wants to use. If the user wants inputs the argument of -sd, the system will execute the scanning function and display the relevant information after that and continuing on the detect function, the system will execute the detect function by comparing the BSSID of the access point that has the same SSID as the legitimate access point with a pre obtained whitelist. Finally, the system will then run the isolation function to isolate and block any potential rogue access points if detected any. Nevertheless, if the user inputs the -his argument the system will execute the history function and display the past scanned access points, detected and isolated potential rogue access point(s) if there are any. Figure 4.1 below presented the system flowchart.

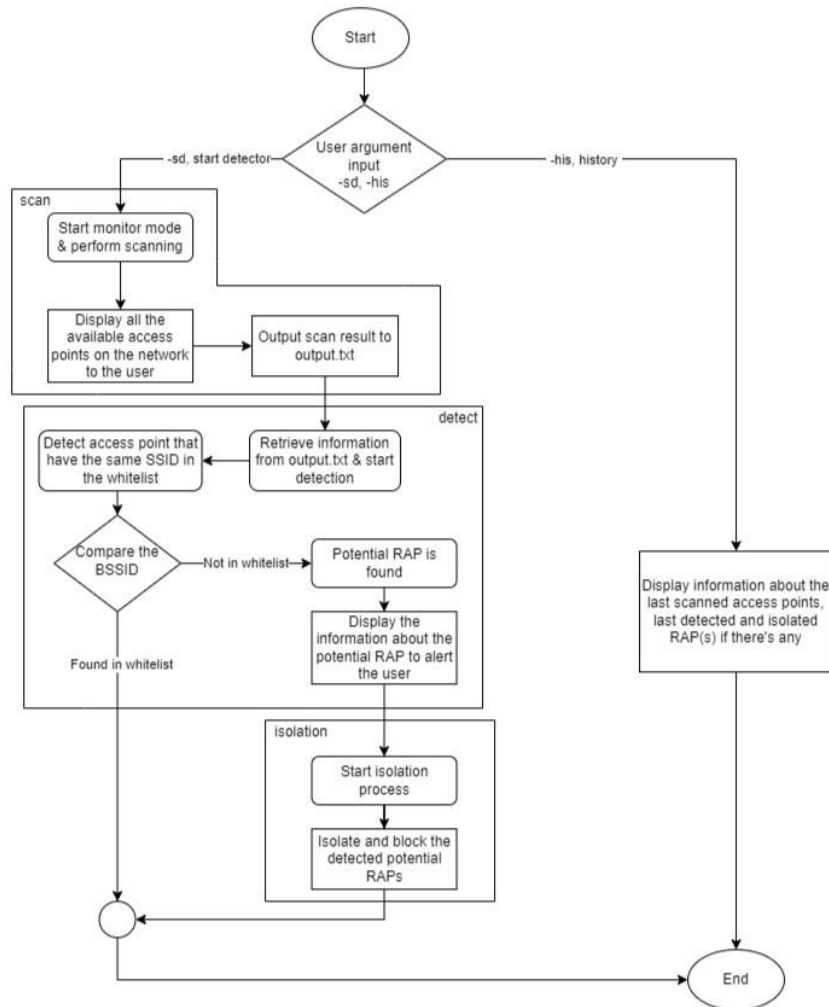


Figure 4.1 System Flowchart

4.2 Sequence Diagram

In this section, a sequence diagram is drawn to illustrate the sequence of interactions between the components of the system. User first initiates the start detector command, the command-line interface (CLI) receives the command and forwards it to the Python script. The Python script invokes the scan.py module to start scanning for the available access points and collect the network information. The scan.py module activates monitor mode (if not already activated) and begins scanning for networks. Upon completion of the scan, the scan.py module retrieves network information and invokes the detect.py module to start detecting for any potential rogue access points that are present in the network. The detect.py module starts comparing the SSID and BSSID of the collected network information with a pre-obtained whitelist to detect if there any potential rogue access points are found. Upon completion of the detection, the script

will then invoke the `isolate.py` module to start isolating the rogue access points. In the `isolate.py` module, it will retrieve the list of detected rogue access points and start the isolation process and block the BSSID of the potential RAPs. Upon completion of the `isolate.py` module, it will return to the python script and display the information to the user. Figure 4.2 below presented the sequence diagram.

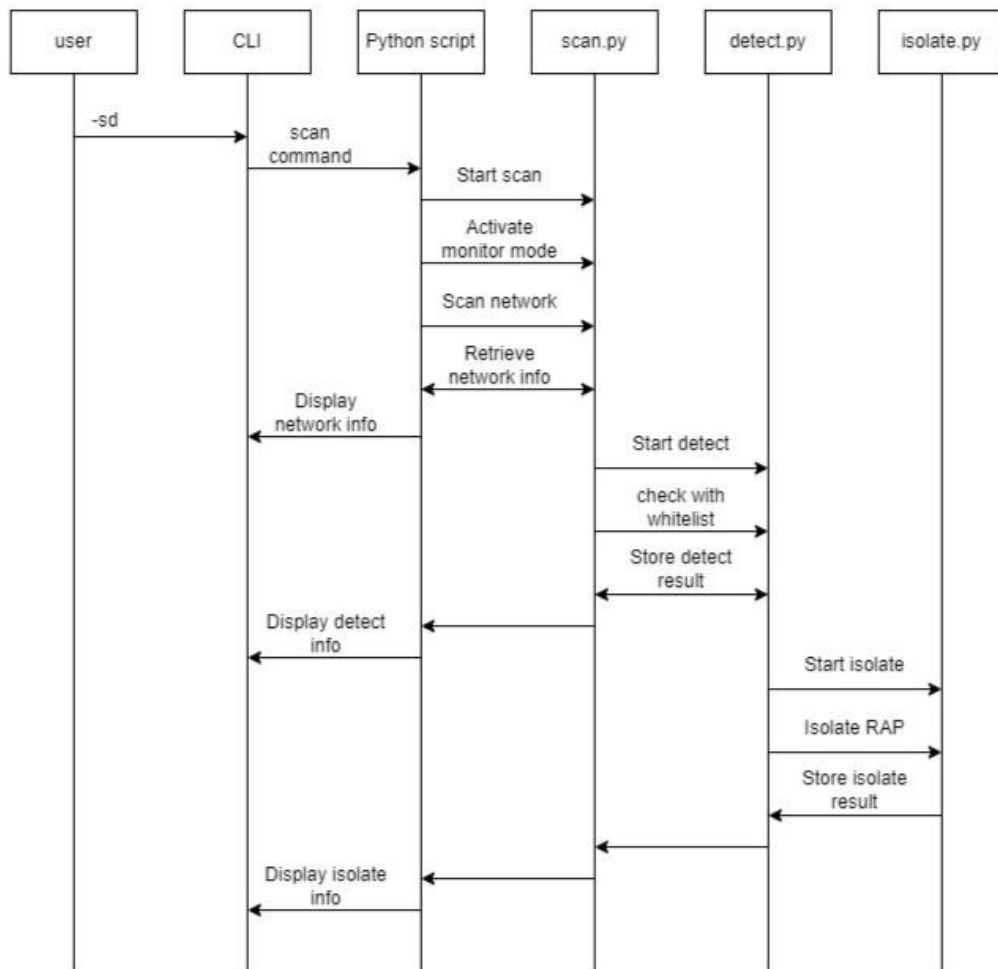


Figure 4.2 Sequence Diagram

CHAPTER 5

System Implementation

In this section, the details of the software setup and the implementation of the system are meticulously documented to provide a clearer and more comprehensive picture of the system design.

5.1 Hardware

One of the hardware involved in this project is a laptop which is the most important component in doing the majority of the research and development of the project. The laptop is used for literature review, information gathering and design and development of the system. It is also a physical platform that allows the usage of various required software like Oracle VM VirtualBox, Kali-Linux and Python. Table 3.1 shows the specifications of the laptop used.

Table 5.1 Specifications of the laptop

Description	Specifications
Model	Asus Vivobook A412D
Processor	AMD Ryzen 5 3500U with Radeon Vega Mobile Gfx 2.10 GHz
Operating System	Windows 11 Home Single Language
Graphic	AMD Radeon(TM) Vega 8 Graphics
Memory	12GB DDR4 RAM
Storage	512GB M.2 NVMe™ PCIe® 3.0 SSD

The next piece of hardware is a high gain wireless USB adapter which it to help provide wireless access to the virtual machine Kali-Linux. Table 3.2 shows the specifications of the wireless USB adapter used.

Table 5.2 Specifications of the wireless USB adapter

Description	Specifications
Model	tp-link TL-WN722N
Standards	IEEE 802.11n/g/b
Interface	USB 2.0
Button	WPS
Security	WEP, WPA/WPA2, WPA-PSK/WPA2-PSK
Dimensions	3.7 x 1.0 x 0.4 in (93.5 x 26 x 11 mm)
System compatibility	Windows 11/10/8.1/8/7/XP, Linux and macOS

5.2 Software

There is also some software that are required in the research and development of this project which includes Oracle VM VirtualBox, Kali-Linux and Python Programming Language. Oracle VM VirtualBox serves as a platform for running virtual machines in an isolated environment, it can allow virtual machines like Kali-Linux to be used without using any physical hardware of the host device. Moreover, Kali-Linux is a system that provide a platform for carrying out any cybersecurity-related works. It has many robust features and high capabilities when it comes to ethical hacking and researching. By using Kali-Linux as a platform to run the system, it is expected to provide the system a better environment and performance to be used. Furthermore, Python Programming Language is used to provide a platform to develop the system's algorithm.

5.3 Setting and Configuration

Before developing the system prototype, there are two software need to be installed which are Oracle VM VirtualBox and the Kali-Linux virtual machine.

1. Oracle VM VirtualBox can be downloaded at the official website <https://www.virtualbox.org/>
2. Kali-Linux virtual machine can be downloaded at the official website <https://www.kali.org/get-kali/#kali-platforms>

5.3.1 Setting up the virtual box for the virtual machine at Oracle VM VirtualBox

In this section, the procedures of setting up the virtual box for the virtual machine on Oracle is shown.

First, click on **New**.

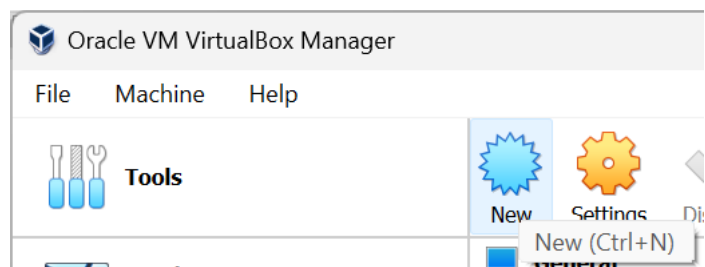


Figure 5.1 New VirtualBox

Give the virtual machine a name and choose **Linux** for type and **Debian (64-bit)** for the version. Click **Next**.

