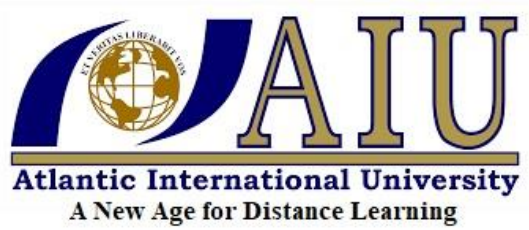


ANTHONY BABAJIDE BALOGUN
ID No: **UB73361SIN82521**

COURSE TOPIC:

WIRELESS NETWORK SECURITY

ATLANTIC INTERNATIONAL UNIVERSITY
MAY 2022

TABLE OF CONTENTS

LIST OF FIGURES

1.0 INTRODUCTION

The primary objective of computer networks is simply to exchange resources. Basically, there are two types of networks such as; Wired and Wireless networks. Network is usually set up by frequency signals in a Wireless network which means accessing the network and its resources without a cable connection. Wireless networking is not new in today's Information Technology's world. It is well known and used in homes, organizations, businesses, schools, hospitals, places of worship etc.

Before wireless applications and devices came into an existence, the traditional way of connecting group of computers together is through wired cables typically installed on the surface and it can also can be hidden on the roofs and basements by making use of a compartment known as a "trunk".

The type of cable mostly used is called a RJ-45 cable. This type of cable has two connectors, one at both ends, these connectors enable a client computer also known as an end user computer to get connected to another computer known as a Server, usually located in a place called Datacenter. Data and Information are deployed on the server for the end users to access in order to perform their work.

In a corporate environment, a wireless network is used to connect different types of wired organizational structures, this allows employees to navigate freely in order to avoid the problems of a physically connected networks.

Moreover, the Internet which is the chain of computers connected together internationally to share resources has become the basic need of human life and activities in such areas as; entertainment, fund transfer, bills payment, ticketing and reservation, hotel management, medicine, engineering, research, media coverage, etc.

Information Technology evolves rapidly. As new variants of virus emerge rapidly in the world of medicine, so also are new technologies in IT world. What we knew way back may not be applicable in today's IT world. So, in this essay, I will like discuss and write on the various ways to secure a wireless network since majority of its users connects from one end of geographical location to another.

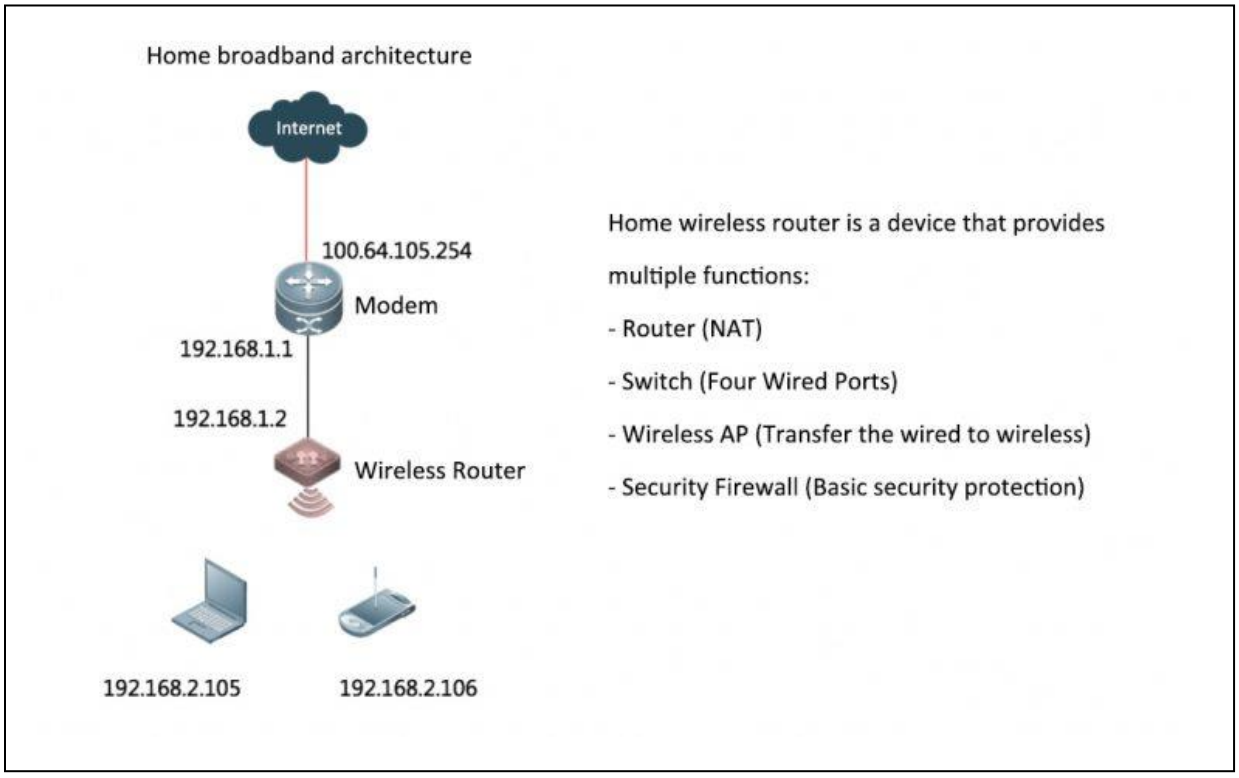
If adequate security measures are not put in place, holding anyone accountable or responsible for any negative or fraudulent activity on any wireless network may prove to be an uphill task.

