Chapter 1

**INTRODUCTION**

The development of communication technology is also supported by the increasing  
progress of infrastructure and technology. One of the developments in communication and information technology is communication using wireless. This is marked by the development of  
the emergence of the network, because it has advantages over the following: Mobility, Scalability,  
Installation Speed and Simplicity, Installation Flexibility, Reduced cost of ownership. Information  
technology is not wireless technology that produces various conveniences also has an impact on  
internet service users, both industrial, educational and independent users.

This development can also be wireless equipment that uses the standard Wireless Fidelity (WiFi) protocol based on the IEEE 802.11 standard. The increasingly widespread use of networks in the business world and the growing need for faster use of internet online services encourage people to take advantage of shared data and shared resources.

With a Wireless Local Area Network (Wireless LAN) users can access information without looking for a place to plug in and can set up a network without pulling cables. Wireless LAN can overcome the problem of lack of wired felt directly by us with the many wireless  
hotspots available everywhere. Besides being able to help and give birth to various positive  
innovations, it also gives birth to a negative side, and this always happens, including the  
development of wireless.

Sending the MAC addresses and the IV in the clear in addition to the frequent use of a single IV and the fact that secret keys are actually shared between communications parties are WEPs major security problems WEP encrypted messages can be easily retrieved using publicly available tools like WEPCrack and Air Snort More discussion about WEP is addressed in later section.

To limit the widespread problems, the problems that will be discussed in this study are  
limited to the Wireless LAN security protocol infrastructure. The analysis was carried out through  
several studies of existing white papers and discourses as well as conducting experiments by  
attacking the Wireless LAN infrastructure. Wireless LAN security protocols used in this study are  
Wireless Protected Access (WPA), Web Proxy, and Virtual Private Network (VPN). By using 3  
attacker tools, namely Network Stumbler, Aircrack, and Wireshark.

The purpose of this study was to test the extent of the security capabilities of the WPA  
protocol, Web Proxy and Virtual Private Network (VPN), against attacks from Software Network  
Stumbler, Aircrack and Wireshark.

Chapter 2

**LITERATURE SURVEY**

[1] The proposed design technique for wireless security in this paper . its describes the motivated to examine the security vulnerabilities and threats imposed by the inherent open nature of wireless communications and to devise efficient defense mechanisms for improving the wireless network security. We first summarize the security requirements of wireless networks, including their authenticity, confidentiality, integrity, and availability issues. Next, a comprehensive overview of security attacks encountered in wireless networks is presented in view of the network protocol architecture, where the potential security threats are discussed at each protocol layer. We also provide a survey of the existing security protocols and algorithms that are adopted in the existing wireless network standards, such as the Bluetooth, Wi-Fi, WiMAX, and the long-term evolution (LTE) systems.

[2] The proposed design technique for Network Security and Cryptography in this paper displayed different plans which are utilized as a part of cryptography for Network security reason. Encode message with firmly secure key which is known just by sending and beneficiary end, is a huge angle to procure powerful security in cloud. The safe trade of key amongst sender and collector is an imperative errand. It can likewise check the respectability of the traded message to confirm the genuineness. This paper quickly presents the idea of PC security, concentrates on the dangers of PC system security later on, work should be possible on key circulation and administration and also ideal cryptography calculation for information security over mists.

# [3] The proposed the design technique is Open cloud software defined wireless network security for the Internet of Things we are proposing a mitigation architecture for security attacks that incorporates a highly programmable monitoring network so as to make it possible to identify attacks. We evaluated the performance of our proposed architecture and compared it with the existing models to obtain various performance measures. The results of our evaluation show that our Op Cloud Sec architecture model can efficiently and effectively meet the security challenges created by the new network paradigm.

[4] The proposed the design technique is a Novel Epidemic Model for Wireless Rechargeable Sensor Network Security In this paper, a novel epidemic model, SILS(Susceptible, Infected, Low-energy, Susceptible), considering the removal, charging and reinfection process of WRSNs is proposed.the local and global stabilities of disease-free and epidemic equilibrium points are

# analyzed and simulated after obtaining the basic reproductive number R0. Detailedly, the simulations further reveal the unique characteristics of SILS when it tends to being stable, and the relationship between the charging rate.