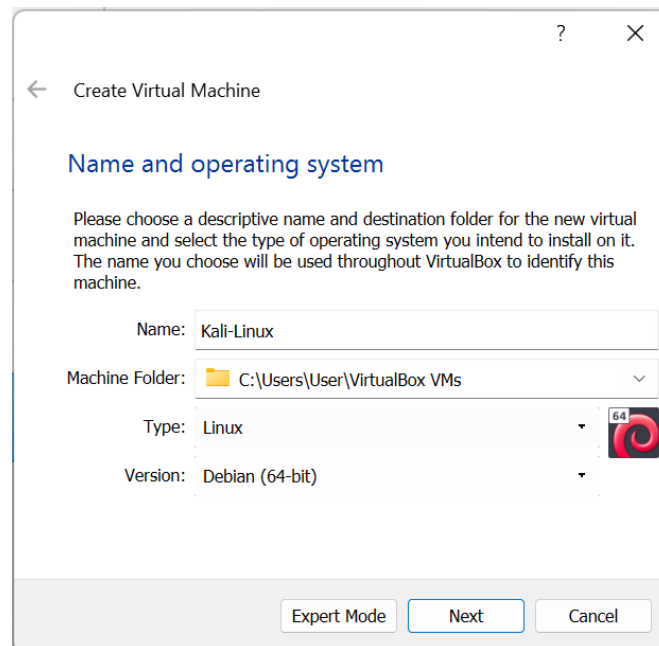


Figure 5.2 Create Virtual Machine

Allocate the memory size preferably 4096 MB. Click **Next**.

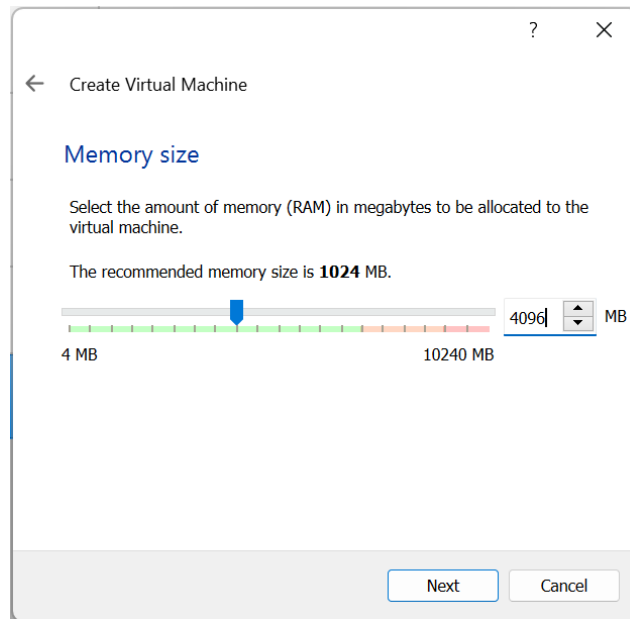


Figure 5.3 Create Virtual Machine (Memory size)

Select **Create a virtual hard disk now**. Click **Create**.

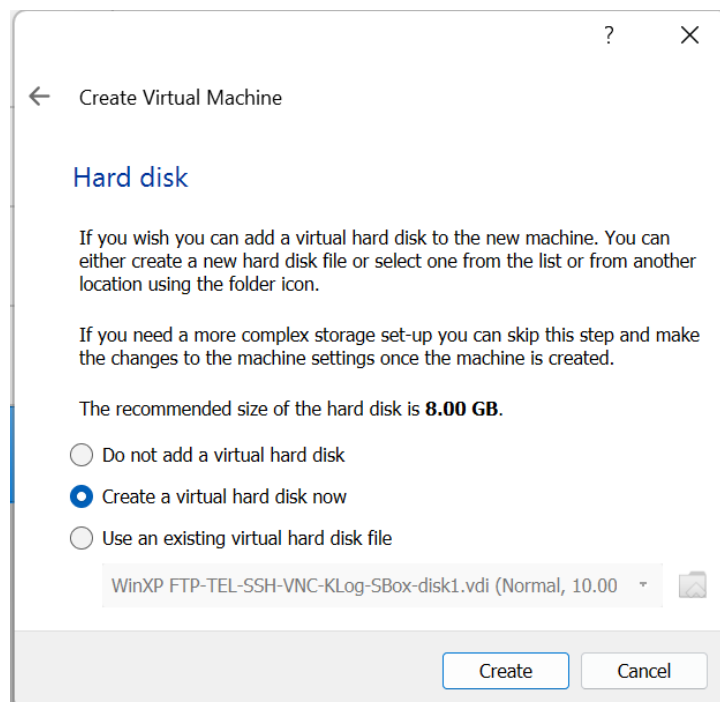


Figure 5.4 Create Virtual Machine (Hard disk)

Select **VDI (VirtualBox Disk Image)**. Click **Next**.

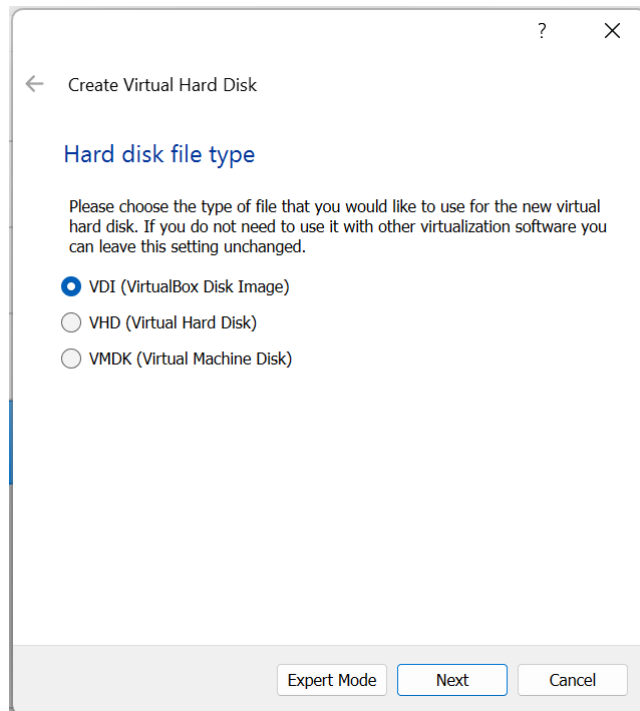


Figure 5.5 Create Virtual Hard Disk

Select **Fixed size** and click **Next**.

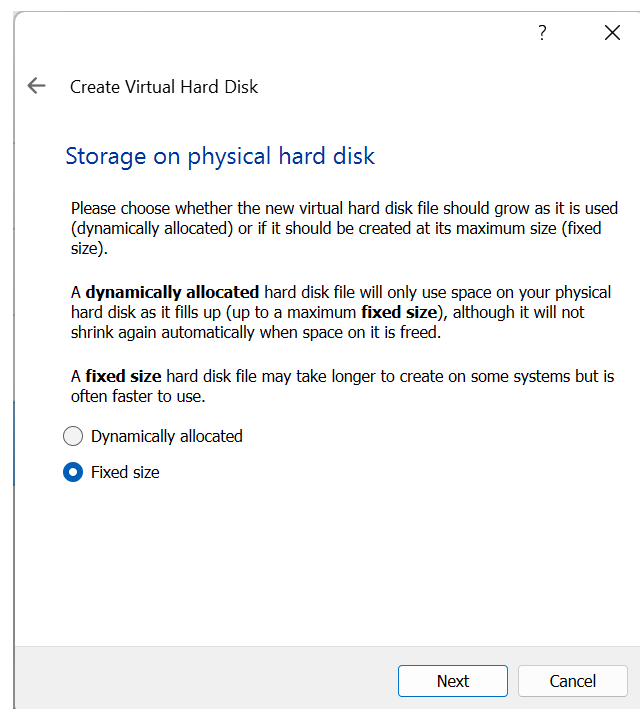


Figure 4.6 Create Virtual Hard Disk (Storage on physical hard disk)

Configure the file location and size. Click **Create**. After clicking on create, the virtual box is successfully created.

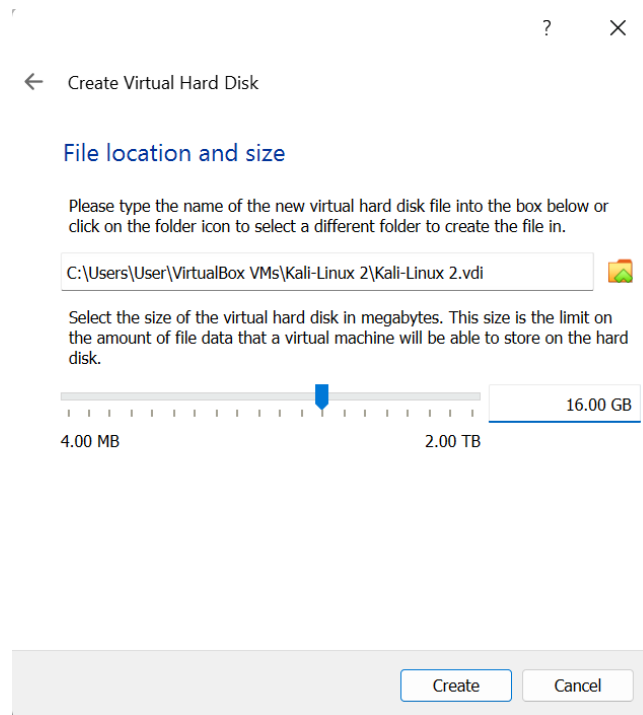


Figure 5.7 Create Virtual Hard Disk (File location and size)

5.3.2 Installing the Kali-Linux virtual machine

When the virtual machine is first boot up, it will bring the user to the installation menu. Select **Graphical install**.

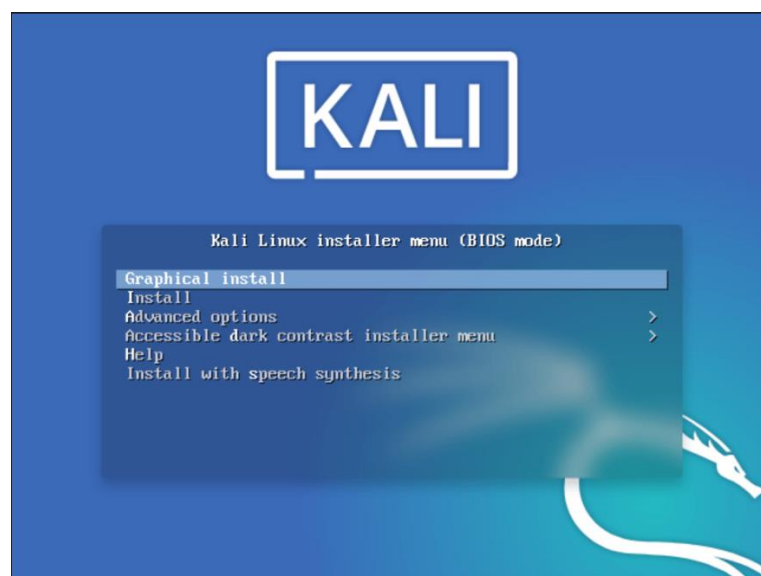


Figure 5.8 Installer menu

CHAPTER 5

Select the preferred language and click **Continue**.



Figure 5.9 Select language

Select the specific location and click **Continue**.