2.0 WIRELESS NETWORK ARCHITECTURE

2.1 Home wireless networking

Home wireless router is a device that performs and provides multiple functions such as; "routing, switching, wireless AP and of course security firewall". NAT assigns different types of private addresses to public addresses before transferring or transmitting an information. In a typical home wireless networking, NAT is performed twice; at the wireless router and at the optical modem.

Figure 1

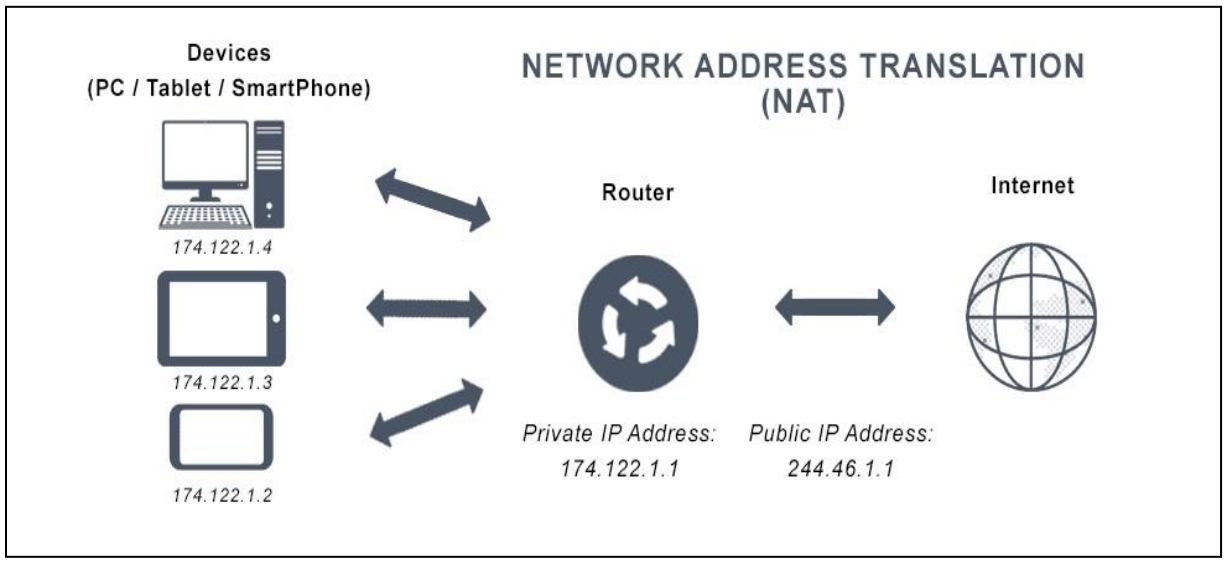


(RS-Tech, 2021)

(Figure 1: Showing home broadband architecture)

NAT allows an IP address to represent a group of computers where a router assigns a computer or group of computers inside a private network a public address. In other words, NAT allows one device to act as a go-between the private network and the public network. NAT main function is to reduce the number of IP Addresses in use on the Internet for security reasons.

Figure 2



(AVINetworks, n.d.)