The table 2.1 summarizes the methodology, advantages and disadvantages for related works

Table 2.1 Literature Survey Table

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Reference paper no** | **Methodology** | **Advantages** | | | |  | **Disadvantages** |
| [1] | A novel epidemic model for wireless rechargeable sensor network security. | Realistic modeling of attack propagation, Optimization of defenses | | | |  | Lack of real-world data, Complexity , Generalization and applicability. |
| [2] | Open cloud software defined wireless network security for the Internet of Things. | Centralized Management With open cloud software and updated from the cloud. | | | |  | Dependency on Cloud Connectivity: on cloud based resources |
| [3] | Network security and cryptography |  | Compliance: Implementing network security measures | | |  | Complexity, high  Cost. |
|  | |  |
|  |  |
|  |
| [4] | Wireless security | Wireless networks provide the flexibility of mobility. | | | |  | Signal Interference and Range Limitations. |

Chapter 3

**METHODOLOGY**

The research focused on how to formulate existing problems and identified and  
formulated based on security aspects of the Wireless LAN protocol. Then develop a hypothesis  
as an answer or initial conclusion and a strategy to test whether the hypothesis is the answer to  
the existing problems.

Stages:  
 In this study the author uses several stages, starting with

* Make a design using an infrastructure topology Large addition of initialization vector size to prevent repetition of initialization vector values.
* Changing the initialization vector selection method to prevent weak keys from occurring, as well as preventing possible replay attacks.
* Change the encryption key for each packet sent (per packet key mixing).

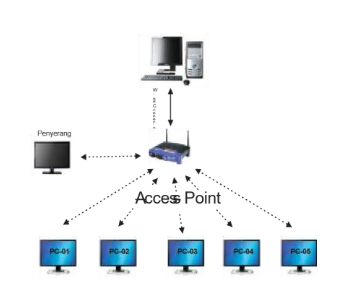


Figure 3.1: Attack Trial

## Better use of message integrity protocol to prevent message modification with 5 (five) wireless users connected to 1 (one) server through 1 (one) access point and 1 (one) attacker.

## Tried attacks on Wireless LAN infrastructure using the WPA, Web Proxy and Virtual Private Network security protocols and access points with different signal strengths, namely at a distance of 5 meters, 10 meters, 15 meters, 20 meters, 25 meters.



Figure 3.2. Trial Position with the difference in distance between attackers

## 3.2 Data analysis

The data were analyzed using several stages of testing as follows:

* Identify or monitor the configuration of hotspot presence using Network Stumbler 0.4.0 software.
* Then deal with opening a wireless network connection. Trying to crack the password on the access point used using the Aircrack-ng-0.9.3-win software.
* The attack was measured for data sent, data received and data lost using Network Stumbler 0.4.0 software .

**3.3 Testing of IP address manipulation attacks is carried out with 2 test methods:**

Method 1:

Connect based on MAC Address and information Get the IP Address and then open a Wireless connection session by logging into the Web Proxy and connecting to the server. Eavesdropping on packets to obtain a valid MAC address using the Network Stumbler software and falsifying the attacker's MAC address and connecting with the access point based on the forged  
MAC address.

Method 2:

Connect with the access point based on the forged MAC Address and get the IP Address and the Wireless LAN connection is opened by logging into the Web Proxy. Connect with the access point based on the fake MAC address and get the IP Address and cannot  
open a Wireless LAN connection session when logging in to the Web Proxy.

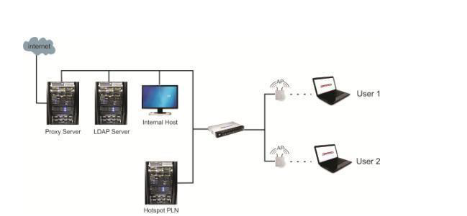


Figure 3.3: Wireless LAN Architecture

From the picture, the architecture of Wireless LAN and wired networks is part of an integrated  
network. Access control of devices that want to connect is done by using the MAC Address of the  
user stored in the LDAP (Lightweight Direction Access Protocol) server. The authentication process into the network is carried out through a Web Proxy that uses the Secure Socket Layer (SSL) protocol. SSL is a security protocol that works above layer 4 (four) OSI (transport layer), where all data that goes through this protocol will be encrypted. After the user is authenticated, the user will get access rights to the internal wired network and to the internal (by using a proxy server).Wireless LAN users use a Web Proxy with SSL protocol in the authentication process, providing security protection against theft of wireless username and password information because the data is transmitted in encrypted form. The wireless user connection process can be seen in Figure 3.2.

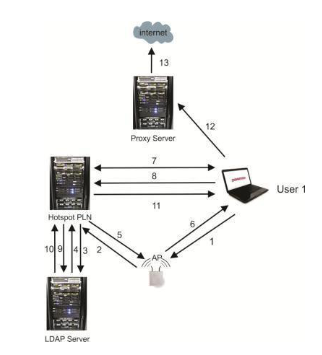


Figure 3.4: Wireless LAN Connection Process

Wireless connection process that occurs is as follows:

Wireless users perform the connection process with the access point using open system  
authentication (without using WEP). Access point performs access control to connection requests from wireless users by querying hotspots based on MAC Address information owned by wireless users. The query received by the hotspot is forwarded to the server to obtain information whether the MAC Address of the wireless user is a registered device. The server confirms whether the MAC address is in the database or not.