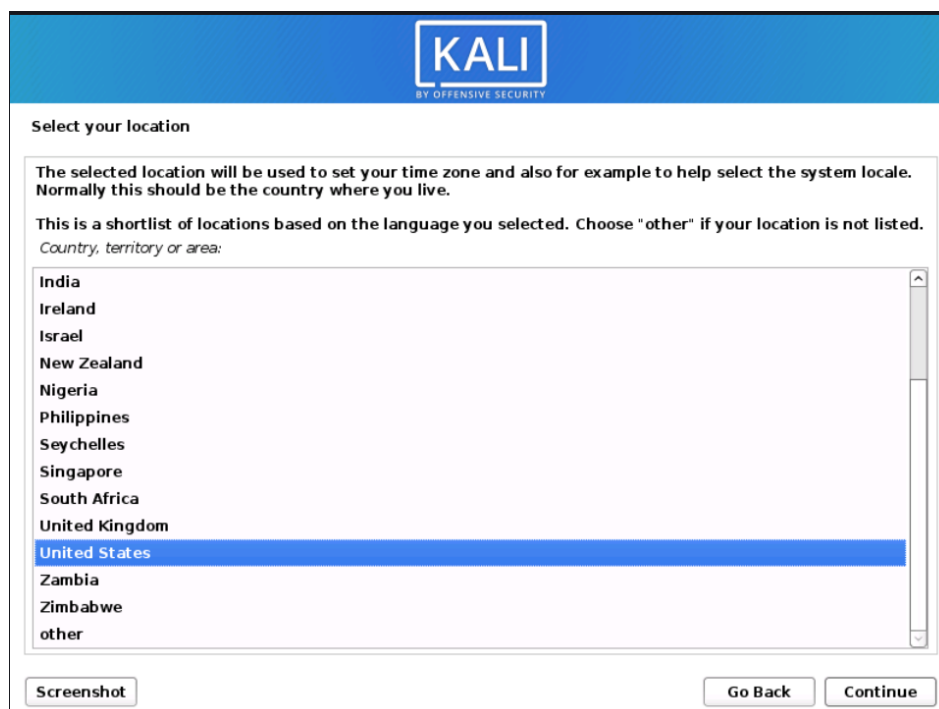


Figure 5.10 Select location

Choose the preferred keyboard layout, preferably American English. Click **Continue**.

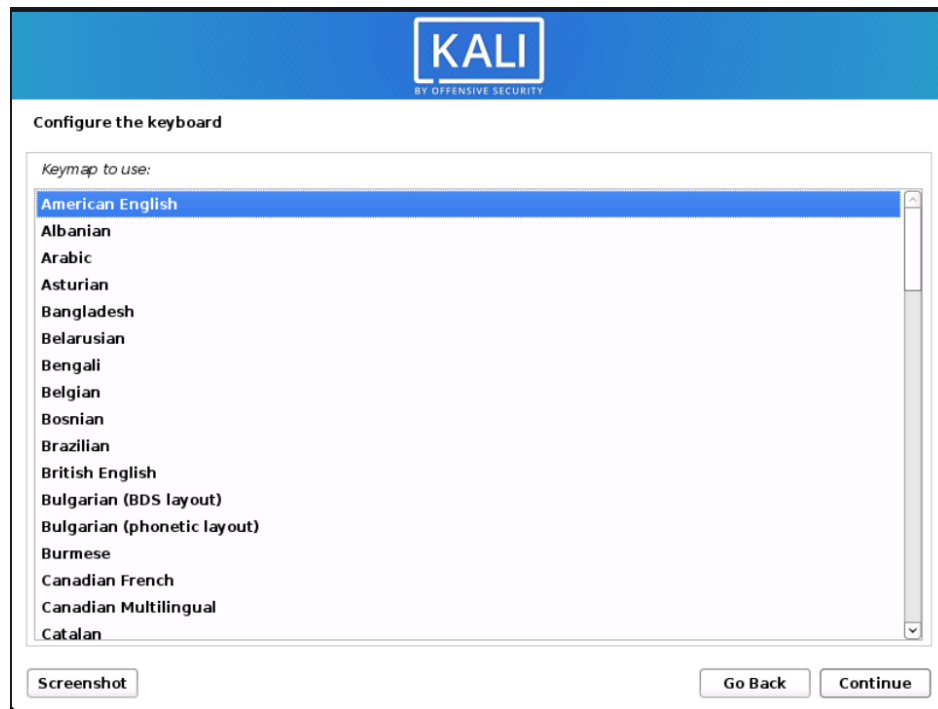


Figure 5.11 Configure keyboard

Name a custom hostname and click **Continue**.



Figure 5.12 Hostname

Leave the domain name blank if the domain name is not known. Click **Continue**.

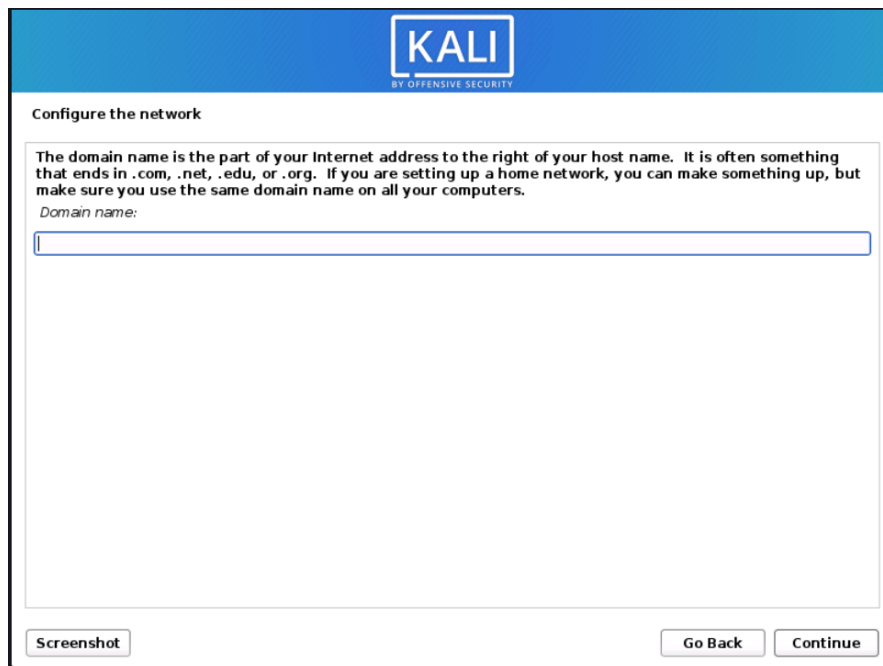


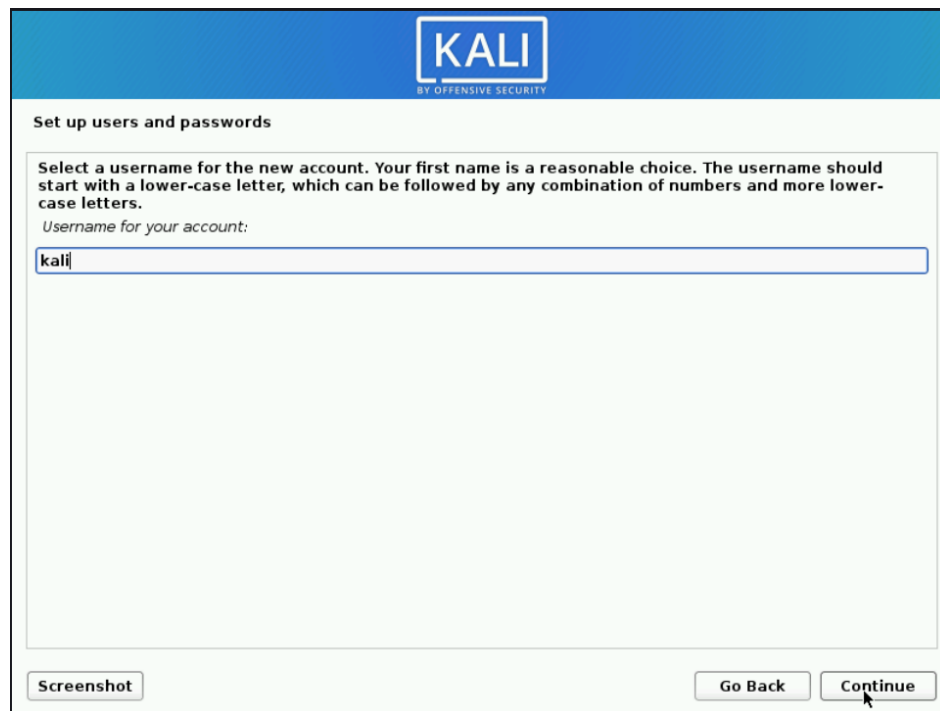
Figure 5.13 Domain name

Configure the full name for the new user. Click **Continue**.



Figure 5.14 Full name

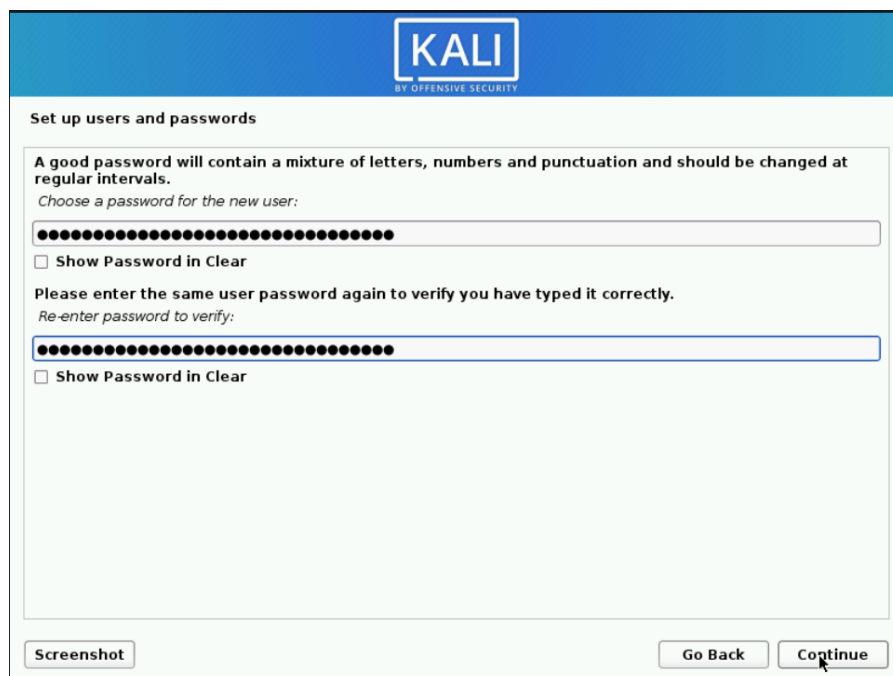
Set the username for the account and click **Continue**.



The screenshot shows the 'Set up users and passwords' screen in Kali Linux. At the top, there is a blue header with the 'KALI BY OFFENSIVE SECURITY' logo. Below the header, the title 'Set up users and passwords' is displayed. The main content area contains instructions: 'Select a username for the new account. Your first name is a reasonable choice. The username should start with a lower-case letter, which can be followed by any combination of numbers and more lower-case letters.' Below this, it says 'Username for your account:' followed by a text input field containing the text 'kali'. At the bottom of the screen, there are three buttons: 'Screenshot' on the left, 'Go Back' in the center, and 'Continue' on the right, with a mouse cursor hovering over the 'Continue' button.

Figure 5.15 Username

Set up the password and make sure the password is remembered and click **Continue**.



The screenshot shows the 'Set up users and passwords' screen in Kali Linux, specifically the password setup step. The header and title are the same as in Figure 5.15. The main content area contains instructions: 'A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.' Below this, it says 'Choose a password for the new user:' followed by a password input field filled with black dots. Underneath the first field is a checkbox labeled 'Show Password in Clear' which is currently unchecked. The next instruction is 'Please enter the same user password again to verify you have typed it correctly.' followed by 'Re-enter password to verify:' and a second password input field also filled with black dots. Below the second field is another 'Show Password in Clear' checkbox, also unchecked. At the bottom, there are three buttons: 'Screenshot' on the left, 'Go Back' in the center, and 'Continue' on the right, with a mouse cursor hovering over the 'Continue' button.