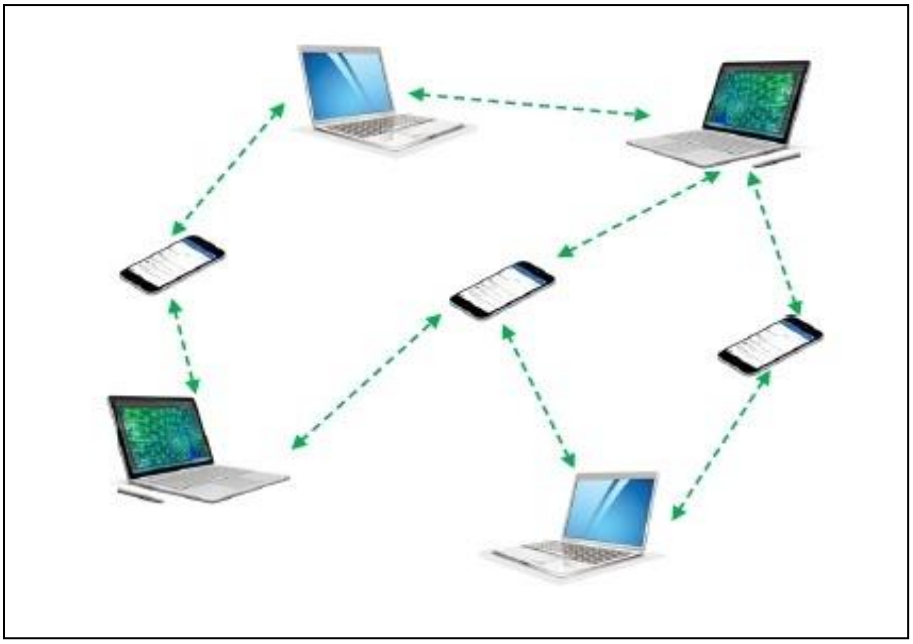
(Figure 2: showing Network Address Translation (NAT))

2.2 Ad-Hoc network architecture

An ad hoc network is voluntarily formed when devices connect and communicate with each other. They are mostly wireless local area networks (WLANs). Devices communicate with each other directly instead of making use of an access points for data transfer. In this network, each device participates in routing processes by using the routing algorithm and send data to other devices through this route.

A typical example will be a scenario where users can create a wireless network on a laptop computer using network infrastructure software included in Windows 8 operating system. This can be achieved by connecting laptops with other wireless terminals to form a LAN communication.

Figure 3



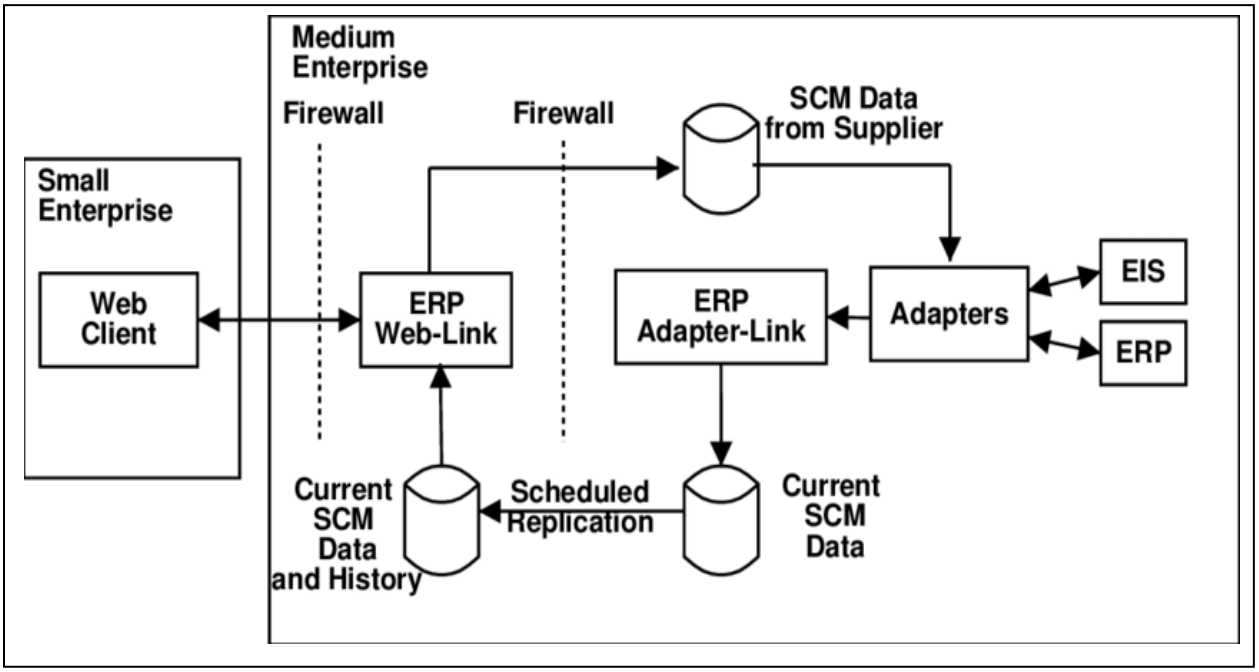
(Tutorialspoint, n.d.)