The hotspot receives information from the server and then confirms the association process is accepted or not based on that information, that is, if the MAC address is registered, the association process is accepted and vice versa. The access point confirms to the wireless user that the association process has been successful or not. If the association process is successful, the following processes will be carried out (seventh process and so on).

After the wireless user gets an IP address, an authentication process is needed to ensure that the wireless user is a user who does have access rights. For that, the wireless user must enter information in the form of a wireless username and password via a Web Proxy that uses the SSL protocol. Where the data that is transmitted will be encrypted so as to prevent the possibility of attackers knowing the secret identity of the wireless user.

The server responds whether the authentication process is accepted or not by checking whether the wireless username and password combination is in the database directory. These protocols provide transmitted plain text.

Strong authentication, encryption and integrity power. Other protocols exist. People do not use  
security at the top layer (application layer) such as the data link layer layer (such as WEP and HTTP, FTP and telnet are not WPA), because it transmits data from secure protocols because all data is "insecure" ” is still transmitted in plain text (clear WebProxy in the Community).

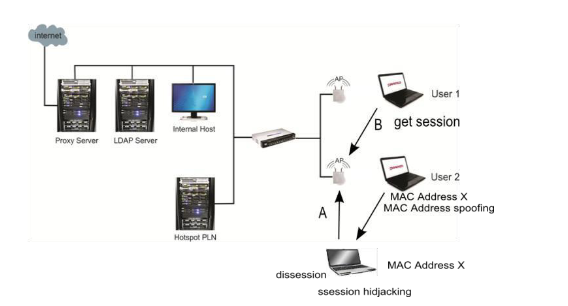


Figure 3.5 :Session Hijacking on Wireless LAN with Web Proxy

**3.4 Attack on Virtual Private Network**

Conducting experimental attacks on hotspots using Virtual Private Network security by  
trying to crack wireless usernames and passwords with different distances and trying to find  
connection sessions. From experiments conducted using aircrack software, the author can only  
identify or monitor the configuration of the presence of a hotspot without being able to solve the  
wireless username and find out the IP Address of the original wireless user, the password of the  
original wireless user without being able to change the wireless IP address.

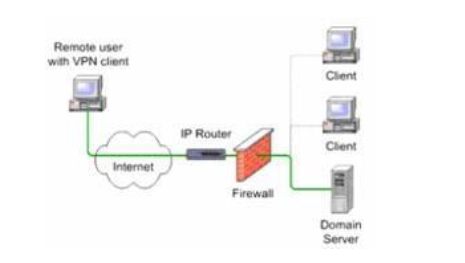


Figure 3.6: Security Network Structure with VPN

Chapter 4

**RESULTS**

In designing the security model, assets Analysis Results with the WPA Protocol network at risk need to be considered such as weak points in the system with the WPA Protocol being able  
to overcome its security, or interference from the attacker, as well as the motivation of the attack  
for each potential weakness. Regarding this, it is very necessary to take the necessary security  
protection measures.