Figure 5.16 Password

Configure the clock based on the time zone. Click **Continue**.



Figure 5.17 Configure clock

Select **Guided – use entire disk** for the partition disks and click **Continue**.

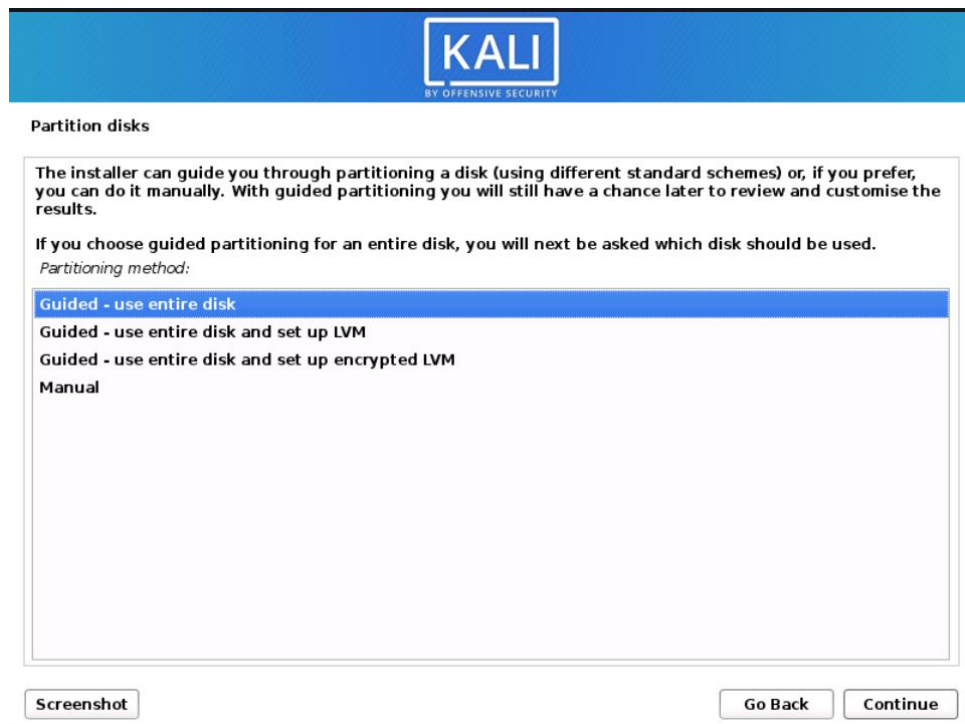


Figure 5.18 Partition disks (method)

Select **SCSI3(0,0,0)(sda)** and click **Continue**.



Figure 5.19 Partition disks (select disk)

Select **All files in one partition** as it is recommended for new users. Click **Continue**.

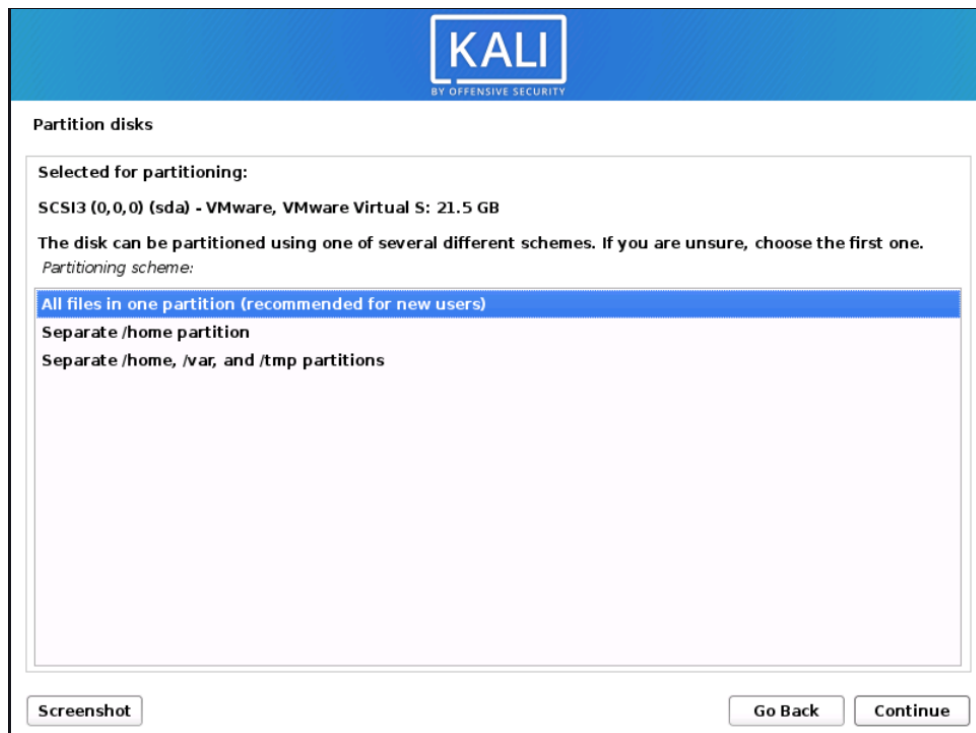


Figure 5.20 Partition disks (scheme)

Select **Finish partitioning and write changes to disk** and click **Continue**.

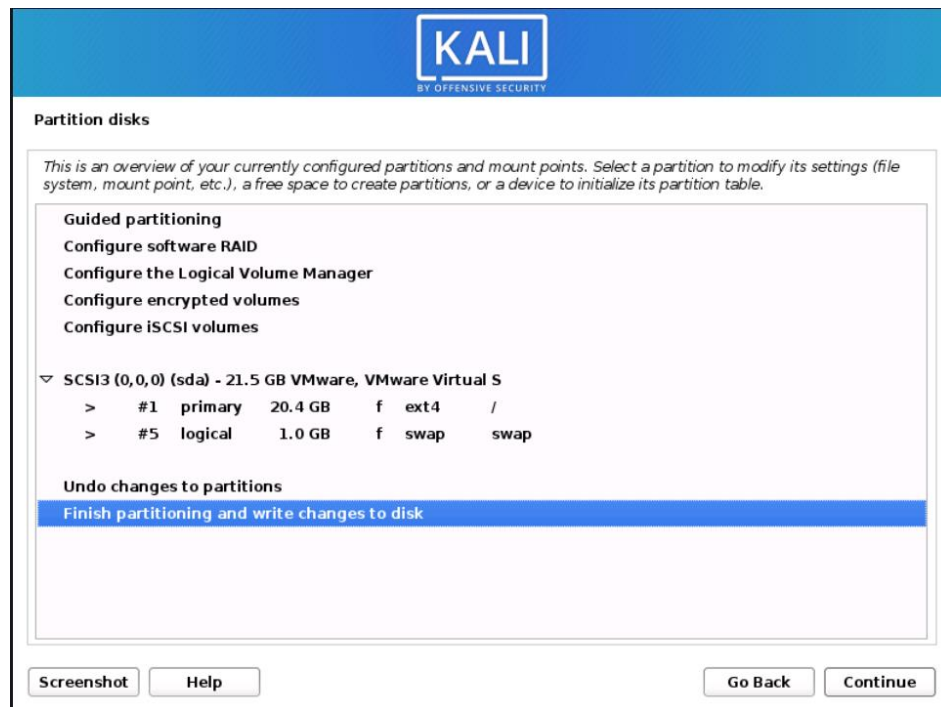


Figure 5.21 Partition disks (overview)

Select **Yes** and click **Continue**.



Figure 5.22 Partition disks (Changes)

Select **Yes** for Install the GRUB boot loader and click **Continue**.

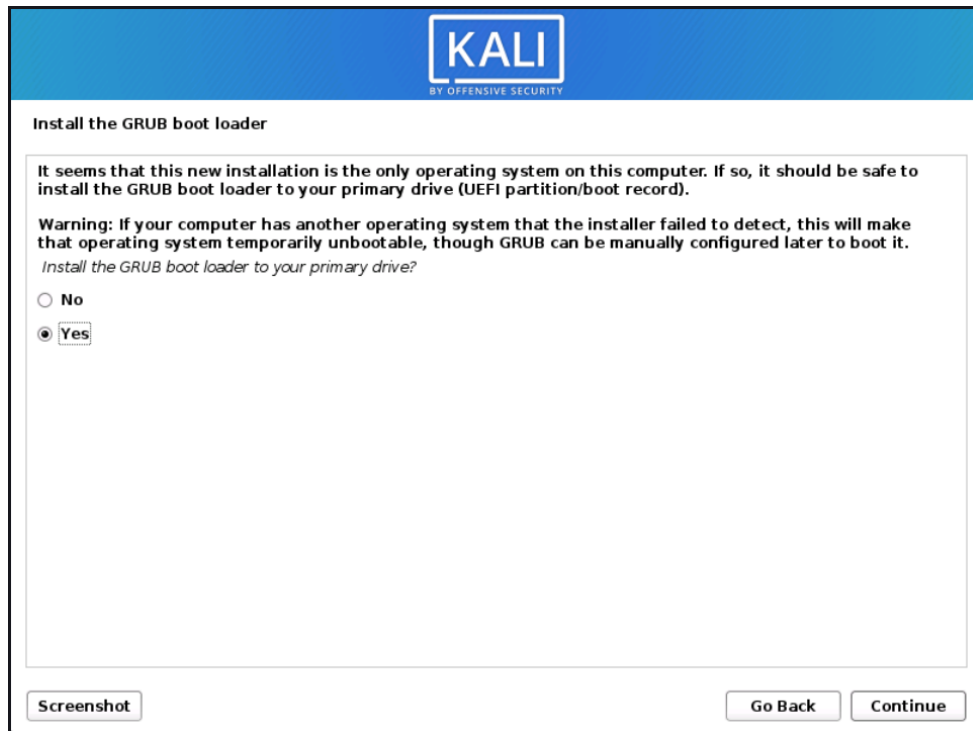


Figure 5.23 Install the GRUB boot loader

Select **/dev/sda** and click **Continue**. After that the virtual machine is successfully installed.