(Figure 3: showing an ad-hoc networking architecture)

2.3 Small and Medium-sized Enterprises Architecture

Enterprise architecture (EA) is used as an approach in order to aligned information technology with business in an organization. Furthermore, other people see it as an approach to keep the business processes aligned with the defined strategies. Every small and medium sized enterprise requires a proper understanding of the architecture in order to function effectively as IT infrastructure forms the backbone of any organization's operations.

Figure 4



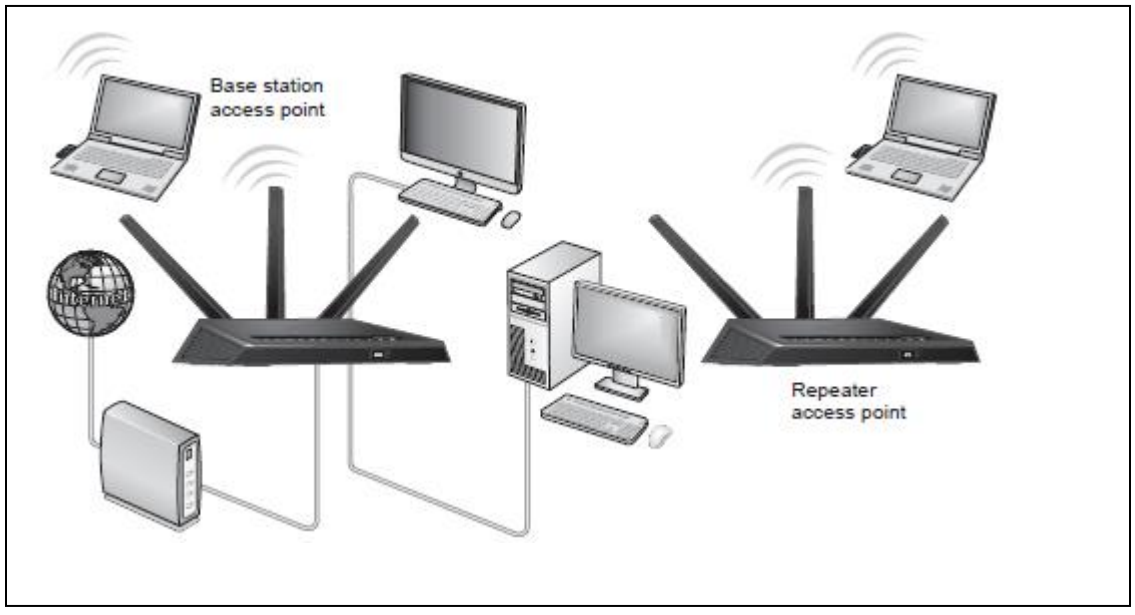
(Menkhaus, n.d.)

(Figure 4: showing Small and Medium-sized Enterprises Architecture)

2.4 WDS Wireless Bridge Network Architecture

WDS stands for Wireless Distribution System. This allows a connection to multiple Access Points. It may provide AP-to-AP wireless bridging in which WDS and APs communicate only with each other and does not permit any wireless stations which is also known as wireless clients to have access to them. Furthermore, it expands a wireless network via various access points. A wireless base station that is connected to the Internet can both have wired and wireless clients, in which the access point serves as a wireless repeater that receives and sends wireless signals.