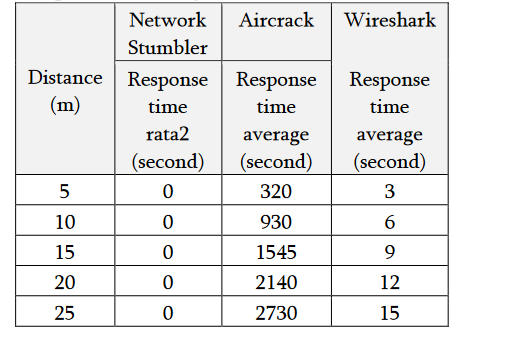


Table 4.1: Results of Attempted Attacks against the WPA Protocol

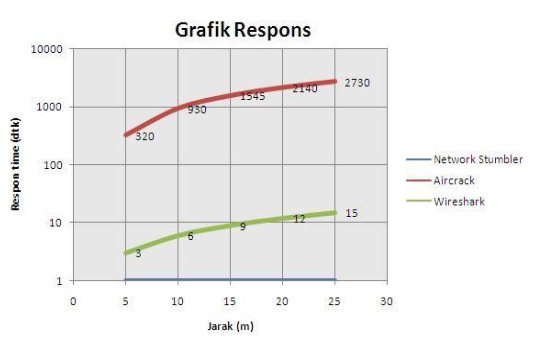


Figure 4.2: Graph of Response Time to the WPA Protocol

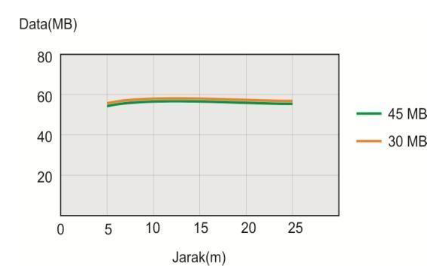


Figure 4.3: Number of Data Packets Receive

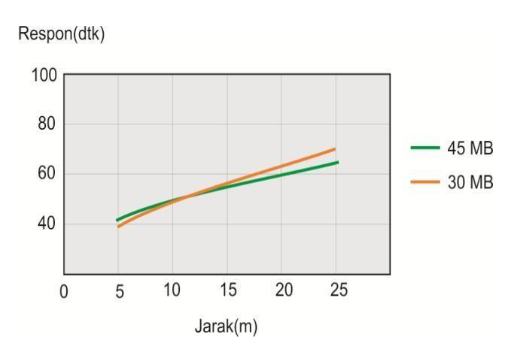


Figure 4.4: IP Address Detection attack experiment results

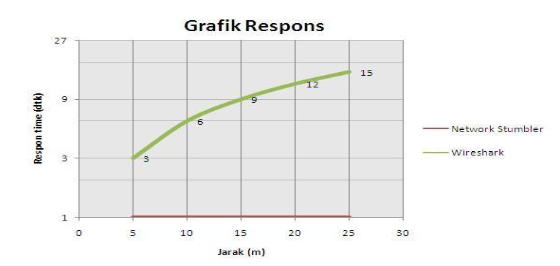


Figure 4.5: Graph of Response Time to Web Proxy Protocol

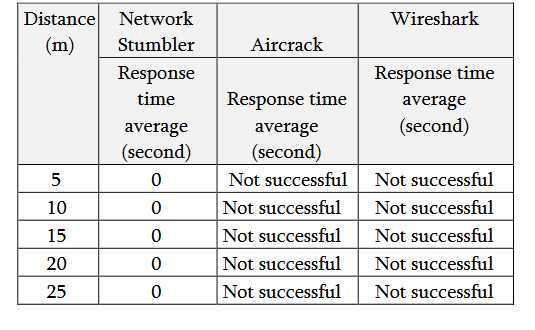


Table 4.6: Results of Attempted Attacks on VPN Protocols

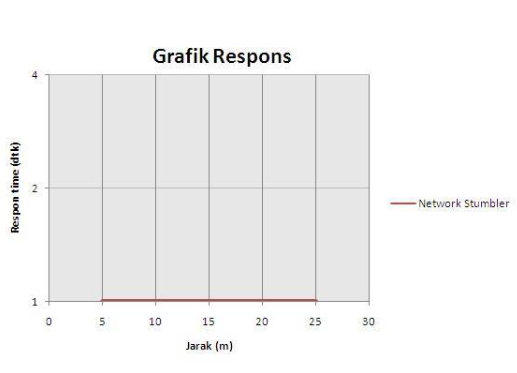


Figure 4.7: Graph of Response Time to VPN Protocol.

Chapter 5

**CONCLUSION**

* The use of security with the WPA protocol, Web Proxy and Virtual Private Network (VPN) does not provide security protection from Network Stumbler.
* Using the WPA protocol, the average response time for Network Stumbler is faster than Wireshark, while the average Aircrack response time is 45 minutes for a distance of 25 m.
* Using the protocol with Web Proxy, the average response time for Network Stumbler is faster than Wireshark, while Aircrack is not successful.
* Using a protocol with a VPN, the average response time for Network Stumbler is faster, while the average response time for Wireshark and Aircrack is not successful.

# REFERENCES

[1] Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A wireless security: Technical challenges,  
recent advances, and future trends.Proceedings of the IEEE,104(9), 1727-1765.

[2] Tayal, S., Gupta, N., Gupta, P., Goyal, D., & Goyal, M. (2017). A review paper on network security and  
cryptography . Advances in Computational Sciences and Technology,10(5), 763-770.

[3] Sharma, P. K., Singh, S., & Park, J. H. (2018). OpCloudSec: Open cloud software defined wireless  
network security for the Internet of Things. Computer Communications,122, 1-8.

[4] Liu, G., Peng, B., & Zhong, X. (2020). A novel epidemic model for wireless rechargeable sensor network security.Sensors,21(1), 123.

[5] Mulyanto , Y., Herfandi , H., & Kirana, R. C. (2022). analisis keamanan wireless local area network (wlan) terhadap serangan brute force dengan metode penetration testing (studi kasus: rs h. lmanambai abdulkadir). Jurnal Informatika Teknologi dan Sains,4(1), 26-35.