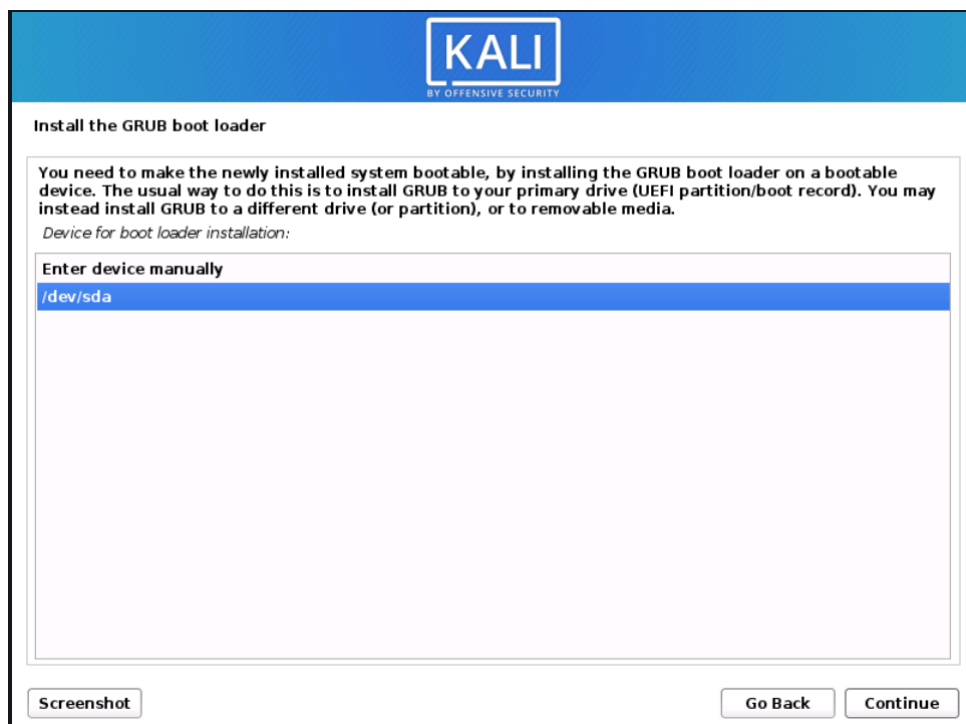


Figure 5.24 Install the GRUB boot loader (installation)

5.4 System Operation

In this part, the system operation will be showcased in detail with screenshot for the scenario including no RAPs are detected and potential RAPs are detected.

5.4.1 Interface

The figure below shows the main interface of the system prototype. Displaying the name of the system, SRAPD and the functions that are available. The source code can be referred at Appendix.

```
(root@kali)-[~/Desktop/FYP]
└─# python srapsd.py

      *****      *****      *      *****      ***
      *      *      *      *      *      *      *      *
      *****      *****      *****      *****      *
      *      *      *      *      *      *      *      *
      *****      *      *      *      *      *      ***

      UTAR SMART ROGUE ACCESS POINT DETECTOR (SRAPD)

      Developed by: Kok Ser Leen (20ACB01907)

      To use this tool, type in:

      -sd : start detector
      -sc : for scan only
      -his : Check history

      eg. python srapsd.py -sd 20
```

Figure 5.25 Interface

5.4.2 Scenario with no RAPs

An access point is set up as shown below.

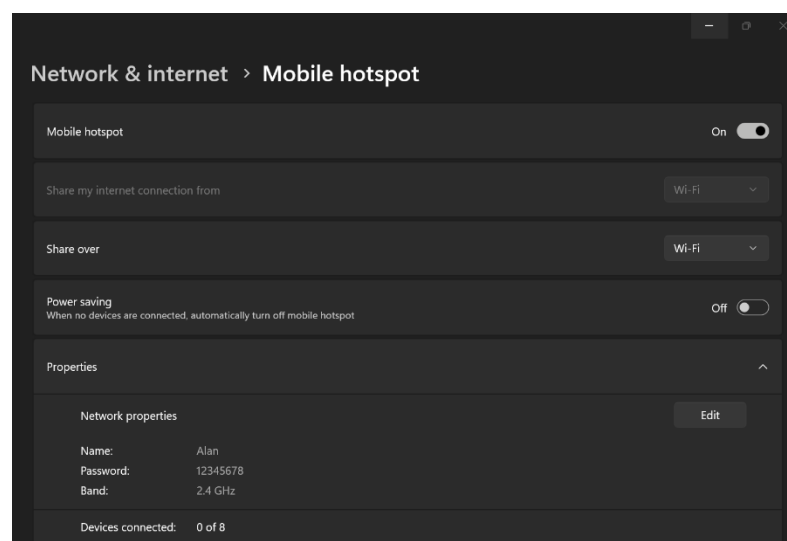


Figure 5.26 Setting up the access point

Next the start detector command line is entered to start the system as shown in the figure below.

```
(root@kali)~/home/alan/Desktop/FYP
# python srapd.py -sd 20
Monitor mode not activated. Activating monitor mode ...

MONITOR MODE ACTIVATED! PROCEEDING...

Scanning network please wait...

{'BSSID': '74:DA:DA:BC:E9:C6', 'Channel': '1', 'Power': '-15', 'SSID': 'RalinkTe dlink-E9C5'}
{'BSSID': 'B2:C5:54:3D:AC:1A', 'Channel': '1', 'Power': '-59', 'SSID': '(null)'}
{'BSSID': 'B2:C5:54:3D:D8:1F', 'Channel': '1', 'Power': '-53', 'SSID': '(null)'}
{'BSSID': 'B2:C5:54:3D:AC:22', 'Channel': '1', 'Power': '-61', 'SSID': '(null)'}
{'BSSID': 'BE:95:75:31:37:96', 'Channel': '3', 'Power': '-23', 'SSID': 'AtherosC Avocafe Pro'}
{'BSSID': '40:9B:CD:37:11:EC', 'Channel': '5', 'Power': '-15', 'SSID': 'AtherosC dlink-11EC'}
{'BSSID': '40:9B:CD:37:1E:68', 'Channel': '5', 'Power': '-51', 'SSID': 'AtherosC intel110'}
{'BSSID': '86:C5:A6:2D:9D:26', 'Channel': '6', 'Power': '-27', 'SSID': 'Alan'}
{'BSSID': 'F4:8C:EB:05:12:E3', 'Channel': '10', 'Power': '-47', 'SSID': 'RalinkTe dlink-12E2'}
Scanning stopped

Detecting for any potential RAP
Please wait ...
*
*
*
*
No RAP is found!

No RAP needs to be isolated. You're safe!
```

Figure 5.27 Start detector result without RAP

The system will first scan the network for the available access point information including the ssid and bssid. After scanning, the system will run the detection module and start detection for any potential RAPs by comparing the ssid and bssid in the whitelist. As for this scenario, the system did not detect any RAP so the message “No RAP is found!” is displayed to the user. Next, the system will run the isolation module to isolate any potential RAPs if there is any. As for this scenario, the system did not detect any RAP so a message is displayed to the user.

The figure below shows the history function when the user uses the `-his` command.

```
(root@kali)-[~/home/alan/Desktop/FYP]
└─# python srapd.py -his
```

BSSID	Ch	dBm	WPS	Lck	Vendor	ESSID
74:DA:DA:BC:E9:C6	1	-15	2.0	No	RalinkTe	dlink-E9C5
B2:C5:54:3D:AC:1A	1	-59	1.0	No		(null)
B2:C5:54:3D:D8:1F	1	-53	1.0	No		(null)
B2:C5:54:3D:AC:22	1	-61	1.0	No		(null)
BE:95:75:31:37:96	3	-23	2.0	No	AtherosC	Avocafe Pro
40:9B:CD:37:11:EC	5	-15	2.0	Yes	AtherosC	dlink-11EC
40:9B:CD:37:1E:68	5	-51	2.0	Yes	AtherosC	intel110
86:C5:A6:2D:9D:26	6	-27	2.0	No		Alan
F4:8C:EB:05:12:E3	10	-47	2.0	No	RalinkTe	dlink-12E2

```

Past Detected RAP:
SSID      BSSID
-----
No potential RAP detected yet!
No isolated BSSID is found

```

Figure 5.28 History without RAP

5.4.2 Scenario with RAP

A rogue access point is set up as shown in the figure below.

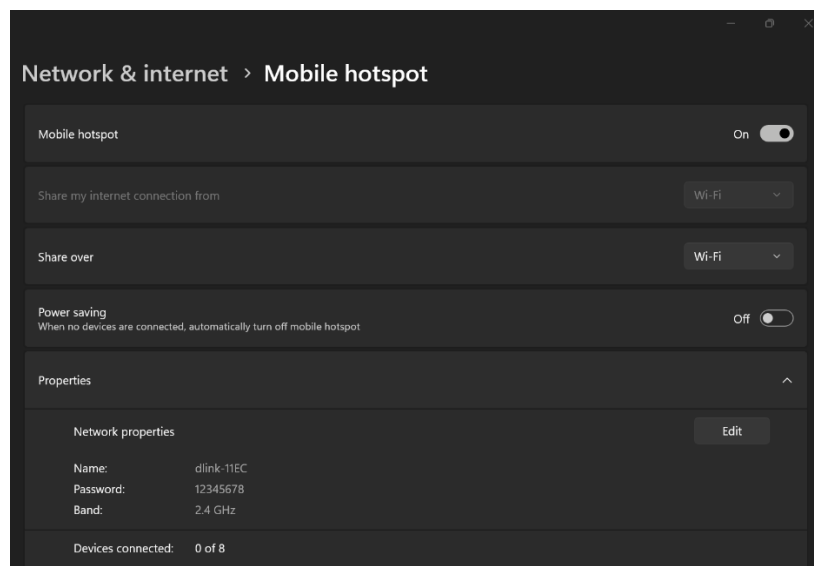


Figure 5.29 Setting up the RAP

Next the start detector command line is entered to start the system as shown in the figure below.

The figure below shows the history function when the user uses the `-his` command.

```
(root@kali) - [~/home/alan/Desktop/FYP]
# python srapd.py -his

HISTORY

BSSID          Ch  dBm  WPS  Lck  Vendor  ESSID
-----
74:DA:DA:BC:E9:C6  1  -35  2.0  No   RalinkTe  dlink-E9C5
B2:C5:54:3D:D8:1F  1  -47  1.0  No           (null)
B2:C5:54:3D:AC:1B  1  -71  1.0  No           (null)
BE:95:75:31:37:96  3  -25  2.0  No   AtherosC  Avocafe Pro
40:9B:CD:37:11:EC  5  -33  2.0  Yes  AtherosC  dlink-11EC
40:9B:CD:37:1E:68  5  -53  2.0  Yes  AtherosC  intel110
40:9B:CD:37:12:0C  5  -69  2.0  Yes  AtherosC  CiscoN010
40:9B:CD:37:11:F8  5  -55  2.0  Yes  AtherosC  dlink-11F8
86:C5:A6:2D:9D:26  6  -23  2.0  No           dlink-11EC
74:DA:DA:BC:EA:3D  9  -51  2.0  No   RalinkTe  dlink-EA3C
B2:C5:54:3D:D7:E6  9  -71  1.0  No           (null)
B2:C5:54:3D:D7:E5  9  -67  1.0  No           (null)
F4:8C:EB:05:12:E3 10  -47  2.0  No   RalinkTe  dlink-12E2
B2:C5:54:3D:AC:1A  1  -59  1.0  No           (null)
B2:C5:54:3D:AC:50  2  -63  1.0  No           (null)

Past Detected RAP:
SSID      BSSID
-----
dlink-11EC  86:C5:A6:2D:9D:26

Isolated BSSIDs:
86:C5:A6:2D:9D:26
```

Figure 5.32 History with RAP

5.5 Implementation Issues and Challenges

One of the issues and challenges of this project is that it is not possible for a single system to perfectly detect all rogue access points from all possible scenarios as this could be due to various factors one of which is the diversity of rogue access point scenarios. Rogue access points can manifest in many different ways and scenarios including Man-in-the-Middle attacks, evil twin attacks, unauthorised employee devices etc. Moreover, new attack techniques will constantly emerge as technology continuously evolve and attacker may introduce more advanced tactics to adapt and overcome existing detection mechanisms. Other than that, effective time management and project planning are necessary to develop a functional system within the constraints of a final year project deadline especially since there are other academic matters that I have to focus on. Moreover, limited resources do pose a significant challenge for developing the system in various aspects, including hardware, software, and access to

CHAPTER 5

networking equipment. Due to the limited budget, I find myself barely have enough money to buy necessary technology including a monitor-mode Wi-Fi adapter. However, the hardware solution might not be the best in terms of quality or capacity because of budgetary constraints. Because of this, sometimes I will run into hardware problems and bugs which could hinder development and have an effect on the dependability and efficiency of the RAP detection system. However, I am still able to successfully develop the system in the end despite the challenges faced.