Figure 5

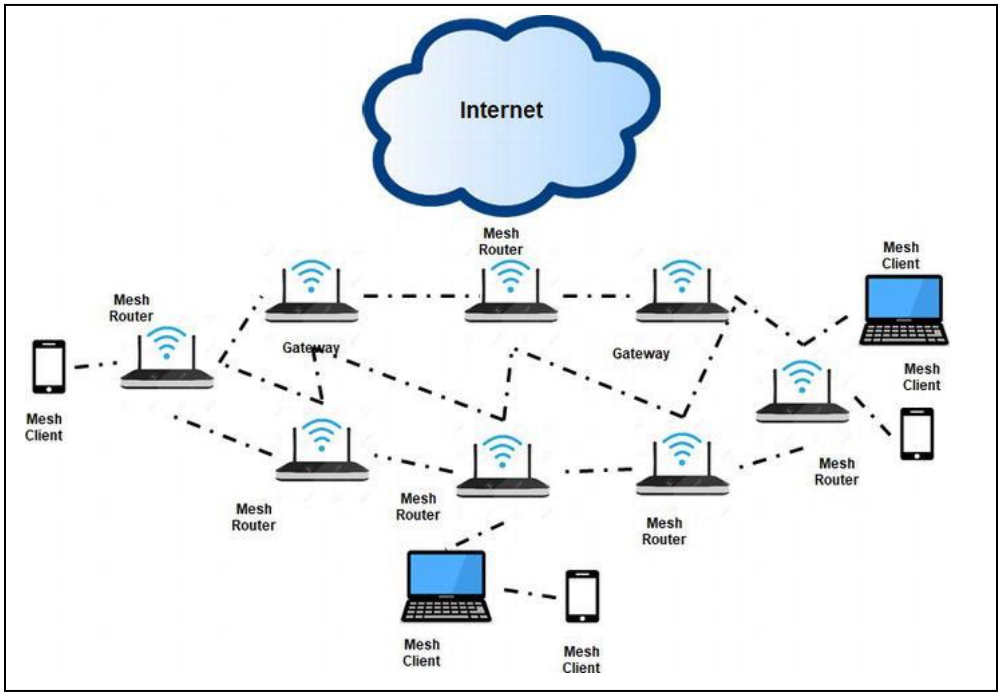


(NETGEAR, n.d.)

(Figure 5: showing WDS wireless bridge network architecture)

2.5 Wireless Mesh Networks Architecture

MN stands for Mesh Network. This is a local network topology in which the infrastructure nodes such as; bridges, switches and other devices connect dynamically and non-hierarchically to various nodes and function with one another in order to efficiently send data to and from clients. Wireless Mesh Network (WNS) refers to a dynamic self-configuring wireless network that uses wireless links to connect different access points allowing an access to a network via one or two root nodes. Furthermore, it comprises of various wireless nodes with access points and each node in the network acts as a forwarding node for transferring data.



(Parvin, 2019)

(Figure 6: showing wireless mesh networking)

3.0 CATEGORIZATION OF SECURITY ISSUES

Security categorization in wireless network can be viewed as the classification of potential vulnerabilities or threats which the system of information may encountered in real-time. They are based on factor like; the impact of any event as a result of any malpractice. However, this depends on the management of the organization system that deals with such problems.

The most important part of wireless network security categorization is to identify the types of information that the organization process. In every situation, threats sometimes damage the confidentiality and integrity of data, that is the reason why organizations classified their potential security issues according to their functional practices. Amongst the common security weaknesses noticeable in a wireless network include; misinformation, falsification of statistical information, theft, data damage, hacking and internal manipulation.

Effective security classification is required in order to understand and identify threats with their potential impacts. These threats can be monitored and classified in various ways such as; the source, the agents and the motives.

4.0 TYPE OF SECURITY THREATS/VULNERABILITIES

4.1 Source of threat

The source of threat varies depending on the information of the system. For example, cloud computing environment deals mostly with third party hacking or even malware attacks. Organization on the other hand may lose information due to internal damages made by the trusted employee.

The ways and manners in which hackers operates has made organizations to reinforced their security measures by acting smartly even before they strike. So, wireless network security has revealed the plans for maintaining high profile security policies.

4.2 Group or Individual Threat

Under this type of threat, one attacker strikes first and if he succeeds in taking control of the system, then the attack turns into an exploit in which other attackers may be involved. The human, environmental and technology-based threats are typical examples of a group or individual threat.