CHAPTER 6

System Evaluation and Discussions

In this chapter, system testing in different networks will be done and discussions on the project challenges and objective evaluation will be documented.

6.1 System Evaluation

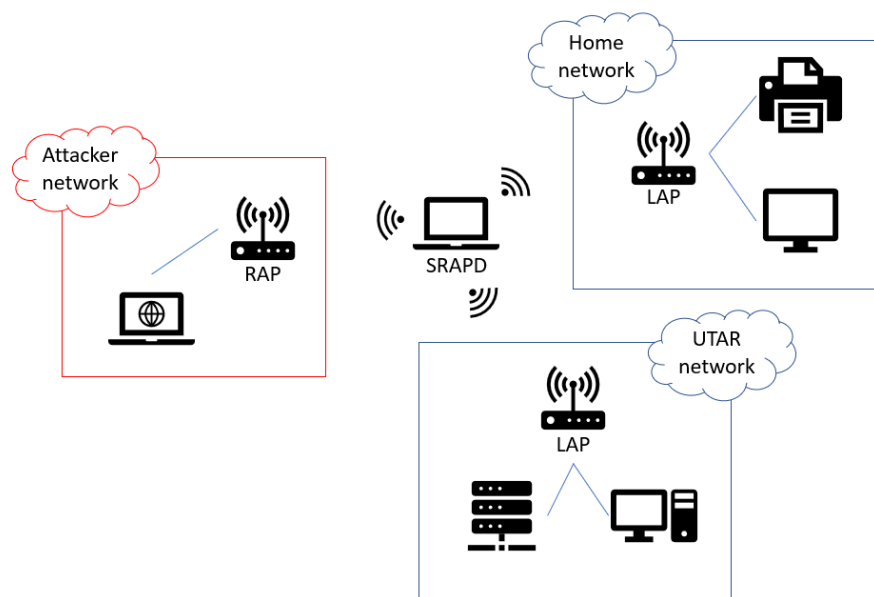


Figure 6.1 Example of the system testing topology

To ensure the effectiveness and deployability of the Smart Rogue Access Point Detection system, the system is deployed and tested in two different networks which are the UTAR network and a house local area network. Both networks' known access points information is obtained and is listed down in the whitelist of the system. Furthermore, the system is tested in multiple network environments to determine its flexibility and performance in different situations. The UTAR network is representative of a typical educational institution network where it will consist of a huge number of connected devices, irregular network traffic patterns and possible security flaws. However, the home local area network offers a residential environment and provides insights on how well the system works in a smaller network with distinct usage patterns

and security issues. Several key metrics are analyzed including detection accuracy, response time, scalability, resource utilisation and incident handling.

6.1.1 Detection Accuracy

Ensuring the security integrity of the network depends critically on the Smart Rogue Access Point Detection system's detection accuracy. The goal of the system is to accurately differentiate between rogue access points (RAPs) and legal ones by comparing discovered access points against a whitelist of authorised devices to reduce false positives and negatives by thorough testing and validation against established network topologies, hence improving its dependability in detecting possible security concerns. Increasing detection accuracy and staying up to date with changing network environments are made possible by regular updates to the whitelist and ongoing optimisation of detection algorithms.

6.1.2 Response Time

The system's swift response is critical in reducing security threats and stopping illegal access to the network in the event that a possible rogue access point is identified. To minimise the threat's impact on network operations and control it, a prompt and firm response is necessary. In contrast, the Smart Rogue Access Point Detection system uses real-time monitoring and alerting techniques to swiftly warn network administrators of security events. It is built with rapid detection and reaction as its top priority. The ultimate goal of the system is to reduce the amount of time between the time of detection and action in order to minimise any potential security breaches and attacks and to preserve the network integrity.

6.1.3 Scalability

The scalability of the Smart Rogue Access Point Detection system becomes more crucial as networks develop and grow in size and complexity. An important factor to take into account is the system's capacity to support expanding network infrastructures and manage higher traffic volumes without sacrificing performance. The system's

ability to grow both vertically and horizontally is assessed through extensive scalability testing to accommodate more devices and access points and adjust to shifting network demands. Scalability evaluations is believed to contribute to the system's continued efficacy and responsiveness when network requirements change over time.

6.1.4 Resource Utilisation

To guarantee effective functioning, maintaining system responsiveness and stability while reducing the impact on underlying infrastructure components requires effective resource utilization as the Smart Rogue Access Point Detection system keeps an eye on and optimises resource utilisation, including CPU, memory and network bandwidth usage. In contrast, the system aims to minimise resource overhead while optimising detection accuracy and performance through the use of lightweight and optimised algorithms. Moreover, to ensure an optimal system performance under fluctuating load situations, bottlenecks can be mitigated through continuous monitoring and optimisation of resource utilisation.

6.1.5 Incident Handling

The Smart Rogue Access Point Detection system's incident handling capabilities are essential when it comes to efficiently responding to security issues and to mitigate potential security breaches and threats. When a rogue access point is identified, the system uses pre-established incident response protocols to contain the threat and stop illegal users from accessing the network. In addition to that, the goal of the system is to reduce the amount of manual interaction in incident response workflows by using specified isolation strategies and automated alerting systems. Nevertheless, procedures for handling security issues should be regularly tested and validated to assist guarantee the efficacy and preparedness for instantaneous response to any potential incidents.

6.2 Project Challenges

I'm a student working on this project, and our tight budget presents obstacles. Given the financial limitations, me as a student working on this project faced challenge in tight

budget in obtaining the gear, software licences and resources required for testing and development. In order to overcome this difficulty, I managed to find some affordable options like open-source software and free or inexpensive hardware fixes. Moreover, to balance my academic responsibilities and the demands of this project poses a challenge for me as well. Attending classes, completing assignments and studying for tests compete for my time and attention, leading me to limited hours for project development. To overcome this challenge, I try to manage my time efficiently and prioritise tasks based on their importance and urgency and setting milestones. Furthermore, it takes a thorough understanding of software development methodologies, wireless communication protocols and network security principles to create a reliable rogue access point detection system. It can be intimidating for a student to navigate the technical difficulties involved in this project. Designing and implementing detection methods, integrating system components, and guaranteeing compatibility with the current network architecture are hurdles for me. In order to overcome these obstacles, I enlist the help of my supervisor, carry out extensive research and make use of web tools to improve my technical abilities.

6.3 Objective Evaluation

The objective evaluation of this project is discussed in this section based on the previously defined project objectives. First, the project's goal of creating an original, intelligent detection algorithm for detecting rogue access points on the UTAR campus network was accomplished effectively. The system is able to effectively detect possible RAPs by combining scanning processes with whitelist-based detection. The algorithm's robustness and usefulness in recognising RAPs across diverse network settings have been demonstrated through intensive research and development efforts. Next, within the UTAR campus network, the system efficiently employs a scanning technique that thoroughly examines the network environment by utilising hardware and software resources, such as a laptop running a virtual Kali-Linux machine to identify the accessible access points. This gives important insights into the existence of both authorised and unauthorised access points. Moreover, the system has an isolation as an extra functionality to separate identified RAPs from the network. The system starts the isolation procedures when it detects a rogue access point in order to stop unwanted

CHAPTER 6

access and reduce any security threats. The potential harm that rogue access point threats can do to data integrity and confidentiality is reduced and network security is improved by taking a proactive stance when responding to security incidents. Furthermore, the project showcases creativity and flexibility in system creation by utilising a mix of hardware and software resources, such as laptops running virtualized Kali-Linux. The system effectively accomplishes its goals while being affordable and available to higher education institutions with comparable network security requirements thanks to resource optimisation. In addition to core functionality, the project implements various miscellaneous features, such as reviewing past detected networks and RAPs. These features provide network administrators with valuable insights into historical network activity, facilitating informed decision-making and proactive security measures. In conclusion, the Smart Rogue Access Point Detection system successfully fulfills its objectives by developing an intelligent detection algorithm and mechanisms, implementing scanning mechanisms, incorporating isolation functionality and leveraging hardware and software resources effectively.

CHAPTER 7

Conclusion & Recommendations

7.1 Conclusion

In conclusion, with the increasing use of wireless networks in today's technological environment, the number of threats present within it are countless and inevitable, one of which is the rogue access point. Whether purposefully installed by criminal actors or unintentionally by staff, these rogue APs provide serious security vulnerabilities since they can facilitate data theft, man-in-the-middle attacks and the proliferation of phony network identities. The goal of solving this problem is to protect networks and stop the spread of rogue access points, especially for tertiary institutions that need practical detection algorithms customized for their networks. Nonetheless, the existing problems with the threats posed by the rogue access points cannot be ignored and this provokes the motive to strengthen network security at these institutions, giving network administrators the tools to improve detection and overall network security as well as minimising the possible risks that rogue access points can introduce by using the system to detect and find the potential rogue access points present within the network by comparing the BSSID in the pre-obtained whitelist and isolate it from the user's network. Nevertheless, the system also helps improve security by keeping a close eye out for illegitimate access points and prevent security breaches and protects private information that are transmitted across the network from prying eyes. Additionally, the system promotes increased user trust among staff, teachers and students by showcasing UTAR's dedication to data security and regulatory compliance. Users can feel secure in the campus network's dependability and security because safeguards are in place to ward off such threats which helps to create a conducive learning and working environment where users can focus on their tasks without concerns about network security risks. Finally, this project participated in a competition named JICaS as a part of the competition's project (A105). In collaboration with 2 of my other coursemates, we received the gold award in the competition, which can be referred to the screenshot and certificate in appendix.

7.2 Recommendations

In wireless networks, attackers can pose a serious security risk by taking advantage of security flaws in wireless networks, rogue access points (RAPs) can acquire unauthorised access and perhaps compromise confidential data. Attackers can spoof the BSSIDs of legitimate access points, which makes it challenging for conventional detection systems to distinguish between malicious and legitimate access points. This is one of the challenges associated with detecting RAPs. In contrast, this section examines suggestions for strengthening the identification of RAPs using BSSID spoofing methods and upgrading wireless networks' general security posture in future research and development efforts.

First, investing in the creation of sophisticated signal analysis algorithms that can identify minute changes in signal intensity and quality connected to fake RAPs is one way to improve RAP identification. These algorithms can distinguish between authentic and spoof access points with accuracy, improving detection accuracy and decreasing false positives by taking into account variables including signal propagation characteristics, ambient interference and client device behaviours. One of the methods can be round time trip analysis which proposed in [24]. Moreover, through the use of anomaly detection and pattern recognition algorithms, machine learning approaches provide an additional means of enhancing RAP detection by identifying patterns and abnormalities suggestive of RAP spoofing in wireless network traffic. Over time, detection systems can become more successful by learning to identify and adjust to new RAP spoofing tactics by using labelled datasets that contain examples of both legitimate and spoofed access points. This is accomplished by training machine learning models with these datasets [25]. Furthermore, real-time threat intelligence feeds and databases with details on known RAPs, malicious access points, and frequent attack signatures can be integrated into detection systems to enhance current detection capabilities. This can give important context and insights for spotting new RAP spoofing methods and emerging threats. RAP spoofing attacks can be proactively detected and countered in real-time by detection systems through the constant update and correlation of this threat intelligence with observed network activity [26].

CHAPTER 7

In conclusion, the recommendations outlined practical strategies for enhancing the detection of rogue access points in wireless networks and mitigating the associated risks of RAP spoofing attacks. Future research and development efforts focusing on the advanced signal analysis algorithms, leveraging machine learning techniques and integrating real-time threat intelligence can further improve the system's ability, efficiency, effectiveness and reliability to detect and respond to RAP spoofing threats, thereby enhancing the overall security posture of the wireless networks.

REFERENCES

1. "About airodump-ng." javapoint. <https://www.javatpoint.com/airodump-ng> (accessed Sep. 5, 2023).
2. A. Ketkhaw and S. Thipchaksurar, "Hidden Rogue Access Point Detection Technique for Wireless Local Area Networks," 2017 21st International Computer Science and Engineering Conference (ICSEC), Bangkok, Thailand, 2017, pp. 1-5, doi: 10.1109/ICSEC.2017.8443803.
3. C. Ampatzi. "Detection and Isolation of a Rogue Access Point." 26-May-2021. [Online]. Available: <https://mdh.diva-portal.org/smash/get/diva2:1567307/FULLTEXT01.pdf>. [Accessed: 17-Apr-2023].
4. "Difference Between Access Point and Router." LigoWave. <https://www.ligowave.com/difference-between-access-point-and-router> (accessed Sep. 5, 2023).
5. J. Breeden II. "What is Wireshark?" Networkworld. <https://www.networkworld.com/article/3663021/what-is-wireshark.html> (accessed Sep. 5, 2023).
6. M. Roomi. "5 Advantages and Disadvantages of SDN | Drawbacks & benefits of SDN." HiTechWhizz. 28-June-2021. [Online]. Available: <https://www.hitechwhizz.com/2021/06/5-advantages-and-disadvantagesdrawbacks-benefits-of-sdn.html>. [Accessed: 18-Apr-2023].
7. S. B. Vanjale, P. B. Mane and S. V. Patil, "Wireless LAN Intrusion Detection and Prevention system for Malicious Access Point," 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2015, pp. 487-490.
8. S. Nikbakhsh, A. B. A. Manaf, M. Zamani and M. Janbeglou, "A Novel Approach for Rogue Access Point Detection on the Client-Side," 2012 26th International Conference on Advanced Information Networking and Applications Workshops, Fukuoka, Japan, 2012, pp. 684-687, doi: 10.1109/WAINA.2012.108.
9. T. Keary. "Software-Defined Networking – SDN Guide." Comparitech. 25-Oct-2020. [Online]. Available: https://www.comparitech.com/net-admin/software-definednetworking/#The_Disadvantages_of_SDN. [Accessed: 18-Apr-2023].
10. "What are the Advantages, Disadvantages, and Architectural Components of SDN?" Zindagi Technologies. 22-Dec-2021. [Online]. Available: <https://zindagitech.com/what-are-the-advantages-disadvantages-and-architecturalcomponents-of-sdn/>. [Accessed: 18-Apr-2023].

REFERENCES

11. "What is an access point in networking?" Juniper Networks.
<https://www.juniper.net/us/en/research-topics/what-is-an-access-point-in-networking.html> (accessed Sep. 5, 2023).
12. W. Kelly. "wireless access point." TechTarget.
<https://www.techtarget.com/searchmobilecomputing/definition/access-point> (accessed Sep. 5, 2023).
13. tracylamv2, "Beware the dangers of the Rogue Access Point," Version 2,
<https://version-2.com/en/2023/11/beware-the-dangers-of-the-rogue-access-point/> (accessed Apr. 12, 2024).
14. W. by: F. Iliadis, "Networking: Rogue access points and Evil Twins," Baeldung on Computer Science, <https://www.baeldung.com/cs/rogue-access-points-evil-twins> (accessed Apr. 12, 2024).
15. K. Igarashi, H. Kato and I. Sasase, "Rogue Access Point Detection by Using ARP Failure under the MAC Address Duplication," 2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Helsinki, Finland, 2021, pp. 1469-1474, doi: 10.1109/PIMRC50174.2021.9569473.
16. S. Shetty, M. Song and L. Ma, "Rogue Access Point Detection by Analyzing Network Traffic Characteristics," MILCOM 2007 - IEEE Military Communications Conference, Orlando, FL, USA, 2007, pp. 1-7, doi: 10.1109/MILCOM.2007.4455018.
17. N. Lovinger, T. Gerlich, Z. Martinasek and L. Malina, "Detection of wireless fake access points," 2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Brno, Czech Republic, 2020, pp. 113-118, doi: 10.1109/ICUMT51630.2020.9222455.
18. S. Anmulwar, S. Srivastava, S. P. Mahajan, A. K. Gupta and V. Kumar, "Rogue access point detection methods: A review," International Conference on Information Communication and Embedded Systems (ICICES2014), Chennai, India, 2014, pp. 1-6, doi: 10.1109/ICICES.2014.7034106.
19. R. Beyah and A. Venkataraman, "Rogue-Access-Point Detection: Challenges, Solutions, and Future Directions," in IEEE Security & Privacy, vol. 9, no. 5, pp. 56-61, Sept.-Oct. 2011, doi: 10.1109/MSP.2011.75.
20. S. Srilasak, K. Wongthavarawat and A. Phonphoem, "Integrated Wireless Rogue Access Point Detection and Counterattack System," 2008 International Conference on Information Security and Assurance (isa 2008), Busan, Korea (South), 2008, pp. 326-331, doi: 10.1109/ISA.2008.103.
21. What is a rogue access point (rogue AP)? - definition from Techopedia,
<https://www.techopedia.com/definition/4082/rogue-access-point-rogue-ap> (accessed Apr. 8, 2024).

REFERENCES

22. “Rogue access point attacks,” Tutorialspoint,
https://www.tutorialspoint.com/wireless_security/wireless_security_rogue_access_point_attacks.htm (accessed Apr. 10, 2024).
23. “What is a Rogue Access Point & How to protect against them,” Nile,
<https://nilesecure.com/network-security/what-is-a-rogue-access-point-how-to-protect-against-them/> (accessed Apr. 12, 2024).
24. Kitisriworapan, S., Jansang, A. & Phonphoem, A. Client-side rogue access-point detection using a simple walking strategy and round-trip time analysis. *J Wireless Com Network* 2020, 252 (2020). <https://doi.org/10.1186/s13638-020-01864-5>
25. K. C. Patel and 2Ajaykumar Patel, Recognition of rogue access points using a machine learning approach, <https://ijcrt.org/papers/IJCRT2212283.pdf> (accessed Apr. 18, 2024).
26. P. Liu, P. Yang, W.-Z. Song, Y. Yan, and X.-Y. Li, Real-time identification of rogue WIFI connections using Environment-Independent Physical Features, https://sensorweb.engr.uga.edu/wp-content/uploads/2019/03/Dropbox_liu2019real.pdf (accessed Apr. 18, 2024).
27. P. Wofford, “Rogue Access Points: The Threat to Public Wireless Networks,” ProQuest | Databases, EBooks and Technology for Research, <https://about.proquest.com/en/>.

APPENDIX

1. Interface

```

srapsd.py  ×  +
1 import argparse
2 import sys
3 import scan as sc
4 import detect as dt
5 import history as his
6 import isolate as iso
7
8 def display_intro():
9     BOLD = "\033[1m"
10    RESET = "\033[0m"
11    RED = "\033[31m"
12    GREEN = "\033[32m"
13    YELLOW = "\033[33m"
14    CYAN = "\033[96m"
15
16    letter_symbols = {
17        'S': ['*****', '* ', '*****', ' *', '*****'],
18        'R': ['*****', '* *', '*****', '* *', '* *'],
19        'A': [' * ', '* *', '*****', '* *', '* *'],
20        'P': ['*****', '* *', '*****', '* ', '* '],
21        'D': ['*** ', '* *', '* *', '* *', '* *', '*** '],
22    }
23
24    text = "SRAPD"
25
26    print("\n\n")
27    for i in range(5):
28        line = ""
29        for letter in text:
30            line += CYAN + '\t' + letter_symbols[letter][i] + RESET + ' '
31        print(line)
32    print(f"{YELLOW}\n\tUTAR SMART ROGUE ACCESS POINT DETECTOR (SRAPD){RESET}")
33    print(f"{YELLOW}\n\tDeveloped by: Kok Ser Leen (20ACB01907){RESET}")
34    print("\nTo use this tool, type in:\n")
35    print("\t-sd : start detector")
36    print("\t-sc : for scan only")
37    print("\t-his : Check history")
38
39

```


APPENDIX

2. Output file (Scan)

1 BSSID	Ch	dBm	WPS	Lck	Vendor	ESSID
2						
3 B2:C5:54:3D:AC:1A	1	-95	1.0	No		(null)
4 74:DA:DA:BC:E9:C6	1	-75	2.0	No	RalinkTe	dlink-E9C5
5 74:DA:DA:BC:EA:3D	4	-73	2.0	No	RalinkTe	dlink-EA3C
6 74:DA:DA:BD:11:E3	4	-95	2.0	Yes	RalinkTe	dlink-11E2
7 40:9B:CD:37:11:EC	5	-91	2.0	Yes	AtherosC	dlink-11EC
8 40:9B:CD:37:12:0C	5	-79	2.0	Yes	AtherosC	CiscoN010
9 58:D5:6E:DE:5F:F0	9	-71	2.0	No	RalinkTe	dlink-5FEF
10 B2:C5:54:3D:D7:E3	10	-95	1.0	No		(null)
11 26:FC:77:09:27:7F	11	-75	2.0	No	AtherosC	P002 Lab
12 B2:C5:54:3D:D8:1F	1	-95	1.0	No		(null)
13 10:27:F5:B5:81:4E	2	-93	2.0	No	AtherosC	Avocafe
14 FA:D0:FC:E1:F7:09	2	-93	2.0	No	AtherosC	Avocafe
15						

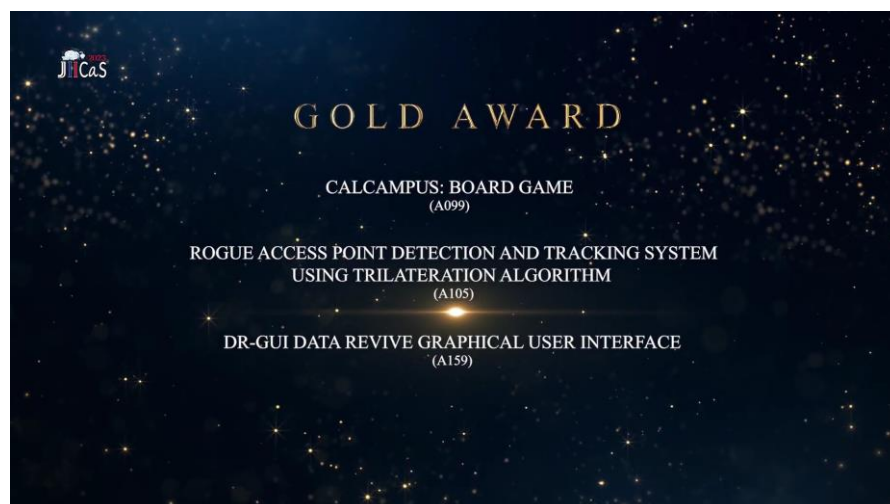
3. Output file (Detect)

RAP_list.txt	
1	Avocafe FA:D0:FC:E1:F7:09
2	

4. Whitelist (Sample)

```
whitelist = [{"10:27:F5:B5:81:4E", "5C:A6:E6:60:69:4E", "Avocafe"}, {"BE:95:75:31:37:96", "Avocafe Pro"}, {"40:9B:CD:37:11:EC", "dlink-11EC"}, {"74:DA:DA:BC:E9:C6", "dlink-E9C5"}, {"40:9B:CD:37:11:F8", "dlink-11F8"}, {"74:DA:DA:BC:EA:3D", "dlink-EA3C"}, {"F4:8C:EB:05:12:E3", "dlink-12E2"}, {"40:9B:CD:37:1E:68", "intel110"}]
```

5. Screenshot (JiiCAS award)



6. Certificate (JiiCAS award)



FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Year 3 Trimester 3	Study week no.: 6
Student Name & ID: Kok Ser Leen (20ACB01907)	
Supervisor: Puan Nor Afifah Binti Sabri	
Project Title: Rogue Access Point Detector in UTAR Campus	

1. WORK DONE

[Please write the details of the work done in the last fortnight.]