4.3 Threat Motivation

It reveals the main reason for a particular threat that occurred. Under this type of threat, the incident management team gathers facts about an attach and analyzed it in order to further understand the facts and figures of the threat. The most common and popular formula use for analyzing the risk of any security threat or weaknesses is:

Risk = Threat x Vulnerability

Furthermore, threat motivation involved a comprehensive analysis of hardware and software related elements as a part of investigating the motives behind any security malpractices or breach.

5.0 WIRELESS NETWORK THREATS INTENTS

5.1 Intentional Threats

This is an intentional action that could result in the theft or damage of computer equipment and data. They include; viruses, denial of service attacks (DOS), theft of data, sabotage and destruction of computer resources

5.2 Intentional Threat in Cloud Environment

Wireless network forms the basis of a cloud computing environment which consists of more than a single network computing models such as; SaaS, PaaS and IaaS.

There exist a lot of intentions by hackers on how to break the security defences built around these models in order to have access to information stored in them.

5.3 Data Leakage or Breach

This is perhaps the most common risk that is dealt with in the cloud computing environment. A human can introduce a breach thereby causing system malfunctioning. An attacker can determine the information about the vulnerabilities of the system which may affect computers just like a case of botnet attack.

5.4 Malpractice of Cloud Resources

By default, and design, cloud applications more powerful and faster in terms of the ways it processes programs as compared to the normal applications. The hackers can exploit the system in the cloud by using the brute force attack which can break encryptions and passwords in order to access the system.

5.5 Malicious Insider Threat

Malicious insider threats are the ones regarded to have legitimate access to the environment and often take up a functional role in organizational business operations. In any organization, a disgruntled employee or ex-employee can be moved to expose or reveal sensitive information. Several reasons exist for an employee to act negatively and thereby acting as an insider threat and such may include, abuse, salary dispute, termination of employment, employee welfare etc.

6.0 WIRELESS NETWORK THREATS EFFECTS

6.1 Theft of Service

This is a situation when a person committed a crime to obtain valuable services by deception or other unlawful means.

6.2 Denial-of-service (DOS)

This type of attack happened when legitimate users are denied or unable to access information systems devices and other network resources due to the actions of a malicious cyber attacker. In order to mitigate denial-of-service (DOS) attack, concerned security engineers introduced a decoy known as the honeypot in the network to detect attackers and to gather attackers modus operandi for analysis as a preventative measure.

6.3 Elevation of Privilege

This is a kind of process in which users enjoys the authorization to certain computer devices and information at an absolute level. Attackers tries to get access to these individuals access privileges in order to have access to such sensitive information to perform their malicious acts.

6.4 Illegal Usage

This involves using the normal services as a threat to other illegal purposes. Cloud networks have brought a change in online resources to users and despite several advantages of the cloud network and the security built around it, there is still a chance of malpractices in form of misusing systems services.

6.5 Threats by Social Messaging Apps

Social messaging application such as WhatsApp and other social media applications poses threats to mobiles users and such include; Malware, Unencrypted Backups, Data Sharing with other Applications, Encryption Vulnerabilities and Malicious Code.

6.6 Social Media Security Risks

The most common security risks that provides financial and social damages to society include; Phishing emails, scams, frauds, human manipulation, Privacy concerns, personal information posted by you, personal information others posted about you, Information about you the social networking sites collect and share with other users.

7.0 WIRELESS NETWORKS SECURITY CHALLENGES

7.1 Security

When data is being transmitted from end to end, security must be of main concern and priority because data must be secured and protected. Therefore, in order to secure data in wireless network, security requirements and ethics to be enforced centered on what is known as CIA trad. CIA stands for; Confidentiality, Integrity and Availability.

7.1.1 Confidentiality

This simply means that, only a receiver whom the information is intended for should only be able to view and read the transmitted data, and if by chance the data is hacked, the hacker will not be able to read the information by making use of the encryption processes.

7.1.2 Integrity

This means that, the transmitted data must get to the receiver in its original form without any modification of sort in the data.

7.1.3 Availability

This simply means that, Network and its resources must be available for use at all time. There should not be any kind of denial when the services are needed.

7.1.4 Non-Repudiation

In this type of situation, the sender must not deny sending or transmitting data to a receiver at any given time. In order to achieve this, a digital signature must be implemented.

7.2 Challenges and Vulnerabilities

7.2.1 Wireless Medium

"Jamming and scrambling" are well known security issues in a wireless network and network attackers uses this medium to disrupt normal operations.

7.2.2 Cooperative MAC

The wireless network uses the Medium Access Control (MAC) protocol at the data layer level which is shared between connection points. So, "Cooperative MAC creates a huge impact on wireless communication performances".

7.2.3 Network Layer

The most advantage of a network is making use of multiple hoping for transmission of data from one node to another. The attacker gains access into the network through unauthorized means in order to change the content of the routing table to affect data transmission.

7.2.4 Transport Layer

In this layer, many connections are created otherwise known as flooding which are known as vulnerable nodes. This will cause the system to hang at every interval thereby causing a "denial of service (DOS)".

8.0 SECURITY SOLUTIONS OF WIRELESS NETWORKS

There are various safety measures adopted and available to resolve wireless network security threats and they are highlighted below:

8.1 Encryption

This is one of the best and safest methods to protect the information transmitted in a wireless network. Organization can make use of various encryption methods but symmetric and asymmetrical key encryption methods are very important in order to implement a well robust and effective data encryption.

8.2 Securing Wireless Access Point

Installing unauthorized wireless connections can play an important role in violating network security. In order to reduce this type of risk to access points, organization can adopt the following countermeasures:

(a) Remove or disconnect all available rogue access points

(b) Default configuration must be updated accordingly as at the right time and the permitted access must be implemented in a safe mode.

8.3 Minimize the Risk of Denial-of-Service Attacks

Removing any detected or observed not to perform well network devices may reduce the risk of DOS attacks and therefore not give an attacker any avenue to gain access to the system and eventually to sensitive data and information.

8.4 Techniques of Signal Hiding

SSID should be turned off when not in use because attacks required a wireless network to be located and identified. The SSID is a sort of a network identifier or an identification number which is broadcast by access points. So, SSIDs should be turned off when not in use in order to prevent the network from external attacks.

8.5 Secure the Wireless Network

The following techniques can be implemented to further secure wireless network;

- Firewall Technology
- Encryption and Decryption
- Avoid connecting through a public hot spot

9.0 CONCLUSION

Wireless networking is not new in today's Information Technology's world. It is well known and used in homes, organizations, businesses, schools, hospitals, places of worship etc. Before wireless applications and devices came into an existence, the traditional way of connecting group of computers together is through wired cables typically installed on the surface and it can also can be hidden on the roofs and basements by making use of a compartment known as a "trunk".

Information Technology evolves rapidly. As new variants of virus emerge rapidly in the world of medicine, so also are new technologies in IT world. What we knew way back may not be applicable in today's IT world. If adequate security measures are not put in place, holding anyone accountable or responsible for any negative or fraudulent activity on any wireless network may prove to be an uphill task.

In this essay, I have reviewed wireless network architecture, different types of security protocols, categorization of the wireless network security issues, the types of wireless network threats and vulnerabilities, wireless network threats intents, wireless network threats effects, wireless network threat challenges, and security solutions of a wireless network which can make network untrustworthy.

10.0 BIBLIOGRAPHY

AVINetworks. (n.d.). *Network Address Translation*. Retrieved from Network Address Translation Definition: https://avinetworks.com/glossary/network-address-translation/

Menkhaus, G. (n.d.). *High-level architecture of IT infrastructure for small and medium-sized enterprises*. Retrieved from High-level architecture of IT infrastructure for small and medium-sized enterprises: https://www.researchgate.net/figure/High-level-architecture-of-IT-infrastructure-for-small-and-medium-sized-enterprises_fig3_220711230

NETGEAR. (n.d.). *What is a wireless distribution system*. Retrieved from https://kb.netgear.com/24106/What-is-a-wireless-distribution-system-and-how-does-it-work-with-my-Nighthawk-router

Parvin, J. R. (2019, June 10). *An Overview of Wireless Mesh Networks*. Retrieved from Mesh architecture based on clients: https://www.intechopen.com/chapters/66938

RS-Tech. (2021, August 2). *6 Different Types of Wireless Networking*. Retrieved from Home wireless networking: https://blog.router-switch.com/2021/08/6-different-types-of-wireless-networking/

Tutorialspoint. (n.d.). *What is ad-hoc network?* Retrieved from What is ad-hoc network?: https://www.tutorialspoint.com/what-is-ad-hoc-network