More research has been done for Chapter 2.

2. WORK TO BE DONE

Aim to add on more previous studies in chapter 2.

3. PROBLEMS ENCOUNTERED

No problems have been encountered so far.

4. SELF EVALUATION OF THE PROGRESS

The progress of the project is going well so far.



Supervisor's signature



Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Year 3 Trimester 3	Study week no.: 7
Student Name & ID: Kok Ser Leen (20ACB01907)	
Supervisor: Puan Nor Afifah Binti Sabri	
Project Title: Rogue Access Point Detector in UTAR Campus	

1. WORK DONE

[Please write the details of the work done in the last fortnight.]

More research has been done in the literature review.

2. WORK TO BE DONE

Aim to add in more diagrams such as system architecture diagram and sequence diagram.

3. PROBLEMS ENCOUNTERED

No problems have been encountered so far.

4. SELF EVALUATION OF THE PROGRESS

The progress of the project is going well so far.



Supervisor's signature



Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Year 3 Trimester 3	Study week no.: 8
Student Name & ID: Kok Ser Leen (20ACB01907)	
Supervisor: Puan Nor Afifah Binti Sabri	
Project Title: Rogue Access Point Detector in UTAR Campus	

1. WORK DONE

[Please write the details of the work done in the last fortnight.]

System architecture diagram and sequence diagram are drawn.

2. WORK TO BE DONE

Start development work on the bonus additional feature which is the isolation of RAPs.

3. PROBLEMS ENCOUNTERED

No problems have been encountered so far.

4. SELF EVALUATION OF THE PROGRESS

The progress of the project is going well so far.



Supervisor's signature



Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Year 3 Trimester 3	Study week no.: 11
Student Name & ID: Kok Ser Leen (20ACB01907)	
Supervisor: Puan Nor Afifah Binti Sabri	
Project Title: Rogue Access Point Detector in UTAR Campus	

1. WORK DONE

[Please write the details of the work done in the last fortnight.]

Development work on the isolation feature is done.

2. WORK TO BE DONE

Require suggestion from supervisor on the system prototype and update the report.

3. PROBLEMS ENCOUNTERED

No problems have been encountered so far.

4. SELF EVALUATION OF THE PROGRESS

The progress of the project is going well so far and the report requires polishing.

Supervisor's signature

Student's signature

POSTER

UTAR
UNIVERSITI TUNKU ABDUL RAHMAN

FACULTY OF INFORMATION COMMUNICATION AND TECHNOLOGY

Rogue Access Point Detector in UTAR Campus

1. Introduction
This detection system is mainly to help network administrators to better detect potential rogue access points present on a network

2. Objective
To provide network administrators with a system that can efficiently and effectively detect & isolate potential rogue access points

3. Method Proposed
Scan the network and use a whitelist to compare the SSID and BSSID of the access points to identify the potential rogue access points and isolate it

4. Conclusion
The rogue access point is a threat that continues to evolve and emerge, mitigation efforts cannot be underestimated and need to take action as soon as possible.

Project Developer: Kok Ser Leen
Project Supervisor: Puan Nor 'Afifah Binti Sabri

PLAGIARISM CHECK RESULT

FYP2_20ACB01907.docx

ORIGINALITY REPORT

6%

SIMILARITY INDEX

4%

INTERNET SOURCES

3%

PUBLICATIONS

3%

STUDENT PAPERS

PRIMARY SOURCES

1

Submitted to South Bank University

Student Paper

1%

2

Liran Ma. "Rogue Access Point Detection by Analyzing Network Traffic Characteristics", MILCOM 2007 - IEEE Military Communications Conference, 10/2007

Publication

1%

3

Submitted to University of Bolton

Student Paper

<1%

4

Somayeh Nikbakhsh. "A Novel Approach for Rogue Access Point Detection on the Client-Side", 2012 26th International Conference on Advanced Information Networking and Applications Workshops, 03/2012

Publication

<1%

5

Submitted to Asia Pacific University College of Technology and Innovation (UCTI)

Student Paper

<1%

6

www.techopedia.com

Internet Source

<1%

PLAGIARISM CHECK RESULT

7	Kosuke Igarashi, Hiroya Kato, Iwao Sasase. "Rogue Access Point Detection by Using ARP Failure under the MAC Address Duplication", 2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), 2021 Publication	<1 %
8	www.packtpub.com Internet Source	<1 %
9	Submitted to University of Denver Student Paper	<1 %
10	dspace.daffodilvarsity.edu.bd:8080 Internet Source	<1 %
11	Submitted to Pathfinder Enterprises Student Paper	<1 %
12	Submitted to Asia Pacific International College Student Paper	<1 %
13	Submitted to Australian College of Business and Technology Student Paper	<1 %
14	Submitted to NCC Education Student Paper	<1 %
15	myfik.unisza.edu.my Internet Source	<1 %
16	www.bengkelkomputek.com Internet Source	<1 %

PLAGIARISM CHECK RESULT

		<1 %
17	Le Wang, Alexander M. Wyglinski. "Detection of man-in-the-middle attacks using physical layer wireless security techniques", Wireless Communications and Mobile Computing, 2016 Publication	<1 %
18	Submitted to Universiti Malaysia Sabah Student Paper	<1 %
19	Submitted to University of Northumbria at Newcastle Student Paper	<1 %
20	jglobal.jst.go.jp Internet Source	<1 %
21	obsproject.com Internet Source	<1 %
22	Submitted to Rochester Institute of Technology Student Paper	<1 %
23	Submitted to Stockholms universitet Student Paper	<1 %
24	za.store.asus.com Internet Source	<1 %
25	sofox.mystrikingly.com Internet Source	<1 %

PLAGIARISM CHECK RESULT

26	www.mdpi.com Internet Source	<1 %
27	Sermet, Yusuf. "Knowledge Generation and Communication in Intelligent and Immersive Systems: A Case Study on Flooding.", The University of Iowa, 2020 Publication	<1 %
28	c.coek.info Internet Source	<1 %
29	hdl.handle.net Internet Source	<1 %
30	honors.libraries.psu.edu Internet Source	<1 %
31	link.springer.com Internet Source	<1 %
32	umpir.ump.edu.my Internet Source	<1 %
33	www.jtec.org.my Internet Source	<1 %
34	www.tokomodemu.com Internet Source	<1 %
35	Bandar Alotaibi, Khaled Elleithy. "Rogue Access Point Detection: Taxonomy, Challenges, and Future Directions", Wireless Personal Communications, 2016	<1 %

PLAGIARISM CHECK RESULT

Publication		
36	Kun Zhou, Miaomiao Tang, Wei Zhang, Yanling Chen et al. "Exposure to Molybdate Results in Metabolic Disorder: An Integrated Study of the Urine Elementome and Serum Metabolome in Mice", Toxics, 2024 Publication	<1 %
37	Submitted to University of Maryland, University College Student Paper	<1 %
38	William Panek. "MCSA Windows Server 2016 Complete Study Guide", Wiley, 2018 Publication	<1 %
39	aaltodoc.aalto.fi Internet Source	<1 %
40	archive.org Internet Source	<1 %
41	eprints.utm.my Internet Source	<1 %
42	jis-eurasipjournals.springeropen.com Internet Source	<1 %
43	utpedia.utp.edu.my Internet Source	<1 %
44	www.avhf.com Internet Source	<1 %

PLAGIARISM CHECK RESULT

Form Title: Supervisor's Comments on Originality Report Generated by Turnitin for Submission of Final Year Project Report (for Undergraduate Programmes)			
Form Number: FM-IAD-005	Rev No.: 0	Effective Date: 01/10/2013	Page No.: 1 of 1




FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

Full Name(s) of Candidate(s)	Kok Ser Leen
ID Number(s)	2001907
Programme / Course	CN
Title of Final Year Project	Rogue Access Point Detector in UTAR Campus

Similarity	Supervisor's Comments (Compulsory if parameters of originality exceed the limits approved by UTAR)
Overall similarity index: <u>6</u> % Similarity by source Internet Sources: <u>4</u> % Publications: <u>3</u> % Student Papers: <u>3</u> %	
Number of individual sources listed of more than 3% similarity: <u>1</u>	Everything ok.
Parameters of originality required, and limits approved by UTAR are as Follows: (i) Overall similarity index is 20% and below, and (ii) Matching of individual sources listed must be less than 3% each, and (iii) Matching texts in continuous block must not exceed 8 words <i>Note: Parameters (i) – (ii) shall exclude quotes, bibliography and text matches which are less than 8 words.</i>	

Note: Supervisor/Candidate(s) is/are required to provide softcopy of full set of the originality report to Faculty/Institute

Based on the above results, I hereby declare that I am satisfied with the originality of the Final Year Project Report submitted by my student(s) as named above.



 Signature of Supervisor

 Signature of Co-Supervisor

Name: Nor Afifah Binti Sabri

Name: _____

Date: 19/4/2024

Date: _____

FYP 2 CHECKLIST



UNIVERSITI TUNKU ABDUL RAHMAN
FACULTY OF INFORMATION & COMMUNICATION
TECHNOLOGY (KAMPAR CAMPUS)

CHECKLIST FOR FYP2 THESIS SUBMISSION

Student ID	20ACB01907
Student Name	Kok Ser Leen
Supervisor Name	Puan Nor Afifah Binti Sabri

TICK (✓)	DOCUMENT ITEMS
	Your report must include all the items below. Put a tick on the left column after you have checked your report with respect to the corresponding item.
✓	Title Page
✓	Signed form of the Declaration of Originality
✓	Acknowledgment
✓	Abstract
✓	Table of Contents
✓	List of Figures (if applicable)
✓	List of Tables (if applicable)
	List of Symbols (if applicable)
✓	List of Abbreviations (if applicable)
✓	Chapters / Content
✓	Bibliography (or References)
✓	All references in bibliography are cited in the thesis, especially in the chapter of literature review
✓	Appendices (if applicable)
✓	Poster
✓	Signed Turnitin Report (Plagiarism Check Result – Form Number: FM-IAD-005)
✓	I agree 5 marks will be deducted due to incorrect format, declare wrongly the ticked of these items, and/or any dispute happening for these items in this report.

*Include this form (checklist) in the thesis (Bind together as the last page)

I, the author, have checked and confirmed all the items listed in the table are included in my report.

(Signature of Student)

Date: 19/04/2024